

WebSphere Application Server



Guía de administración de Load Balancer

Versión 6.1

WebSphere Application Server



Guía de administración de Load Balancer

Versión 6.1

Nota

Antes de utilizar esta información y el producto al que da soporte, asegúrese de leer la información general del Apéndice E, "Avisos", en la página 493.

Primera edición (mayo de 2006)

Esta edición se aplica a:

WebSphere Application Server, Versión 6.1

y a todos los releases y modificaciones posteriores hasta que se indique lo contrario en nuevas ediciones.

Puede solicitar publicaciones a través del representante de IBM o a través de la sucursal de IBM que presta servicio en su localidad.

© Copyright International Business Machines Corporation 2005. Reservados todos los derechos.

Contenido

Tablas	xiii
-------------------------	-------------

Figuras	xv
--------------------------	-----------

Acerca de este manual	xvii
--	-------------

A quién va dirigido este manual	xvii
Información de consulta.	xvii
Accesibilidad	xvii
¿Cómo enviar sus comentarios?	xvii

Documentos relacionados y sitios

Web.	xix
---------------------	------------

Parte 1. Introducción a Load Balancer	1
--	----------

Capítulo 1. Visión general de Load Balancer	3
--	----------

Descripción de Load Balancer	3
¿Qué componentes de Load Balancer puedo utilizar?	3
Ventajas de utilizar Load Balancer	4
Cómo Load Balancer puede proporcionar alta disponibilidad	6
Dispatcher	6
CBR	6
Cisco CSS Controller o Nortel Alteon Controller	6
Nuevas características	6

Capítulo 2. Visión general de los componentes de Load Balancer	9
---	----------

Componentes de Load Balancer	9
Visión general del componente Dispatcher	9
Gestión de servidores locales con Dispatcher	10
Gestión de servidores que utilizan Dispatcher y Metric Server	11
Gestión de servidores locales y remotos con Dispatcher.	12
Visión general del componente CBR (Content Based Routing)	12
Gestión de servidores locales con CBR	13
Visión general del componente Site Selector	14
Gestión de servidores locales y remotos con Site Selector y Metric Server	14
Visión general del componente Cisco CSS Controller	15
Visión general del componente Nortel Alteon Controller	17

Capítulo 3. Gestión de la red: determinación de las características de Load Balancer que se van a utilizar	19
---	-----------

Funciones de gestor, asesores y Metric Server (para los componentes Dispatcher, CBR, y Site Selector)	19
---	----

Características del componente Dispatcher	19
Administración remota	19
Ubicación compartida	19
Alta disponibilidad	20
Afinidad del cliente con el servidor	20
Equilibrio de carga basado en normas	20
Direccionamiento basado en contenido con el método de reenvío cbr de Dispatcher.	21
Equilibrio de carga de área amplia.	22
Correlación de puertos	22
Configuración de Dispatcher en una red privada	22
Clúster comodín y puerto comodín	22
Detección de ataques para "rechazo de servicio"	23
Anotaciones en binario	23
Alertas	23

Características del componente CBR (Content Based Routing)	23
Comparación entre el método de reenvío cbr de componente CBR y de componente Dispatcher	24
Administración remota	24
Ubicación compartida	24
CBR con varias instancias de Caching Proxy	24
Provisión de direccionamiento basado en contenido para conexiones SSL	24
Creación de particiones del servidor	24
Equilibrio de carga basado en normas	25
Afinidad del cliente con el servidor	25
Alta disponibilidad con Dispatcher y CBR	26
Anotaciones en binario	26
Alertas	26

Características del componente Site Selector	26
Administración remota	26
Ubicación compartida	26
Alta disponibilidad	26
Afinidad del cliente con el servidor	26
Equilibrio de carga basado en normas	27
Equilibrio de carga de área amplia.	27
Alertas	27

Características del componente Cisco CSS Controller	27
Administración remota	28
Ubicación compartida	28
Alta disponibilidad	28
Anotaciones en binario	28
Alertas	28

Características del componente Nortel Alteon Controller	28
Administración remota	29
Ubicación compartida	29
Alta disponibilidad	29
Anotaciones en binario	29
Alertas	29

Capítulo 4. Instalación de Load Balancer	31
---	-----------

Requisitos del sistema AIX e instalación	31
--	----

Requisitos de sistemas AIX	31
Instalación en sistemas AIX	32
Antes de instalar	32
Pasos de instalación	33
Requisitos del sistema HP-UX e instalación.	35
Requisitos de sistemas HP-UX	35
Instalación en sistemas HP-UX	35
Antes de instalar	35
Pasos de instalación	35
Requisitos del sistema Linux e instalación	37
Requisitos de sistemas Linux	37
Instalación para sistemas Linux.	37
Antes de instalar	37
Pasos de instalación	37
Requisitos del sistema Solaris e instalación	39
Requisitos de Solaris	39
Instalación para Solaris	39
Antes de instalar	39
Pasos de instalación	39
Requisitos del sistema Windows e instalación	40
Requisitos de sistemas Windows	40
Instalación en sistemas Windows	40
Antes de instalar	41
Pasos de instalación	41

Parte 2. Componente Dispatcher . . 43

Capítulo 5. Configuración de inicio rápido 45

Qué necesita	45
Preparativos	46
Configuración del componente Dispatcher	47
Configuración con la línea de mandatos	47
Prueba de la configuración	47
Configuración con la interfaz gráfica de usuario (GUI)	48
Asistente de configuración	48
Tipos de configuraciones de clúster, puerto y servidor	48

Capítulo 6. Planificación de Dispatcher 51

Consideraciones de planificación	51
Métodos de reenvío	52
Direccionamiento a nivel de MAC de Dispatcher (método de reenvío mac)	53
NAT/NAPT de Dispatcher (método de reenvío nat)	53
Direccionamiento basado en contenido de Dispatcher (método de reenvío cbr)	55
Pasos de ejemplo para configurar los métodos de reenvío nat o cbr de Dispatcher.	57
Creación de particiones del servidor: servidores lógicos configurados con un servidor físico (dirección IP)	58
Creación de particiones del servidor con asesores HTTP o HTTPS	58
Ejemplo para configurar un servidor físico en servidores lógicos	59
Alta disponibilidad	60
Alta disponibilidad sencilla	60

Alta disponibilidad mutua	61
-------------------------------------	----

Capítulo 7. Configuración de Dispatcher 63

Visión general de las tareas de configuración	63
Métodos de configuración	63
Línea de mandatos	63
Scripts	64
GUI	64
Configuración con el asistente de configuración	66
Configuración de la máquina Dispatcher	66
Paso 1. Iniciar la función de servidor	68
Paso 2. Iniciar la función de ejecutor	68
Paso 3. Definir la dirección de no reenvío (si es distinta del nombre de sistema principal)	68
Paso 4. Definir un clúster y establecer opciones de clúster	69
Paso 5. Crear un alias para la tarjeta de interfaz de red	69
Paso 6. Definir puertos y establecer opciones de puertos	70
Paso 7. Definir máquinas servidor con equilibrio de carga	70
Paso 8. Iniciar la función de gestor (opcional)	71
Paso 9. Iniciar la función de asesor (opcional)	71
Paso 10. Definir las proporciones del clúster según sea necesario.	71
Configuración de máquinas de servidor para el equilibrio de carga	72
Paso 1. Crear un alias para el dispositivo de bucle de retorno	72
Paso 2. Comprobar si hay una ruta adicional	76
Paso 3. Suprimir todas las rutas adicionales	77
Paso 4. Verificar que el servidor esté configurado correctamente	77
Alternativas de alias de bucle de retorno de Linux cuando se utiliza el reenvío MAC de Load Balancer	78

Capítulo 8. Despliegue de Dispatcher en Load Balancer para IPv4 y IPv6. . . 81

Plataformas admitidas para Load Balancer para IPv4 y IPv6	82
Plataformas admitidas para el equilibrio de carga en espacio de usuario	82
Consideraciones especiales de la plataforma Linux	82
Restricciones de servidores de programa de fondo	82
Instalación de Load Balancer para IPv4 y IPv6.	83
Consideraciones especiales y limitaciones para Load Balancer para IPv4 y IPv6	83
Configurar dirección local de enlace de IPv6	84
Pares de clúster/servidor homogéneos	84
Características de Dispatcher no admitidas	84
Configuración de asesores	84
Configuración de la alta disponibilidad	85
Ubicación compartida de servidores	86
Característica de afinidad para sistemas que se ejecutan en espacio de usuario (Linux)	86
Configuración de Metric Server.	87

Habilitar el proceso de paquetes IPv6 en Load Balancer para IPv4 y IPv6	88
Creación de alias del dispositivo de interfaz en Load Balancer para IPv4 y IPv6	88
Pasos de configuración de clúster requeridos para Linux en zSeries	91
Mandatos de Dispatcher (dscontrol) para Load Balancer para IPv4 y IPv6	92
Diferencias de sintaxis de mandato	92
Mandatos dscontrol admitidos	92
Mandatos dscontrol no admitidos	95

Parte 3. Componente CBR (Content Based Routing) 97

Capítulo 9. Configuración de inicio rápido 99

Qué necesita	99
Preparativos	99
Configuración del componente CBR	100
Configuración con la línea de mandatos	100
Prueba de la configuración	102
Configuración con la interfaz gráfica de usuario (GUI)	102
Configuración con el asistente de configuración	102
Tipos de configuraciones de clúster, puerto y servidor	102

Capítulo 10. Planificación de CBR (Content Based Routing) 105

Consideraciones de planificación	105
Peticiones de equilibrio de carga para distintos tipos de contenido	106
División del contenido del sitio para obtener un mejor tiempo de respuesta	106
Provisión de una copia de seguridad del contenido del servidor Web	107
Utilización de varios procesos Caching Proxy para mejorar la utilización de la CPU	107
Utilización de equilibrio de carga basado en normas con CBR	107
Equilibrio de carga entre conexiones completamente seguras (SSL)	107
Equilibrio de carga de cliente a proxy en SSL y de proxy a servidor en HTTP	108

Capítulo 11. Configuración de CBR (Content Based Routing) 109

Visión general de las tareas de configuración	109
Métodos de configuración	109
Línea de mandatos	110
Scripts	111
GUI	111
Asistente de configuración	113
Configuración de la máquina CBR	113
Paso 1. Configurar Caching Proxy para que pueda utilizar CBR	113
Paso 2. Iniciar la función de servidor	115
Paso 3. Iniciar la función de ejecutor	115

Paso 4. Definir un clúster y establecer opciones de clúster	115
Paso 5. Crear un alias para la tarjeta de interfaz de red (opcional)	115
Paso 6. Definir puertos y establecer opciones de puertos	116
Paso 7. Definir máquinas servidor con equilibrio de carga	117
Paso 8. Añadir normas a la configuración	117
Paso 9. Añadir servidores a las normas	117
Paso 10. Iniciar la función de gestor (opcional)	117
Paso 11. Iniciar la función de asesor (opcional)	117
Paso 12. Definir las proporciones del clúster según sea necesario	118
Paso 13. Iniciar Caching Proxy	118
Ejemplo de configuración CBR	118

Parte 4. Componente Site Selector 119

Capítulo 12. Configuración de inicio rápido 121

Qué necesita	121
Preparativos	121
Configuración del componente Site Selector	122
Configuración con la línea de mandatos	122
Prueba de la configuración	123
Configuración con la interfaz gráfica de usuario (GUI)	123
Configuración con el asistente de configuración	123

Capítulo 13. Planificación de Site Selector 125

Consideraciones de planificación	125
Consideraciones de TTL	127
Utilización de la característica proximidad de red	128

Capítulo 14. Configuración de Site Selector 131

Visión general de las tareas de configuración	131
Métodos de configuración	131
Línea de mandatos	131
Scripts	132
GUI	132
Asistente de configuración	134
Configuración de la máquina Site Selector	134
Paso 1. Iniciar la función de servidor	134
Paso 2. Iniciar el servidor de nombres	134
Paso 3. Definir un nombre de sitio y establecer las opciones del nombre de sitio	134
Paso 4. Definir máquinas servidor con equilibrio de carga	135
Paso 5. Iniciar la función de gestor (opcional)	135
Paso 6. Iniciar la función de asesor (opcional)	135
Paso 7. Definir la métrica del sistema (opcional)	135
Paso 8. Definir las proporciones del nombre de sitio según sea necesario	135
Configuración de máquinas de servidor para el equilibrio de carga	136

Parte 5. Componente Cisco CSS Controller 137

Capítulo 15. Configuración de inicio rápido 139

Qué necesita.	139
Preparativos.	139
Configuración del componente Cisco CSS Controller	140
Configuración con la línea de mandatos	140
Prueba de la configuración	141
Configuración con la interfaz gráfica de usuario (GUI)	141

Capítulo 16. Planificación de Cisco CSS Controller. 143

Requisitos del sistema	143
Consideraciones de planificación	143
Colocación del consultor en la red	144
Alta disponibilidad	146
Cálculo de pesos	147
Determinación de problemas	147

Capítulo 17. Configuración de Cisco CSS Controller. 149

Visión general de las tareas de configuración	149
Métodos de configuración	149
Línea de mandatos	149
XML	150
GUI	151
Configuración de la máquina Controlador para Conmutadores Cisco CSS	152
Paso 1. Iniciar la función de servidor	152
Paso 2. Iniciar la interfaz de línea de mandatos	152
Paso 3. Configurar el consultor	152
Paso 3. Configurar un contenido de propietario	153
Paso 4. Verificar que los servicios están definidos correctamente	153
Paso 5. Configurar métrica	153
Paso 6. Iniciar el consultor	153
Paso 7. Iniciar Metric Server (opcional)	153
Paso 8. Configurar alta disponibilidad (opcional)	153
Comprobación de la configuración	154

Parte 6. Componente Nortel Alteon Controller 155

Capítulo 18. Configuración de inicio rápido 157

Qué necesita.	157
Preparativos.	158
Configuración del componente Nortel Alteon Controller	158
Configuración con la línea de mandatos	158
Prueba de la configuración	159
Configuración con la interfaz gráfica de usuario (GUI)	159

Capítulo 19. Planificación de Nortel Alteon Controller. 161

Requisitos del sistema	161
Consideraciones de planificación	161
Colocación del consultor en la red	162
Atributos de servidor en el conmutador (establecidos por el controlador)	165
Configuración de servidores de reserva.	165
Configuración de grupos	166
Alta disponibilidad	167
Ajuste	169
Determinación de problemas	169

Capítulo 20. Configuración de Nortel Alteon Controller. 171

Visión general de las tareas de configuración	171
Métodos de configuración	171
Línea de mandatos	171
XML	172
GUI	173
Configuración de Nortel Alteon Controller	174
Paso 1. Iniciar la función de servidor	174
Paso 2. Iniciar la interfaz de línea de mandatos	174
Paso 3. Definir un consultor de Conmutador Nortel Alteon Web	175
Paso 4. Añadir un servicio al consultor de conmutador	175
Paso 5. Configurar métrica	175
Paso 6. Iniciar el consultor	175
Paso 7. Configurar alta disponibilidad (opcional)	175
Paso 8. Iniciar Metric Server (opcional)	175
Paso 9. Renovar la configuración de Nortel Alteon Controller	175
Comprobación de la configuración	176

Parte 7. Funciones y características avanzadas de Load Balancer 177

Capítulo 21. Funciones del gestor, asesores y Metric Server para Dispatcher, CBR y Site Selector 179

Optimización del equilibrio de carga que proporciona Load Balancer	180
Proporción de la importancia otorgada a la información de estado	180
Pesos	181
Intervalos del gestor	183
Umbral de sensibilidad	183
Índice de suavizado	183
Utilización de scripts para generar una alerta o anotar anomalías en el servidor	184
Asesores	185
Cómo funcionan los asesores	186
Inicio y detención de un asesor	186
Intervalos de asesor	187
Tiempo de espera de informe del asesor	187

Tiempo de espera de conexión y recepción del asesor para los servidores	188
Reintento del asesor	188
Lista de asesores	188
Configuración del asesor HTTP o HTTPS utilizando la opción de petición y respuesta (URL)	190
Utilización del asesor automático en una configuración WAN de dos niveles	192
Crear asesores personalizados (personalizables)	192
Asesor WAS.	194
Convenio de denominación.	194
Compilación.	194
Ejecución.	195
Rutinas necesarias.	195
Orden de búsqueda	195
Denominación y vía de acceso.	196
Asesor de ejemplo.	196
Metric Server	196
Restricción para WLM	196
Requisitos previos.	196
Cómo utilizar Metric Server	197
Asesor del gestor de carga de trabajo	198
Restricción para Metric Server.	199

Capítulo 22. Características avanzadas para Dispatcher, CBR y Site Selector. 201

Utilización de servidores con ubicación compartida	203
Para el componente Dispatcher	203
Para el componente CBR	204
Para el componente Site Selector	204
Alta disponibilidad	204
Configurar la alta disponibilidad	205
Capacidad de detección de anomalías utilizando pulsos y destino de alcance.	207
Estrategia de recuperación	208
Utilización scripts	209
Configurar la ubicación compartida y la alta disponibilidad (sistemas Windows)	211
Configuración de equilibrio de carga basado en normas	212
¿Cómo se evalúan las normas?	213
Utilización de normas basadas en la dirección IP de cliente.	213
Utilización de normas basadas en el puerto de cliente.	214
Utilización de normas basadas en la hora del día	214
Utilización de normas basadas en el tipo de servicio (TOS)	214
Utilización de normas basadas en las conexiones por segundo.	215
Utilización de normas basadas en el total de conexiones activas.	215
Utilización de normas basadas en ancho de banda reservado y ancho de banda compartido	216
Norma de toda la métrica	217
Norma de media de la métrica	218
Utilización de normas que son siempre ciertas	218

Utilización de normas basadas en el contenido de peticiones	219
Alteración temporal de la afinidad entre puertos	219
Adición de normas a la configuración	220
Opción de evaluación del servidor para normas	220
Cómo funciona la característica de afinidad para Load Balancer	221
Comportamiento cuando la afinidad está inhabilitada	222
Comportamiento cuando la afinidad está habilitada	222
Afinidad entre puertos	222
Máscara de dirección de afinidad (stickymask)	223
Desactivar temporalmente el manejo de conexiones de servidor	224
Opción de afinidad de la norma basada en el contenido de la petición de cliente	224
Afinidad de cookies activos	225
Afinidad de cookies pasivos	227
Afinidad de URI	228
Configurar soporte de Dispatcher de área amplia	229
Sintaxis de mandatos.	230
Utilización de asesores remotos con el soporte de área amplia de Dispatcher	230
Ejemplo de configuración	232
Soporte de GRE (Encapsulamiento genérico de direccionamiento)	234
Utilización del enlace explícito	236
Utilización de una configuración de red privada	236
Utilizar un clúster comodín para combinar configuraciones de servidores	237
Utilizar un clúster comodín para equilibrar la carga de cortafuegos	238
Utilizar un clúster comodín con Caching Proxy para el proxy transparente	238
Utilizar el puerto comodín para dirigir el tráfico de puerto no configurado	239
Puerto comodín para manejar el tráfico FTP	239
Detección de ataques para rechazo de servicio (DoS)	239
Utilización del registro cronológico binario para analizar estadísticas de servidor	241
Utilización de un cliente con ubicación compartida	242

Capítulo 23. Características avanzadas de Cisco CSS Controller y Nortel Alteon Controller 243

Ubicación compartida	243
Alta disponibilidad	243
Configuración	244
Detección de anomalías	245
Estrategia de recuperación	245
Ejemplos	246
Optimización del equilibrio de carga que proporciona Load Balancer	246
Importancia dada a la información métrica	246
Pesos	247
Tiempos de inactividad en el cálculo de pesos	247
Umbral de sensibilidad	248
Asesores	248

Cómo funcionan los asesores	248
Tiempos de inactividad del asesor	249
Tiempo de espera de conexión y recepción del asesor para los servidores	249
Reintento del asesor	249
Crear asesores personalizados (personalizables)	250
Convenio de denominación.	251
Compilación.	251
Ejecución.	252
Rutinas necesarias.	252
Orden de búsqueda	252
Denominación y vía de acceso.	253
Asesor de ejemplo.	253
Metric Server	253
Requisitos previos.	253
Cómo utilizar Metric Server	253
Asesor del gestor de carga de trabajo	255
Utilización del registro cronológico binario para analizar estadísticas de servidor	256
Utilización de scripts para generar una alerta o anotar anomalías en el servidor	257

Parte 8. Administración y resolución de problemas de Load Balancer 259

Capítulo 24. Operación y gestión de Load Balancer 261

Administración remota de Load Balancer	261
RMI (Remote Method Invocation)	262
Administración basada en la Web	263
Utilización de archivos de anotaciones cronológicas de Load Balancer	265
Para Dispatcher, CBR y Site Selector.	265
Para Cisco CSS Controller y Nortel Alteon Controller	267
Utilización del componente Dispatcher	268
Inicio y detención de Dispatcher	268
Utilización del valor de tiempo de espera sin actividad	268
Utilización del tiempo de espera de conexiones finalizadas y del tiempo de espera sin actividad con el fin de controlar la limpieza de registros de conexión	269
Informe a la GUI — la opción de menú Supervisar	269
Utilización de Simple Network Management Protocol con el componente Dispatcher.	269
Utilización de ipchains o tablas ip para rechazar todo el tráfico con el fin de proteger la máquina de Load Balancer (sistemas Linux)	276
Utilización del componente CBR (Content Based Routing)	277
Inicio y detención de CBR	277
Control de CBR	277
Utilización de archivos de anotaciones cronológicas de CBR	278
Utilización del componente Site Selector	278
Inicio y detención de Site Selector	278

Control de Site Selector	278
Utilización de archivos de anotaciones cronológicas de Site Selector	278
Utilización del componente Cisco CSS Controller	278
Inicio y detención de Cisco CSS Controller	278
Control de Cisco CSS Controller	278
Utilización de archivos de anotaciones cronológicas de Cisco CSS Controller	279
Utilización del componente Nortel Alteon Controller	279
Inicio y detención de Nortel Alteon Controller	279
Control de Nortel Alteon Controller	279
Utilización de archivos de anotaciones cronológicas de Nortel Alteon Controller	279
Utilización del componente Metric Server	280
Inicio y detención de Metric Server	280
Utilización de archivos de anotaciones cronológicas de Metric Server	280

Capítulo 25. Resolución de problemas 281

Recopilación de información para la resolución de problemas	281
Información general (siempre es necesaria)	281
Problemas de alta disponibilidad (HA)	282
Problemas del asesor	283
Problemas de CBR (Content Based Routing)	284
No se puede acceder al clúster	284
Todo lo demás no funciona.	284
Actualizaciones.	285
Código Java	285
Enlaces de utilidad	285
Tablas de resolución de problemas	285
Comprobación de los números de puerto de Dispatcher	299
Comprobación de los números de puerto de CBR	300
Comprobación de los números de puerto de Site Selector	301
Comprobación de los números de puerto de Cisco CSS Controller	301
Comprobación de los números de puerto de Nortel Alteon Controller	302
Resolución de problemas comunes—Dispatcher	303
Problema: no se ejecutará Dispatcher	303
Problema: no responderán Dispatcher y el servidor	303
Problema: no se equilibran las peticiones de Dispatcher	303
Problema: la función de alta disponibilidad de Dispatcher no funciona	304
Problema: no se han podido añadir pulsos (plataforma Windows)	304
Problema: rutas adicionales (Windows 2000)	304
Problema: los asesores no funcionan correctamente	304
Problema: Dispatcher, Microsoft IIS y SSL no funcionan (plataforma Windows).	305
Problema: conexión de Dispatcher con una máquina remota	305
Problema: el mandato dscontrol o lbadm da un error	305

Problema: aparece el mensaje de error "No se puede encontrar el archivo..." al intentar consultar la ayuda en línea (plataforma Windows)	306
Problema: la GUI (interfaz gráfica de usuario) no se inicia correctamente	306
Problema: error al ejecutar Dispatcher con Caching Proxy instalado.	306
Problema: la GUI (interfaz gráfica de usuario) no se muestra correctamente	306
Problema: en la plataforma Windows, las ventanas de ayuda a veces desaparecen detrás de otras ventanas abiertas	307
Problema: Load Balancer no puede procesar y reenviar una trama	307
Problema: se muestra una pantalla azul cuando se inicia el ejecutor de Load Balancer	307
Problema: la vía de acceso al descubrimiento impide el tráfico de retorno con Load Balancer	307
Problema: no funciona la alta disponibilidad de la modalidad de área amplia de Load Balancer	308
Problema: se cierra la comunicación de la GUI (o tiene un comportamiento inesperado) cuando se intenta cargar un archivo de configuración de gran tamaño.	309
Problema: lbadmin realiza una desconexión del servidor después de actualizar la configuración	309
Problema: las direcciones IP no se resuelven correctamente en la conexión remota	310
Problema: la interfaz de Load Balancer coreana muestra fonts solapados o no deseados en sistemas AIX y Linux.	310
Problema: en sistemas Windows, se devuelve una dirección del alias en lugar de la dirección local cuando se emiten mandatos como hostname.	310
Problema: en la plataforma Windows, se produce un comportamiento de la GUI inesperado al utilizar tarjetas de vídeo Matrox AGP	311
Problema: comportamiento inesperado al ejecutar "rmmod ibmlb" (sistemas Linux)	311
Problema: tiempo de respuesta lento cuando se ejecutan mandatos en la máquina de Dispatcher.	311
Problema: el asesor SSL o HTTPS no registra cargas del servidor (cuando se utiliza el reenvío mac)	312
Problema: se produce una desconexión del sistema principal si se cambia el tamaño de la ventana del navegador Netscape cuando se utiliza la administración Web	312
Problema: está habilitada la agrupación de sockets y el servidor Web se enlaza a 0.0.0.0	312
Problema: en sistemas Windows, aparecen caracteres nacionales Latin-1 dañados en la ventana de indicador de mandatos	313
Problema: en HP-UX, se produce un error de falta de memoria/hebra de Java	313
Problema: en los sistemas Windows, los asesores y los destinos de alcance marcan como inactivos todos los servidores	313

Problema: en la plataforma Windows, se resuelve la dirección IP con el nombre de sistema principal cuando se ha configurado más de una dirección con el adaptador	314
Problema: en sistemas Windows, después de una caída de la red, los asesores no funcionan en una configuración de alta disponibilidad	315
Problema: en sistemas Linux, no utilice el mandato "IP address add" cuando cree un alias de varios clústeres en el dispositivo de bucle de retorno	316
Problema: mensaje de error "dirección del direccionador no especificada o no válida para el método del puerto"	316
Problema: en sistemas Solaris, los procesos de Load Balancer finalizan cuando sale de la ventana de terminal desde la que se han iniciado	317
Problema: Se ha producido un retardo al cargar una configuración de Load Balancer.	317
Problema: en sistemas Windows, aparece un mensaje de error de conflicto de dirección IP	317
Problema: las dos máquinas, primaria y de reserva, están activas en una configuración de alta disponibilidad	318
Problema: no se pueden realizar las peticiones del cliente cuando el sistema intenta devolver respuestas de páginas de gran tamaño	318
Problema: en sistemas Windows, se produce el error "el servidor no responde" cuando se emite dscontrol o lbadmin	318
Problema: es posible que las máquinas de Dispatcher de alta disponibilidad no se puedan sincronizar en sistemas Linux para S/390 en controladores qeth.	319
Problema: sugerencias para configurar la alta disponibilidad	319
Problema: en Linux, existen limitaciones de configuración de Dispatcher cuando se utilizan servidores zSeries o S/390 que disponen de tarjetas OSA (Open System Adapter	321
Problema: en algunas versiones de Linux, se produce una pérdida de memoria al ejecutar Dispatcher configurado con el gestor y los asesores	323
Problema: en SUSE Linux Enterprise Server 9, Dispatcher reenvía paquetes, pero éstos no llegan al servidor de programa de fondo	323
Problema: en sistemas Windows, el mensaje de conflicto entre direcciones IP aparece durante la toma de control de alta disponibilidad	324
Problema: iptables de Linux puede impedir el direccionamiento de paquetes	325
Problema: no se puede añadir un servidor IPv6 a la configuración de Load Balancer en sistemas Solaris.	325
Aparece un mensaje de aviso Java al instalar arreglos de servicio	325
Actualización del conjunto de archivos Java con la instalación de Load Balancer	326
Resolución de problemas comunes—CBR	326

Problema: no se ejecutará CBR	326
Problema: el mandato cbrcontrol o lbadmin da un error	326
Problema: no se equilibra la carga de las peticiones	327
Problema: en sistemas Solaris, el mandato cbrcontrol executor start da un error.	327
Problema: error sintáctico o de configuración	327
Problema: en la plataforma Windows, se produce un comportamiento de la GUI inesperado al utilizar tarjetas de vídeo Matrox AGP	327
Problema: se produce una desconexión del sistema principal si se cambia el tamaño de la ventana del navegador Netscape cuando se utiliza la administración Web	328
Problema: en la plataforma Windows, aparecen caracteres nacionales Latin-1 dañados en la ventana de indicador de mandatos	328
Problema: en HP-UX, se produce un error de falta de memoria/hebra de Java	328
Problema: en los sistemas Windows, los asesores y los destinos de alcance marcan como inactivos todos los servidores	328
Problema: en sistemas Windows, se resuelve la dirección IP con el nombre de sistema principal cuando se ha configurado más de una dirección con el adaptador	329
Resolución de problemas comunes—Site Selector	329
Problema: no se ejecutará Site Selector	329
Problema: Site Selector no utiliza el algoritmo de turno rotativo en el tráfico de clientes Solaris.	329
Problema: el mandato sscontrol o lbadmin da un error	329
Problema: no se ha podido iniciar sserver en la plataforma Windows	330
Problema: Site Selector con rutas duplicadas no equilibra la carga correctamente	330
Problema: en la plataforma Windows, se produce un comportamiento de la GUI inesperado al utilizar tarjetas de vídeo Matrox AGP	330
Problema: se produce una desconexión del sistema principal si se cambia el tamaño de la ventana del navegador Netscape cuando se utiliza la administración Web	331
Problema: en la plataforma Windows, aparecen caracteres nacionales Latin-1 dañados en la ventana de indicador de mandatos	331
Problema: en HP-UX, se produce un error de falta de memoria/hebra de Java	331
Problema: en los sistemas Windows, los asesores y los destinos de alcance marcan como inactivos todos los servidores	331
Resolución de problemas comunes—Cisco CSS Controller	332
Problema: no se iniciará ccoserver	332
Problema: el mandato ccocontrol o lbadmin da un error	332
Problema: no se ha podido crear el registro en el puerto 13099	332

Problema: en la plataforma Windows, se produce un comportamiento de la GUI inesperado al utilizar tarjetas de vídeo Matrox AGP	333
Problema: se ha recibido un error de conexión al añadir un consultor	333
Problema: no se actualizan los pesos en el conmutador	333
Problema: el mandato refresh no ha actualizado la configuración del consultor	333
Problema: se produce una desconexión del sistema principal si se cambia el tamaño de la ventana del navegador Netscape cuando se utiliza la administración Web	333
Problema: en la plataforma Windows, aparecen caracteres nacionales Latin-1 dañados en la ventana de indicador de mandatos	334
Problema: en HP-UX, se produce un error de falta de memoria/hebra de Java	334
Resolución de problemas comunes—Nortel Alteon Controller	334
Problema: no se iniciará nalserv	334
Problema: el mandato nalcontrol o lbadmin da un error	334
Problema: no se ha podido crear el registro en el puerto 14099	335
Problema: en la plataforma Windows, se produce un comportamiento de la GUI inesperado al utilizar tarjetas de vídeo Matrox AGP	335
Problema: se produce una desconexión del sistema principal si se cambia el tamaño de la ventana del navegador Netscape cuando se utiliza la administración Web	335
Problema: se ha recibido un error de conexión al añadir un consultor	336
Problema: no se actualizan los pesos en el conmutador	336
Problema: el mandato refresh no ha actualizado la configuración del consultor	336
Problema: en sistemas Windows, aparecen caracteres nacionales Latin-1 dañados en la ventana de indicador de mandatos	336
Problema: en HP-UX, se produce un error de falta de memoria/hebra de Java	337
Resolución de problemas comunes—Metric Server	337
Problema: Metric Server IOException en la plataforma Windows al ejecutar archivos de métrica del usuario .bat o .cmd	337
Problema: Metric Server no informa de las cargas en la máquina de Load Balancer.	337
Problema: el archivo de anotaciones cronológicas de Metric Server informa de que "Es necesaria la firma para acceder al agente"	337
Problema: en sistemas AIX, cuando se ejecuta Metric Server bajo mucha presión, la salida del mandato ps -vg podría dañarse	338
Problema: configuración de Metric Server en una configuración de dos niveles con el equilibrio de carga de Site Selector entre Dispatchers de alta disponibilidad	338

Problema: los scripts, en ejecución en máquinas Solaris de varias CPU, producen mensajes de consola no deseados	339
Problema: en Load Balancer para IPv6, no se pueden recuperar los valores de Metric Server en sistemas Linux	340
Problema: Después de iniciar Metric Server, el valor de métrica devuelve -1	340

Parte 9. Referencia de mandatos 343

Capítulo 26. Cómo leer un diagrama de sintaxis 345

Símbolos y puntuación	345
Parámetros	345
Ejemplos de sintaxis	345

Capítulo 27. Referencia de mandatos para Dispatcher y CBR 347

Diferencias de configuración entre CBR y Dispatcher	348
dscontrol advisor — controlar el asesor.	349
dscontrol binlog — controlar el archivo de anotaciones cronológicas binario	354
dscontrol cluster — configurar clústeres	355
dscontrol executor — control del ejecutor	359
dscontrol file — gestionar archivos de configuración	364
dscontrol help — mostrar o imprimir ayuda para este mandato	366
dscontrol highavailability — controlar alta disponibilidad	367
dscontrol host — configurar un máquina remota	371
dscontrol logstatus — mostrar valores de anotaciones cronológicas de servidor	372
dscontrol manager — controlar el gestor	373
dscontrol metric — configurar métrica del sistema	379
dscontrol port — configurar puertos.	380
dscontrol rule — configurar normas.	386
dscontrol server — configurar servidores	392
dscontrol set — configurar anotaciones cronológicas de servidor.	398
dscontrol status — mostrar si el gestor y los asesores se están ejecutando	399
dscontrol subagent — configurar subagente SNMP	400

Capítulo 28. Referencia de mandatos para Site Selector 403

sscontrol advisor — controlar el asesor.	404
sscontrol file — gestionar archivos de configuración	409
sscontrol help — mostrar o imprimir ayuda para este mandato	411
sscontrol logstatus — mostrar valores de anotaciones cronológicas de servidor	412
sscontrol manager — controlar el gestor	413
sscontrol metric — configurar métrica del sistema	418
sscontrol nameserver — controlar el servidor de nombres	419

sscontrol rule — configurar normas	420
sscontrol server — configurar servidores	423
sscontrol set — configurar anotaciones cronológicas de servidor	425
sscontrol sitename — configurar un nombre de sitio	426
sscontrol status — mostrar si el gestor y los asesores se están ejecutando	429

Capítulo 29. Referencia de mandatos para Cisco CSS Controller. 431

cococontrol consultant — configurar y controlar un consultor	432
cococontrol controller — gestionar el controlador	435
cococontrol file — gestionar archivos de configuración	437
cococontrol help — mostrar o imprimir ayuda para este mandato	438
cococontrol highavailability — controlar alta disponibilidad	439
cococontrol metriccollector — configurar recopilador de métricas	442
cococontrol ownercontent — controlar el nombre de propietario y la norma de contenido.	444
cococontrol service — configurar un servicio	447

Capítulo 30. Referencia de mandatos para Nortel Alteon Controller. 449

nalcontrol consultant — configurar y controlar un consultor	450
nalcontrol controller — gestionar el controlador	453
nalcontrol file — gestionar archivos de configuración	455
nalcontrol help — mostrar o imprimir ayuda para este mandato	456
nalcontrol highavailability — controlar alta disponibilidad	457
nalcontrol metriccollector — configurar recopilador de métricas	460
nalcontrol server — configurar un servidor	462
nalcontrol service — configurar un servicio	464

Apéndice A. GUI: instrucciones generales 467

Apéndice B. Sintaxis de la norma de contenido (patrón) 475

Sintaxis de la norma de contenido (patrón):	475
Palabras clave reservadas	475

Apéndice C. Archivos de configuración de ejemplo 479

Archivos de configuración de Load Balancer de ejemplo	479
Archivo de configuración de Dispatcher — Sistemas AIX, Linux y Solaris	479
Archivo de configuración de Dispatcher — Sistemas Windows.	482
Asesor de ejemplo.	485

Apéndice D. Ejemplo de configuración de alta disponibilidad de 2 niveles con Dispatcher, CBR y Caching Proxy	489
Configuración de la máquina servidor	489

Apéndice E. Avisos	493
Marcas registradas.	495

Glosario	497
Índice.	507

Tablas

1.	Imágenes installp de AIX	32
2.	Mandatos de instalación de AIX.	34
3.	Detalles de instalación de los paquetes de HP-UX para Load Balancer	35
4.	Tareas de configuración para la función Dispatcher	63
5.	Mandatos para crear alias del dispositivo de bucle de retorno (lo0) para Dispatcher	73
6.	Mandatos para suprimir todas las rutas adicionales para Dispatcher	77
7.	Tareas de configuración para el componente CBR	109
8.	Mandatos para crear alias para la NIC	116
9.	Tareas de configuración para el componente Site Selector	131
10.	Tareas de configuración para el componente Cisco CSS Controller	149
11.	Tareas de configuración para el componente Nortel Alteon Controller	171
12.	Tareas de configuración avanzada para Load Balancer	179
13.	Tareas de configuración avanzada para Load Balancer	201
14.	Tabla de resolución de problemas de Dispatcher	286
15.	Tabla de resolución de problemas de CBR	292
16.	Tabla de resolución de problemas de Site Selector	294
17.	Tabla de resolución de problemas de Controlador para Conmutadores Cisco CSS	295
18.	Tabla de resolución de problemas de Nortel Alteon Controller	297
19.	Tabla de resolución de problemas de Metric Server	298

Figuras

1. Ejemplo de una representación física de un sitio que utiliza Dispatcher para gestionar servidores locales 10
2. Ejemplo de un sitio que utiliza Dispatcher y Metric Server para gestionar servidores 11
3. Ejemplo de un sitio que utiliza Dispatcher para gestionar servidores locales y remotos. . . . 12
4. Ejemplo de un sitio que utiliza CBR para gestionar servidores locales 13
5. Ejemplo de un sitio que utiliza Site Selector y Metric Server para gestionar servidores locales y remotos 14
6. Ejemplo de un sitio que utiliza Cisco CSS Controller y Metric Server para gestionar servicios locales 16
7. Ejemplo de un sitio que utiliza Nortel Alteon Controller para gestionar servidores locales . . 17
8. Configuración local sencilla de Dispatcher 45
9. Ejemplo de Dispatcher configurado con un solo clúster y 2 puertos 48
10. Ejemplo de Dispatcher configurado con dos clústeres, cada uno con un puerto 49
11. Ejemplo de Dispatcher configurado con 2 clústeres, cada uno con 2 puertos 50
12. Ejemplo para utilizar los métodos de reenvío nat o cbr de Dispatcher 57
13. Ejemplo de Dispatcher con alta disponibilidad sencilla 60
14. Ejemplo de Dispatcher con alta disponibilidad mutua 61
15. Ejemplo de las direcciones IP necesarias para la máquina Dispatcher 68
16. Configuración local sencilla de CBR 99
17. Ejemplo de CBR configurado con un solo clúster y 2 puertos 102
18. Ejemplo de CBR configurado con dos clústeres, cada uno con un puerto. 103
19. Ejemplo de CBR configurado con 2 clústeres, cada uno con 2 puertos 104
20. Archivo de configuración de CBR para sistemas AIX, Linux y Solaris 114
21. Archivo de configuración de CBR para sistemas HP-UX. 114
22. Archivo de configuración de CBR para sistemas Windows 115
23. Configuración sencilla de Site Selector 121
24. Ejemplo de un entorno DNS 126
25. Configuración sencilla de Cisco CSS Controller. 139
26. Ejemplo de un consultor conectado detrás de los conmutadores 145
27. Ejemplo de consultor (con el asociado de alta disponibilidad opcional), configurado detrás del conmutador con la interfaz de usuario delante del conmutador 146
28. Configuración sencilla de Nortel Alteon Controller. 157
29. Ejemplo de un consultor conectado detrás del conmutador 163
30. Ejemplo de consultor conectado mediante una intranet delante de un conmutador 164
31. Ejemplo de consultor detrás del conmutador e interfaz de usuario delante del conmutador . 165
32. Ejemplo de consultor configurado con servidores de reserva 166
33. Ejemplo de alta disponibilidad de Nortel Alteon Controller y Conmutador Nortel Alteon Web 169
34. Ejemplo de una configuración WAN de dos niveles que utiliza el asesor automático . . . 192
35. Ejemplo de una configuración que consta de un único segmento LAN 229
36. Ejemplo de configuración mediante servidores locales y remotos 230
37. Configuración del ejemplo de área amplia con varios Load Balancer remotos 232
38. Configuración del ejemplo de área amplia con una plataforma de servidor que da soporte a GRE 235
39. Ejemplo de una red privada que utiliza Dispatcher 237
40. Mandatos SNMP para Sistemas Linux y UNIX 271
41. La interfaz gráfica de usuario (GUI) que muestra la expansión de la estructura de árbol de la GUI del componente Dispatcher. . 468
42. La interfaz gráfica de usuario (GUI) que muestra la expansión de la estructura de árbol de la GUI del componente CBR. . . . 469
43. La interfaz gráfica de usuario (GUI) que muestra la expansión de la estructura de árbol de la GUI del componente Site Selector. . 470
44. La interfaz gráfica de usuario (GUI) que muestra la expansión de la estructura de árbol de la GUI del componente Cisco CSS Controller. 471
45. La interfaz gráfica de usuario (GUI) que muestra la expansión de la estructura de árbol de la GUI del componente Nortel Alteon Controller. 472
46. Ejemplo de configuración de alta disponibilidad de 2 niveles con Dispatcher, CBR y Caching Proxy. 489

Acerca de este manual

En este manual se describe cómo planificar la instalación, configuración, utilización y solución de problemas de IBM WebSphere Application Server Load Balancer para sistemas operativos AIX, HP-UX, Linux, Solaris y Windows. Anteriormente, este producto se llamaba Edge Server Network Dispatcher, SecureWay Network Dispatcher, eNetwork Dispatcher e Interactive Network Dispatcher.

A quién va dirigido este manual

El manual *Guía de administración de Load Balancer* se ha escrito para aquellos administradores de red y de sistemas expertos que estén familiarizados con sus sistemas operativos y con el suministro de servicios de Internet. No es necesario tener conocimientos previos de Load Balancer.

Este manual no está concebido para dar soporte a varios releases de Load Balancer.

Información de consulta

El sitio Web del Centro de información de Edge Components tiene un enlace a la versión actual de este manual en formatos HTML y PDF.

Para obtener las actualizaciones más actuales sobre Load Balancer, visite la página de soporte del sitio Web y pulse el enlace correspondiente al sitio de notas técnicas.

Para acceder a estas páginas Web y las páginas relacionadas, vaya a las direcciones URL enumeradas en "Documentos relacionados y sitios Web" en la página xix.

Accesibilidad

Las características de accesibilidad ayudan al usuario que tiene discapacidades físicas, como por ejemplo una movilidad restringida o una visión limitada, a utilizar satisfactoriamente los productos de software. Éstas son las principales características de accesibilidad en Load Balancer:

- Puede utilizar el software lector de pantalla y un sintetizador de discurso digital para oír lo que se visualiza en la pantalla. También puede utilizar el software de reconocimiento de voz, como por ejemplo IBM ViaVoice, para entrar datos y para navegar por la interfaz de usuario.
- Puede utilizar las características utilizando el teclado en lugar del ratón.
- Puede configurar y administrar las características de Load Balancer utilizando editores de texto estándar o interfaces de línea de mandatos en lugar de las interfaces gráficas proporcionadas. Para obtener más información sobre la accesibilidad de características específicas, consulte la documentación sobre dichas características.

¿Cómo enviar sus comentarios?

Sus comentarios son importantes para ayudarnos a proporcionar la información más precisa y de la mayor calidad posible. Para enviar comentarios sobre este manual o sobre cualquier otro documento de Edge Components:

- Envíe sus comentarios por correo electrónico a hojacom@es.ibm.com. Asegúrese de incluir el título y el número de serie del manual, la versión y, si es aplicable, la ubicación específica del texto sobre el que está realizando los comentarios (por ejemplo, un número de página o un número de tabla).

Documentos relacionados y sitios Web

- *Conceptos, planificación e instalación de Edge Components* GC11-3237-00
- *Guía de programación de Edge Components* GC11-3238-00
- *Guía de administración de Caching Proxy* GC11-3239-00
- Página principal del sitio Web de IBM: www.ibm.com/
- Producto IBM WebSphere Application Server: www.ibm.com/software/webservers/appserv/
- Sitio Web de la biblioteca de IBM WebSphere Application Server: www.ibm.com/software/webservers/appserv/was/library/
- Sitio Web de soporte de IBM WebSphere Application Server: www.ibm.com/software/webservers/appserv/was/support/
- Centro de información de IBM WebSphere Application Server: www.ibm.com/software/webservers/appserv/infocenter.html
- Centro de información de IBM WebSphere Application Server Edge Components: www.ibm.com/software/webservers/appserv/ecinfocenter.html

Parte 1. Introducción a Load Balancer

Esta parte proporciona una visión general de Load Balancer y sus componentes, una descripción de alto nivel de características de configuración que están disponibles, una lista de requisitos de hardware y software e instrucciones de instalación. Contiene los capítulos siguientes:

- Capítulo 1, “Visión general de Load Balancer”, en la página 3
- Capítulo 2, “Visión general de los componentes de Load Balancer”, en la página 9
- Capítulo 3, “Gestión de la red: determinación de las características de Load Balancer que se van a utilizar”, en la página 19
- Capítulo 4, “Instalación de Load Balancer”, en la página 31

Capítulo 1. Visión general de Load Balancer

Este capítulo proporciona una visión general de Load Balancer e incluye los apartados siguientes:

- “Descripción de Load Balancer”
- “¿Qué componentes de Load Balancer puedo utilizar?”
- “Ventajas de utilizar Load Balancer” en la página 4
- “Cómo Load Balancer puede proporcionar alta disponibilidad” en la página 6
- “Nuevas características” en la página 6

Si desea una lista de alto nivel de las características de configuración proporcionadas por cada uno de los componentes de Load Balancer, para ayudarle a planificar qué características utilizar para gestionar la red, consulte el Capítulo 3, “Gestión de la red: determinación de las características de Load Balancer que se van a utilizar”, en la página 19.

Descripción de Load Balancer

Load Balancer es una solución de software para distribuir peticiones de cliente entrantes entre servidores. Esta solución aumenta el rendimiento de los servidores dirigiendo las peticiones de la sesión TCP/IP a servidores distintos dentro de un grupo de servidores; de este modo, se equilibran las peticiones entre todos los servidores. Este equilibrio de carga es transparente a los usuarios y otras aplicaciones. Load Balancer resulta de utilidad para aplicaciones como servidores de correo electrónico, servidores de la World Wide Web, consultas de base de datos paralelo distribuidas y otras aplicaciones TCP/IP.

Cuando Load Balancer se utiliza con servidores Web, puede ayudar a maximizar el potencial de su sitio proporcionando una solución completa, flexible y escalable a problemas de intensa demanda. Si los visitantes de su sitio no pueden comunicar en los momentos de mayor demanda, utilice Load Balancer para encontrar automáticamente el servidor óptimo para gestionar las peticiones entrantes, así mejorará la satisfacción de los clientes y la rentabilidad.

¿Qué componentes de Load Balancer puedo utilizar?

IMPORTANTE: si utiliza Load Balancer para IPv4 y IPv6, sólo está disponible el componente Dispatcher. Consulte el Capítulo 8, “Despliegue de Dispatcher en Load Balancer para IPv4 y IPv6”, en la página 81 para obtener más información.

Load Balancer consta de los cinco componentes siguientes que se pueden utilizar ya sea por separado o juntos para proporcionar resultados de equilibrio de carga superiores:

- Puede utilizar el componente **Dispatcher** por sí mismo para equilibrar la carga en servidores dentro de una red de área local o una red de área amplia utilizando varios pesos y medidas que se establecen dinámicamente mediante Dispatcher. Este componente proporciona equilibrio de carga entre servicios específicos, como HTTP, FTP, SSL, NNTP, IMAP, POP3, SMTP, SIP y Telnet. No utiliza un servidor de nombres de dominio para correlacionar nombres de dominio con direcciones IP.

Para el protocolo HTTP, también puede utilizar el dispositivo Direccionamiento basado en contenido de Dispatcher para equilibrar la carga según el contenido de la petición del cliente. El servidor elegido es el resultado de comparar el URL con una norma especificada. El direccionamiento basado en contenido (método de reenvío cbr) del Dispatcher *no* requiere Caching Proxy.

- Para el protocolo HTTP y HTTPS (SSL), puede utilizar el componente CBR (**Content Based Routing**) para equilibrar la carga según el contenido de la petición del cliente. Un cliente envía una petición a Caching Proxy y Caching Proxy envía la petición al servidor adecuado. El servidor elegido es el resultado de comparar el URL con una norma especificada.

Nota: El componente CBR (Content Based Routing) está disponible en todas las plataformas excepto donde se ejecuta la JVM de 64 bits. De modo alternativo, puede utilizar el método de reenvío cbr del componente Dispatcher de Load Balancer para proporcionar direccionamiento basado en contenido sin utilizar Caching Proxy. Si desea más información, consulte el apartado “Direccionamiento basado en contenido de Dispatcher (método de reenvío cbr)” en la página 55.

- Puede utilizar el componente **Site Selector** para equilibrar la carga en servidores dentro de una red de área local o una red de área amplia utilizando un algoritmo de turno rotativo para el DNS o un algoritmo más avanzado especificado por el usuario. Site Selector funciona junto con un servidor de nombres para correlacionar nombres DNS con direcciones IP.
- Puede utilizar el componente **Cisco CSS Controller** o **Nortel Alteon Controller** para generar pesos del servidor que luego se envían al Conmutador Cisco CSS o el Conmutador Nortel Alteon Web respectivamente para una selección de servidor, una optimización de carga y una tolerancia a errores óptimas.

Si desea más información sobre los componentes Dispatcher, CBR, Site Selector, Cisco CSS Controller, y Nortel Alteon Controller, consulte el apartado “Componentes de Load Balancer” en la página 9.

Ventajas de utilizar Load Balancer

El número de usuarios y redes conectado a Internet global aumenta exponencialmente. Este aumento produce problemas de escalabilidad que pueden limitar el acceso de los usuarios a los sitios conocidos.

Actualmente, los administradores de redes utilizan varios métodos para intentar maximizar el acceso. Con algunos de estos métodos, puede elegir de modo aleatorio un usuario distinto si una selección anterior es lenta o no responde. Este enfoque es engorroso, pesado e ineficaz. Otro método es el algoritmo de turno rotativo estándar, en el que el servidor de nombres de dominio selecciona servidores por turno para gestionar las peticiones. Este enfoque es mejor, pero sigue siendo ineficaz porque envía tráfico sin tener en cuenta la carga de trabajo del servidor. Además, aún cuando el servidor dé un error, se le seguirán enviando las peticiones.

La necesidad de una solución más completa ha dado como resultado Load Balancer. Esta solución ofrece muchas ventajas sobre las soluciones anteriores y de la competencia:

Escalabilidad

A medida que aumenta el número de peticiones de cliente, puede añadir servidores dinámicamente, proporcionando soporte para decenas de millones de peticiones al día, en decenas o incluso centenas de servidores.

Uso eficaz del equipo

El equilibrio de carga asegura que cada grupo de servidores hace un uso óptimo del hardware minimizando los puntos conflictivos que suelen aparecer con un método de turno rotativo estándar.

Integración sencilla

Load Balancer utiliza protocolos TCP/IP o UDP/IP estándar. Puede añadirlo a la red existente sin realizar ningún cambio físico en la red. Es sencillo de instalar y configurar.

Menos carga adicional

Con el método sencillo de reenvío de nivel mac, el componente Dispatcher sólo presta atención a los flujos de cliente a servidor de entrada. No tiene que comprobar los flujos de servidor a cliente de salida. Esto reduce significativamente el impacto en la aplicación comparado con otros enfoques y puede producir un rendimiento de red mejorado.

Alta disponibilidad

Los componentes Dispatcher, Cisco CSS Controller y Nortel Alteon Controller ofrecen una alta disponibilidad integrada, utilizando una máquina de reserva que permanece preparada en todo momento para hacerse con el control del equilibrio de carga en caso de que la máquina servidor primaria dé un error. Cuando uno de los servidores da un error, el otro servidor sigue atendiendo las peticiones. Este proceso impide que haya un servidor como único punto de error y hace que el sitio esté altamente disponible.

Para obtener más información, consulte el apartado “Cómo Load Balancer puede proporcionar alta disponibilidad” en la página 6

Direccionamiento basado en contenido (con el componente CBR o el componente Dispatcher)

Junto con Caching Proxy, el componente CBR tiene la capacidad de dirigir mediante proxy peticiones HTTP y HTTPS (SSL) a servidores específicos según el contenido solicitado. Por ejemplo, si una petición contiene la serie “/cgi-bin/” en la parte del directorio de la dirección URL y el nombre de servidor es un servidor local, CBR puede dirigir la petición al mejor servidor de un conjunto de servidores específicamente asignados para gestionar peticiones cgi.

Nota: El componente CBR (Content Based Routing) está disponible en todas las plataformas excepto donde se ejecuta la JVM de 64 bits. De modo alternativo, puede utilizar el método de reenvío cbr del componente Dispatcher de Load Balancer para proporcionar direccionamiento basado en contenido sin utilizar Caching Proxy. Si

desea más información, consulte el apartado “Direccionamiento basado en contenido de Dispatcher (método de reenvío cbr)” en la página 55.

El componente Dispatcher también proporciona direccionamiento basado en contenido, pero no requiere tener instalado Caching Proxy. Dado que el direccionamiento basado en contenido del componente Dispatcher se realiza en el kernel a medida que se reciben los paquetes, puede proporcionar un direccionamiento basado en contenido *más rápido* que el componente CBR. El componente Dispatcher realiza direccionamiento basado en contenido para HTTP (con la norma de tipo de “contenido”) y HTTPS (con afinidad de ID de sesión SSL).

Nota: Sólo el componente CBR puede utilizar la norma de contenido para HTTPS (SSL) cuando se equilibra la carga de tráfico según el contenido de la petición HTTP, que requiere el descifrado y nuevo cifrado de mensajes.

Cómo Load Balancer puede proporcionar alta disponibilidad

Dispatcher

El componente Dispatcher ofrece una característica de alta disponibilidad integrada, que evita que el Dispatcher sea un único punto de error de la red. Esta característica implica el uso de una segunda máquina Dispatcher que supervisa la máquina principal o, primaria, y está preparada para hacerse con el control del equilibrio de carga en caso de que la máquina primaria dé un error en un momento dado. El componente Dispatcher también ofrece alta disponibilidad mutua que permite que dos máquinas sean a la vez primaria y secundaria (de reserva) entre sí. Consulte el apartado “Configurar la alta disponibilidad” en la página 205.

CBR

También puede alcanzar un nivel de alta disponibilidad utilizando el componente de CBR cuando se utiliza una configuración de dos niveles con una máquina de Dispatcher que equilibra la carga entre varios servidores que tienen el componente CBR.

Cisco CSS Controller o Nortel Alteon Controller

Los controladores tienen una característica de alta disponibilidad para impedir que el controlador sea un único punto de error. Se puede configurar un controlador como primario en una máquina y un controlador de reserva en otra máquina. El de reserva supervisa el primario y está preparado para hacerse con el control de la tarea de proporcionar pesos de servidor a los conmutadores en caso de que el primario dé un error. Si desea más información, consulte el apartado “Alta disponibilidad” en la página 243.

Nuevas características

Load Balancer para IBM WebSphere Application Server Versión 6.1 contiene varias características nuevas. Las más significativas de ellas se enumeran aquí.

- **Soporte para ejecutar procesos de equilibrio de carga en espacio de usuario en sistemas Linux**

Se ha añadido soporte a las instalaciones de Load Balancer para IPv4 y IPv6 para ejecutar procesos de equilibrio de carga en espacio de usuario en lugar de hacerlo en espacio de kernel. Para los sistemas Linux, ya no hay dependencia del módulo de kernel.

Para obtener la información más reciente sobre qué sistemas soportan el proceso en espacio de usuario (sin kernel), consulte el siguiente sitio Web:

<http://www.ibm.com/support/docview.wss?rs=180&uid=swg27006921>.

Para obtener más información, consulte el apartado “Plataformas admitidas para Load Balancer para IPv4 y IPv6” en la página 82.

- **Soporte para HP 11iv2 en PA-RISC (soporte eliminado para HP 11iv1)**

Si desea información sobre los requisitos de hardware y software, consulte el siguiente sitio Web: <http://www.ibm.com/support/docview.wss?rs=180&uid=swg27006921>.

- **Soporte para Linux en sistemas zSeries de 64 bits**

El soporte para Linux en sistemas zSeries de 64 bits sólo se proporciona para instalaciones de Load Balancer para IPv4 y IPv6.

Para obtener información sobre Load Balancer para IPv4 y IPv6 y consideraciones especiales para ejecutar Linux en sistemas zSeries de 64 bits, consulte Capítulo 8, “Despliegue de Dispatcher en Load Balancer para IPv4 y IPv6”, en la página 81.

Si desea información sobre los requisitos de hardware y software, consulte el siguiente sitio Web: <http://www.ibm.com/support/docview.wss?rs=180&uid=swg27006921>.

- **Soporte del asesor SIP**

Se ha añadido el soporte para un asesor SIP (Session Initiation Protocol). El asesor SIP que recibe soporte sólo se ejecuta en el protocolo TCP.

Para obtener más información, consulte la página 188.

- **En sistemas Linux, soporte de configuraciones de cliente con ubicación compartida**

Esta característica se aplica a todos los componentes de Load Balancer.

Los clientes que se encuentran en la misma máquina que Load Balancer sólo reciben soporte en sistemas Linux.

Para obtener más información, consulte el apartado “Utilización de un cliente con ubicación compartida” en la página 242.

- **Soporte para el navegador Firefox**

Si desea información sobre las versiones de Firefox soportadas y sobre todos los navegadores soportados, consulte el siguiente sitio Web: <http://www.ibm.com/support/docview.wss?rs=180&uid=swg27006921>.

Capítulo 2. Visión general de los componentes de Load Balancer

En este capítulo se ofrece una visión general de los componentes de Load Balancer e incluye los siguientes apartados:

- “Componentes de Load Balancer”
- “Visión general del componente Dispatcher”
- “Visión general del componente CBR (Content Based Routing)” en la página 12
- “Visión general del componente Site Selector” en la página 14
- “Visión general del componente Cisco CSS Controller” en la página 15
- “Visión general del componente Nortel Alteon Controller” en la página 17

Para obtener una lista de las características de configuración de alto nivel que proporciona cada uno de los componentes de Load Balancer, para ayudarle a planificar qué características desea utilizar para gestionar la red, consulte el Capítulo 3, “Gestión de la red: determinación de las características de Load Balancer que se van a utilizar”, en la página 19.

Componentes de Load Balancer

Los cinco componentes de Load Balancer son: Dispatcher, CBR (Content Based Routing), Site Selector, Cisco CSS Controller y Nortel Alteon Controller. Load Balancer le ofrece la flexibilidad de utilizar los componentes por separado o juntos en función de la configuración del sitio. En este apartado se proporciona una visión general de estos componentes.

IMPORTANTE: si utiliza Load Balancer para IPv4 y IPv6, sólo está disponible el componente Dispatcher. Consulte el Capítulo 8, “Despliegue de Dispatcher en Load Balancer para IPv4 y IPv6”, en la página 81 para obtener más información.

Visión general del componente Dispatcher

El componente Dispatcher equilibra el tráfico entre servidores a través de una combinación exclusiva de software de equilibrio de carga y gestión. Dispatcher también puede detectar un servidor con anomalías y reenviar el tráfico sin pasar por el mismo. Dispatcher da soporte a HTTP, FTP, SSL, SMTP, NNTP, IMAP, POP3, Telnet, SIP y a cualquier otra aplicación basada en UDP sin estado o TCP.

Todas las peticiones de cliente enviadas a una máquina de Dispatcher se dirigen al servidor “más idóneo” en función de los pesos que se establecen de forma dinámica. Puede utilizar los valores por omisión de dichos pesos o cambiar los valores durante el proceso de configuración.

Dispatcher ofrece tres métodos de envío (que se especifican en el puerto):

- El método de reenvío MAC (**mac**). Con este método de reenvío, Dispatcher equilibra la carga de la petición entrante en el servidor. El servidor devuelve la respuesta directamente al cliente sin ninguna participación por parte de Dispatcher.
- Método de envío NAT/NAPT (**nat**). Si se utiliza la aptitud de NAT (Conversión de direcciones de red) / NAPT (Conversión de puertos de direcciones de red) de

Dispatcher se eliminará la limitación de que los servidores de programas de fondo tenga que estar en la red conectada localmente. Cuando desee que los servidores estén situados en ubicaciones remotas, puede utilizar la técnica NAT en lugar de una técnica GRE (Encapsulamiento genérico de direccionamiento) / WAN (Red de área amplia). Con este método de reenvío, Dispatcher equilibra la carga de la petición entrante en el servidor. El servidor devuelve la respuesta a Dispatcher. A continuación, la máquina Dispatcher devuelve la respuesta al cliente.

- Método de reenvío para direccionamiento basado en contenido (**cbr**). Sin Caching Proxy, el componente Dispatcher permite realizar el direccionamiento basado en contenido para HTTP (utilizando la norma de tipo "contenido") y HTTPS (utilizando la afinidad de ID de sesión SSL). Para el tráfico HTTP y HTTPS, el componente Dispatcher puede proporcionar un direccionamiento basado en contenido *más rápido* que el componente CBR. Con el método de reenvío cbr, Dispatcher equilibra la carga de la petición entrante en el servidor. El servidor devuelve la respuesta a Dispatcher. A continuación, la máquina Dispatcher devuelve la respuesta al cliente.

El componente Dispatcher es la clave que permite la gestión estable y eficaz de una red de servidores grande y escalable. Con Dispatcher, puede enlazar muchos servidores individuales en lo que parecerá ser un solo servidor virtual. Así, su sitio se presenta como una sola dirección IP ante los demás. Dispatcher funciona independientemente de un servidor de nombres de dominio; todas las peticiones se envían a la dirección IP de la máquina Dispatcher.

Dispatcher proporciona distintas ventajas al equilibrar la carga de tráfico para servidores agrupados en clúster, resultando en una gestión estable y eficaz del sitio.

Gestión de servidores locales con Dispatcher

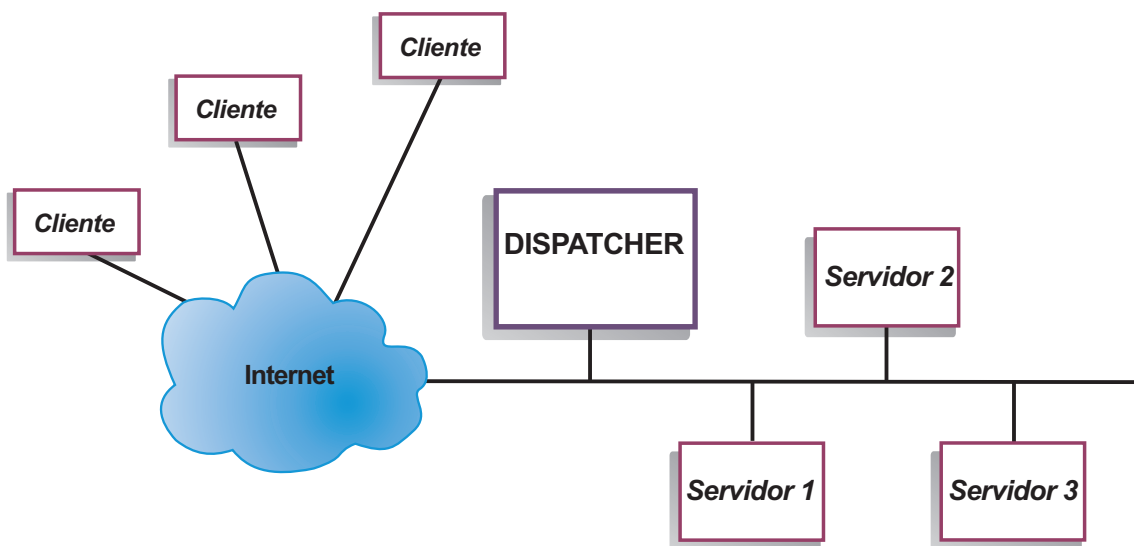


Figura 1. Ejemplo de una representación física de un sitio que utiliza Dispatcher para gestionar servidores locales

La Figura 1 muestra una representación física del sitio utilizando una configuración de red Ethernet. La máquina Dispatcher puede instalarse sin realizar ningún cambio físico en la red. Cuando se utiliza el método de reenvío MAC, una vez que

Dispatcher ha dirigido una petición de cliente al servidor óptimo, la respuesta se envía directamente del servidor al cliente sin la participación de Dispatcher.

Gestión de servidores que utilizan Dispatcher y Metric Server

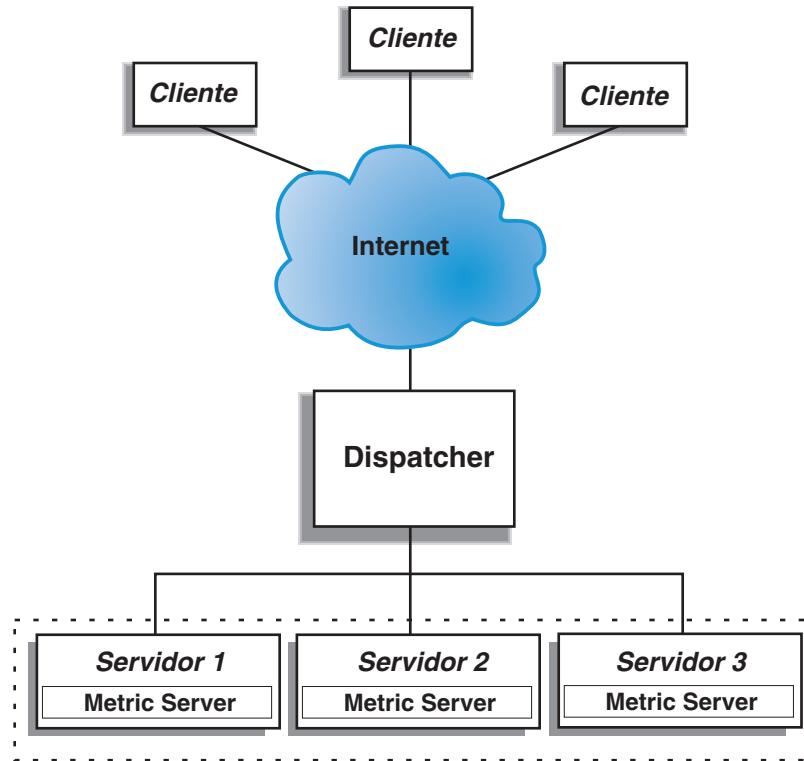


Figura 2. Ejemplo de un sitio que utiliza Dispatcher y Metric Server para gestionar servidores

En la Figura 2 se muestra un sitio en el que todos los servidores están en una red local. El componente Dispatcher se utiliza para reenviar peticiones y Metric Server se utiliza para proporcionar información de carga del sistema a la máquina Dispatcher.

En este ejemplo, el daemon de Metric Server está instalado en cada servidor de programa de fondo. Puede utilizar Metric Server con el componente Dispatcher o cualquier otro componente de Load Balancer.

Gestión de servidores locales y remotos con Dispatcher

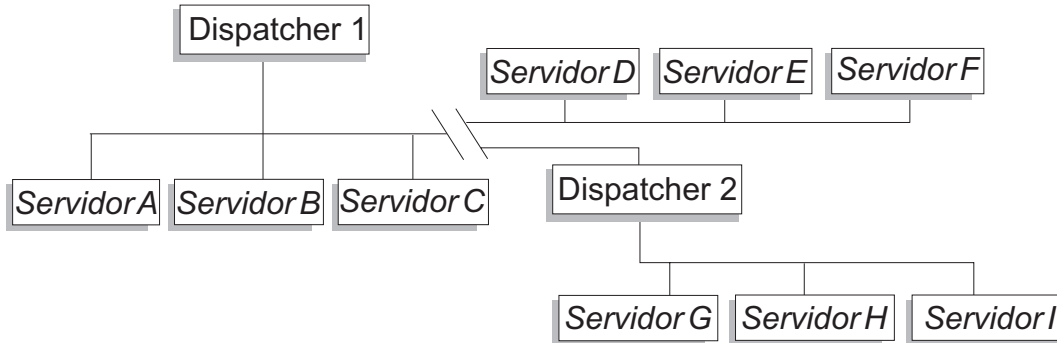


Figura 3. Ejemplo de un sitio que utiliza Dispatcher para gestionar servidores locales y remotos

El soporte de área amplia en Dispatcher permite utilizar los servidores locales y remotos (servidores en distintas subredes). En la Figura 3 se muestra una configuración en la que un sistema Dispatcher local (Dispatcher 1) sirve de punto de entrada para todas las peticiones. Distribuye estas peticiones entre sus propios servidores locales (ServidorA, ServidorB, ServidorC) y el sistema Dispatcher remoto (Dispatcher 2), que equilibrará la carga de sus servidores locales (ServidorG, ServidorH, ServidorI).

Al utilizar el método de reenvío NAT de Dispatcher o al utilizar el soporte de GRE, el soporte de área amplia con Dispatcher también puede lograrse sin utilizar una máquina Dispatcher en el sitio remoto (donde están ServidorD, ServidorE y ServidorF). Si desea más información, consulte los apartados “NAT/NAPT de Dispatcher (método de reenvío nat)” en la página 53 y “Soporte de GRE (Encapsulamiento genérico de direccionamiento)” en la página 234.

Visión general del componente CBR (Content Based Routing)

CBR funciona con Caching Proxy para enviar mediante proxy las peticiones de cliente a los servidores HTTP o HTTPS (SSL) especificados. Permite manipular detalles de almacenamiento en antememoria a fin de conseguir una recuperación de documentos Web más rápida con menos requisitos de ancho de banda de red. CBR y Caching Proxy examina las peticiones HTTP utilizando tipos de normas especificadas.

Nota: El componente CBR (Content Based Routing) está disponible en todas las plataformas excepto donde se ejecuta la JVM de 64 bits. De modo alternativo, puede utilizar el método de reenvío cbr del componente Dispatcher de Load Balancer para proporcionar direccionamiento basado en contenido sin utilizar Caching Proxy. Si desea más información, consulte el apartado “Direccionamiento basado en contenido de Dispatcher (método de reenvío cbr)” en la página 55.

CBR le ofrece la capacidad de especificar un conjunto de servidores que manejan una petición basándose en una expresión normal que coincide con el contenido de la petición. Puesto que CBR permite especificar varios servidores para cada tipo de petición, se puede equilibrar la carga de las peticiones para que la respuesta de cliente sea óptima. CBR también detecta cuando un servidor incluido en un conjunto ha sufrido una anomalía y deja de direccionar peticiones a dicho servidor.

El algoritmo de equilibrio de carga que el componente CBR utiliza es idéntico al algoritmo probado que utiliza el componente Dispatcher.

Cuando Caching Proxy recibe una petición, ésta se compara con las normas definidas en el componente CBR. Si se encuentra una coincidencia, se elige uno de los servidores asociados a dicha norma para manejar la petición. Caching Proxy realiza su proceso normal para enviar mediante proxy la petición al servidor elegido.

CBR tiene las mismas funciones que Dispatcher, a excepción de la alta disponibilidad, el subagente SNMP, el área amplia y unos pocos mandatos de configuración.

Caching Proxy debe estar en ejecución para que CBR pueda empezar a equilibrar la carga de peticiones de cliente.

Gestión de servidores locales con CBR

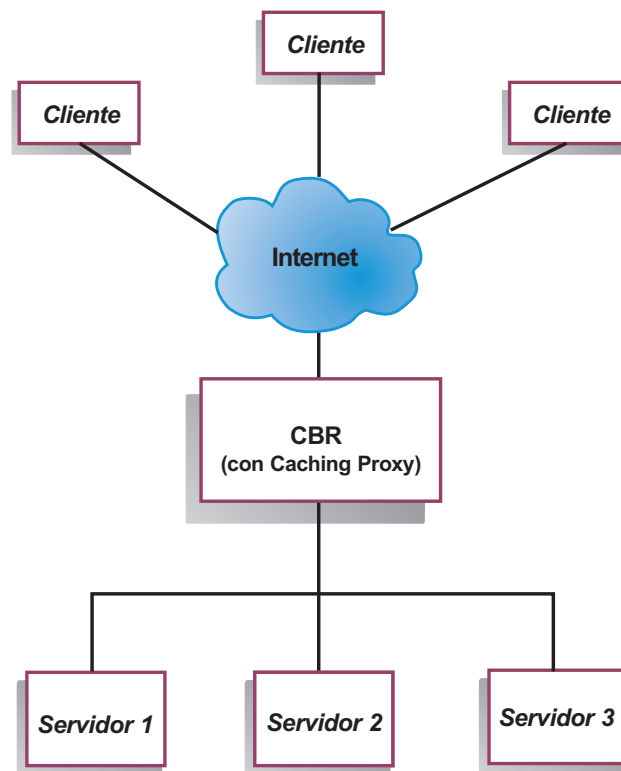


Figura 4. Ejemplo de un sitio que utiliza CBR para gestionar servidores locales

La Figura 4 muestra una representación lógica de un sitio en el que se emplea CBR para enviar mediante proxy algún contenido de servidores locales. El componente CBR utiliza Caching Proxy para enviar peticiones de cliente (HTTP o HTTPS) a los servidores basándose en el contenido del URL.

Visión general del componente Site Selector

Site Selector actúa como servidor de nombres que funciona junto con otros servidores de nombres en un sistema de nombres de dominio para equilibrar la carga entre un grupo de servidores utilizando las medidas y los pesos que se recopilan. Puede crear una configuración del sitio que le permita equilibrar la carga del tráfico entre un grupo de servidores basándose en el nombre de dominio utilizado para la petición de un cliente.

Un cliente somete una petición para la resolución de un nombre de dominio a un servidor de nombres dentro de su red. El servidor de nombres reenvía la petición al sistema Site Selector. A continuación, Site Selector resuelve el nombre de dominio en una dirección IP de uno de los servidores que se ha configurado bajo el nombre del sitio. Site Selector devuelve la dirección IP del servidor seleccionado al servidor de nombres. El servidor de nombres devuelve la dirección IP al cliente.

Metric Server es un componente de supervisión del sistema de Load Balancer que debe instalarse en cada servidor con equilibrio de carga incluido en la configuración. Con Metric Server, Site Selector puede supervisar el nivel de actividad de un servidor, detectar si un servidor tiene la carga menos pesada y detectar un servidor anómalo. La carga es una medición del esfuerzo del servidor. Si personaliza los archivos de script de métrica del sistema, puede controlar el tipo de medidas utilizadas para medir la carga. Puede configurar Site Selector de modo que se adapte a su entorno, teniendo en cuenta factores como la frecuencia de acceso, el número total de usuarios y los tipos de acceso (por ejemplo, consultas breves, consultas de larga ejecución o cargas con mucha utilización de la CPU).

Gestión de servidores locales y remotos con Site Selector y Metric Server

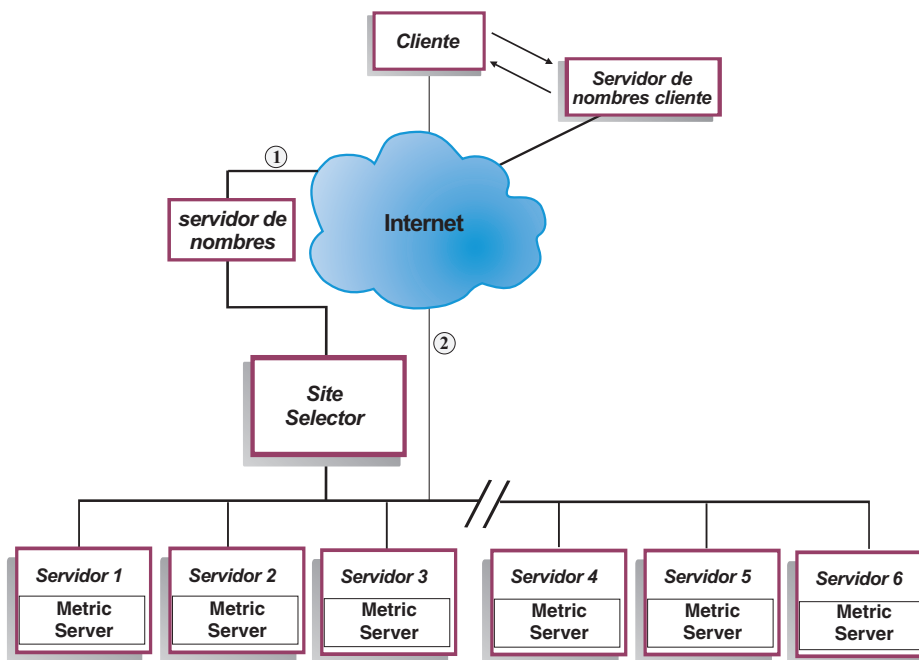


Figura 5. Ejemplo de un sitio que utiliza Site Selector y Metric Server para gestionar servidores locales y remotos

La Figura 5 en la página 14 muestra un sitio en el que se utiliza el componente Site Selector para responder a peticiones. Servidor1, Servidor2 y Servidor3 son locales. Servidor4, Servidor5 y Servidor6 son remotos.

Un cliente somete una petición para la resolución de un nombre de dominio a un servidor de nombres de cliente. El servidor de nombres reenvía la petición a través del DNS a la máquina Site Selector (ruta 1). A continuación, Site Selector resuelve el nombre de dominio en una dirección IP de uno de los servidores. Site Selector devuelve la dirección IP del servidor seleccionado al servidor de nombres de cliente. El servidor de nombres devuelve la dirección IP al cliente.

Una vez que el cliente ha recibido la dirección IP del servidor, el cliente dirige las peticiones de la aplicación directamente al servidor seleccionado (ruta 2).

Nota: En este ejemplo, Metric Server proporciona información de carga del sistema a la máquina Site Selector. El agente de Metric Server está instalado en cada servidor de programa de fondo. Utilice Metric Server junto con Site Selector; de lo contrario, Site Selector sólo puede emplear un método de selección en forma de turno rotativo para realizar el equilibrio de carga.

Visión general del componente Cisco CSS Controller

Cisco CSS Controller forma una solución complementaria junto con conmutadores CSS 11000 de Cisco. La solución combinada mezcla las habilidades del direccionamiento de contenido y el reenvío de paquetes de los conmutadores CSS 1100 con los sofisticados algoritmos de Load Balancer para determinar la información de carga y la disponibilidad del *servicio* (base de datos o aplicación de servidor de programa de fondo). La función Cisco CSS Controller emplea el algoritmo de cálculo estándar, los asesores estándares y personalizados de Load Balancer y Metric Server para determinar la métrica, el estado y la carga del servicio. Con esta información Cisco CSS Controller genera pesos de servicio, que enviará a Conmutador Cisco CSS para obtener una selección de servicio, optimización de la carga y tolerancia de errores óptimos .

Cisco CSS Controller realiza un seguimiento de muchos criterios, incluidos:

- Conexiones activas y velocidad de conexión (número de conexiones dentro de un ciclo de cálculo del peso).
- Disponibilidad de aplicación y base de datos, que se facilita a través del uso de asesores estándares y personalizados y de agentes residentes en el servicio adaptados a la aplicación específica
- Utilización de la CPU
- Utilización de la memoria
- Métrica del sistema personalizable por el usuario

Cuando un Conmutador Cisco CSS, sin Cisco CSS Controller, determina el estado de un servicio que proporciona contenido, utiliza tiempos de respuestas para peticiones de contenido u otras medidas de red. Con Cisco CSS Controller instalado, estas actividades se descargan de Conmutador Cisco CSS a Cisco CSS Controller. Cisco CSS Controller influye el peso del servicio o la habilidad de servir contenido, y activa o suspende un servicio como apropiado cuando el servicio deja de estar disponible o vuelve a estarlo.

Cisco CSS Controller:

- Utiliza una interfaz SNMP publicada para obtener información de conexión de Conmutador Cisco CSS
- Utiliza la entrada del asesor para analizar disponibilidad de servicio y el tiempo de respuesta
- Utiliza la información de Metric Server para analizar la carga del sistema
- Genera pesos para cada servicio en la configuración

Los pesos se aplican a todos los servicios de un puerto. Para cualquier puerto concreto, las peticiones se distribuyen entre los servicios en función del peso relativo que dichos servicios tienen entre sí. Por ejemplo, si un servicio se establece en el peso 10 y el otro en 5, el servicio establecido en 10 recibe el doble de peticiones que el servidor establecido en 5. Los pesos se proporcionan a Conmutador Cisco CSS mediante SNMP. Cuando el peso de cualquier servicio se fija en un valor más alto, Conmutador Cisco CSS dirige más peticiones a dicho servicio.

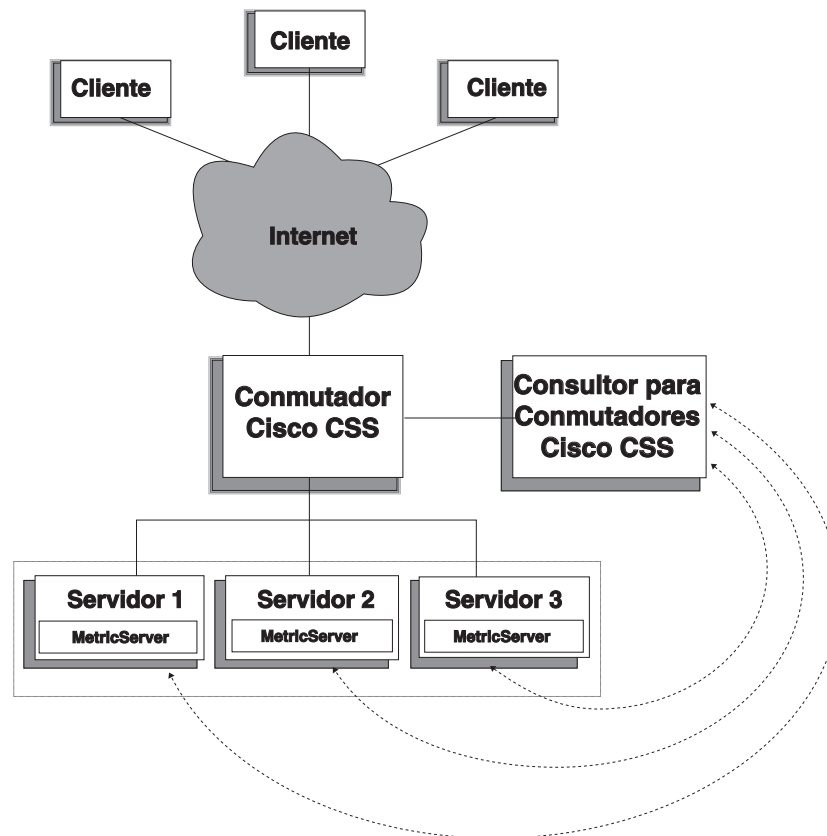


Figura 6. Ejemplo de un sitio que utiliza Cisco CSS Controller y Metric Server para gestionar servicios locales

Cisco CSS Controller, junto con Conmutador Cisco CSS, ofrece una solución que incluye lo "mejor de los dos mundos", que combina la conmutación de contenido a velocidad de cable con la optimización del conocimiento sofisticado de aplicaciones, tolerancia de errores y carga del servicio. Cisco CSS Controller forma parte de una solución complementaria global entre Conmutador Cisco CSS y IBM WebSphere Application Server Load Balancer.

Visión general del componente Nortel Alteon Controller

Nortel Alteon Controller junto con la familia de conmutadores Web de Nortel Alteon ofrece una solución complementaria que combina la capacidad y velocidad de reenvío de paquetes de los conmutadores con los algoritmos sofisticados de Load Balancer para determinar los pesos de servidores.

Nortel Alteon Controller permite desarrollar asesores personalizados capaces de realizar evaluaciones más inteligentes que tienen en cuenta la aplicación sobre la disponibilidad y carga de las aplicaciones utilizadas para desplegar servicios.

Metric Server facilita información de carga del sistema, como la información de utilización de la CPU y la memoria, y una infraestructura para que desarrolle medidas de carga del sistema personalizadas.

Nortel Alteon Controller recopila muchos tipos de datos de la métrica para determinar los pesos para los servidores en los que los conmutadores de Web de Nortel Alteon equilibran la carga.

- Conexiones activas y nuevas
- Disponibilidad de aplicación y base de datos, que se facilita a través del uso de asesores estándares y personalizados y de agentes residentes en el servicio adaptados a la aplicación específica
- Utilización de la CPU
- Utilización de la memoria
- Métrica del servidor personalizable por el usuario
- Accesibilidad

Nortel Alteon Controller utiliza SNMP para comunicarse con el conmutador. La información de configuración, estado y conexión se recupera del conmutador. Cuando el controlador ha calculado los pesos de servidores, éstos se definen en el conmutador. El conmutador utiliza los pesos definidos por el controlador para seleccionar el mejor servidor para manejar peticiones de cliente para un servicio.

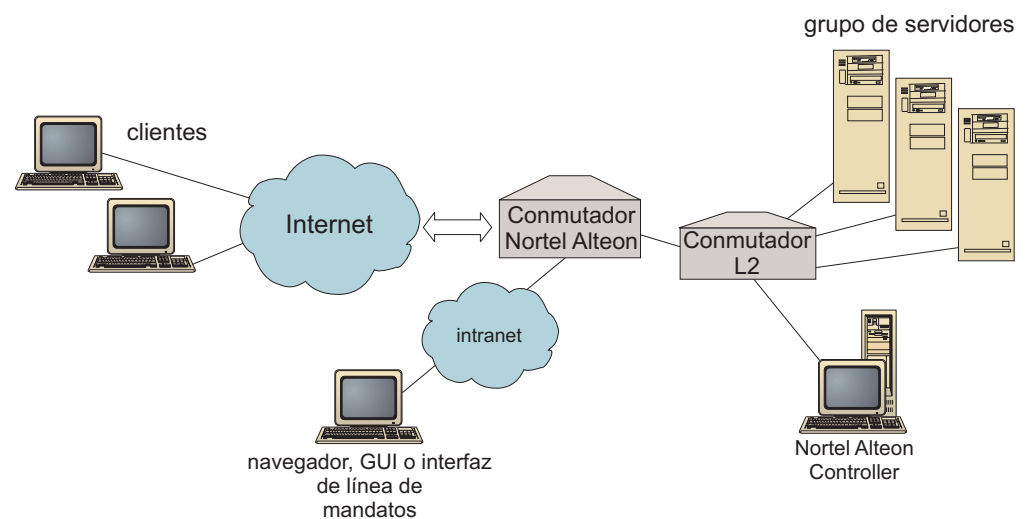


Figura 7. Ejemplo de un sitio que utiliza Nortel Alteon Controller para gestionar servidores locales

Puede gestionar el controlador mediante un navegador, una GUI remota o una interfaz de línea de mandatos remota.

Nortel Alteon Controller junto con la familia de conmutadores Web de Nortel Alteon ofrece una solución que incluye "lo mejor de los dos mundos", que combina la conmutación de paquetes a velocidad de cable con la optimización del conocimiento sofisticado de aplicaciones, tolerancia de errores y carga del servidor. Nortel Alteon Controller forma parte de una solución complementaria entre la familia de conmutadores de Web de la familia Nortel Alteon y WebSphere de IBM.

Capítulo 3. Gestión de la red: determinación de las características de Load Balancer que se van a utilizar

En este capítulo se enumeran las características de configuración de los componentes de Load Balancer para que pueda determinar qué características va a utilizar para gestionar la red:

- “Funciones de gestor, asesores y Metric Server (para los componentes Dispatcher, CBR, y Site Selector)”
- “Características del componente Dispatcher”
- “Características del componente CBR (Content Based Routing)” en la página 23
- “Características del componente Site Selector” en la página 26
- “Características del componente Cisco CSS Controller” en la página 27
- “Características del componente Nortel Alteon Controller” en la página 28

IMPORTANTE: si utiliza Load Balancer para IPv4 y IPv6, sólo está disponible el componente Dispatcher. Consulte el Capítulo 8, “Despliegue de Dispatcher en Load Balancer para IPv4 y IPv6”, en la página 81 para obtener más información.

Funciones de gestor, asesores y Metric Server (para los componentes Dispatcher, CBR, y Site Selector)

Para optimizar el equilibrio de carga entre servidores y asegurar que se selecciona el servidor “correcto”, consulte los apartados:

- “Optimización del equilibrio de carga que proporciona Load Balancer” en la página 180
- “Asesores” en la página 185
- “Metric Server” en la página 196

Características del componente Dispatcher

Dispatcher admite el equilibrio de carga entre los servidores HTTP, FTP, SSL, SMTP, NNTP, IMAP, POP3, Telnet, SIP y cualquier otro TCP o aplicación basada en UDP sin estado.

Administración remota

- Para ejecutar la configuración de Load Balancer desde una máquina aparte de aquella donde reside Load Balancer, consulte el apartado “Administración remota de Load Balancer” en la página 261.

(Si utiliza la instalación de Load Balancer para IPv4 y IPv6, no está disponible esta característica).

Ubicación compartida

- Para ejecutar Dispatcher en la misma máquina que el servidor Web en el que va a equilibrar la carga, consulte el apartado “Utilización de servidores con ubicación compartida” en la página 203.

Alta disponibilidad

- Para utilizar Dispatcher con el fin de eliminar limitaciones de un punto de error único en la red, consulte los apartados “Alta disponibilidad sencilla” en la página 60 y “Alta disponibilidad mutua” en la página 61.
(Si utiliza la instalación de Load Balancer para IPv4 y IPv6, está disponible la característica de alta disponibilidad sencilla, pero no la alta disponibilidad mutua).

Afinidad del cliente con el servidor

Cuando equilibra la carga de tráfico SSL (HTTPS):

- Para asegurarse de que el cliente utiliza el mismo servidor SSL para varias conexiones, consulte el apartado “Cómo funciona la característica de afinidad para Load Balancer” en la página 221.
- Para asegurarse de que el cliente utiliza el mismo servidor para tráfico HTTP y SSL, consulte el apartado “Afinidad entre puertos” en la página 222.
(Si utiliza la instalación de Load Balancer para IPv4 y IPv6, no está disponible la característica de afinidad entre puertos).
- Para asegurarse de que el cliente utiliza el mismo servidor para varias conexiones, consulte el apartado “Cómo funciona la característica de afinidad para Load Balancer” en la página 221.
- Para asegurarse de que un grupo de clientes utilizan el mismo servidor para varias conexiones, consulte el apartado “Máscara de dirección de afinidad (stickymask)” en la página 223.
(Si utiliza la instalación de Load Balancer para IPv4 y IPv6, no está disponible la característica stickymask (máscara de permanencia en memoria)).
- Para quitar un servidor de la configuración (por ejemplo, para fines de mantenimiento) sin interrumpir el tráfico del cliente, consulte el apartado “Desactivar temporalmente el manejo de conexiones de servidor” en la página 224.

Equilibrio de carga basado en normas

Para dirigir los clientes a conjuntos de servidores distintos para la misma dirección Web, puede añadir “normas” a la configuración de Dispatcher. Para obtener más información, consulte el apartado “Configuración de equilibrio de carga basado en normas” en la página 212.

- Para dirigir clientes a conjuntos de servidores distintos según la dirección IP de origen del cliente, consulte el apartado “Utilización de normas basadas en la dirección IP de cliente” en la página 213.
- Para dirigir clientes a conjuntos de servidores distintos según el puerto del cliente, consulte el apartado “Utilización de normas basadas en el puerto de cliente” en la página 214.
- Para dirigir clientes a conjuntos de servidores distintos según la hora del día, consulte el apartado “Utilización de normas basadas en la hora del día” en la página 214.
- Para dirigir clientes a servidores según los bits TOS (Tipo de servicio) de paquetes de red, consulte el apartado “Utilización de normas basadas en el tipo de servicio (TOS)” en la página 214.
- Para dirigir clientes a conjuntos de servidores distintos según el tráfico del sitio:

- Utilizando conexiones por segundo, consulte el apartado “Utilización de normas basadas en las conexiones por segundo” en la página 215.
- Utilizando el número total de conexiones activas, consulte el apartado “Utilización de normas basadas en el total de conexiones activas” en la página 215.
- Reservando y compartiendo el ancho de banda para direcciones Web distintas, consulte el apartado “Utilización de normas basadas en ancho de banda reservado y ancho de banda compartido” en la página 216.
- Asegurando que el tráfico se mide correctamente para cada uno de los conjuntos de servidores, consulte el apartado “Opción de evaluación del servidor para normas” en la página 220.
- Para dirigir el tráfico de desbordamiento a un conjunto de servidores por omisión (por ejemplo, los servidores que responderán “site busy”, sitio ocupado), consulte el apartado “Utilización de normas que son siempre ciertas” en la página 218.
- Para alterar temporalmente la afinidad del cliente con el fin de asegurarse de que el cliente no se “adhiera” a un servidor con desbordamiento, consulte el apartado “Alteración temporal de la afinidad entre puertos” en la página 219.

Si utiliza la instalación de Load Balancer para IPv4 y IPv6, no está disponible el equilibrio de carga basado en normas.

Direccionamiento basado en contenido con el método de reenvío cbr de Dispatcher

Para asegurarse de que los clientes SSL vuelven al mismo servidor SSL, según el ID de SSL de la petición de cliente

- Consulte la página 55.

Para dirigir los clientes HTTP a conjuntos de servidores distintos utilizando normas según la correspondencia del contenido del URL de la petición de cliente, consulte los apartados “Direccionamiento basado en contenido de Dispatcher (método de reenvío cbr)” en la página 55 y “Utilización de normas basadas en el contenido de peticiones” en la página 219 para obtener más información.

- Para distinguir entre URL determinados y sus aplicaciones de servicio, consulte el apartado “Creación de particiones del servidor: servidores lógicos configurados con un servidor físico (dirección IP)” en la página 58.
- Para asegurarse de que los clientes vuelven al mismo servidor cuando solicitan un contenido similar en varias conexiones utilizando cookies creados por los servidores Web, consulte el apartado “Afinidad de cookies pasivos” en la página 227.
- Para equilibrar la carga del tráfico Web con servidores proxy de colocación en antememoria que permiten que se coloque en antememoria un contenido único en cada servidor (así aumenta el tamaño de la antememoria del sitio al eliminar la colocación en antememoria del contenido redundante en varias máquinas) consulte el apartado “Afinidad de URI” en la página 228.

(Si utiliza la instalación de Load Balancer para IPv4 y IPv6, no está disponible el método de reenvío cbr de Dispatcher).

Comparación entre el método de reenvío cbr del componente Dispatcher y del componente CBR

La ventaja de utilizar el método de reenvío cbr de Dispatcher es que proporciona una respuesta más rápida a las peticiones de cliente que el componente CBR. Además, el reenvío cbr de Dispatcher *no* requiere la instalación y utilización de Caching Proxy.

Si la red incluye tráfico SSL (de cliente a través de servidor) completamente seguro, la ventaja de utilizar el componente CBR (junto con Caching Proxy) es que puede procesar el cifrado y descifrado necesario para realizar direccionamiento basado en contenido. Para conexiones completamente seguras, el reenvío cbr de Dispatcher sólo se puede configurar con la afinidad de ID de SSL porque no puede procesar el cifrado y descifrado para realizar el direccionamiento basado en contenido verdadero en el URL de la petición de cliente.

Equilibrio de carga de área amplia

Se puede conseguir el equilibrio de carga de área amplia por varios métodos distintos.

- Para equilibrar la carga en servidores remotos utilizando la característica de área amplia de Dispatcher, consulte los apartados: “Configurar soporte de Dispatcher de área amplia” en la página 229 y “Soporte de GRE (Encapsulamiento genérico de direccionamiento)” en la página 234.

Nota: Es necesario un Dispatcher adicional en el sitio remoto si no se admite GRE en el sitio remoto.

- Para equilibrar la carga en servidores remotos utilizando el método de reenvío nat de Dispatcher, consulte el apartado “NAT/NAPT de Dispatcher (método de reenvío nat)” en la página 53.

Nota: No es necesario *ningún* Dispatcher adicional en el sitio remoto si se utiliza el método de reenvío nat.

(Si utiliza la instalación de Load Balancer para IPv4 y IPv6, no está disponible la característica de equilibrio de carga de área amplia).

Correlación de puertos

- Para equilibrar la carga de una dirección Web con varios daemons de servidor en la misma máquina, donde cada daemon está a la escucha en un puerto único, consulte el apartado “NAT/NAPT de Dispatcher (método de reenvío nat)” en la página 53.

(Si utiliza la instalación de Load Balancer para IPv4 y IPv6, no está disponible esta característica).

Configuración de Dispatcher en una red privada

- Para incluir el tráfico del Dispatcher en una red distinta que el tráfico del cliente (con el fin de mejorar el rendimiento disminuyendo la competencia por los recursos en la red externa), consulte el apartado “Utilización de una configuración de red privada” en la página 236.

Clúster comodín y puerto comodín

- Para combinar varias direcciones Web en una sola configuración, consulte el apartado “Utilizar un clúster comodín para combinar configuraciones de servidores” en la página 237.

- Para equilibrar la carga de cortafuegos, consulte el apartado “Utilizar un clúster comodín para equilibrar la carga de cortafuegos” en la página 238.
- Para dirigir el tráfico de todos los puertos de destino, consulte el apartado “Utilizar el puerto comodín para dirigir el tráfico de puerto no configurado” en la página 239.

Detección de ataques para “rechazo de servicio”

- Para detectar posibles ataques para “rechazo de servicio”, consulte el apartado “Detección de ataques para rechazo de servicio (DoS)” en la página 239.

Anotaciones en binario

- Para analizar el tráfico del servidor, consulte el apartado “Utilización del registro cronológico binario para analizar estadísticas de servidor” en la página 241.

Alertas

- Para generar alertas cuando se marquen los servidores como activos o inactivos, consulte el apartado “Utilización de scripts para generar una alerta o anotar anomalías en el servidor” en la página 184.

Características del componente CBR (Content Based Routing)

CBR integra el equilibrio de carga con Caching Proxy de WebSphere Application Server para dirigir mediante proxy peticiones de cliente a los servidores HTTP o HTTPS (SSL) especificados. Para utilizar CBR, debe instalarse y configurarse Caching Proxy en la misma máquina. Si desea información sobre cómo configurar Caching Proxy con el fin de utilizar CBR, consulte el apartado “Paso 1. Configurar Caching Proxy para que pueda utilizar CBR” en la página 113.

Nota: El componente CBR (Content Based Routing) está disponible en todas las plataformas excepto donde se ejecuta la JVM de 64 bits. De modo alternativo, puede utilizar el método de reenvío cbr del componente Dispatcher de Load Balancer para proporcionar direccionamiento basado en contenido sin utilizar Caching Proxy. Si desea más información, consulte el apartado “Direccionamiento basado en contenido de Dispatcher (método de reenvío cbr)” en la página 55.

Con el componente CBR (o el método de reenvío cbr del componente Dispatcher), puede proporcionar estas ventajas a sus clientes:

- Equilibre la carga de peticiones de cliente para distintos tipos de contenido a conjuntos de servidores. (Consulte el apartado “Peticiones de equilibrio de carga para distintos tipos de contenido” en la página 106).
- Mejore el tiempo de respuesta dividiendo óptimamente el contenido del sitio entre los servidores Web. (Consulte el apartado “División del contenido del sitio para obtener un mejor tiempo de respuesta” en la página 106).
- Asegúrese de que el tráfico del cliente sea ininterrumpido cuando haya un anomalía del servidor permitiendo que se asignen varios servidores a cada tipo de contenido. (Consulte el apartado “Provisión de una copia de seguridad del contenido del servidor Web” en la página 107).

Comparación entre el método de reenvío cbr de componente CBR y de componente Dispatcher

Si la red requiere un tráfico SSL (de cliente a través de servidor) completamente seguro, la ventaja de utilizar el componente CBR (junto con Caching Proxy) es que puede procesar el cifrado/descifrado SSL para realizar direccionamiento basado en contenido.

Para conexiones SSL completamente seguras, sólo se puede configurar el reenvío cbr de Dispatcher con la afinidad de ID de SSL porque no puede procesar el cifrado/descifrado para realizar el direccionamiento basado en contenido verdadero en el URL de la petición de cliente.

Para tráfico HTTP, la ventaja de utilizar el método de reenvío cbr de Dispatcher es que proporciona una respuesta más rápida a las peticiones de cliente que el componente CBR. Además, el reenvío cbr de Dispatcher *no* requiere la instalación y utilización de Caching Proxy.

Administración remota

- Para ejecutar la configuración de Load Balancer desde una máquina aparte de aquella donde reside Load Balancer, consulte el apartado “Administración remota de Load Balancer” en la página 261.

Ubicación compartida

- Se puede ejecutar CBR en la misma máquina que un servidor Web del que se está equilibrando la carga. Si desea más información, consulte el apartado “Utilización de servidores con ubicación compartida” en la página 203.

CBR con varias instancias de Caching Proxy

- Para mejorar la utilización de la CPU utilizando varios procesos Caching Proxy, consulte el apartado “Utilización de varios procesos Caching Proxy para mejorar la utilización de la CPU” en la página 107.

Provisión de direccionamiento basado en contenido para conexiones SSL

Para permitir direccionamiento basado en contenido de tráfico SSL:

- Utilizando una conexión segura en ambos sentidos (cliente a proxy y proxy a servidor), consulte el apartado “Equilibrio de carga entre conexiones completamente seguras (SSL)” en la página 107.
- Utilizando conexiones seguras sólo de cliente a proxy, consulte el apartado “Equilibrio de carga de cliente a proxy en SSL y de proxy a servidor en HTTP” en la página 108.

Creación de particiones del servidor

- Para distinguir entre URL determinados y sus aplicaciones de servicio, consulte el apartado “Creación de particiones del servidor: servidores lógicos configurados con un servidor físico (dirección IP)” en la página 58.

Equilibrio de carga basado en normas

Para dirigir los clientes a conjuntos de servidores distintos para la misma dirección Web, puede añadir "normas" a la configuración de CBR. Para obtener más información, consulte el apartado "Configuración de equilibrio de carga basado en normas" en la página 212.

- Para dirigir clientes a conjuntos de servidores distintos según el contenido de la dirección URL solicitada, consulte el apartado "Utilización de normas basadas en el contenido de peticiones" en la página 219.
- Para dirigir clientes a conjuntos de servidores distintos según la dirección IP de origen del cliente, consulte el apartado "Utilización de normas basadas en la dirección IP de cliente" en la página 213.
- Para dirigir clientes a conjuntos de servidores distintos según la hora del día, consulte el apartado "Utilización de normas basadas en la hora del día" en la página 214.
- Para dirigir clientes a conjuntos de servidores distintos según el tráfico del sitio:
 - Utilizando conexiones por segundo, consulte el apartado "Utilización de normas basadas en las conexiones por segundo" en la página 215.
 - Utilizando el número total de conexiones activas, consulte el apartado "Utilización de normas basadas en el total de conexiones activas" en la página 215.
- Para dirigir el tráfico de desbordamiento a un conjunto de servidores por omisión (por ejemplo, el servidor o los servidores que responderán "site busy", sitio ocupado), consulte el apartado "Utilización de normas que son siempre ciertas" en la página 218.
- Para alterar temporalmente la afinidad del cliente con el fin de asegurarse de que el cliente no se "adhiera" a un servidor con desbordamiento, consulte el apartado "Alteración temporal de la afinidad entre puertos" en la página 219.

Afinidad del cliente con el servidor

- Para asegurarse de que el cliente vuelve al mismo servidor para varias conexiones, consulte el apartado "Cómo funciona la característica de afinidad para Load Balancer" en la página 221.
- Para quitar un servidor de la configuración (por ejemplo, para fines de mantenimiento) sin interrumpir el tráfico del cliente, consulte el apartado "Desactivar temporalmente el manejo de conexiones de servidor" en la página 224.
- Para asegurarse de que los clientes vuelven al mismo servidor cuando solicitan un contenido similar en varias conexiones sin confiar en cookies creados por los servidores Web, consulte el apartado "Afinidad de cookies activos" en la página 225.
- Para asegurarse de que los clientes vuelven al mismo servidor cuando solicitan un contenido similar en varias conexiones utilizando cookies creados por los servidores Web, consulte el apartado "Afinidad de cookies pasivos" en la página 227.
- Para equilibrar la carga del tráfico Web con servidores proxy de colocación en antememoria que permiten que se coloque en antememoria un contenido único en cada servidor (así aumenta el tamaño de la antememoria del sitio al eliminar la colocación en antememoria del contenido redundante en varias máquinas) consulte el apartado "Afinidad de URI" en la página 228.

Alta disponibilidad con Dispatcher y CBR

- Para eliminar las limitaciones de un punto único de anomalía en la red utilizando Dispatcher en una configuración de dos niveles con CBR, consulte el apartado “Cómo Load Balancer puede proporcionar alta disponibilidad” en la página 6.

Anotaciones en binario

- Para analizar el tráfico del servidor, consulte el apartado “Utilización del registro cronológico binario para analizar estadísticas de servidor” en la página 241.

Alertas

- Para generar alertas cuando se marquen los servidores como activos o inactivos, consulte el apartado “Utilización de scripts para generar una alerta o anotar anomalías en el servidor” en la página 184.

Características del componente Site Selector

Site Selector equilibra la carga de peticiones de servicio de nombres entre un grupo de servidores.

Administración remota

- Para ejecutar la configuración de Load Balancer desde una máquina aparte de aquella donde reside Load Balancer, consulte el apartado “Administración remota de Load Balancer” en la página 261.

Ubicación compartida

- Se puede ejecutar Site Selector en la misma máquina que el servidor del que se está equilibrando la carga sin tener que realizar pasos de configuración adicionales.

Alta disponibilidad

- La característica de alta disponibilidad está inherentemente disponible a través de metodologías de sistema de nombres de dominio (DNS) utilizando varios Site Selectors redundantes, suponiendo que la configuración del servidor de nombres padre es correcta y que los métodos de recuperación de DNS normales se encuentran en su lugar. Por ejemplo, entre los métodos de recuperación de DNS normales están: retransmisión de consultas y reintento de transferencias de zona.
- Para eliminar las limitaciones de un punto único de anomalía en la red utilizando Dispatcher en una configuración de dos niveles con Site Selector, consulte el apartado “Cómo Load Balancer puede proporcionar alta disponibilidad” en la página 6.

Afinidad del cliente con el servidor

- Para asegurarse de que el cliente utiliza el mismo servidor para varias peticiones de servidor de nombres, consulte el apartado “Cómo funciona la característica de afinidad para Load Balancer” en la página 221.
- Para asegurarse de que haya afinidad de cliente con servidor utilizando el método DNS estándar de establecer el TTL (Tiempo de duración), consulte el apartado “Consideraciones de TTL” en la página 127.

Equilibrio de carga basado en normas

Para dirigir peticiones de cliente a conjuntos de servidores distintos para la resolución de nombres de dominio, puede añadir "normas" a la configuración de Site Selector. Para obtener más información, consulte el apartado "Configuración de equilibrio de carga basado en normas" en la página 212.

- Para dirigir clientes a conjuntos de servidores distintos según la dirección IP de origen del cliente, consulte el apartado "Utilización de normas basadas en la dirección IP de cliente" en la página 213.
- Para dirigir clientes a conjuntos de servidores distintos según la hora del día, consulte el apartado "Utilización de normas basadas en la hora del día" en la página 214.
- Para dirigir clientes a conjuntos de servidores distintos según los valores de carga de métrica del conjunto de servidores, consulte los apartados:
 - "Norma de toda la métrica" en la página 217
 - "Norma de media de la métrica" en la página 218
- Para dirigir el tráfico de desbordamiento a un conjunto de servidores por omisión (por ejemplo, el servidor o los servidores que responderán "site busy", sitio ocupado), consulte el apartado "Utilización de normas que son siempre ciertas" en la página 218.

Equilibrio de carga de área amplia

Se puede ejecutar Site Selector tanto en redes de área local (LAN) como en redes de área amplia (WAN).

En entornos de WAN:

- Para equilibrar la carga de peticiones del servidor de nombres de cliente utilizando el método de selección de turno rotativo sopesado, no es necesario ningún paso de configuración adicional.
- Para tener en cuenta la proximidad de red del servidor de nombres de cliente a los servidores que proporcionan la aplicación solicitada (los servidores de destino), consulte el apartado "Utilización de la característica proximidad de red" en la página 128.

Alertas

- Para generar alertas cuando se marquen los servidores como activos o inactivos, consulte el apartado "Utilización de scripts para generar una alerta o anotar anomalías en el servidor" en la página 184.

Características del componente Cisco CSS Controller

Cisco CSS Controller mejora las posibilidades de equilibrio de carga de servidores de los Conmutadores Cisco con mayor aplicación y consciencia del sistema. El controlador utiliza medidas más sensibles a la aplicación y al sistema para calcular dinámicamente los pesos del servidor. Los pesos se proporcionan al conmutador con SNMP. El conmutador utiliza los pesos cuando procesa peticiones de cliente lo que produce una optimización de la carga del servidor y una tolerancia a errores mejorada.

Para optimizar el equilibrio de carga entre servidores y asegurar que se selecciona el servidor "correcto", consulte los apartados:

- "Optimización del equilibrio de carga que proporciona Load Balancer" en la página 246

- “Asesores” en la página 248 y “Crear asesores personalizados (personalizables)” en la página 250
- “Metric Server” en la página 253

Administración remota

- Para ejecutar la configuración de Load Balancer desde una máquina aparte de aquella donde reside Load Balancer, consulte el apartado “Administración remota de Load Balancer” en la página 261.

Ubicación compartida

- Se puede ejecutar Cisco CSS Controller en la misma máquina que el servidor del que se está equilibrando la carga sin tener que realizar pasos de configuración adicionales.

Alta disponibilidad

- Para eliminar las limitaciones de un punto único de anomalía en la red, los dos, Conmutador Cisco CSS y Cisco CSS Controller, tienen posibilidades de alta disponibilidad. Para el conmutador, están disponibles las posibilidades de alta disponibilidad utilizando el protocolo de redundancia de CSS. Para Cisco CSS Controller, se utiliza un protocolo propietario que permite la configuración de reposo dinámico de dos controladores.
Si desea más información sobre cómo configurar la característica de alta disponibilidad, consulte el apartado “Alta disponibilidad” en la página 146.

Anotaciones en binario

- Para analizar el tráfico del servidor, consulte el apartado “Utilización del registro cronológico binario para analizar estadísticas de servidor” en la página 256.

Alertas

- Para generar alertas cuando se marquen los servidores como activos o inactivos, consulte el apartado “Utilización de scripts para generar una alerta o anotar anomalías en el servidor” en la página 257.

Características del componente Nortel Alteon Controller

Nortel Alteon Controller mejora las posibilidades de equilibrio de carga de servidores de los Conmutadores Nortel Alteon con mayor aplicación y consciencia del sistema. El controlador utiliza medidas más sensibles a la aplicación y al sistema para calcular dinámicamente los pesos del servidor. Los pesos se proporcionan al conmutador con SNMP. El conmutador utiliza los pesos cuando procesa peticiones de cliente lo que produce una optimización de la carga del servidor y una tolerancia a errores mejorada.

Para optimizar el equilibrio de carga entre servidores y asegurar que se selecciona el servidor “correcto”, consulte los apartados:

- “Optimización del equilibrio de carga que proporciona Load Balancer” en la página 246
- “Asesores” en la página 248 y “Crear asesores personalizados (personalizables)” en la página 250
- “Metric Server” en la página 253

Administración remota

- Para ejecutar la configuración de Load Balancer desde una máquina aparte de aquélla donde reside Load Balancer, consulte el apartado “Administración remota de Load Balancer” en la página 261.

Ubicación compartida

- Se puede ejecutar Nortel Alteon Controller en la misma máquina que el servidor del que se está equilibrando la carga sin tener que realizar pasos de configuración adicionales.

Alta disponibilidad

- Para eliminar las limitaciones de un punto único de anomalía en la red, los dos, Conmutador Nortel Alteon Web y Nortel Alteon Controller, tienen posibilidades de alta disponibilidad. Para el conmutador, es posible la alta disponibilidad utilizando el protocolo de redundancia para conexiones con servidores y para servicios. Nortel Alteon Controller proporciona una alta disponibilidad utilizando un protocolo propietario que permite la configuración de reposo dinámico de dos controladores.

Si desea más información sobre cómo configurar la característica de alta disponibilidad, consulte el apartado “Alta disponibilidad” en la página 167.

Anotaciones en binario

- Para analizar el tráfico del servidor, consulte el apartado “Utilización del registro cronológico binario para analizar estadísticas de servidor” en la página 256.

Alertas

- Para generar alertas cuando se marquen los servidores como activos o inactivos, consulte el apartado “Utilización de scripts para generar una alerta o anotar anomalías en el servidor” en la página 257.

Capítulo 4. Instalación de Load Balancer

Este capítulo proporciona información sobre la instalación de Load Balancer mediante herramientas de paquetes del sistema y los requisitos de todos los sistemas operativos admitidos.

- “Requisitos del sistema AIX e instalación”
- “Requisitos del sistema HP-UX e instalación” en la página 35
- “Requisitos del sistema Linux e instalación” en la página 37
- “Requisitos del sistema Solaris e instalación” en la página 39
- “Requisitos del sistema Windows e instalación” en la página 40

Para obtener instrucciones de instalación con el programa de instalación del producto, consulte el documento *Conceptos, planificación e instalación de Edge Components*.

Java 2 SDK se instala automáticamente con Load Balancer en todas la plataformas.

Si va a migrar desde una versión anterior de Load Balancer, o si va a volver a instalar un sistema operativo, antes de la instalación puede guardar cualquier archivo de configuración o archivo de script anterior para Load Balancer.

- Después de la instalación, coloque los archivos de configuración en el directorio `.../ibm/edge/lb/servers/configurations/componente` (donde *componente* puede ser dispatcher, cbr, ss, cco o nal).
- Después de la instalación, coloque los archivos de script (por ejemplo, goIdle y goStandby) en el directorio `.../ibm/edge/lb/servers/bin` para poder ejecutarlos.

Dependiendo del tipo de instalación, no se proporcionarán todos los paquetes de Load Balancer que se listan en este apartado.

- En las instalaciones de Edge Component que pueden proporcionar tanto Load Balancer como Caching Proxy, están disponibles todos los paquetes de componentes de instalación de Load Balancer.
- En las instalaciones de Edge Component que pueden proporcionar Load Balancer pero no Caching Proxy, con Load Balancer no se incluye el paquete del componente CBR.
- En instalaciones de Edge Component para IPv6 (Load Balancer para IPv4 y IPv6), con Load Balancer se incluye el paquete del componente Dispatcher. No se incluyen los paquetes de componente CBR, Site Selector y controlador. Si desea obtener el orden de instalación recomendado de los paquetes de Load Balancer para IPv4 y IPv6, consulte “Instalación de Load Balancer para IPv4 y IPv6” en la página 83.

Requisitos del sistema AIX e instalación

Requisitos de sistemas AIX

Si desea información sobre los requisitos de hardware y software, incluidos los navegadores soportados, consulte la siguiente página Web: <http://www.ibm.com/support/docview.wss?rs=180&uid=swg27006921>

Instalación en sistemas AIX

En Tabla 1 se listan las imágenes installp para Load Balancer y el orden de instalación recomendado utilizando la herramienta de instalación de paquetes del sistema.

Tabla 1. Imágenes installp de AIX

Base	ibmlb.base.rte
Administración (con mensajes)	<ul style="list-style-type: none">• ibmlb.admin.rte• ibmlb.msg.idioma.admin
Controlador de dispositivo	ibmlb.lb.driver
Licencia	ibmlb.lb.license
Componentes de Load Balancer (con los mensajes)	<ul style="list-style-type: none">• ibmlb.componente.rte• ibmlb.msg.idioma.lb
Documentación (con los mensajes)	<ul style="list-style-type: none">• ibmlb.doc.rte• ibmlb.msg.en_US.doc
Metric Server	ibmlb.ms.rte

Donde *componente* puede ser: disp (Dispatcher), cbr (CBR), ss (Site Selector), cco (Cisco CSS Controller) o nal (Nortel Alteon Controller). De modo opcional, puede seleccionar qué componente o componentes desea instalar.

Donde *idioma* puede ser:

- en_US
- de_CH
- de_DE
- es_ES
- fr_CA
- fr_CH
- fr_FR
- it_CH
- it_IT
- ja_JP
- Ja_JP
- ko_KR
- pt_BR
- zh_CN
- ZH_CN
- zh_TW
- Zh_TW

El paquete de documentación sólo incluye la documentación en inglés. El conjunto de las traducciones de la documentación de Load Balancer están en el siguiente sitio Web: www.ibm.com/software/webservers/appserv/ecinfocenter.html.

Antes de instalar

Si tiene una versión anterior instalada, desinstale esa copia antes de instalar la versión actual. Primero, asegúrese de que se han detenido todos los ejecutores y

servidores. A continuación, para desinstalar el producto completo, entre el mandato **installp -u ibmlb** (o el nombre anterior, por ejemplo **intnd**). Para desinstalar catálogos de archivos determinados, deberá listarlos específicamente en lugar de indicar el nombre de paquete.

Cuando instala el producto, tiene la opción de instalar cualquiera de los elementos siguientes o todos ellos:

- Base
- Administración (con los mensajes)
- Controlador de dispositivo (necesario)
- Licencia (necesaria)
- Componente Dispatcher (con los mensajes)
- Componente CBR (con los mensajes)
- Componente Site Selector (con los mensajes)
- Componente Cisco CSS Controller (con los mensajes)
- Componente Nortel Alteon Controller (con los mensajes)
- Documentación (con los mensajes)
- Metric Server

Pasos de instalación

Siga estos pasos para instalar Load Balancer para sistemas AIX:

1. Inicie la sesión como root.
2. Inserte el soporte del producto o, si realiza la instalación desde la Web, copie las imágenes de instalación en un directorio.
3. Instale la imagen de instalación. Utilice la herramienta SMIT para instalar Load Balancer para AIX porque SMIT asegura la instalación automática de todos los mensajes.

Con **SMIT**:

Seleccione

Instalación y mantenimiento de software

Seleccione

Instalar y actualizar software

Seleccione

Instalar y actualizar desde el último software disponible

Entre El dispositivo o el directorio que contenga las imágenes installp

Entre En el *SOFTWARE a instalar, la información adecuada para especificar las opciones (o seleccione Listar).

Pulse **Bien**

Cuando finalice el mandato, pulse **Hecho** y a continuación seleccione **Salir de Smit** del menú Salir o pulse **F12**. Si utiliza SMITTY, pulse **F10** para salir del programa.

Con la línea de mandatos:

Si va a instalar desde un CD, debe entrar los mandatos siguientes para montar el CD:

```
mkdir /cdrom
mount -v cdrfs -p -r /dev/cd0 /cdrom
```

Consulte la tabla siguiente con el objeto de determinar qué mandato o mandatos ha de entrar para instalar los paquetes de Load Balancer que desea

para sistemas AIX:

Tabla 2. Mandatos de instalación de AIX

Base	installp -acXgd <i>dispositivo</i> ibmlb.base.rte
Administración (con los mensajes)	installp -acXgd <i>dispositivo</i> ibmlb.admin.rte ibmlb.msg. <i>idioma</i> .admin
Controlador de dispositivo	installp -acXgd <i>dispositivo</i> ibmlb.lb.driver
Licencia	installp -acXgd <i>dispositivo</i> ibmlb.lb.license
Componentes de Load Balancer (con msgs). Incluye: Dispatcher, CBR, Site Selector, Cisco CSS Controller y Nortel Alteon Controller	installp -acXgd <i>dispositivo</i> ibmlb.componente.rte ibmlb.msg. <i>idioma</i> .lb
Documentos (con los mensajes)	installp -acXgd <i>dispositivo</i> ibmlb.doc.rte ibmlb.msg.en_US.lb
Metric Server	installp -acXgd <i>dispositivo</i> ibmlb.ms.rte

donde *dispositivo* es:

- /cdrom si va a instalar desde un CD.
- /dir (el directorio que contiene las imágenes installp) si va a instalar desde un sistema de archivos.

Asegúrese de que la columna de resultados en el resumen contiene SATISFACTORIO para cada parte de Load Balancer que instale (APLICAR). No continúe hasta que todas las partes que desea instalar se hayan aplicado satisfactoriamente.

Nota: Para generar una lista de catálogos de archivos de una imagen installp, incluidos todos los catálogos de mensajes disponibles, entre:

```
installp -ld dispositivo
```

donde *dispositivo* es:

- /cdrom si va a instalar desde un CD.
- /dir (el directorio que contiene las imágenes installp) si va a instalar desde un sistema de archivos.

Para desmontar el CD, escriba:

```
umount /cdrom
```

4. Verifique si el producto se ha instalado. Entre el mandato siguiente:

```
lslpp -h | grep ibmlb
```

Si se ha instalado todo el producto, este mandato devolverá el resultado indicado a continuación:

```
ibmlb.base.rte  
ibmlb.admin.rte  
ibmlb.lb.driver  
ibmlb.lb.license  
ibmlb.<componente>.rte  
ibmlb.doc.rte  
ibmlb.ms.rte  
ibmlb.msg.idioma.admin  
ibmlb.msg.en_US.doc  
ibmlb.msg.idioma.lb
```

Entre las vías de acceso de instalación de Load Balancer se incluyen:

- Administración: **/opt/ibm/edge/lb/admin**
- Componentes de Load Balancer: **/opt/ibm/edge/lb/servers**

- Metric Server: `/opt/ibm/edge/lb/ms`
- Documentación (Guía de administración): `/opt/ibm/edge/lb/documentation`

Para la administración remota de Load Balancer, con RMI (Remote Method Invocation), tendrá que instalar los paquetes de: administración, base, componentes y licencia en el cliente. Para obtener información sobre RMI, consulte el apartado “RMI (Remote Method Invocation)” en la página 262.

Requisitos del sistema HP-UX e instalación

Requisitos de sistemas HP-UX

Si desea información sobre los requisitos de hardware y software, incluidos los navegadores soportados, consulte la siguiente página Web: <http://www.ibm.com/support/docview.wss?rs=180&uid=swg27006921>

Instalación en sistemas HP-UX

Este apartado explica cómo instalar Load Balancer en sistemas HP-UX utilizando el CD del producto.

Antes de instalar

Antes de comenzar el procedimiento de instalación, asegúrese de que tiene autorización de raíz para instalar el software:

Si tiene una versión anterior instalada, debería desinstalar esa copia antes de instalar la versión actual. En primer lugar, asegúrese de que ha detenido el ejecutor y el servidor. A continuación, para desinstalar Load Balancer, consulte el apartado “Instrucciones para desinstalar los paquetes” en la página 36.

Pasos de instalación

En la Tabla 3 se enumeran los nombres de los paquetes de instalación de Load Balancer y el orden recomendado para instalarlos utilizando la herramienta de instalación de paquetes del sistema.

Tabla 3. Detalles de instalación de los paquetes de HP-UX para Load Balancer

Descripción del paquete	Nombre del paquete de HP-UX
Base	<code>ibmlb.base</code>
Administración y mensajes	<code>ibmlb.admin</code> <code>ibmlb.nlv-idioma</code>
Licencia de Load Balancer	<code>ibmlb.lic</code>
Componentes de Load Balancer	<code>ibmlb.componente</code>
Documentación	<code>ibmlb.doc</code>
Metric Server	<code>ibmlb.ms</code>
Notas: <ol style="list-style-type: none"> 1. La variable <i>idioma</i> hace referencia a la sustitución de uno de los siguientes códigos específicos de idioma: <code>de_DE</code>, <code>en_US</code>, <code>es_ES</code>, <code>fr_FR</code>, <code>it_IT</code>, <code>ja_JP</code>, <code>ko_KR</code>, <code>zh_CN</code>, <code>zh_TW</code>. 2. La variable <i>componente</i> hace referencia a la sustitución de una de las siguientes: <code>disp</code> (dispatcher), <code>cbr</code> (CBR), <code>ss</code> (Site Selector), <code>cco</code> (Cisco CSS Controller) o <code>nal</code> (Nortel Alteon Controller). 3. El paquete de documentación (<code>ibmlb.doc</code>) sólo incluye la documentación en inglés. El conjunto de las traducciones de la documentación de Load Balancer están en el siguiente sitio Web: www.ibm.com/software/webserver/appserv/ecinfocenter.html. 	

Nota: Los sistemas HP-UX no dan soporte al entorno local de Portugués de Brasil (pt_BR). Los entornos locales soportados en sistemas HP-UX son:

- de_DE.iso88591
- en_US.iso88591
- es_ES.iso88591
- fr_FR.iso88591
- it_IT.iso88591
- ja_JP.SJIS
- ko_KR.eucKR
- zh_CN.hp15CN
- zh_TW.big5

Instrucciones para instalar los paquetes

El procedimiento especificado a continuación facilita detalles sobre los pasos necesarios para completar esta tarea.

1. Conéctese como superusuario local root.

```
su - root
Contraseña: contraseña
```

2. Emita el mandato de instalación para instalar los paquetes:

```
swinstall -s /origen nombre_paquete
```

donde *origen* es el directorio absoluto de la ubicación del paquete y *nombre_paquete* es el nombre del paquete.

El siguiente mandato instala únicamente el paquete base de Load Balancer (ibmlb.base), si realiza la instalación desde el directorio raíz del CD:

```
swinstall -s /origen ibmlb.base
```

Si realiza la instalación desde el directorio raíz, emita el siguiente mandato para instalar todos los paquetes de Load Balancer:

```
swinstall -s /origen ibmlb
```

3. Compruebe la instalación de los paquetes de Load Balancer

Emita el mandato **swlist** para enumerar todos los paquetes que ha instalado. Por ejemplo,

```
swlist -l fileset ibmlb
```

Instrucciones para desinstalar los paquetes

Utilice el mandato **swremove** para desinstalar los paquetes. Elimine los paquetes en el orden inverso en el que se instalaron. Por ejemplo, emita los siguientes mandatos:

- Para desinstalar todos los paquetes de Load Balancer:

```
swremove ibmlb
```

Para desinstalar un paquete individual, como por ejemplo el componente Dispatcher:

```
swremove ibmlb.disp
```

Requisitos del sistema Linux e instalación

Requisitos de sistemas Linux

Si desea obtener los requisitos de hardware y software, incluidos los navegadores soportados, consulte la siguiente página Web: <http://www.ibm.com/support/docview.wss?rs=180&uid=swg27006921>

Instalación para sistemas Linux

Este apartado explica cómo instalar Load Balancer en Linux utilizando el CD del producto.

Antes de instalar

Antes de comenzar el procedimiento de instalación, asegúrese de que tiene autorización de raíz para instalar el software:

Si tiene una versión anterior instalada, debería desinstalar esa copia antes de instalar la versión actual. Primero, asegúrese de que se han detenido todos los ejecutores y servidores. Después, a fin de desinstalar el producto completo, entre el mandato **rpm -e nombrepaquete**. Al desinstalar, invierta el orden utilizado para la instalación de los paquetes asegurándose de que los paquetes de administración se desinstalen los últimos.

Pasos de instalación

Para instalar Load Balancer:

1. Realice los preparativos para la instalación.

- Inicie la sesión como root.
- Inserte el soporte de almacenamiento del producto o baje el producto desde el sitio Web e instale la imagen de instalación utilizando RPM (Red Hat Packaging Manager).

La imagen de instalación es un archivo que tiene el formato

eBLX-versión:tar.z.

- Descomprima el archivo tar en un directorio temporal entrando el mandato: **tar -xf eBLX-versión:tar.z**. El resultado es un conjunto de archivos con la extensión .rpm.

A continuación figura una lista de los paquetes instalables de RMP.

- *ibmlb-base-versión-release.hardw.rpm* (Base)
- *ibmlb-admin-versión-release.hardw.rpm* (Administración)
- *ibmlb-lic-versión-release.hardw.rpm* (Licencia)
- *ibmlb-componente-versión-release.hardw.rpm* (Componente de LB)
- *ibmlb-doc-versión-release.hardw.rpm* (Documentación)
- *ibmlb-ms-versión-release.hardw.rpm* (Metric Server)

Donde —

- *versión-release* es el release actual, por ejemplo: 6.1-0
- *hardw* es uno de los siguientes valores: i386, ppc64, ppc, s390, s390x, x86_64
- *componente* es uno de los siguientes valores: disp (componente Dispatcher), cbr (componente CBR), ss (componente Site Selector), cco (Cisco CSS Controller), nal (Nortel Alteon Controller)

El paquete de documentación sólo incluye la documentación en inglés. El conjunto de las traducciones de la documentación de Load Balancer están en el siguiente sitio Web: www.ibm.com/software/webservers/appserv/ecinfocenter.html.

- El orden en el que se instalan los paquetes es importante. A continuación figura una lista de paquetes necesarios y el orden en el que deberían instalarse:
 - Base (base)
 - Administración (admin)
 - Licencia (lic)
 - Componentes de Load Balancer (disp, cbr, ss, cco, nal)
 - Metric Server (ms)
 - Documentación (doc)

El mandato para instalar los paquetes debe emitirse desde el mismo directorio donde residen los archivos RPM. Emita el siguiente mandato para instalar cada paquete: **rpm -i paquete.rpm**.

Sistemas Red Hat Linux: debido a un problema conocido del sistema Red Hat Linux, también será necesario suprimir los archivos RPM `_db*` o se producirá un error.

- Entre las vías de acceso de instalación de Load Balancer se incluyen:
 - Administración: **/opt/ibm/edge/lb/admin**
 - Componentes de Load Balancer: **/opt/ibm/edge/lb/servers**
 - Metric Server: **/opt/ibm/edge/lb/ms**
 - Documentación: **/opt/ibm/edge/lb/documentation**
- Para desinstalar los paquetes, invierta el orden utilizado para la instalación de los paquetes asegurándose de que el paquete de administración se desinstale el último.

2. Verifique si el producto se ha instalado. Entre el mandato siguiente:

rpm -qa | grep ibmlb

Si instala el producto completo aparecerá lo siguiente:

- *ibmlb-base-versión-release*
- *ibmlb-admin-versión-release*
- *ibmlb-lic-versión-release*
- *ibmlb-dsp-versión-release*
- *ibmlb-cbr-versión-release*
- *ibmlb-ss-versión-release*
- *ibmlb-cco-versión-release*
- *ibmlb-nal-versión-release*
- *ibmlb-doc-versión-release*
- *ibmlb-ms-versión-release*

Para la administración remota de Load Balancer, con RMI (Remote Method Invocation), debe instalar los paquetes de: administración, base, componentes y licencia en el cliente. Para obtener información sobre RMI, consulte el apartado “RMI (Remote Method Invocation)” en la página 262.

Requisitos del sistema Solaris e instalación

Requisitos de Solaris

Si desea información sobre los requisitos de hardware y software, incluidos los navegadores soportados, consulte la siguiente página Web: <http://www.ibm.com/support/docview.wss?rs=180&uid=swg27006921>

Instalación para Solaris

Este apartado explica cómo instalar Load Balancer en sistemas Solaris utilizando el CD del producto.

Antes de instalar

Antes de comenzar el procedimiento de instalación, asegúrese de que tiene autorización de raíz para instalar el software:

Si tiene una versión anterior instalada, desinstale esa copia antes de instalar la versión actual. En primer lugar, asegúrese de que ha detenido todos los ejecutores y los servidores. A continuación, para desinstalar Load Balancer, escriba **pkgrm nombre_paquete**.

Pasos de instalación

Para instalar Load Balancer:

1. Realice los preparativos para la instalación.

- Inicie la sesión como usuario root.
- Inserte el CD-ROM que contiene el software de Load Balancer en la unidad correspondiente.

En el indicador de mandatos, entre **pkgadd -d nombreVíaAcceso**, donde *nombreVíaAcceso* es el nombre de dispositivo de la unidad de CD-ROM o el directorio en el disco duro donde se ubica el paquete; por ejemplo: **pkgadd -d /cdrom/cdrom0/**.

A continuación figura una lista de los paquetes visualizados y el orden recomendado en el que deberían instalarse.

- ibmlbbase (Base)
- ibmlbadm (Administración)
- ibmlblic (Licencia)
- ibmlbdisp (componente Dispatcher)
- ibmlbcbr (componente CBR)
- ibmlbss (componente Site Selector)
- ibmlbcc (componente Cisco CSS Controller)
- ibmlbna (componente Nortel Alteon Controller)
- ibmlbdoc (documentación)
- ibmlbms (Metric Server)

El paquete de documentación (ibmlbdoc) sólo incluye la documentación en inglés. El conjunto de las traducciones de la documentación de Load Balancer están en el siguiente sitio Web: www.ibm.com/software/webservers/appserv/ecinfocenter.html.

Si desea instalar todos los paquetes, escriba simplemente "all" y pulse Intro. Si desea instalar algunos de los componentes, entre el nombre o nombres correspondientes a los paquetes a instalar, separados por un espacio o una

coma, y pulse Intro. Puede que se le solicite que cambie permisos de directorios o archivos existentes. Sólo tiene que pulsar Intro o responder “yes” (sí). Tiene que instalar los paquetes de requisito previo (porque se realiza la instalación por orden alfabético no por orden de requisito previo). Si responde “all” (todo) sólo responda “yes” (sí) a todas las solicitudes y la instalación se realizará satisfactoriamente.

Si desea instalar únicamente el componente Dispatcher con la documentación y Metric Server, debe instalar los paquetes siguientes: `ibmlbbase`, `ibmlbadm`, `ibmlblic`, `ibmldisp`, `ibmlbdoc` y `ibmlbms`.

Para la administración remota de Load Balancer, con RMI (Remote Method Invocation), tendrá que instalar los paquetes de: administración, base, componentes y licencia en el cliente. Para obtener información sobre RMI, consulte el apartado “RMI (Remote Method Invocation)” en la página 262.

Las vías de acceso de instalación de Load Balancer son las siguientes:

- Los componentes de Load Balancer residen en el directorio de instalación `/opt/ibm/edge/lb/servers`.
- La administración instalada reside en el directorio `/opt/ibm/edge/lb/admin`
- El Metric Server instalado reside en el directorio `/opt/ibm/edge/lb/ms`
- La documentación instalada reside en el directorio `/opt/ibm/edge/lb/documentation`

2. Verifique si el producto se ha instalado. Emita este mandato: `pkginfo | grep ibm`.

Requisitos del sistema Windows e instalación

Requisitos de sistemas Windows

Si desea información sobre los requisitos de hardware y software, incluidos los navegadores soportados, consulte la siguiente página Web: <http://www.ibm.com/support/docview.wss?rs=180&uid=swg27006921>

Instalación en sistemas Windows

Este apartado explica cómo instalar Load Balancer en sistemas Windows utilizando el CD del producto.

Paquetes de instalación

Se le proporcionará diversos paquetes de instalación:

- Administración
- Licencia
- Dispatcher
- CBR (Content Based Routing)
- Site Selector
- Cisco CSS Controller
- Nortel Alteon Controller
- Documentación
- Metric Server

Para la administración remota de Load Balancer, con RMI (Remote Method Invocation), deberá instalar los paquetes de administración, licencia y componentes en el cliente. Para obtener información sobre RMI, consulte el apartado “RMI (Remote Method Invocation)” en la página 262.

Antes de instalar

Restricciones: La versión Windows de Load Balancer no se puede instalar en la misma máquina con IBM Firewall.

Antes de comenzar el procedimiento de instalación, asegúrese de que ha iniciado la sesión como Administrador o como usuario con privilegios administrativos.

Si tiene una versión anterior instalada, debería desinstalar esa copia antes de instalar la versión actual. Para desinstalar utilizando **Agregar o quitar programas**, realice lo siguiente:

1. Pulse **Inicio** > **Configuración** (para Windows 2000) > **Panel de control**
2. Efectúe una doble pulsación en **Agregar/quitar programas**
3. Seleccione *IBM WebSphere Edge Components* (o el nombre anterior, por ejemplo, *IBM Edge Server*)
4. Pulse **Cambiar/quitar**

Pasos de instalación

Para instalar Load Balancer:

1. Inserte el CD-ROM de Load Balancer en la unidad de CD-ROM y aparecerá automáticamente la ventana de instalación.
2. El paso siguiente sólo es necesario si la ejecución automática del CD no ha funcionado en el sistema. Con el ratón, pulse el botón 1 del ratón 1 para realizar estas tareas:
 - Pulse **Inicio**.
 - Seleccione **Ejecutar**.
 - Especifique la unidad de disco de CD-ROM seguida de setup.exe; por ejemplo:
`E:\setup`
3. Seleccione el **Idioma** en el que desea leer el proceso de instalación.
4. Pulse **Aceptar**.
5. Siga las instrucciones del programa de instalación.
6. Si desea cambiar la unidad o el directorio de destino, pulse **Examinar**.
7. Tiene la opción de seleccionar “Todo el producto Load Balancer” o “Su elección de componentes”.
8. Una vez completada la instalación, aparecerá un mensaje para solicitarle que reinicie el sistema antes de utilizar Load Balancer. Esto es necesario para asegurarse de que se han instalado todos los archivos y de que se ha añadido la variable de entorno IBMLBPATH al registro.

Entre las vías de acceso de instalación de Load Balancer se incluyen:

- Administración: **C:\Archivos de programa\IBM\edge\lb\admin**
- Componentes de Load Balancer: **C:\Archivos de programa\IBM\edge\lb\servers**
- Metric Server: **C:\Archivos de programa\IBM\edge\lb\ms**
- Documentación (Guía de administración): **C:\Archivos de programa\IBM\edge\lb\documentation**

Nota: La documentación del directorio de instalación sólo contiene la documentación en inglés. El conjunto de las traducciones de la

documentación de Load Balancer están en el siguiente sitio Web:
www.ibm.com/software/webservers/appserv/ecinfocenter.html.

Parte 2. Componente Dispatcher

Esta parte proporciona información sobre la configuración de inicio rápido, consideraciones de planificación y describe los métodos para configurar el componente Dispatcher de Load Balancer. Contiene los capítulos siguientes:

- Capítulo 5, “Configuración de inicio rápido”, en la página 45
- Capítulo 6, “Planificación de Dispatcher”, en la página 51
- Capítulo 7, “Configuración de Dispatcher”, en la página 63
- Capítulo 8, “Despliegue de Dispatcher en Load Balancer para IPv4 y IPv6”, en la página 81

Capítulo 5. Configuración de inicio rápido

Este ejemplo de inicio rápido muestra cómo configurar tres estaciones de trabajo conectadas localmente utilizando el método de reenvío mac del componente Dispatcher para equilibrar la carga del tráfico de la Web entre dos servidores Web. La configuración debería ser básicamente igual para equilibrar cualquier otro tráfico de aplicación TCP o UDP sin estado.

IMPORTANTE: si utiliza Load Balancer para IPv4 y IPv6, consulte también el Capítulo 8, “Despliegue de Dispatcher en Load Balancer para IPv4 y IPv6”, en la página 81.

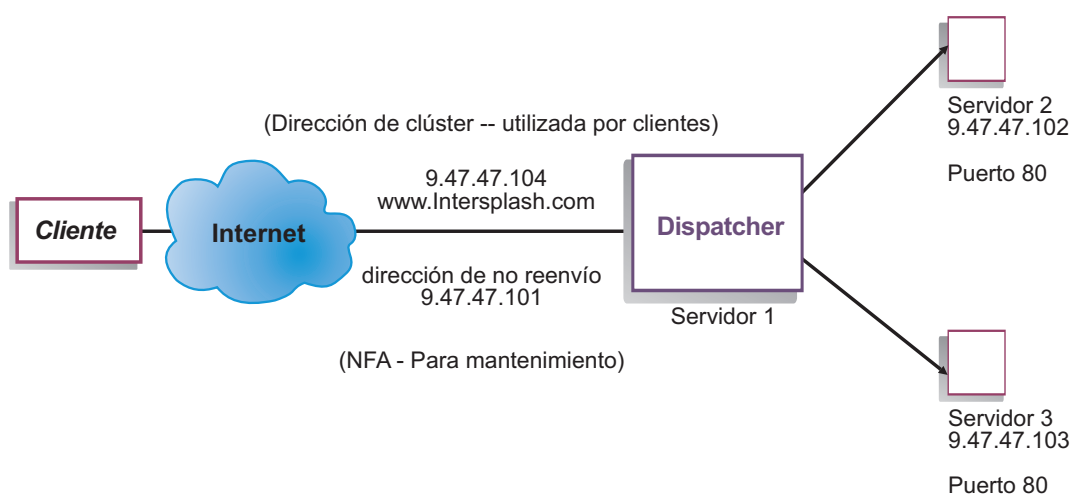


Figura 8. Configuración local sencilla de Dispatcher

El método de reenvío mac es el método por omisión por medio del cual Dispatcher equilibra la carga de peticiones entrantes al servidor y el servidor devuelve la respuesta directamente al cliente. Para obtener más información sobre el método de reenvío MAC de Dispatcher, consulte el apartado “Direccionamiento a nivel de MAC de Dispatcher (método de reenvío mac)” en la página 53.

Nota: La configuración se puede completar utilizando sólo dos estaciones de trabajo con Dispatcher ubicado en una de las estaciones de trabajo del servidor Web. Esta configuración representa una configuración colocada. Podrá encontrar procedimientos para establecer configuraciones más complejas en el apartado “Configuración de la máquina Dispatcher” en la página 66.

Qué necesita

Para el ejemplo de inicio rápido, necesita tres estaciones de trabajo y cuatro direcciones IP. Una estación de trabajo es la máquina de Dispatcher; las otras dos son los servidores Web. Cada servidor Web requiere una dirección IP. La estación de trabajo de Dispatcher requiere dos direcciones: la dirección de no reenvío (NFA) y la dirección del clúster (la dirección en la que se equilibra la carga) que puede proporcionar a clientes para acceder al sitio Web.

Nota: NFA es la dirección que el mandato **hostname** devuelve. Esta dirección se utiliza para fines administrativos, como la configuración remota.

Preparativos

1. Para este ejemplo de configuración conectada localmente, configure las estaciones de trabajo en el mismo segmento de la LAN. Asegúrese de que el tráfico de red entre las tres máquinas no tenga que pasar por direccionadores o puentes. (Para establecer configuraciones con servidores remotos, consulte el apartado “Configurar soporte de Dispatcher de área amplia” en la página 229).
2. Configure los adaptadores de red de las tres estaciones de trabajo. Para este ejemplo, suponga que tiene la configuración de red siguiente:

Estación de trabajo	Nombre	Dirección IP
1	servidor1.Intersplashx.com	9.47.47.101
2	servidor2.Intersplashx.com	9.47.47.102
3	servidor3.Intersplashx.com	9.47.47.103
Máscara de red = 255.255.255.0		

Cada una de las estaciones de trabajo sólo contiene una tarjeta de interfaz de red Ethernet estándar.

3. Asegúrese de que servidor1.Intersplashx.com puede ejecutar ping de servidor2.Intersplashx.com y servidor3.Intersplashx.com.
4. Asegúrese de que servidor2.Intersplashx.com y servidor3.Intersplashx.com pueden ejecutar ping de servidor1.Intersplashx.com.
5. Asegúrese de que los contenidos son idénticos en los dos servidores Web (Servidor 2 y Servidor 3). Esto puede conseguirse duplicando los datos de ambas estaciones de trabajo, utilizando un sistema de archivos compartido tal como NFS, AFS o DFS o bien por cualquier otro medio apropiado para el sitio.
6. Asegúrese de que los servidores Web en servidor2.Intersplashx.com y servidor3.Intersplashx.com son operacionales. Utilice un navegador Web para solicitar páginas directamente de **http://servidor2.Intersplashx.com** y **http://servidor3.Intersplashx.com**.
7. Obtenga otra dirección IP válida para este segmento de la LAN. Esta será la dirección que proporcionará a los clientes que deseen acceder a su sitio. Para este ejemplo utilizará:
Name= www.Intersplashx.com
IP=9.47.47.104
8. Configure las dos estaciones de trabajo de servidor Web para aceptar tráfico de www.Intersplashx.com.
Añada un alias para www.Intersplashx.com a la interfaz de **bucle de retorno** en servidor2.Intersplashx.com y servidor3.Intersplashx.com.
 - En sistemas AIX:
ifconfig lo0 alias www.Intersplashx.com netmask 255.255.255.0
 - En sistemas Solaris 9:
ifconfig lo0:1 plumb www.Intersplashx.com netmask 255.255.255.0 up
 - Para otros sistemas operativos consulte la Tabla 5 en la página 73.
9. Suprima cualquier ruta adicional que pueda haberse creado como resultado de añadir un alias a la interfaz de bucle de retorno. Consulte el apartado “Paso 2. Comprobar si hay una ruta adicional” en la página 76.

Ahora ha completado todos los pasos de configuración que son necesarios en las dos estaciones de trabajo de servidor Web.

Configuración del componente Dispatcher

Con Dispatcher, puede crear una configuración mediante la línea de mandatos, el asistente de configuración o la interfaz gráfica de usuario (GUI).

Nota: Los valores de los parámetros deben escribirse en caracteres del idioma inglés. Las únicas excepciones son los valores de parámetros para los nombres de sistemas principales y de archivos.

Configuración con la línea de mandatos

Si va a utilizar la línea de mandatos, siga estos pasos:

1. Inicie dserver en Dispatcher:
 - En sistemas AIX, HP-UX, Linux o Solaris, ejecute el mandato siguiente como usuario root: **dserver**
 - En sistemas Windows, dserver se ejecuta como un servicio que se inicia automáticamente.
2. Inicie la función de ejecutor de Dispatcher:
dscontrol executor start
3. Añada la dirección de clúster a la configuración de Dispatcher:
dscontrol cluster add www.Intersplashx.com
4. Añada el puerto de protocolo HTTP a la configuración de Dispatcher:
dscontrol port add www.Intersplashx.com:80
5. Añada cada uno de los servidores Web a la configuración de Dispatcher:
dscontrol server add www.Intersplashx.com:80:server2.Intersplashx.com
dscontrol server add www.Intersplashx.com:80:servidor3.Intersplashx.com
6. Configure la estación de trabajo de manera que acepte tráfico para la dirección de clúster:
dscontrol executor configure www.Intersplashx.com
7. Inicie la función de gestor de Dispatcher:
dscontrol manager start
Dispatcher ahora equilibrará la carga según el rendimiento del servidor.
8. Inicie la función de consejero de Dispatcher:
dscontrol advisor start http 80
Dispatcher se asegurará ahora de que las peticiones del cliente no se envíen a un servidor Web con anomalías.

Ya se ha completado la configuración básica con los servidores conectados localmente.

Prueba de la configuración

Compruebe si la configuración funciona:

1. Desde el navegador Web, vaya a la ubicación **http://www.Intersplashx.com**. Si se visualiza una página, significa que la configuración funciona.
2. Vuelva a cargar la página en el navegador Web.

3. Observe los resultados de este mandato: **dscontrol server report www.Intersplashx.com:80:**. La columna de conexiones totales de los dos servidores debería sumarse a "2."

Configuración con la interfaz gráfica de usuario (GUI)

Si desea información sobre cómo utilizar la GUI de Dispatcher, consulte el apartado "GUI" en la página 64 y el Apéndice A, "GUI: instrucciones generales", en la página 467.

Asistente de configuración

Si desea información sobre cómo utilizar el Asistente de configuración, consulte el apartado "Configuración con el asistente de configuración" en la página 66.

Tipos de configuraciones de clúster, puerto y servidor

Hay muchos modos de configurar Load Balancer para dar soporte a su sitio. Si sólo tiene un nombre de sistema principal para el sitio al que se conectarán todos sus clientes, puede definir un solo clúster de servidores. Para cada uno de estos servidores, configure el puerto a través del que Load Balancer se comunica. Consulte la Figura 9.

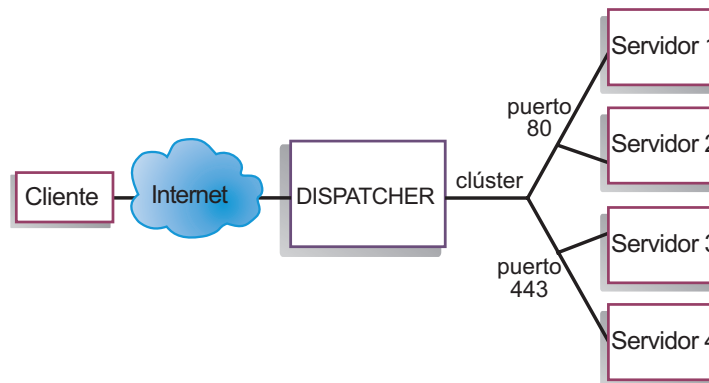


Figura 9. Ejemplo de Dispatcher configurado con un solo clúster y 2 puertos

En este ejemplo del componente Dispatcher, se define un clúster en www.productworks.com. Este clúster tiene dos puertos: el puerto 80 para HTTP y el puerto 443 para SSL. Un cliente que solicita <http://www.productworks.com> (puerto 80) va a un servidor distinto que un cliente que solicita <https://www.productworks.com> (puerto 443).

Podría resultar adecuado otro modo de configurar Load Balancer si tiene un sitio de un tamaño muy grande con muchos servidores dedicados a cada protocolo admitido. En este caso, quizá desee definir un clúster para cada protocolo con un solo puerto pero con muchos servidores, como se muestra en la Figura 10.

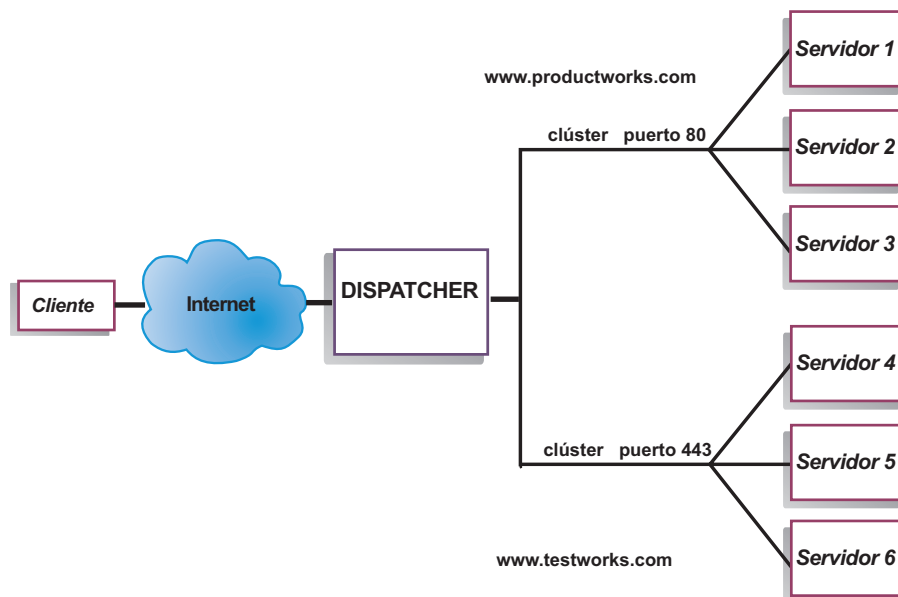


Figura 10. Ejemplo de Dispatcher configurado con dos clústeres, cada uno con un puerto

En este ejemplo del componente Dispatcher, se definen dos clústeres: `www.productworks.com` para el puerto 80 (HTTP) y `www.testworks.com` para el puerto 443 (SSL).

Podría ser necesario un tercer modo de configurar Load Balancer si el sitio alberga el contenido de varias empresas o departamentos, en el que cada uno entra al sitio con un URL distinto. En este caso, quizá desee definir un clúster para cada empresa o departamento y luego definir los puertos en los que va a recibir conexiones en ese URL, como se muestra en la Figura 11.

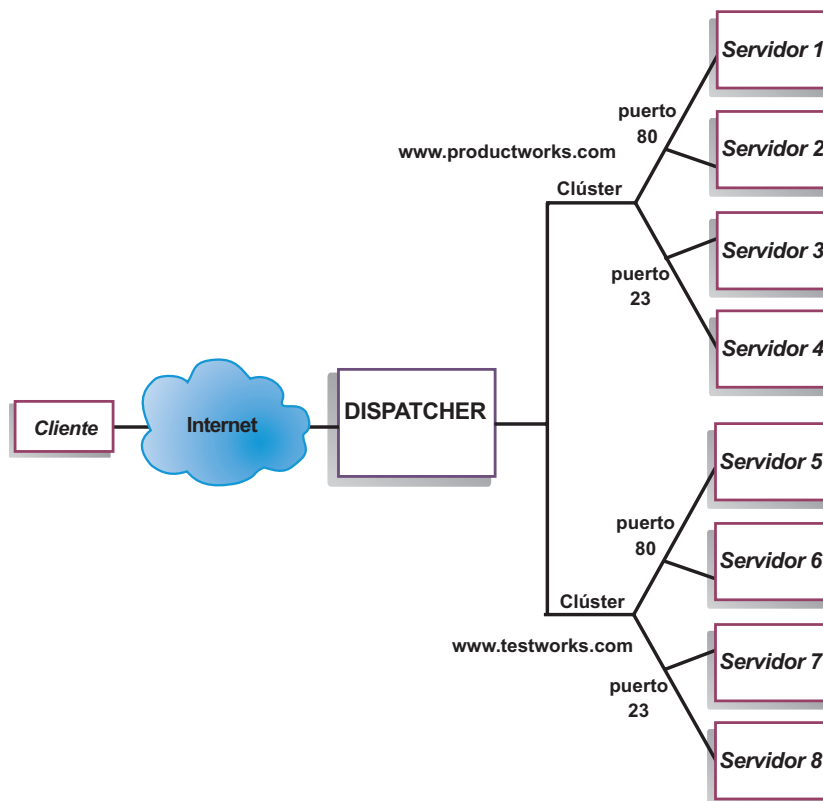


Figura 11. Ejemplo de Dispatcher configurado con 2 clústeres, cada uno con 2 puertos

En este ejemplo del componente Dispatcher, se definen dos clústeres con el puerto 80 para HTTP y el puerto 23 para Telnet para cada uno de los sitios en www.productworks.com y www.testworks.com.

Capítulo 6. Planificación de Dispatcher

En este capítulo se describe lo que debe tener en cuenta el planificador de la red antes de instalar y configurar el componente Dispatcher.

- Si desea obtener una visión general de características que están disponibles para gestionar la red consulte el Capítulo 3, “Gestión de la red: determinación de las características de Load Balancer que se van a utilizar”, en la página 19.
- Si desea información sobre cómo configurar parámetros de equilibrio de carga de Dispatcher, consulte el Capítulo 7, “Configuración de Dispatcher”, en la página 63.
- Consulte el Capítulo 8, “Despliegue de Dispatcher en Load Balancer para IPv4 y IPv6”, en la página 81 si utiliza Load Balancer para IPv4 y IPv6.
- Si desea información sobre cómo configurar Load Balancer para obtener funciones más avanzadas, consulte el Capítulo 22, “Características avanzadas para Dispatcher, CBR y Site Selector”, en la página 201.
- Si desea información sobre administración autenticada remota, archivos de anotaciones cronológicas de Load Balancer y el uso de los componentes de Load Balancer consulte el Capítulo 24, “Operación y gestión de Load Balancer”, en la página 261.

Este capítulo incluye los apartados siguientes:

- “Consideraciones de planificación”
- “Direccionamiento a nivel de MAC de Dispatcher (método de reenvío mac)” en la página 53
- “NAT/NAPT de Dispatcher (método de reenvío nat)” en la página 53
- “Direccionamiento basado en contenido de Dispatcher (método de reenvío cbr)” en la página 55
- “Creación de particiones del servidor: servidores lógicos configurados con un servidor físico (dirección IP)” en la página 58
- “Alta disponibilidad” en la página 60

Nota: Para versiones anteriores, cuando el producto se conocía con el nombre de Network Dispatcher, el nombre del mandato de control de Dispatcher era `ndcontrol`. El nombre del mandato de control de Dispatcher ahora es `dscontrol`.

Consideraciones de planificación

IMPORTANTE: si utiliza Load Balancer para IPv4 y IPv6, consulte también el Capítulo 8, “Despliegue de Dispatcher en Load Balancer para IPv4 y IPv6”, en la página 81.

Dispatcher consta de estas funciones:

- **dsserver** gestiona las peticiones de la línea de mandatos al ejecutor, el gestor y los asesores.
- El **ejecutor** admite el equilibrio de carga según el puerto de conexiones TCP y UDP. Se pueden reenviar conexiones a servidores según el tipo de petición recibida (por ejemplo, HTTP, FTP, SSL, etc.). Siempre se ejecuta el ejecutor cuando se utiliza el componente Dispatcher para el equilibrio de carga.
- El **gestor** establece los pesos que utiliza el ejecutor basándose en:

- Contadores internos del ejecutor
- Información de retorno de los servidores proporcionada por los asesores
- Información de retorno de un programa de supervisión del sistema, como Metric Server o WLM.

La utilización del gestor es opcional. No obstante, si no se utiliza el gestor, se realiza el equilibrio de carga utilizando la planificación de turno rotativo sopesado según los pesos del servidor actual y no están disponibles los asesores.

- Los **asesores** consultan los servidores y analizan los resultados por protocolo antes de llamar al gestor para establecer pesos según corresponda. Actualmente, hay asesores disponibles para los protocolos siguientes: HTTP, FTP, SSL, SMTP, NNTP, IMAP, POP3, SIP y Telnet.

Dispatcher también ofrece asesores que no intercambian información específica del protocolo, como el asesor de DB2 que informa sobre el estado de los servidores de DB2 y el asesor de ping que informa de si el servidor responde o no a un mandato ping. Si desea una lista completa de asesores, consulte el apartado “Lista de asesores” en la página 188.

También tiene la opción de escribir sus propios asesores (consulte el apartado “Crear asesores personalizados (personalizables)” en la página 192).

El uso de asesores es opcional, pero se recomienda.

- Para configurar y gestionar el ejecutor, los asesores y el gestor, utilice la línea de mandatos (**dscontrol**) o la interfaz gráfica de usuario (**lbadmin**).
- Se proporciona un **archivo de configuración de ejemplo** que se va a utilizar para configuración y administración de la máquina Dispatcher. Consulte el Apéndice C, “Archivos de configuración de ejemplo”, en la página 479. Después de haber instalado el producto, este archivo se puede encontrar en el subdirectorio **...ibm/edge/lb/servers/samples** donde se ubica Load Balancer.
- El **subagente SNMP** permite que una aplicación de gestión SNMP supervise el estado de Dispatcher.

Las tres funciones clave de Dispatcher (ejecutor, gestor y asesores) actúan conjuntamente para equilibrar y entregar las peticiones entrantes entre servidores. Junto con las peticiones de equilibrio de carga, el ejecutor supervisa el número de conexiones nuevas, de conexiones activas y de conexiones en un estado de finalizadas. El ejecutor también recoge la basura de conexiones finalizadas o restablecidas y suministra esta información al gestor.

El gestor recopila información del ejecutor, los asesores y un programa de supervisión del sistema, como Metric Server. Basándose en la información que recibe, el gestor ajusta cómo se pesan las máquinas servidor en cada puerto y proporciona al ejecutor el nuevo cálculo de pesos para utilizarlo en el equilibrado de nuevas conexiones.

Los asesores supervisan cada servidor en el puerto asignado para determinar el tiempo de respuesta del servidor y la disponibilidad, asimismo proporcionan esta información al gestor. Los asesores también supervisan si un servidor está activo o inactivo. Sin el gestor ni los asesores, el ejecutor realiza la planificación de turno rotativo según los pesos del servidor actuales.

Métodos de reenvío

Con Dispatcher, puede seleccionar uno entre tres métodos de reenvío especificados a nivel de puerto: reenvío MAC, reenvío NAT/NAPT o reenvío CBR (Content Based Routing).

Direccionamiento a nivel de MAC de Dispatcher (método de reenvío mac)

Con el método de reenvío MAC de Dispatcher (el método de reenvío por omisión), Dispatcher equilibra la carga de la petición de entrada con el servidor seleccionado y el servidor devuelve la respuesta *directamente* al cliente sin la participación de Dispatcher. Con este método de reenvío, el Dispatcher sólo tiene en cuenta los flujos de entrada del cliente al servidor. No tiene que comprobar los flujos de salida del servidor al cliente. Esto reduce significativamente el impacto en la aplicación y puede producir un rendimiento de red mejorado.

Se puede seleccionar el método de reenvío cuando se añade un puerto con el mandato **dscontrol port add clúster:puerto method valor**. El valor del método de reenvío por omisión es **mac**. Puede especificar el parámetro del método sólo cuando se añade el puerto. Una vez que se ha añadido el puerto, no puede cambiar el valor del método de reenvío. Si desea más información, consulte el apartado “dscontrol port — configurar puertos” en la página 380.

Limitación de Linux: los sistemas Linux utilizan un modelo según el sistema principal de anunciar direcciones de hardware a direcciones IP utilizando ARP. Este modelo es incompatible con el servidor final o los requisitos de ubicación compartida de alta disponibilidad para el método de reenvío mac de Load Balancer. Consulte el apartado “Alternativas de alias de bucle de retorno de Linux cuando se utiliza el reenvío MAC de Load Balancer” en la página 78, donde se describen varias soluciones para alterar el comportamiento del sistema Linux con el fin de que sea compatible con el reenvío mac de Load Balancer.

Limitación de Linux cuando se utilizan servidores zSeries o S/390: existen limitaciones cuando se utilizan servidores zSeries o S/390 que disponen de tarjetas OSA (Open System Adapter). Consulte el “Problema: en Linux, existen limitaciones de configuración de Dispatcher cuando se utilizan servidores zSeries o S/390 que disponen de tarjetas OSA (Open System Adapter)” en la página 321 para obtener soluciones alternativas posibles.

NAT/NAPT de Dispatcher (método de reenvío nat)

Con la posibilidad NAT (Network Address Translation) o NAPT (Network Address Port Translation) de Dispatcher se elimina la limitación para servidores de equilibrio de carga de estar ubicados en una red conectada localmente. Si desea tener servidores situados en ubicaciones remotas, puede utilizar la técnica de método de reenvío NAT en lugar de utilizar una técnica de encapsulación GRE/WAN. También puede utilizar la característica NAPT para acceder a varios daemons del servidor que residen en cada máquina servidor con equilibrio de carga, donde cada daemon está a la escucha en un puerto único.

Puede configurar un servidor con varios daemons de dos modos distintos:

- Con NAT, puede configurar varios daemons del servidor para responder a peticiones en direcciones IP distintas. A esto también se le conoce como enlace del daemon de servidor con una dirección IP.
- Con NAPT, puede configurar varios daemons del servidor (en ejecución en el mismo servidor físico) para que estén a la escucha en números de puerto distintos.

Esta aplicación funciona bien con protocolos de aplicación de nivel superior como HTTP, SSL, IMAP, POP3, NNTP, SMTP, Telnet, etc.

Limitaciones:

- La implementación de NAT/NAPT de Dispatcher es una implementación *sencilla* de esta característica. Analiza y opera únicamente sobre el contenido de cabeceras de paquetes TCP/IP. No analiza el contenido de la parte de datos de los paquetes. Para Dispatcher, NAT/NAPT no funcionará con protocolos de aplicación, como FTP, que incorporan las direcciones o números de puerto en la parte de datos de los mensajes. Esta es una limitación conocida de NAT/NAPT según la cabecera.
- NAT/NAPT de Dispatcher no puede funcionar junto con el clúster comodín o la característica de puerto comodín.

Necesitará tres direcciones IP para la máquina de Dispatcher – dirección nfa, dirección del clúster y dirección de retorno. Para implementar NAT/NAPT, realice lo siguiente (consulte también el apartado “Pasos de ejemplo para configurar los métodos de reenvío nat o cbr de Dispatcher” en la página 57):

- Establezca el parámetro **clientgateway** en el mandato **dscontrol executor set**. Clientgateway es una dirección IP que se utiliza como la dirección del direccionador a través del cual el tráfico de la dirección de retorno se reenvía de Load Balancer a clientes. Este valor debe establecerse en una dirección IP que no sea cero antes de poder utilizar NAT/NAPT. Si desea más información, consulte el apartado “dscontrol executor — control del ejecutor” en la página 359.
- Añada un puerto utilizando el mandato **dscontrol port add clúster:puerto method valor**. El valor del método de reenvío debería establecerse en **nat**. Puede especificar el parámetro del método sólo cuando se añade el puerto. Después de añadir el puerto, no puede cambiar el valor del método de reenvío. Si desea más información, consulte el apartado “dscontrol port — configurar puertos” en la página 380.

Nota: Si no establece la dirección de pasarela cliente (clientgateway) en un valor que no sea cero, el método de reenvío sólo puede ser **mac** (método de reenvío basado en MAC).

- Añada un servidor utilizando los parámetros: mapport, returnaddress y router con el mandato **dscontrol**. Por ejemplo:

```
dscontrol server add clúster:puerto:servidor mapport valor returnaddress direcciónretorno router direcciónretorno
```

– **mapport** (opcional)

Este parámetro correlaciona un número de puerto de destino de la petición de cliente (que es para Dispatcher) con el número de puerto del servidor que Dispatcher utiliza para equilibrar la carga de la petición del cliente. Mapport permite que Load Balancer reciba una petición de cliente en un puerto y la transmita a un puerto distinto en la máquina servidor. Con mapport puede equilibrar la carga de peticiones de cliente en una máquina servidor que podría tener varios daemons del servidor en ejecución. El valor por omisión de mapport es el número de puerto de destino de la petición de cliente.

– **returnaddress**

La dirección de retorno es una dirección o nombre de sistema principal único que puede configurar en la máquina de Dispatcher. Dispatcher utiliza la dirección de retorno como su dirección de origen cuando equilibra la carga de la petición del cliente al servidor. Esto asegura que el servidor devuelve el paquete a la máquina de Dispatcher en lugar de enviar el paquete directamente al cliente. (Dispatcher reenviará entonces el paquete IP al cliente). Debe especificar el valor de dirección de retorno cuando añade el

servidor. No puede modificar la dirección de retorno a no ser que quite el servidor y lo añada de nuevo. La dirección de retorno no puede ser igual que la del clúster, la del servidor o la NFA.

– **router**

La dirección del direccionador en el servidor remoto. Si se trata de un servidor conectado localmente, entre la dirección del servidor, salvo que éste se encuentre en la misma máquina que Load Balancer. En dicho caso, continúe utilizando la dirección del direccionador real.

Si desea más información sobre el mandato **dscontrol server** utilizando los parámetros `mapport`, `returnaddress` y `router`, consulte el apartado “`dscontrol server` — configurar servidores” en la página 392.

Direccionamiento basado en contenido de Dispatcher (método de reenvío cbr)

El componente Dispatcher permite realizar direccionamiento basado en contenido para HTTP (con la norma de tipo “content” (contenido) y HTTPS (con afinidad de ID de sesión SSL) sin tener que utilizar Caching Proxy. Para el tráfico de HTTP y HTTPS, el método de reenvío cbr de componente Dispatcher puede proporcionar un direccionamiento basado en contenido más rápido que el componente CBR, que requiere Caching Proxy.

Para HTTP: la selección de servidor para Direccionamiento basado en contenido de Dispatcher se basa en el contenido de una dirección URL o de una cabecera HTTP. Se configura utilizando la norma de tipo “content” (contenido). Cuando configure la norma de contenido, especifique la serie de búsqueda “patrón” y un conjunto de servidores en la norma. Cuando se procesa una nueva petición de entrada, esta norma compara la serie especificada con el URL del cliente o con la cabecera HTTP especificada de la petición del cliente.

Si Dispatcher encuentra la serie en la petición del cliente, reenvía la petición a uno de los servidores dentro de la norma. Luego Dispatcher transmite los datos de respuesta del servidor al cliente (método de reenvío “cbr”).

Si Dispatcher no encuentra la serie en la petición del cliente, *no* selecciona un servidor del conjunto de servidores dentro de la norma.

Nota: La norma de contenido se configura en el componente Dispatcher del mismo modo que se configura en el componente CBR. Dispatcher puede utilizar la norma de contenido para el tráfico HTTP. No obstante, el componente CBR puede utilizar la norma de contenido para los *dos tipos de* tráfico, HTTP y HTTPS (SSL).

Para HTTPS (SSL): CBR (Content Based Routing) de Dispatcher equilibra la carga basándose en el campo de ID de sesión SSL de la petición de cliente. Con SSL, una petición de cliente contiene el ID de sesión SSL de una sesión anterior y los servidores mantienen una antememoria de sus conexiones SSL anteriores. La afinidad de sesiones de ID de SSL de Dispatcher permite al cliente y el servidor establecer una nueva conexión utilizando los parámetros de seguridad de la conexión anterior con el servidor. Al eliminar la renegociación de parámetros de seguridad SSL, como claves compartidas y algoritmos de cifrado, los servidores ahorran ciclos de CPU y el cliente obtiene una respuesta más rápida. Para habilitar la afinidad de ID de sesión SSL: el tipo de **protocolo** especificado para el puerto debe ser **SSL** y el **tiempo de permanencia en memoria** del puerto debe

establecerse en un valor que no sea cero. Si se ha superado el tiempo de permanencia en memoria, el cliente debe enviarse a un servidor distinto del anterior.

Necesitará tres direcciones IP para la máquina de Dispatcher – dirección nfa, dirección del clúster y dirección de retorno. Para implementar Direccionamiento basado en contenido de Dispatcher (vea también “Pasos de ejemplo para configurar los métodos de reenvío nat o cbr de Dispatcher” en la página 57):

- Establezca el parámetro **clientgateway** en el mandato **dscontrol executor set**. Clientgateway es una dirección IP que se utiliza como la dirección del direccionador a través del cual el tráfico de la dirección de retorno se reenvía del Dispatcher a los clientes. Clientgateway toma por omisión el valor cero. Este valor debe establecerse en una dirección IP que no sea cero antes de poder añadir un método de reenvío de direccionamiento basado en contenido. Si desea más información, consulte el apartado “dscontrol executor — control del ejecutor” en la página 359.
- Añada un puerto utilizando el parámetro **method** y el parámetro **protocol** en el mandato **dscontrol port add**. El valor del método de reenvío debería establecerse en **cbr**. El tipo de protocolo del puerto puede ser HTTP o SSL. Si desea más información, consulte el apartado “dscontrol port — configurar puertos” en la página 380.

Nota: Si no establece la dirección de pasarela cliente (clientgateway) en un valor que no sea cero, el método de reenvío sólo puede ser **mac**.

- Añada un servidor utilizando los parámetros: mapport, returnaddress y router
dscontrol server add *clúster:puerto:servidor* **mapport** *valor* **returnaddress** *direcciónretorno* **router** *direcciónretorno*

Nota: Para obtener información sobre cómo configurar el servidor utilizando los parámetros mapport (opcional), returnaddress y router, consulte la página 54.

- **Para HTTP:** realice la configuración utilizando normas basadas en el contenido de la petición del cliente (tipo de norma **content**). Por ejemplo,
dscontrol rule 125.22.22.03:80:contentRule1 **type** content **pattern** *patrón*
Donde *patrón* especifica el patrón que se va a utilizar para la norma de tipo content (contenido). Si desea más información sobre el tipo de norma content, consulte el apartado “Utilización de normas basadas en el contenido de peticiones” en la página 219. Si desea más información sobre expresiones válidas para *patrón*, consulte el Apéndice B, “Sintaxis de la norma de contenido (patrón)”, en la página 475.

Nota: La característica de réplica del registro de conexión de alta disponibilidad (que asegura que no se eliminará una conexión de cliente cuando una máquina Dispatcher de reserva se haga con el control de la máquina primaria) *no* se admite con direccionamiento basado en contenido de Dispatcher.

Pasos de ejemplo para configurar los métodos de reenvío nat o cbr de Dispatcher

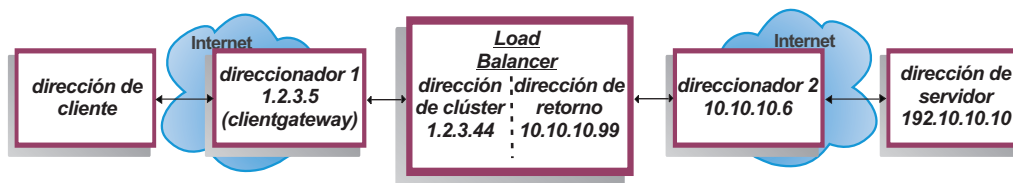


Figura 12. Ejemplo para utilizar los métodos de reenvío nat o cbr de Dispatcher

Necesitará al menos tres direcciones IP para la máquina de Dispatcher. Para la Figura 12, son necesarios estos pasos con el fin de configurar mínimamente los métodos de reenvío nat o cbr de Dispatcher:

1. Inicie el ejecutor
`dscontrol executor start`
2. Defina la pasarela de cliente
`dscontrol executor set clientgateway 1.2.3.5`
 NOTA: si la subred no tiene un direccionador local, debe configurar una máquina para que realice IP Forwarding (reenvío IP) y lo utilice como la clientgateway (pasarela de cliente). Consulte la documentación del sistema operativo para determinar cómo habilitar IP Forwarding.
3. Defina la dirección del clúster
`dscontrol cluster add 1.2.3.44`
4. Configure la dirección del clúster
`dscontrol executor configure 1.2.3.44`
5. Defina el puerto con un método de nat o cbr
`dscontrol port add 1.2.3.44:80 method nat`
 o bien
`dscontrol port add 1.2.3.44:80 method cbr protocol http`
6. Configure una dirección de retorno de alias en Load Balancer (utilizando la tarjeta Ethernet 0)
 NOTA: En sistemas Linux, no es necesario poner un alias a la dirección de retorno si utiliza el reenvío nat en una máquina con ubicación compartida.
`dscontrol executor configure 10.10.10.99`
 O bien, utilice el mandato `ifconfig` (sólo para Linux o UNIX):
 AIX: `ifconfig en0 alias 10.10.10.99 netmask 255.255.255.0`
 HP-UX: `ifconfig lan0:1 10.10.10.99 netmask 255.255.255.0 up`
 Linux: `ifconfig eth0:1 10.10.10.99 netmask 255.255.255.0 up`
 Solaris: `ifconfig eri0 addif 10.10.10.99 netmask 255.255.255.0 up`
7. Defina los servidores finales
`dscontrol server add 1.2.3.4:80:192.10.10.10`
`router 10.10.10.6 returnaddress 10.10.10.99`

La pasarela de cliente (1.2.3.5) es la dirección 1 del direccionador entre Load Balancer y el cliente. El direccionador (10.10.10.6) es la dirección 2 del direccionador entre Load Balancer y el servidor final. Si no está seguro de la clientgateway o de la dirección 2 del direccionador, puede utilizar un programa `tracert` con la dirección del cliente (o servidor) para determinar la dirección del direccionador. La sintaxis exacta de este programa diferirá según el sistema operativo que se utilice. Debería consultar la documentación del sistema operativo para obtener más información con respecto a este programa.

Si el servidor se encuentra en la misma subred que Load Balancer (es decir, no se devuelve ningún direccionador con traceroute) escriba la dirección del servidor como la dirección del direccionador. Sin embargo, si el servidor se encuentra en la misma máquina que Load Balancer, la dirección del direccionador debe especificarse en el campo de direccionador en lugar de la dirección del servidor. La dirección del direccionador es la que se utiliza en el mandato "server add" en la máquina Load Balancer del paso 7.

Creación de particiones del servidor: servidores lógicos configurados con un servidor físico (dirección IP)

Con la creación de particiones del servidor, puede distinguir más entre los URL en particular y sus aplicaciones específicas. Por ejemplo, un servidor Web puede servir páginas JSP, páginas HTML, archivos GIF, peticiones de base de datos, etc. Load Balancer ahora proporciona la posibilidad de crear una partición de un clúster y un servidor específico de un puerto en varios servidores lógicos. Esto permite asesorar sobre un servicio en particular en la máquina para detectar si se ejecuta más rápido un motor de servlets o una petición de base de datos, o si no se ejecuta nada.

La creación de particiones del servidor permite a Load Balancer detectar, por ejemplo, que el servicio HTML atiende páginas rápidamente, pero que la conexión de la base de datos se ha quedado inactiva. Esto permite distinguir la carga según una carga de trabajo específica de servicio granular, en lugar del peso en todo el servidor únicamente.

Creación de particiones del servidor con asesores HTTP o HTTPS

La creación de particiones del servidor puede resultar de utilidad cuando se utiliza junto con asesores HTTP y HTTPS. Por ejemplo, cuando dispone de un servidor HTML que gestiona páginas HTML, GIF y JSP, si define (añadiendo) el servidor una vez bajo el puerto 80, recibirá sólo un valor de carga para todo el servidor HTTP. Esto podría ser confuso dado que es posible que el servicio GIF no esté funcionando en el servidor. Dispatcher aún envía páginas GIF al servidor, pero el cliente detecta un tiempo de espera excedido o una anomalía.

Si define el servidor tres veces (por ejemplo, ServerHTML, ServerGIF, ServerJSP) bajo el puerto y define el parámetro **advisorrequest** del servidor con una serie distinta para cada servidor lógico, podrá consultar el estado del servicio en particular en el servidor. ServerHTML, ServerGIF y ServerJSP representan tres servidores lógicos de partición de un servidor físico. Para ServerJSP, puede definir la serie **advisorrequest** para consultar el servicio en la máquina que gestiona páginas JSP. Para ServerGIF, puede definir la serie **advisorrequest** para consultar el servicio GIF. Y para ServerHTML, puede definir **advisorrequest** para consultar el servicio HTML. Por lo tanto, si el cliente no obtiene respuesta de **advisorrequest** para consultar el servicio GIF, Dispatcher marcará ese servidor lógico (ServerGIF) como inactivo, mientras que los otros dos servidores lógicos podrían funcionar bien. Dispatcher no reenvía ningún GIF más al servidor físico, pero aún puede enviar peticiones JSP y HTML al servidor.

Si desea más información sobre el parámetro **advisorrequest**, consulte el apartado "Configuración del asesor HTTP o HTTPS utilizando la opción de petición y respuesta (URL)" en la página 190.

Ejemplo para configurar un servidor físico en servidores lógicos

Dentro de la configuración de Dispatcher, puede representar un servidor físico o uno lógico utilizando la jerarquía de *clúster:puerto:servidor*. El servidor puede ser una dirección IP única de la máquina (servidor físico) con un nombre simbólico o en un formato de dirección IP. O bien, si define el servidor para representar un servidor con particiones, debe proporcionar una dirección del servidor resoluble para el servidor físico en el parámetro **address** del mandato **dscontrol server add**. Si desea más información, consulte el apartado “dscontrol server — configurar servidores” en la página 392.

A continuación figura un ejemplo de cómo crear particiones físicas de servidores en servidores lógicos para gestionar distintos tipos de peticiones.

```
Cluster: 1.1.1.1
  Port: 80
    Server: A (IP address 1.1.1.2)
              HTML server
    Server: B (IP address 1.1.1.2)
              GIF server
    Server: C (IP address 1.1.1.3)
              HTML server
    Server: D (IP address 1.1.1.3)
              JSP server
    Server: E (IP address 1.1.1.4)
              GIF server
    Server: F (IP address 1.1.1.4)
              JSP server
  Rule1: /*.htm
    Server: A
    Server: C
  Rule2: /*.jsp
    Server: D
    Server: F
  Rule3: /*.gif
    Server: B
    Server: E
```

En este ejemplo, el servidor 1.1.1.2 se divide en 2 servidores lógicos de partición: "A" (que gestiona peticiones HTML) y "B" (que gestiona peticiones GIF). El servidor 1.1.1.3 se divide en 2 servidores lógicos de partición: "C" (que gestiona las peticiones HTML) y "D" (que gestiona las peticiones JSP). El servidor 1.1.1.4 se divide en 2 servidores lógicos de partición: "E" (que gestiona las peticiones GIF) y "F" (gestiona las peticiones JSP).

Alta disponibilidad

Alta disponibilidad sencilla

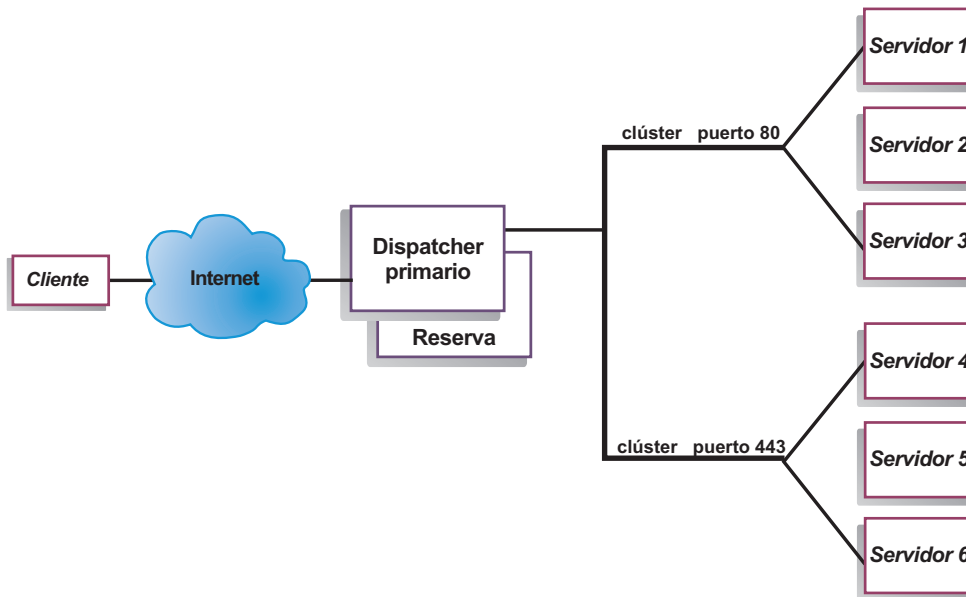


Figura 13. Ejemplo de Dispatcher con alta disponibilidad sencilla

La característica de alta disponibilidad conlleva el uso de una segunda máquina de Dispatcher. La primera máquina de Dispatcher realiza el equilibrio de carga para todo el tráfico del cliente del mismo modo que en una configuración de Dispatcher sencilla. La segunda máquina de Dispatcher supervisa el “estado” de la primera y se hace con el control de la tarea de equilibrio de carga si detecta que la primera máquina de Dispatcher ha producido un error.

Se asigna a cada una de las dos máquinas un rol específico, ya sea *primaria* o *reserva*. La máquina primaria envía datos de conexión a la máquina de reserva de forma constante. Mientras que la primaria está *activa* (equilibrando la carga), la de reserva está en estado de *espera*, continuamente actualizada y preparada para hacerse con el control, si es necesario.

Se hace referencia a las sesiones de comunicación entre las dos máquinas como *pulsos*. Los pulsos permiten que cada máquina supervise el estado de la otra.

Si la máquina de reserva detecta que la máquina activa ha producido un error, se hará con el control y comenzará a equilibrar la carga. En el punto en que se invierten los *estados* de las dos máquinas: la máquina de reserva pasa a estar *activa* y la primaria pasa a estar en *espera*.

En la configuración de alta disponibilidad, la máquina primaria y la de reserva deben estar en la misma subred con una configuración idéntica.

Si desea información sobre cómo configurar la característica de alta disponibilidad, consulte el apartado “Alta disponibilidad” en la página 204.

Alta disponibilidad mutua

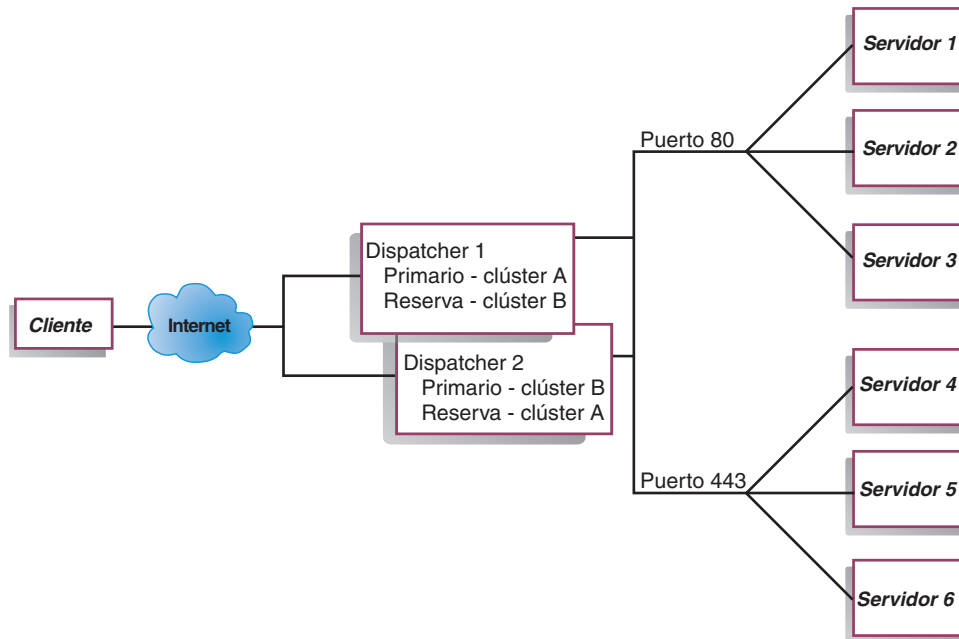


Figura 14. Ejemplo de Dispatcher con alta disponibilidad mutua

La característica de alta disponibilidad mutua conlleva el uso de dos máquinas de Dispatcher. Las dos máquinas realizan de forma activa el equilibrio de carga del tráfico del cliente y las dos máquinas proporcionan una reserva entre sí. En una configuración de alta disponibilidad sencilla, sólo una máquina realiza el equilibrio de carga. En una configuración de alta disponibilidad mutua, las dos máquinas equilibran la carga de una parte del tráfico del cliente.

Para la alta disponibilidad mutua, se asigna el tráfico del cliente a cada máquina de Dispatcher según la dirección del clúster. Cada clúster se puede configurar con NFA (dirección de no reenvío) de su Dispatcher primario. La máquina de Dispatcher primaria normalmente realiza el equilibrio de carga para ese clúster. En el caso de una anomalía, la otra máquina realiza el equilibrio de carga para su propio clúster y para el clúster del Dispatcher con anomalía.

Si desea una ilustración de una configuración de alta disponibilidad mutua con un "conjunto de clústeres A" compartido y un "conjunto de clústeres B" compartido, consulte la Figura 14. Cada Dispatcher puede dirigir paquetes activamente para su clúster *primario*. Si el Dispatcher fuera a tener una anomalía y ya no pudiera dirigir más paquetes activamente para su clúster primario, entonces el otro Dispatcher podría hacerse con el control del direccionamiento de paquetes para su clúster de *reserva*.

Nota: Las dos máquinas deben configurar sus conjuntos de clústeres compartidos del mismo modo. Es decir, los puertos utilizados y los servidores bajo cada puerto deben ser idénticos en las dos configuraciones.

Si desea información sobre cómo configurar la alta disponibilidad y la alta disponibilidad mutua, consulte el apartado "Alta disponibilidad" en la página 204.

Capítulo 7. Configuración de Dispatcher

Antes de llevar a cabo los pasos de este capítulo, consulte el Capítulo 6, “Planificación de Dispatcher”, en la página 51. En este capítulo se explica cómo crear una configuración básica para el componente Dispatcher de Load Balancer.

- Consulte el Capítulo 8, “Despliegue de Dispatcher en Load Balancer para IPv4 y IPv6”, en la página 81 si utiliza Load Balancer para IPv4 y IPv6.
- En el Capítulo 21, “Funciones del gestor, asesores y Metric Server para Dispatcher, CBR y Site Selector”, en la página 179 y el Capítulo 22, “Características avanzadas para Dispatcher, CBR y Site Selector”, en la página 201 encontrará configuraciones más complejas de Load Balancer.
- En el Capítulo 24, “Operación y gestión de Load Balancer”, en la página 261 encontrará información sobre la administración autenticada remota, las anotaciones cronológicas de Load Balancer y el uso de los componentes de Load Balancer.

Nota: En las versiones anteriores, cuando el producto se denominaba Network Dispatcher, el nombre del mandato de control de Dispatcher era `ndcontrol`. El nombre de mandato de control de Dispatcher es ahora **`dscontrol`**.

Visión general de las tareas de configuración

IMPORTANTE: si utiliza Load Balancer para IPv4 y IPv6, consulte el Capítulo 8, “Despliegue de Dispatcher en Load Balancer para IPv4 y IPv6”, en la página 81.

antes de empezar a realizar los pasos de configuración indicados en esta tabla, asegúrese de que la máquina Dispatcher y todas las máquinas de servidores están conectadas a la red, tienen direcciones IP válidas y que pueden enviar una sonda de paquetes Internet entre sí.

Tabla 4. Tareas de configuración para la función Dispatcher

Tarea	Descripción	Información relacionada
Configurar la máquina Dispatcher.	Configura la configuración de equilibrio de carga.	“Configuración de la máquina Dispatcher” en la página 66
Configurar máquinas en las que se va a equilibrar la carga.	Crea un alias para el dispositivo de bucle de retorno, comprueba si hay una ruta adicional y suprime todas las rutas adicionales.	“Configuración de máquinas de servidor para el equilibrio de carga” en la página 72

Métodos de configuración

Hay cuatro métodos básicos para la configuración de Dispatcher:

- Línea de mandatos
- Scripts
- Interfaz gráfica de usuario (GUI)
- Asistente de configuración

Línea de mandatos

Es la manera más directa que configurar Dispatcher. Los valores de los parámetros de mandatos deben especificarse en caracteres del idioma inglés. Las únicas

excepciones son los nombres de sistema principal (que se utilizan en los mandatos cluster, server y highavailability) y nombres de archivo (que se utilizan en los mandatos de archivo).

Para iniciar Dispatcher desde la línea de mandatos:

1. Emita el mandato **dsserver** en el indicador de mandatos. Para detener el servicio, escriba **dsserver stop**

Nota: En sistemas Windows, pulse **Inicio > Configuración** (en Windows 2000) **> Panel de control > Herramientas administrativas > Servicios**. Pulse con el botón derecho del ratón en **IBM Dispatcher** y seleccione **Iniciar**. Para detener el servicio, efectúe los mismos pasos y seleccione **Detener**.

2. A continuación, emita los mandatos de control de Dispatcher que desee para definir la configuración. En los procedimientos de esta publicación se da por supuesto que se utiliza la línea de mandatos. El mandato es **dscontrol**. Para obtener más información sobre los mandatos, consulte el Capítulo 27, “Referencia de mandatos para Dispatcher y CBR”, en la página 347.

Puede utilizar una versión minimizada de los parámetros del mandato **dscontrol** escribiendo las letras exclusivas de los parámetros. Por ejemplo, para obtener ayuda sobre el mandato para guardar archivos, puede escribir **dscontrol he f** en lugar de **dscontrol help file**.

Para iniciar la interfaz de línea de mandatos, emita **dscontrol** para recibir un indicador de mandatos de **dscontrol**.

Para finalizar la interfaz de línea de mandatos, emita **exit** o **quit**.

Scripts

Puede entrar mandatos para configurar Dispatcher en un archivo de script de configuración y ejecutarlos juntos. Consulte el apartado “Archivos de configuración de Load Balancer de ejemplo” en la página 479.

Nota: Para ejecutar rápidamente el contenido de un archivo de script (por ejemplo, *miscript*), use cualquiera de los siguientes mandatos:

- Para actualizar la configuración actual, ejecute los siguientes mandatos ejecutables desde el archivo *descript*:
dscontrol file appendload miscript
- Para sustituir completamente la configuración actual, ejecute los siguientes mandatos ejecutables desde el archivo de script:
dscontrol file newload miscript

Para guardar la configuración actual en un archivo de script (por ejemplo, *guardascript*), ejecute el siguiente mandato:

dscontrol file save guardascript

Este mandato guardará el archivo de script de configuración en el directorio **...ibm/edge/lb/servers/configurations/dispatcher**.

GUI

Para obtener instrucciones generales y un ejemplo de la interfaz gráfica de usuario (GUI), consulte la Figura 41 en la página 468.

Para iniciar la GUI, siga estos pasos:

1. Asegúrese de que dsserver se está ejecutando
 - En sistemas AIX, HP-UX, Linux o Solaris, ejecute el siguiente mandato como usuario root:
dsserver
 - En sistemas Windows, dsserver se ejecuta como un servicio que se inicia automáticamente.
2. Efectúe una de las siguientes acciones, en función del sistema operativo:
 - En sistemas AIX, HP-UX, Linux o Solaris, escriba **lbadmin**
 - En sistemas Windows: pulse **Inicie > Programas > IBM WebSphere > Edge Components > IBM Load Balancer > Load Balancer**

Para configurar el componente Dispatcher desde la GUI, primero debe seleccionar **Dispatcher** en la estructura de árbol. Inicie el ejecutor y el gestor una vez que se ha conectado a un sistema principal. También puede crear clústeres que contengan puertos y servidores, así como iniciar asesores para el gestor.

La GUI puede utilizarse para llevar a cabo las mismas tareas que realizaría con el mandato **dscontrol**. Por ejemplo, para definir un clúster mediante la línea de mandatos, especifique el mandato **dscontrol cluster add clúster**. Para definir un clúster desde la GUI, pulse con el botón derecho en el Ejecutor y, en el menú emergente, pulse **Añadir clúster**. Escriba la dirección del clúster en la ventana emergente y pulse **Aceptar**.

Los archivos de configuración de Dispatcher preexistentes pueden cargarse con las opciones **Cargar nueva configuración** (para sustituir completamente la configuración actual) y **Añadir a la configuración actual** (para actualizar la configuración actual) que aparecen en el menú emergente **Sistema principal**. Debe guardar de forma periódica la configuración de Dispatcher en un archivo con la opción **Guardar archivo de configuración como** que también se encuentra en el menú emergente **Sistema principal**. El menú **Archivo** situado en la parte superior de la GUI, permite guardar en un archivo las conexiones actuales del sistema principal o restaurar conexiones que se encuentran en archivos existentes en todos los componentes de Load Balancer.

Los mandatos de configuración también pueden ejecutarse de forma remota. Para obtener más información, consulte el apartado “RMI (Remote Method Invocation)” en la página 262.

Para poder ejecutar un mandato desde la GUI: resalte el nodo Sistema principal en el árbol de la GUI y seleccione **Enviar mandato....** en el menú emergente Sistema principal. En el campo de entrada de mandatos, escriba el mandato que desea ejecutar, por ejemplo: **executor report**. El resultado y el historial de los mandatos se ejecutan en la sesión actual y aparecen en la ventana que se proporciona.

Para acceder a la **Ayuda**, pulse el icono de signo de interrogación situado en la esquina superior derecha de la ventana de Load Balancer.

- **Ayuda: Nivel de campo** — describe cada campo, los valores por omisión
- **Ayuda: Cómo puedo** — lista las tareas que pueden llevarse a cabo desde esa pantalla
- **InfoCenter** — proporciona acceso centralizado a la información del producto

Si desea más información sobre cómo utilizar la GUI, consulte el Apéndice A, “GUI: instrucciones generales”, en la página 467.

Configuración con el asistente de configuración

Si va a utilizar el asistente de configuración, siga estos pasos:

1. Inicie dserver en Dispatcher:
 - En sistemas AIX, HP-UX, Linux o Solaris, ejecute lo siguiente como usuario root:
dserver
 - En sistemas Windows, dserver se ejecuta como un servicio que se inicia automáticamente.
2. Inicie la función de asistente de Dispatcher, **dswizard**.

El asistente le guiará, paso a paso, a través del proceso de creación de una configuración básica para el componente Dispatcher. Se formularán preguntas sobre la red. Se le orientará a lo largo de la configuración de un clúster para que Dispatcher equilibre la carga del tráfico de un grupo de servidores.

Configuración de la máquina Dispatcher

Antes de configurar la máquina Dispatcher, debe establecer el usuario root (en sistemas AIX, HP-UX, Linux o Solaris) o el administrador en sistemas Windows.

En todas las plataformas soportadas, Load Balancer puede tener un servidor **con ubicación compartida**. Ubicación compartida significa que Load Balancer puede residir físicamente en una máquina servidor en la que se está efectuando el equilibrio de carga.

En la máquina Dispatcher, al utilizar el método de reenvío MAC, como mínimo se necesitan dos direcciones IP válidas. Para CBR o el método de reenvío NAT, como mínimo se necesitarán tres direcciones IP válidas.

- Una dirección IP específica para la máquina Dispatcher
Esta dirección IP es la dirección IP primaria de la máquina Dispatcher y se denomina dirección de no reenvío (NFA). Por omisión es la misma dirección que la devuelta por el mandato **hostname**. Utilice esta dirección para conectarse a la máquina para fines administrativos, como realizar la configuración remota utilizando Telnet o acceder al subagente SNMP. Si la máquina Dispatcher ya puede hacer ping a otras máquinas en la red, no es necesario realizar ninguna otra acción para configurar la dirección de no reenvío.
- Una dirección IP para cada clúster
Una dirección de clúster es una dirección asociada con un nombre de sistema principal (como **www.suempresa.com**). El cliente utilizará esta dirección IP para conectarse a los servidores de un clúster. Esta es la dirección en la que Dispatcher equilibrará la carga.
- Para CBR o el reenvío NAT, una dirección IP para la dirección de retorno
Dispatcher utiliza la dirección de retorno como su dirección origen al realizar el equilibrio de carga de las peticiones del cliente al servidor. Esto garantiza que el servidor devuelve el paquete a la máquina Dispatcher en lugar de enviar el paquete directamente al cliente. (Dispatcher reenviará el paquete IP al cliente). Al añadir el servidor, deberá especificar el valor de la dirección de retorno. No puede modificar la dirección de retorno a menos que elimine el servidor y lo añada de nuevo.

Sólo sistemas Solaris:

- Por omisión, Dispatcher se ha configurado para equilibrar la carga del tráfico en las tarjetas de interfaz de red Ethernet de 100Mbps. El adaptador Ethernet de 100Mbps por omisión se especifica en el archivo `ibmlb.conf` como `eri`. No obstante, también se proporciona soporte para otros tipos de tarjetas de interfaz, incluidas: `le`, `ce`, `ge`, `hme`, `eri`, `bge`, `vge`, `qfe`, `dfme`, `fji` y `fje`.

Por ejemplo, para cambiar el valor por omisión, edite el archivo `/opt/ibm/edge/lb/servers/ibmlb.conf` como se indica a continuación:

- Para utilizar un adaptador Ethernet de 10 Mbps, sustituya `eri` por `le`.
- Para utilizar un adaptador Ethernet de 1Gbps, sustituya `eri` por `ge`.
- Para utilizar un adaptador multipuerto, sustituya `eri` por `qfe`.

Para dar soporte a varios tipos de adaptadores, duplique la línea en el archivo `ibmlb.conf` y modifique cada línea de forma que coincida con el tipo de dispositivo.

Por ejemplo, si tiene previsto utilizar dos adaptadores Ethernet de 100Mbps, el archivo `ibmlb.conf` debe tener una sola línea que especifique el dispositivo `eri`.

Si tiene previsto utilizar un adaptador Ethernet de 10 Mbps y un adaptador Ethernet de 100Mbps, es necesario especificar dos líneas en el archivo `ibmlb.conf`: una línea que especifique el dispositivo `le` y una línea que especifique el dispositivo `eri`.

Nota: El archivo `ibmlb.conf` proporciona entrada para el mandato **autopush** de Solaris y debe ser compatible con el mandato `autopush`.

- Para determinar el tipo de interfaz de red Ethernet que se utiliza en su máquina, emita el siguiente mandato desde el indicador de mandatos de Solaris:

```
ifconfig -a
```

Si obtiene la siguiente salida:

```
lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL>
    mtu 8232 index 1 inet 127.0.0.1 netmask ff000000
eri0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4>
    mtu 1500 index 2 inet 9.42.93.208
    netmask fffffc00 broadcast 9.42.95.255 ether 0:3:ba:2d:24:45
```

Edite el archivo `ibmlb.conf` como se indica a continuación:

```
eri -1 0 ibmlb
```

- Si se inicia o detiene el ejecutor de Dispatcher desconfigurará todos los alias de los adaptadores listados en el archivo `ibmlb.conf`. Para volver a configurar automáticamente los alias de dichos adaptadores (excepto los que utiliza el componente Dispatcher de Load Balancer), utilice el archivo de script **goAliases**. Hay un script de ejemplo que está en el directorio `...ibm/edge/lb/servers/samples` y debe moverse al directorio `...ibm/edge/lb/servers/bin` antes de ejecutarse. El script `goAliases` se ejecuta automáticamente cuando se inicia o detiene el ejecutor de Dispatcher.

Por ejemplo, si se configuran los clústeres X e Y para que los utilice el componente CBR en cualquiera de los adaptadores listados en `ibmlb.conf`, los clústeres X e Y se desconfiguran cuando se emiten los mandatos **dscontrol executor start** o **dscontrol executor stop**. Es posible que no sea el resultado que desee. Cuando se configuran los clústeres X e Y en el script `goAliases`, los clústeres se configuran automáticamente después de iniciar o detener el ejecutor de Dispatcher.

Asegúrese de que IP Forwarding no está habilitado para el protocolo TCP/IP.

La Figura 15 muestra un ejemplo de Dispatcher configurada con un solo clúster, dos puertos y tres servidores.



Figura 15. Ejemplo de las direcciones IP necesarias para la máquina Dispatcher

Para obtener ayuda sobre los mandatos que se utilizan en este procedimiento, consulte el Capítulo 27, “Referencia de mandatos para Dispatcher y CBR”, en la página 347.

Para obtener un archivo de configuración de ejemplo, consulte el apartado “Archivos de configuración de Load Balancer de ejemplo” en la página 479.

Paso 1. Iniciar la función de servidor

Sistemas AIX, HP-UX, Linux o Solaris: para iniciar la función de servidor, escriba `dsserver`.

Sistemas Windows: la función de servidor se inicia automáticamente como un servicio.

Nota: Un archivo de configuración por omisión (`default.cfg`) se carga de forma automática al iniciar `dsserver`. Si el usuario decide guardar la configuración de Dispatcher en `default.cfg`, todo lo que se guarde en este archivo se carga automáticamente la próxima vez que se inicie `dsserver`.

Paso 2. Iniciar la función de ejecutor

Para iniciar la función de ejecutor, escriba el mandato `dscontrol executor start`. En este momento también puede cambiar varios valores del ejecutor. Consulte el Capítulo 27, “Referencia de mandatos para Dispatcher y CBR”, en la página 347.

Paso 3. Definir la dirección de no reenvío (si es distinta del nombre de sistema principal)

La dirección de no reenvío se utiliza para conectarse a la máquina para fines administrativos, como la utilización de Telnet o SMTP para esta máquina. Por omisión esta dirección es el nombre de sistema principal.

Para definir la dirección de no reenvío, escriba el mandato `dscontrol executor set nfa dirección_IP` o edite el archivo de configuración de ejemplo. `dirección_IP` es el nombre simbólico o la dirección IP.

Paso 4. Definir un clúster y establecer opciones de clúster

Dispatcher equilibrará las peticiones enviadas a la dirección del clúster para los servidores configurados en los puertos de dicho clúster.

El clúster es el nombre simbólico, la dirección decimal separada por puntos o la dirección especial 0.0.0.0 que define un clúster comodín. Para definir un clúster, emita el mandato **dscontrol cluster add**. Para establecer las opciones del clúster, emita el mandato **dscontrol cluster set** o puede utilizar la GUI para emitir mandatos. Los clústeres comodín pueden utilizarse para emparejar varias direcciones IP para los paquetes entrantes sobre los cuales se realizará un equilibrio de carga. Consulte los apartados “Utilizar un clúster comodín para combinar configuraciones de servidores” en la página 237, “Utilizar un clúster comodín para equilibrar la carga de cortafuegos” en la página 238 y “Utilizar un clúster comodín con Caching Proxy para el proxy transparente” en la página 238 para obtener más información.

Paso 5. Crear un alias para la tarjeta de interfaz de red

Después de definir el clúster, normalmente debe configurar la dirección del clúster en una de las tarjetas de interfaz de red de la máquina Dispatcher. Para ello, emita el mandato **dscontrol executor configure** *dirección_clúster*. Este buscará un adaptador con una dirección existente que pertenezca a la misma subred que la dirección del clúster. A continuación, emitirá el mandato de configuración del adaptador del sistema operativo utilizando el adaptador que ha encontrado y la máscara de red correspondiente a la dirección existente encontrada en dicho adaptador. Por ejemplo:

```
dscontrol executor configure 204.67.172.72
```

No se recomienda configurar la dirección del clúster en los casos de clústeres añadidos a un servidor en espera en modalidad de alta disponibilidad o de clústeres añadidos a un sistema Dispatcher de área amplia que actúa como servidor remoto. Tampoco es necesario ejecutar el mandato **executor configure** si utiliza el script **goldle** de ejemplo en modalidad autónoma. Para obtener información sobre el script **goldle**, utilice “Utilización scripts” en la página 209.

En contadas ocasiones es posible que tenga una dirección de clúster que no coincida con ninguna subred para las direcciones existentes. En este caso, utilice la segunda forma del mandato **executor configure** y proporcione de forma explícita el nombre de interfaz y la máscara de red. Utilice **dscontrol executor configure** *dirección_interfaz nombre_interfaz máscara_red*.

Algunos ejemplos son:

```
dscontrol executor configure 204.67.172.72 en0 255.255.0.0
(Sistemas AIX)
dscontrol executor configure 204.67.172.72 eth0:1 255.255.0.0
(Sistemas Linux)
dscontrol executor configure 204.67.172.72 eri0 255.255.0.0
(Sistemas Solaris)
dscontrol executor configure 204.67.172.72 en1 255.255.0.0
(Sistemas Windows)
```

Sistemas Windows

Para utilizar la segunda forma del mandato **executor configure** en sistemas Windows, debe determinar el nombre de interfaz que utilizará. Si la máquina sólo tiene una tarjeta Ethernet, el nombre de interfaz es **en0**. Si sólo tiene una tarjeta

Token Ring, el nombre de interfaz es tr0. Si tiene varias tarjetas de cualquiera de los dos tipos, será necesario determinar la correlación de las tarjetas. Siga estos pasos:

1. En la línea de mandatos, inicie el ejecutor: `dscontrol executor start`
2. Ejecute el mandato: `dscontrol executor xm 1`

La salida se mostrará en la pantalla. Para determinar el nombre de interfaz que debe utilizarse para la configuración de Load Balancer, busque la dirección IP de la máquina de Load Balancer en las líneas que figuran a continuación de Number of NIC records.

La dirección IP de la máquina de Load Balancer aparecerá como: `ia->ia_addr` El nombre de la interfaz asociada aparecerá como: `ifp->if_name`.

Los nombres asignados por el mandato `executor configure` están correlacionados con los nombres de interfaz listados en este mandato.

Después de obtener esta información de correlación, puede crear un alias en la interfaz de red para la dirección del clúster.

Utilización de mandatos `ifconfig` para configurar alias de clúster

En sistemas Linux o UNIX, el mandato `executor configure` ejecuta mandatos `ifconfig`.

Sistemas Solaris y HP-UX: al utilizar aplicaciones de servidores específicos del enlace que enlazan a una lista de direcciones IP que no contienen el IP del servidor, utilice el mandato **`arp publish`** en lugar de `ifconfig` para establecer de forma dinámica una dirección IP en la máquina Load Balancer. Por ejemplo:

```
arp -s <clúster> dirección MAC de <Load Balancer > pub
```

Paso 6. Definir puertos y establecer opciones de puertos

Para definir un puerto, escriba el mandato **`dscontrol port add`** *clúster:puerto*, edite el archivo de configuración de ejemplo o utilice la GUI. *Clúster* es el nombre simbólico o la dirección IP. *Puerto* es el número del puerto que utiliza para dicho protocolo. En este momento también puede cambiar varios valores del puerto. Debe definir y configurar todos los servidores para un puerto. Consulte el Capítulo 27, “Referencia de mandatos para Dispatcher y CBR”, en la página 347.

El número de puerto 0 (cero) se utiliza para especificar un puerto comodín. Este puerto aceptará tráfico para un puerto que no esté destinado a ninguno de los puertos definidos en el clúster. El puerto comodín se utiliza para configurar normas y servidores para cualquier puerto. Esta función también puede utilizarse si tiene una configuración de servidor y norma idéntica para varios puertos. El tráfico de un puerto podría afectar a las decisiones de equilibrio de carga para el tráfico en otros puertos. Consulte el apartado “Utilizar el puerto comodín para dirigir el tráfico de puerto no configurado” en la página 239 para obtener más información sobre cuándo utilizar un puerto comodín.

Paso 7. Definir máquinas servidor con equilibrio de carga

Para definir una máquina servidor con equilibrio de carga, escriba el mandato **`dscontrol server add`** *clúster:puerto:servidor*, edite el archivo de configuración de ejemplo o utilice la GUI. *Clúster* y *servidor* pueden ser un nombre simbólico o la

dirección IP. *Puerto* es el número del puerto que utiliza para dicho protocolo. Debe definir más de un servidor por puerto en un clúster para llevar a cabo el equilibrio de carga.

Servidores específicos del enlace: Si el componente Dispatcher está realizando el equilibrio de carga para servidores específicos del enlace, los servidores *deben* estar configurados para enlazar con la dirección del clúster. Puesto que Dispatcher reenvía paquetes sin cambiar la dirección IP de destino, cuando los paquetes alcanzan el servidor, los paquetes todavía contienen la dirección del clúster como destino. Si se ha configurado un servidor para enlazar a una dirección IP distinta de la dirección del clúster, el servidor no podrá aceptar peticiones cuyo destino es el clúster.

Para determinar si el servidor es específico del enlace, emita el mandato `netstat -an` y busque `server:port`. Si el servidor no es específico del enlace, el resultado del mandato será `0.0.0.0:80`. Si el servidor es específico del enlace, verá una dirección parecida a `192.168.15.103:80`.

Nota: Para sistemas Solaris y Linux: cuando se utilizan asesores, los servidores específicos del enlace no pueden tener la ubicación compartida.

Ubicación compartida de varias direcciones: En una configuración de ubicación compartida, la dirección de la máquina servidor con ubicación compartida *no* tiene que ser idéntica a la dirección de no reenvío (NFA). Puede utilizar otra dirección si la máquina se ha definido con varias direcciones IP. Para el componente Dispatcher, el servidor con ubicación compartida debe definirse como **collocated** utilizando el mandato **dscontrol server**. Para obtener más información sobre los servidores con ubicación compartida, consulte el apartado “Utilización de servidores con ubicación compartida” en la página 203.

Para obtener más información sobre la sintaxis del mandato `dscontrol server`, consulte el apartado “`dscontrol server` — configurar servidores” en la página 392.

Paso 8. Iniciar la función de gestor (opcional)

La función de gestor mejora el equilibrio de carga. Para iniciar el gestor, escriba el mandato **dscontrol manager start**, edite el archivo de configuración de ejemplo o utilice la GUI.

Paso 9. Iniciar la función de asesor (opcional)

Los asesores proporcionan al gestor más información sobre la capacidad que tienen de las máquinas de servidor con equilibrio de carga para responder a las peticiones. Un asesor es específico de un protocolo. Por ejemplo, para iniciar el asesor HTTP, emita el siguiente mandato:

```
dscontrol advisor start http puerto
```

Para obtener una lista de asesores junto con sus puertos por omisión, consulte el Capítulo 27, “Referencia de mandatos para Dispatcher y CBR”, en la página 347. Para obtener una descripción de cada asesor, consulte el apartado “Lista de asesores” en la página 188.

Paso 10. Definir las proporciones del clúster según sea necesario

Si inicia asesores, puede modificar la proporción de la importancia dada a la información de asesor que se incluye en las decisiones para el equilibrio de carga.

Para definir las proporciones del clúster, emita el mandato **dscontrol cluster set clúster proportions**. Para obtener más información, consulte el apartado “Proporción de la importancia otorgada a la información de estado” en la página 180.

Configuración de máquinas de servidor para el equilibrio de carga

Realice los siguientes pasos si una de estas condiciones es true:

- Si utiliza el método de reenvío MAC y es una máquina servidor de programa de fondo.
- Si utiliza el método de reenvío MAC y éste es un servidor con ubicación compartida configurado como máquina en espera de alta disponibilidad.

Notas:

1. Los procedimientos para suprimir los alias del bucle de retorno deberán indicarse en los scripts go* por si la máquina pasara a activa.
2. Si se ha configurado como máquina activa de alta disponibilidad, los procedimientos para crear alias del bucle de retorno deberán indicarse en los scripts go* por si la máquina pasa a estar en espera.

Al utilizar el método de reenvío MAC, Dispatcher sólo equilibrará la carga en servidores que permiten que el adaptador de bucle de retorno se configure con una dirección IP adicional, para la que el servidor de programa de fondo nunca responderá a las peticiones ARP (protocolo de resolución de direcciones). Para configurar las máquinas de servidor con equilibrio de carga, siga los pasos indicados en este apartado.

Paso 1. Crear un alias para el dispositivo de bucle de retorno

Para que las máquinas de servidor con equilibrio de carga funcionen, debe establecer (o preferiblemente asignar un alias) el dispositivo de bucle de retorno (a menudo llamado lo0) en la dirección del clúster. Cuando se utiliza el método de reenvío mac, el componente Dispatcher no cambia la dirección IP de destino en el paquete TCP/IP antes de reenviar el paquete a una máquina servidor TCP. Si se establece o crea un alias del bucle de retorno para la dirección de clúster, las máquinas de servidor con equilibrio de carga aceptarán un paquete que iba dirigido a la dirección del clúster.

Si utiliza un sistema operativo que da soporte a los alias de interfaz de red (como los sistemas AIX, HP-UX, Linux, Solaris o Windows), debe crear un alias del dispositivo de bucle de retorno para la dirección de clúster. La ventaja de utilizar un sistema operativo que dé soporte a los alias es la capacidad de poder configurar las máquinas de servidores con equilibrio de carga de modo que presten servicio para varias direcciones de clúster.

IMPORTANTE: en sistemas Linux, consulte el apartado “Alternativas de alias de bucle de retorno de Linux cuando se utiliza el reenvío MAC de Load Balancer” en la página 78.

Si dispone de un servidor con un sistema operativo que no da soporte a los alias, debe establecer el bucle de retorno para la dirección del clúster.

Utilice el mandato correspondiente al sistema operativo, tal como se muestra en la Tabla 5 en la página 73 para establecer u otorgar un alias al dispositivo de bucle de retorno.

Tabla 5. Mandatos para crear alias del dispositivo de bucle de retorno (lo0) para Dispatcher

AIX 4.3 o anteriores	ifconfig lo0 alias dirección_clúster netmask máscara_red Nota: Utilice la máscara de red del adaptador primario
AIX 5.x	ifconfig lo0 alias dirección_clúster netmask 255.255.255.255
HP-UX	ifconfig lo0:1 dirección_clúster up
Linux	<p>Seleccione uno de los siguientes mandatos:</p> <ul style="list-style-type: none"> • ip -4 addr add dirección_clúster/32 dev lo • ifconfig lo:1 dirección_clúster netmask 255.255.255.255 up <p>IMPORTANTE: Una vez que ha emitido uno de los mandatos de configuración en la máquina, utilice siempre el mismo mandato de configuración (ip o ifconfig) o se pueden producir resultados imprevistos.</p>
OS/2	ifconfig lo dirección_clúster
OS/390	<p>Configuración de un alias de bucle de retorno en el sistema OS/390</p> <ul style="list-style-type: none"> • En el miembro (archivo) del parámetro IP, será necesario que un administrador cree una entrada en la lista de direcciones locales. Por ejemplo <pre>HOME ;Address Link 192.168.252.11 tr0 192.168.100.100 ltr1 192.168.252.12 loopback</pre> <ul style="list-style-type: none"> • Pueden definirse varias direcciones para el bucle de retorno. • Por omisión, se configura la dirección de bucle de retorno 127.0.0.1.
Solaris 7	ifconfig lo0:1 dirección_clúster 127.0.0.1 up
Solaris 8, Solaris 9 y Solaris 10	ifconfig lo0:1 plumb dirección_clúster netmask máscara_red up

Tabla 5. Mandatos para crear alias del dispositivo de bucle de retorno (lo0) para Dispatcher (continuación)

Windows Server 2003	<ol style="list-style-type: none"> 1. Pulse Inicie y después pulse Panel de control. 2. Si todavía no lo ha hecho, añada el Controlador MS Loopback Adapter. <ol style="list-style-type: none"> a. Pulse Agregar hardware. De esta manera se iniciará el asistente para añadir hardware. b. Pulse Siguiente c. Seleccione Sí, ya he conectado el hardware y pulse Siguiente. d. Si MS Loopback Adapter ya aparece en la lista, es que ya está instalado; pulse Cancelar para salir. e. Si MS Loopback Adapter <i>no</i> está en la lista, seleccione Agregar un dispositivo nuevo y pulse Siguiente. f. Para seleccionar el hardware de una lista, para el panel Buscar nuevo hardware, pulse No y después Siguiente. g. Seleccione Adaptadores de red y pulse Siguiente. h. En el panel Seleccionar adaptador de red, seleccione Microsoft en la lista Fabricantes y, a continuación, seleccione Microsoft Loopback Adapter. i. Pulse Siguiente y, a continuación, vuelva a pulsar Siguiente para instalar los valores por omisión (o seleccione Utilizar disco y, a continuación, inserte el CD y realice la instalación desde aquí). j. Pulse Finalizar para terminar la instalación. 3. En el Panel de control, haga una doble pulsación en Conexiones de red y de acceso telefónico. 4. Seleccione la conexión con Nombre de dispositivo "Microsoft Loopback Adapter". 5. Seleccione Propiedades en el menú desplegable. 6. Seleccione Protocolo de Internet (TCP/IP) y pulse Propiedades. 7. Pulse Utilizar la siguiente dirección IP. Rellene la <i>dirección IP</i> con la dirección de clúster y la <i>máscara de subred</i> con la máscara de subred del servidor del programa de fondo. Nota: No entre una dirección de direccionador. Utilice el localhost como el servidor DNS por omisión.
---------------------	--

Tabla 5. Mandatos para crear alias del dispositivo de bucle de retorno (lo0) para Dispatcher (continuación)

Windows 2000	<ol style="list-style-type: none"> 1. Pulse Inicio, Configuración y después Panel de control. 2. Si todavía no lo ha hecho, añada el Controlador MS Loopback Adapter. <ol style="list-style-type: none"> a. Efectúe una doble pulsación en Agregar/quitar hardware. De esta manera se iniciará el asistente para agregar/quitar hardware. b. Pulse Siguiente, seleccione Añadir/Resolución de problemas de un dispositivo y pulse Siguiente. c. La pantalla parpadea y presenta el panel Elegir un dispositivo de hardware. d. Si MS Loopback Adapter ya aparece en la lista, es que ya está instalado; pulse Cancelar para salir. e. Si MS Loopback Adapter <i>no</i> está en la lista, seleccione Agregar un dispositivo nuevo y pulse Siguiente. f. Para seleccionar el hardware de una lista, para el panel Buscar nuevo hardware, pulse No y después Siguiente. g. Seleccione Adaptadores de red y pulse Siguiente. h. En el panel Seleccionar adaptador de red, seleccione Microsoft en la lista Fabricantes y, a continuación, seleccione Microsoft Loopback Adapter. i. Pulse Siguiente y, a continuación, vuelva a pulsar Siguiente para instalar los valores por omisión (o seleccione Utilizar disco y, a continuación, inserte el CD y realice la instalación desde aquí). j. Pulse Finalizar para terminar la instalación. 3. En el Panel de control, haga una doble pulsación en Conexiones de red y de acceso telefónico. 4. Seleccione la conexión con Nombre de dispositivo "Microsoft Loopback Adapter" y pulse el botón derecho del ratón en el mismo. 5. Seleccione Propiedades en el menú desplegable. 6. Seleccione Protocolo de Internet (TCP/IP) y pulse Propiedades. 7. Pulse Utilizar la siguiente dirección IP. Rellene la <i>dirección IP</i> con la dirección del clúster y la <i>máscara de subred</i> con la máscara de subred por omisión (255.0.0.0). Nota: No entre una dirección de direccionador. Utilice el localhost como el servidor DNS por omisión.
--------------	---

Tabla 5. Mandatos para crear alias del dispositivo de bucle de retorno (lo0) para Dispatcher (continuación)

Windows NT	<ol style="list-style-type: none"> 1. Pulse Inicio y después Configuración. 2. Pulse Panel de control y, a continuación, pulse una doble pulsación en Red. 3. Si todavía no lo ha hecho, añada el Controlador MS Loopback Adapter. <ol style="list-style-type: none"> a. En la ventana Red, pulse Adaptadores. b. Seleccione MS Loopback Adapter y pulse Aceptar. c. Cuando se le solicite, inserte los discos o el CD de instalación. d. En la ventana Red, pulse Protocolos. e. Seleccione Protocolo TCP/IP y pulse Propiedades. f. Seleccione MS Loopback Adapter y pulse Aceptar. 4. Establezca la dirección de bucle de retorno para su dirección de clúster. Acepte la máscara de subred por omisión (255.0.0.0) y no especifique una dirección de pasarela. <p>Nota: Puede que tenga que salir y volver a entrar en la configuración de la red antes de que MS Loopback Driver aparezca bajo la configuración TCP/IP.</p>
------------	--

Paso 2. Comprobar si hay una ruta adicional

En algunos sistemas operativos, es posible que se haya una ruta por omisión y es necesario eliminarla.

- Compruebe si hay una ruta adicional en los sistemas operativos Windows con el siguiente mandato:

```
route print
```

IMPORTANTE: En Windows 2003 se deben ignorar todas las rutas adicionales.

Si se detectan problemas con el direccionamiento después de la creación de alias, elimine el alias y vuélvalo a añadir utilizando una máscara de red distinta.

- Compruebe si hay una ruta adicional en todos los Sistemas Linux y UNIX con el siguiente mandato:

```
netstat -nr
```

Ejemplo de Windows:

1. Tras escribir **route print**, aparecerá una tabla parecida al ejemplo siguiente. (Este ejemplo muestra cómo localizar y eliminar una ruta adicional para el clúster 9.67.133.158 con una máscara de subred por omisión de 255.0.0.0).

Rutas activas:

Dirección red	Máscara de red	Direc. pasarela	Interfaz	Métrica
0.0.0.0	0.0.0.0	9.67.128.1	9.67.133.67	1
9.0.0.0	255.0.0.0	9.67.133.158	9.67.133.158	1
9.67.128.0	255.255.248.0	9.67.133.67	9.67.133.67	1
9.67.133.67	255.255.255.255	127.0.0.1	127.0.0.1	1
9.67.133.158	255.255.255.255	127.0.0.1	127.0.0.1	1
9.255.255.255	255.255.255.255	9.67.133.67	9.67.133.67	1
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
224.0.0.0	224.0.0.0	9.67.133.158	9.67.133.158	1
224.0.0.0	224.0.0.0	9.67.133.67	9.67.133.67	1
255.255.255.255	255.255.255.255	9.67.133.67	9.67.133.67	1

2. Busque la dirección del clúster en la columna "Dirección de pasarela". Si tiene una ruta adicional, la dirección del clúster aparecerá dos veces. En el ejemplo dado, la dirección del clúster (9.67.133.158) aparece en la fila 2 y la fila 8.

- Busque la dirección de red en cada fila en la que aparece la dirección del clúster. Necesitará una de estas rutas y deberá suprimir la otra que sobra. La ruta adicional que debe suprimirse es la ruta cuya dirección de red empieza por el primer dígito de la dirección de clúster, seguida de tres ceros. En el ejemplo siguiente, la ruta adicional es la que aparece en la fila dos, que tiene la dirección de red **9.0.0.0**:

```
9.0.0.0    255.0.0.0    9.67.133.158    9.67.133.158    1
```

Paso 3. Suprimir todas las rutas adicionales

Debe suprimir la ruta adicional. Utilice el mandato correspondiente al sistema operativo que se muestra en la Tabla 6 para suprimir la ruta adicional.

Ejemplo: para suprimir la ruta adicional tal como se muestra en la tabla de ejemplo "Rutas activas" para el paso 2, escriba:

```
route delete 9.0.0.0 9.67.133.158
```

Tabla 6. Mandatos para suprimir todas las rutas adicionales para Dispatcher

HP-UX	route delete <i>dirección_clúster</i> <i>dirección_clúster</i>
Windows	route delete <i>dirección_red</i> <i>dirección_clúster</i> (en un indicador MS-DOS) Nota: Cada vez que reinicie el sistema debe suprimir la ruta adicional. En Windows 2003, no es posible suprimir rutas. En Windows 2003 se deben ignorar todas las rutas adicionales. Si se detectan problemas con el direccionamiento después de la creación de alias, elimine el alias y vuélvalo a añadir utilizando una máscara de red distinta.

Si se utiliza el ejemplo que se muestra en la Figura 15 en la página 68 y se configura una máquina servidor que se ejecuta en un sistema AIX, el mandato sería:

```
route delete -net 204.0.0.0 204.67.172.72
```

Paso 4. Verificar que el servidor esté configurado correctamente

Para verificar si un servidor de programa de fondo está configurado correctamente, siga los pasos siguientes desde una máquina distinta que esté en la misma subred cuando Load Balancer no esté configurado y el clúster no esté configurado:

- Emita el mandato:

```
arp -d clúster
```

- Emita el mandato:

```
ping clúster
```

No debe haber ninguna respuesta. Si hay una respuesta al mandato ping, asegúrese de que no se haya ejecutado el mandato ifconfig y se haya asociado la dirección del clúster con la interfaz. Asegúrese de que no haya ninguna máquina con una entrada ARP publicada para la dirección de clúster.

- Emita el mandato ping al servidor de programa de fondo e inmediatamente después emita el mandato:

```
arp -a
```

En la salida del mandato, debería ver la dirección MAC del servidor. Emita el mandato:

```
arp -s clúster dirección_mac_servidor
```

4. Emita el mandato ping al clúster. Se debe obtener una respuesta. Emita una petición http, telnet u otra petición dirigida al clúster que tiene previsto que maneje el servidor de programa de fondo. Asegúrese de que funciona correctamente.
5. Emita el mandato:
`arp -d clúster`
6. Emita el mandato ping al clúster. No debe haber ninguna respuesta.

Nota: Si hay una respuesta, emita una instrucción `arp clúster` para obtener la dirección MAC de la máquina mal configurada. A continuación, repita los pasos 1 a 6.

Alternativas de alias de bucle de retorno de Linux cuando se utiliza el reenvío MAC de Load Balancer

Algunas versiones de sistemas Linux emiten respuestas ARP para cualquier dirección IP configurada en la máquina en cualquier interfaz que exista en la máquina. También puede elegir una dirección IP de origen para consultas ARP who-has en función de todas las direcciones IP que existen en la máquina, independientemente de las interfaces en las que se han configurado esas direcciones. Esto provoca que todo el tráfico del clúster se dirija a un solo servidor de una manera indeterminada.

Cuando se utiliza el método de reenvío MAC de Dispatcher, debe emplearse un mecanismo que garantice que las pilas de servidores de programas de fondo puedan aceptar el tráfico dirigido al clúster, incluida la máquina en espera de alta disponibilidad con ubicación compartida, cuando se utilizan simultáneamente la alta disponibilidad y la ubicación compartida.

En la mayoría de los casos, debe otorgar un alias a la dirección de clúster en el bucle de retorno; por lo tanto, los servidores de programas de fondo deben tener un alias del clúster en el bucle de retorno, y si utiliza la alta disponibilidad y la ubicación compartida, los servidores de equilibrio de carga en espera deben tener alias de clúster en el bucle de retorno.

Para asegurarse de que sistemas Linux no publican direcciones en el bucle de retorno, puede utilizar cualquiera de las cuatro soluciones siguientes para hacer que sistemas Linux sea compatibles con el reenvío MAC de Dispatcher.

1. Utilice un kernel que no publique las direcciones. Esta es la opción preferida, ya que no provoca una actividad adicional por paquete y no requiere una reconfiguración por kernel.

- United Linux 1 / SLES8 con SP2(x86) o SP3 (las demás arquitecturas) y posterior contiene el parche oculto Julian ARP. Asegúrese de que siempre está en vigor antes de crear un alias para la dirección de clúster con el mandato:

```
# sysctl -w net.ipv4.conf.all.hidden=1 net.ipv4.conf.lo.hidden=1
```

Después se pueden crear alias de los clústeres de la forma normal, como:

```
# ifconfig lo:1 $CLUSTER_ADDRESS netmask 255.255.255.255 up
```

- Utilice `arp_ignore sysctl`, disponible en las versiones 2.4.25 y 2.6.5 y posteriores, aunque debe tener en cuenta que las distribuciones algunas veces incluyen características de otras versiones. Antes de crear alias para las direcciones de clúster asegúrese de que se ha habilitado mediante los mandatos:

```
# sysctl -w net.ipv4.conf.all.arp_ignore=3
net.ipv4.conf.all.arp_announce=2
```

A continuación, debe crear alias a los clústeres con el siguiente mandato:

```
# ip addr add $CLUSTER_ADDRESS/32 scope host dev lo
```

Se debe especificar un mandato similar en los scripts go* de la configuración con ubicación compartida de alta disponibilidad.

- Nota: al utilizar sysctl, asegúrese de que estos valores seguirán en vigor después de sucesivos rearranques añadiendo los valores en /etc/sysctl.conf.

2. Utilice tablas IP para redirigir todo el tráfico de clúster entrante hacia el sistema principal local. Si utiliza este método, no configure el adaptador de bucle de retorno con un alias. En su lugar, utilice el mandato:

```
# iptables -t nat -A PREROUTING -d $CLUSTER_ADDRESS -j REDIRECT
```

Este mandato hace que los sistemas Linux realicen una conversión de direcciones de red (NAT) de destino en cada paquete, que convierte la dirección del clúster en la dirección de interfaz. Este método tiene aproximadamente una penalización en el rendimiento del 6,4% de conexiones por segundo. Este método funciona en cualquier distribución de stock soportada; no es necesario ningún módulo kernel ni aplicar parche, compilarlo e instalarlo en el kernel.

3. Aplique la versión 1.2.0 o posterior del módulo noarp. El código fuente del kernel debe estar disponible y configurado correctamente; también deben estar disponibles las herramientas de desarrollo (gcc, gnu make, etc.). Cada vez que se amplía el kernel se debe compilar e instalar el módulo. Está disponible en <http://www.masarlabs.com/noarp/>. Puesto que el código del kernel por sí mismo no se modifica, es menos intrusiva que la solución número 4 (indicada más abajo) y es menos propensa a errores. También debe configurarse antes de crear un alias de dirección de clúster en el bucle de retorno. Por ejemplo:

```
# modprobe noarp
# noarpctl add $CLUSTER_ADDRESS dir_primaria_nic
```

donde *dir_primaria_nic* es una dirección en la misma subred que la dirección de clúster. Después se pueden crear alias de los clústeres de la forma normal, como:

```
# ifconfig lo:1 dirección_clúster netmask 255.255.255.255 up
```

Nota: Para las configuraciones con ubicación compartida de alta disponibilidad, se debe indicar noarpctl adds y dels en los scripts go*. Esto asegura que el sistema Load Balancer activo pueda utilizar ARP para la dirección del clúster y que el sistema Load Balancer en espera, que actúa como servidor, no empiece a recibir de forma accidental (es decir, de forma indeterminada) todo el tráfico del clúster.

4. Obtenga el parche Julian en el siguiente sitio Web: <http://www.ssi.bg/~ja/#hidden>. Siga las instrucciones de distribuciones para aplicar el parche y compilar un kernel apto para su uso con dicha distribución. Si es un sistema Load Balancer de alta disponibilidad con ubicación compartida, asegúrese de que uname -r coincida con el kernel suministrado por la distribución, así como que empiece con el archivo .config del kernel de distribución. Después de compilar, instalar y ejecutar el kernel con el parche oculto Julian, siga las instrucciones especificadas bajo la primera solución descrita para habilitar el parche.

Nota: Si se ejecuta un kernel personalizado, puede tener consecuencias en el soporte de la distribución.

Capítulo 8. Despliegue de Dispatcher en Load Balancer para IPv4 y IPv6

Hay soporte disponible para el esquema de direccionamiento IP ampliado de IPv6 con Load Balancer para IPv4 y IPv6. Load Balancer para IPv4 y IPv6 es una imagen de instalación aparte que únicamente consta del componente Dispatcher. El tipo de instalación proporciona el equilibrio de carga para el tráfico de IPv4 e IPv6 a servidores configurados dentro de la red que utilizan el reenvío de paquetes según el método MAC de Dispatcher.

En este capítulo se describen las diferencias de configuración y las limitaciones de Dispatcher en la instalación Load Balancer para IPv4 y IPv6 de este producto y se incluyen estos apartados:

- “Plataformas admitidas para Load Balancer para IPv4 y IPv6” en la página 82
- “Instalación de Load Balancer para IPv4 y IPv6” en la página 83
- “Consideraciones especiales y limitaciones para Load Balancer para IPv4 y IPv6” en la página 83
- “Habilitar el proceso de paquetes IPv6 en Load Balancer para IPv4 y IPv6” en la página 88
- “Creación de alias del dispositivo de interfaz en Load Balancer para IPv4 y IPv6” en la página 88
- “Pasos de configuración de clúster requeridos para Linux en zSeries” en la página 91
- “Mandatos de Dispatcher (dscontrol) para Load Balancer para IPv4 y IPv6” en la página 92

Si desea información general sobre el componente Dispatcher, consulte los apartados y capítulos siguientes:

- Si desea obtener una visión general de características de Dispatcher que están disponibles para gestionar la red consulte el apartado “Características del componente Dispatcher” en la página 19.
- Si desea información sobre cómo planificar parámetros de equilibrio de carga de Dispatcher, consulte el Capítulo 6, “Planificación de Dispatcher”, en la página 51.
- Si desea información sobre cómo configurar parámetros de equilibrio de carga de Dispatcher, consulte el Capítulo 7, “Configuración de Dispatcher”, en la página 63.
- Si desea información sobre cómo configurar Load Balancer para obtener funciones más avanzadas, consulte el Capítulo 22, “Características avanzadas para Dispatcher, CBR y Site Selector”, en la página 201.
- Si desea información sobre archivos de anotaciones cronológicas de Load Balancer y el uso de los componentes de Load Balancer consulte el Capítulo 24, “Operación y gestión de Load Balancer”, en la página 261.

Es importante observar que con la instalación de Load Balancer para IPv4 y IPv6, la sintaxis de mandato de Dispatcher (dscontrol) es idéntica con una excepción. El delimitador de mandatos dscontrol es un símbolo arroba (@), en lugar de dos puntos (:), cuando se utiliza Load Balancer para IPv4 y IPv6. Donde se haga referencia a mandatos en otros capítulos de este documento, recuerde sustituir (@) por (:) como el delimitador dentro de mandatos dscontrol.

Plataformas admitidas para Load Balancer para IPv4 y IPv6

Hay instalaciones Load Balancer para IPv4 y IPv6 disponibles para todas las plataformas admitidas con la excepción de Windows 2000.

Si desea información sobre los requisitos del sistema de hardware y software, visite la siguiente página Web: <http://www.ibm.com/support/docview.wss?rs=180&uid=swg27006921>

Plataformas admitidas para el equilibrio de carga en espacio de usuario

En algunas plataformas admitidas, como todas las arquitecturas Linux, las instalaciones de Load Balancer para IPv4 y IPv6 ejecutan procesos de equilibrio de carga de espacio de usuario en lugar de hacerlo en espacio de kernel. Para los sistemas, ya no hay dependencia del módulo de kernel.

Para obtener la información más reciente sobre qué plataformas admiten el equilibrio de carga en el espacio de usuario (sin kernel), consulte el siguiente sitio Web: <http://www.ibm.com/support/docview.wss?rs=180&uid=swg27006921>.

Los sistemas admitidos que ejecutan procesos de equilibrio de carga en espacio de usuario tienen procedimientos de configuración distintos de aquellos sistemas que ejecutan procesos de equilibrio de carga en espacio de kernel. Estas diferencias se tratarán en este apartado sobre Load Balancer para IPv4 y IPv6.

Consideraciones especiales de la plataforma Linux

Linux en sistemas zSeries

- **Linux en sistemas zSeries requiere libstdc++.so.5:** existe un requisito que Linux en sistemas zSeries deben tener rpm paquete libstdc++.so.5 para poderse instalar correctamente; de lo contrario, la instalación no se realizará correctamente.
- **Restricción cuando se utiliza la interfaz qeth/OSA:** en Linux en sistemas zSeries, existe una restricción cuando se utiliza una interfaz qeth/OSA. No se da soporte al reenvío de forma nativa fuera de una interfaz qeth/OSA. No obstante, existe un método alternativo porque los sistemas Linux se ejecutan en espacio de usuario y pueden dar soporte a la transmisión a través de túnel de Linux.

Soporte de transmisión a través de túnel de Linux

En sistemas Linux, las instalaciones de Load Balancer para IPv4 y IPv6 pueden reenviar a través de túneles como IPIP y IPGRE. Cuando se utiliza Linux en máquinas zSeries con una interfaz qeth/OSA, se puede definir un túnel Linux que atraviese la interfaz qeth/OSA. Los sistemas Linux pueden realizar reenvíos entre máquinas que se encuentran en los mismos dispositivos qeth/OSA o en otros, o en cualquier otro sitio de la red.

Restricciones de servidores de programa de fondo

Sistemas Solaris: no se da soporte al equilibrio de carga del tráfico IPv6 a los servidores de programa de fondo Solaris 5.8. En Solaris 5.8, existe una incompatibilidad con un paquete IPv6 reenviado por MAC y la pila IPv6 de Solaris. Cuando se configura el clúster en un servidor de programa de fondo Solaris 5.8 mediante el mandato `ifconfig lo0 (loopback)`, el paquete llega al nodo Solaris 5.8, pero no se acepta. No obstante, puede utilizar las instalaciones de Load Balancer para IPv4 y IPv6 para equilibrar la carga del tráfico IPv4 a los servidores de programa de fondo Solaris 5.8.

Sistemas z/OS: no se da soporte al equilibrio de carga del tráfico IPv6 a servidores de programa de fondo z/OS. No obstante, puede equilibrar la carga del tráfico IPv4 a los servidores de programa de fondo z/OS mediante instalaciones de Load Balancer para IPv4 y IPv6.

Instalación de Load Balancer para IPv4 y IPv6

En Load Balancer para IPv4 y IPv6, los pasos de instalación y los nombres de paquete son iguales que los pasos de instalación y los nombres de paquete de Load Balancer que admite sólo direcciones de servidor IPv4. No obstante, se proporcionan menos paquetes del componente Load Balancer, porque sólo está disponible el componente Dispatcher.

Cuando se utilizan herramientas de paquetes del sistema, el orden recomendado para instalar los paquetes es ligeramente distinto para las instalaciones de Load Balancer para IPv4 y IPv6. El paquete de componente de administración debe instalarse después del paquete del componente Dispatcher. El orden recomendado para instalar paquetes para Load Balancer para IPv4 y IPv6 utilizando las herramientas de paquetes del sistema es el siguiente: base, licencia, componente Dispatcher, administración, documentación, Metric Server

Por ejemplo, para los sistemas AIX a continuación se muestra una lista de los paquetes de Load Balancer para IPv4 y IPv6 en el orden recomendado de instalación:

- `ibmlb.base.rte` (paquete base)
- `ibmlb.lb.license` (paquete de licencia, si se instala desde CD)
- `ibmlb.lb.driver` (paquete de controlador de dispositivo, que es un paquete exclusivo sólo para AIX)
- `ibmlb.disp.rte` y `ibmlb.msg.idioma.lb` (paquete del componente Dispatcher con paquetes de mensajes)
- `ibmlb.admin.rte` y `ibmlb.msg.idioma.admin` (paquete de administración con paquete de mensajes)
- `ibmlb.doc.rte` y `ibmlb.msg.en_US.doc` (paquete de documentación con paquete de mensajes)
- `ibmlb.ms.rte` (paquete de Metric Server)

Es importante observar que hay que desinstalar cualquier versión anterior de Load Balancer antes de instalar Load Balancer para IPv4 y IPv6. No pueden instalarse dos Load Balancers en la misma máquina.

Para obtener instrucciones de instalación del producto, consulte el Capítulo 4, “Instalación de Load Balancer”, en la página 31.

Consideraciones especiales y limitaciones para Load Balancer para IPv4 y IPv6

El componente Dispatcher ofrece muchas, pero no todas, de las funciones disponibles con el componente Dispatcher en instalaciones de Load Balancer que admiten sólo IPv4. En los temas siguientes se describen las diferencias de configuración especiales y las limitaciones funcionales de Dispatcher proporcionadas con Load Balancer para IPv4 y IPv6.

Configurar dirección local de enlace de IPv6

Con el direccionamiento IPv6, cada máquina de la configuración de Load Balancer debe tener una dirección local de enlace de IPv6.

La dirección local de enlace es la dirección utilizada para el tráfico de descubrimiento cercano para IPv6. Sin esta dirección en la máquina de Load Balancer y en los servidores de programa de fondo, el descubrimiento cercano no se produce y las máquinas no se detectan entre sí. Load Balancer para IPv6 no puede reenviar tráfico sin tener configurada una dirección IPv6 local de enlace en una interfaz de cada máquina de la configuración de Load Balancer.

Pares de clúster/servidor homogéneos

Cuando configura Load Balancer para IPv4 y IPv6, todos los servidores deben ser homogéneos dentro del clúster. Por ejemplo, si se define Clúster1 con una dirección IPv4, todos los servidores bajo Clúster1 deben ser IPv4. Si se define Clúster2 con una dirección IPv6, todos los servidores definidos bajo Clúster2 deben ser IPv6. Además, el protocolo que el cliente utiliza para enviar paquetes IP tiene que tener el mismo formato IP del clúster.

El soporte de un entorno cliente IPv4 e IPv6 combinado requiere que para cada definición de clúster lógico, deben definirse dos definiciones de clúster reales – un clúster IPv4 y un clúster IPv6. Load Balancer direcciona los clientes que envían paquetes IPv4 al clúster lógico utilizando direcciones IPv4 configuradas para el clúster. Load Balancer direcciona los clientes que envían paquetes IPv6 al clúster lógico utilizando direcciones IPv6 configuradas para el clúster.

Características de Dispatcher no admitidas

Muchas de las características de Dispatcher descritas en el Capítulo 6, “Planificación de Dispatcher”, en la página 51 y las que se describen en el Capítulo 22, “Características avanzadas para Dispatcher, CBR y Site Selector”, en la página 201 están disponibles en Load Balancer para IPv4 y IPv6.

A continuación figura una lista de resumen de las características de Dispatcher que *no* se admiten en Load Balancer para IPv4 y IPv6:

- cbr, método de reenvío
- nat, método de reenvío
- administración remota
- equilibrio de carga basado en normas
- subagente SNMP
- equilibrio de carga de área amplia
- soporte del protocolo UDP

Si desea obtener una descripción de alto nivel de características de Dispatcher que están disponibles para gestionar la red consulte el apartado “Características del componente Dispatcher” en la página 19.

Configuración de asesores

Si utiliza el protocolo IPv6 en la máquina y desea utilizar asesores, debe asegurarse de que la siguiente línea está incluida en el archivo de **protocolo**.

```
ipv6-icmp 58 IPv6-ICMP
```

En los sistemas Linux y UNIX, el archivo de protocolo reside en el directorio `/etc/protocols`. En los sistemas Windows, el archivo de protocolo reside en el directorio `C:\windows\system32\drivers\etc\`.

Restricción cuando se utilizan asesores: si Load Balancer se está ejecutando en un sistema con varias tarjetas de adaptador de red, no puede forzar que la dirección IP de origen del paquete sea una dirección específica cuando desea que el tráfico del asesor fluya sobre un adaptador concreto. (La propiedad `-DLB_ADV_SRC_ADDR` no está disponible para utilizarse con instalaciones de Load Balancer para IPv4 y IPv6.)

Si desea más información sobre asesores, consulte el apartado “Asesores” en la página 248.

Configuración de la alta disponibilidad

Si utiliza el protocolo IPv6 en la máquina y desea utilizar la alta disponibilidad, debe comprobar si `protocol 58` está definido como ICMPv6 en el archivo de **protocolo**. Si desea información sobre cómo editar el archivo de protocolo, consulte “Configuración de asesores” en la página 84.

En instalaciones de Load Balancer para IPv4 y IPv6, se admite la configuración de una máquina de Dispatcher de alta disponibilidad con las siguientes limitaciones o consideraciones especiales:

- No se admite la alta disponibilidad mutua.
- Los pares de pulsos (que es el mecanismo entre los Dispatchers primario y de reserva para detectar anomalías de Dispatcher) deben estar ambos en formato IPv4 o ambos en formato IPv6.
- En sistemas que se ejecutan en espacio de usuario, como los sistemas Linux: en un entorno de alta disponibilidad o un entorno autónomo, no debe poner un alias a la dirección de clúster para el adaptador de red.
- En sistemas que se ejecutan en espacio de usuario, como los sistemas Linux: los scripts `go*` y `highavailChange` pueden trasladarse del directorio `.../ibm/edge/lb/servers/samples` al directorio `.../ibm/edge/lb/servers/bin` para anotar los cambios de estado de alta disponibilidad de la máquina Dispatcher, aunque no es necesario cambiar estos scripts.
- Para Linux en sistemas zSeries que utilizan una interfaz qeth/OSA: sólo para este tipo de interfaz de red, no se aplica la prohibición general de utilizar alias de interfaz para las direcciones de clúster. En su lugar, utilice el siguiente procedimiento para asegurarse de que el tráfico de clúster se entrega al invitado Linux a través de un adaptador OSA:
 - Los scripts `go*` son necesarios y deben modificarse tal como se indica a continuación con los mandatos especificados en “Pasos de configuración de clúster requeridos para Linux en zSeries” en la página 91:
 - `goActive`: añada los mandatos `ip` y `iptables/ip6tables` para configurar la dirección de clúster y añada la norma `iptables`.
 - `goStandby`: añada los mandatos `ip` y `iptables/ip6tables` para desconfigurar la dirección de clúster y elimine la norma `iptables`.
 - `goInOp`: añada los mandatos `ip` y `iptables/ip6tables` para desconfigurar la dirección de clúster y eliminar la norma `iptables`.
 - `goIdle`: este script no debe crearse.

Si desea más información sobre la característica de alta disponibilidad, consulte el apartado “Alta disponibilidad” en la página 204.

Ubicación compartida de servidores

La ubicación compartida es una configuración en la que Load Balancer puede residir en la misma máquina que un servidor para el que equilibra la carga de peticiones.

Al utilizar instalaciones de Load Balancer para IPv4 y IPv6, la característica de ubicación compartida está disponible en todos los sistemas operativos soportados, excepto en sistemas Windows y en sistemas que se ejecutan en espacio de usuario, como los sistemas Linux.

Para obtener más información sobre los servidores con ubicación compartida, consulte el apartado “Utilización de servidores con ubicación compartida” en la página 203.

Característica de afinidad para sistemas que se ejecutan en espacio de usuario (Linux)

La característica de afinidad de Load Balancer para sistemas que se ejecutan en espacio de usuario, como sistemas Linux, funciona de forma distinta que la característica de afinidad de otros sistemas operativos que se ejecutan en el espacio de kernel.

Para los sistemas que se ejecutan en el espacio de usuario, Load Balancer correlaciona una dirección IP de cliente con un servidor de programa de fondo. La afinidad se establece una vez que coincide con el clúster la dirección IP de destino de un paquete, el puerto de destino coincide con el puerto de Load Balancer y la dirección IP de origen coincide.

Cuando la afinidad está establecida, los paquetes subsiguientes se envían al mismo servidor de programa de fondo. Cuando la afinidad se interrumpe, debido a que un servidor está apagado o se ha eliminado, se interrumpe toda la afinidad, y por consiguiente, las conexiones a dicho servidor.

Además, en la línea de mandatos o en los clientes de la GUI no aparece información de "conexión". Sólo se utiliza el número de registros de afinidad activos.

Este enfoque ofrece las ventajas de proporcionar una afinidad resistente y de ser más eficaz para Load Balancer.

La desventaja de sistemas que procesan el equilibrio de carga en el kernel es que al utilizar la afinidad IP se incrementa la carga adicional de CPU y memoria para el mecanismo de reenvío de conexiones. En sistemas que procesan el sistema en espacio de usuario, el método de afinidad que se utiliza disminuye el uso de CPU y de memoria si se compara con el reenvío de conexiones.

Además, debido a que este modelo de registro único en sistemas que se ejecutan en espacio de usuario, los valores stickytime y staletimeout asociados con la afinidad se han fusionado en un solo valor: staletimeout. Debido a que si se elimina un registro de afinidad también se interrumpen las conexiones, cuando se migra de un sistema que se procesa en el espacio de kernel a un sistema que se procesa en espacio de usuario, debe utilizarse el valor máximo de staletimeout y stickytime como el nuevo valor de staletimeout para Load Balancer que se ejecuta en el sistema de espacio de usuario.

Para obtener información general sobre la característica de afinidad para sistemas que se procesan en espacio de kernel, a diferencia del espacio de usuario, consulte “Cómo funciona la característica de afinidad para Load Balancer” en la página 221.

Configuración de Metric Server

Si utiliza el protocolo IPv6 en la máquina y desea utilizar Metric Server, debe comprobar si protocolo 58 está definido como ICMPv6 en el archivo **protocol**. Si desea información sobre cómo editar el archivo de protocolo, consulte “Configuración de asesores” en la página 84.

En una configuración de Load Balancer que admita los clústeres IPv4 y IPv6, los servidores que ejecutan la función de Metric Server pueden configurarse únicamente como un servidor IPv4 o únicamente como un servidor IPv6, pero no ambos. Para obligar a Metric Server a utilizar un protocolo, IPv4 o IPv6, especifique la propiedad Java `java.rmi.server.hostname` en el script de `metricserver`.

IMPORTANTE: El `hostname` especificado en la propiedad Java debe ser la dirección IP física del Metric Server.

En sistemas UNIX o Linux: para que Metric Server se comunique a través de la dirección IPV6 `2002:92a:8f7a:162:9:42:92:67`, especifique la propiedad Java después de `$LB_CLASSPATH` en el script de inicio de `metricserver` (en el directorio `/usr/bin`) como se indica a continuación:

```
/opt/ibm/edge/lb/java/jre/bin/java ..... $LB_CLASSPATH
-Djava.rmi.server.hostname=2002:92a:8f7a:162:9:42:92:67
com.ibm.internet.nd.sma.SMA_Agent
$LB_RMIPORT $LOG_LEVEL $LOG_SIZE $LOG_DIRECTORY $KEYS_DIRECTORY
$SCRIPT_DIRECTORY &
```

En sistemas Windows: para que Metric Server se comunique a través de la dirección IPv6 `2002:92a:8f7a:162:9:42:92:67`, debe editar el archivo `metricserver.cmd` (en el directorio `C:\winnt\system32`), como se indica a continuación:

```
start/min /wait %IBMLBPATH%\java\jre\bin\java
-Djava.rmi.server.hostname=2002:92a:8f7a:162:9:42:92:67
-Djava.net.preferIPv4Stack=false
-Djava.net.preferIPv6Stack=true
-Xrs -cp
%LB_CLASSPATH% com.ibm.internet.nd.sma.SMA_Agent
%RMI_PORT% %LOG_LEVEL% %LOG_SIZE% %LOG_DIRECTORY% %KEYS_DIRECTORY%
%SCRIPT_DIRECTORY%
goto done

:stop
%IBMLBPATH%\java\jre\bin\java
-Djava.rmi.server.hostname=2002:92a:8f7a:162:9:42:92:67
-Djava.net.preferIPv4Stack=false
-Djava.net.preferIPv6Stack=true
-cp %LB_CLASSPATH% com.ibm.internet.nd.sma.SMA_AgentStop %RMI_PORT%
:done
```

Para obtener más información, consulte el apartado “Metric Server” en la página 196.

Habilitar el proceso de paquetes IPv6 en Load Balancer para IPv4 y IPv6

En sistemas AIX, Linux y Windows: antes de iniciar el ejecutor (`dscontrol executor start`), debe emitirse lo siguiente desde la línea de mandatos como usuario root:

- Para sistemas AIX: `autoconf6`
Para habilitar el proceso ininterrumpido de paquetes IPv6 (después de un rearranque del sistema), edite el archivo `/etc/rc.tcpip` y elimine la marca de comentario de la siguiente línea y añada el distintivo `-A: start`
`/usr/sbin/autoconf6 " " -A`
- Para sistemas Linux: `modprobe ipv6`
- Para sistemas Windows: `netsh interface ipv6 install`

Estos mandatos habilitan el proceso de paquetes IPv6 en los sistemas operativos respectivos. Emita sólo una vez este mandato. A partir de entonces, puede iniciar y detener el ejecutor tantas veces como sea necesario.

Si no emite el mandato para habilitar el proceso de paquetes IPv6 en estos sistemas, no se iniciará el ejecutor.

En sistemas HP-UX y Solaris: con el mandato `ifconfig`, debe ejecutarse el mandato `plumb` de las direcciones IPv6 y configurarse una interfaz para que Dispatcher inspeccione los paquetes IPv6. Antes de iniciar el ejecutor (`dscontrol executor start`), emita lo siguiente desde la línea de mandatos como usuario root:

- Para sistemas HP-UX:
`ifconfig device inet6 up`
- Para sistemas Solaris:
`ifconfig device inet6 plumb`
`ifconfig device inet6 dirección/prefijo up`

Si no emite estos mandatos, se iniciará el ejecutor, pero no se podrá visualizar ningún paquete IPv6.

Creación de alias del dispositivo de interfaz en Load Balancer para IPv4 y IPv6

Para configurar la dirección del clúster en una tarjeta de interfaz de red (NIC) de la máquina de Dispatcher, puede emitir el mandato `dscontrol executor configure dirección_clúster`. El mandato `dscontrol executor configure` ejecuta los mandatos de configuración de adaptador del sistema operativo (por ejemplo, `ifconfig`, `dsconfig` (sólo IPv6) o mandatos `ip`). De modo alternativo, para poner un alias a la tarjeta NIC de la máquina de Dispatcher puede determinar emitir directamente los mandatos de configuración de adaptador del sistema operativo, en lugar de utilizar el mandato `executor configure`.

Nota: Para los sistemas que se ejecutan en espacio de usuario, como los sistemas Linux: no debe configurar la dirección del clúster utilizando el mandato `dscontrol executor configure` ni con el mandato `ip` o `ifconfig`. Load Balancer anuncia de manera nativa la dirección del clúster en la red. Además, la dirección del clúster no aparecerá con alias en ninguna interfaz. Esto es normal.

Sin embargo, esto **no se aplica** a Linux en zSeries que utilice una interfaz qeth/OSA. Para esta plataforma se deberá configurar la dirección de clúster. Consulte el apartado “Pasos de configuración de clúster requeridos para Linux en zSeries” en la página 91 para obtener más información.

Para poner un alias al dispositivo de bucle de retorno (lo0) en servidores a los que se les está equilibrando la carga, debe utilizar los mandatos de configuración de adaptador del sistema operativo.

Para la instalación de Load Balancer para IPv4 y IPv6, se pueden utilizar estos mandatos para poner un alias a la interfaz de red y al dispositivo de bucle de retorno (*nombre_interfaz*).

En sistemas AIX (5.x):

- Para direcciones IPv6:

```
ifconfig nombre_interfaz inet6 dirección_clúster/longitud_prefijo alias
```

Por ejemplo, para poner un alias al dispositivo de bucle de retorno en servidores a los que se está equilibrando la carga:

```
ifconfig lo0 inet6 2002:4a::541:56/128 alias
```

- Para direcciones IPv4: no hay cambios. Consulte la Tabla 5 en la página 73 para poner un alias al dispositivo de bucle de retorno en servidores a los que se está equilibrando la carga.

En sistemas HP-UX:

- Para direcciones IPv6:

```
ifconfig nombre_interfaz:alias inet6 dirección_clúster up prefix longitud_prefijo
```

Por ejemplo, para poner un alias al dispositivo de bucle de retorno en servidores a los que se está equilibrando la carga:

```
ifconfig lo0:1 inet6 3ffe:34::24:45 up prefix 128
```

- Para direcciones IPv4: no hay cambios. Consulte la Tabla 5 en la página 73 para poner un alias al dispositivo de bucle de retorno en servidores a los que se está equilibrando la carga.

En sistemas Linux:

- Para direcciones IPv6 o IPv4:

```
ip -versión addr add dirección_clúster/longitud_prefijo dev lo
```

Por ejemplo, para poner un alias al dispositivo de bucle de retorno en servidores a los que se está equilibrando la carga:

```
ip -6 addr add 3ffe:34::24:45/128 dev lo
```

```
ip -4 addr add 12.42.38.125/32 dev lo
```

Nota: También puede utilizar el mandato `ifconfig`. Consulte Tabla 5 en la página 73 para poner un alias al dispositivo de bucle de retorno mediante el mandato `ifconfig`.

Una vez que ha emitido uno de los mandatos de configuración en la máquina, es importante utilizar siempre el mismo mandato de configuración (**ip** o **ifconfig**) o se pueden producir resultados imprevistos.

En sistemas Solaris 8, 9 y 10:

- Para direcciones IPv6:

```
ifconfig nombre_interfaz inet6 addif dirección_clúster/longitud_prefijo up
```

Por ejemplo, para poner un alias al dispositivo de bucle de retorno en servidores a los que se está equilibrando la carga:

```
ifconfig lo0 inet6 addif 3ffe:34::24:45/128 up
```

- Para direcciones IPv4: no hay cambios. Consulte la Tabla 5 en la página 73 para poner un alias al dispositivo de bucle de retorno en servidores a los que se está equilibrando la carga.

En sistemas Windows 2003 (Windows 2000 y Windows NT no admiten IPv6):

- Para direcciones IPv4: no hay cambios. Consulte la Tabla 5 en la página 73 para poner un alias al dispositivo de bucle de retorno en servidores a los que se está equilibrando la carga.
- Para direcciones IPv6:
 1. Utilice el mandato `ipconfig /all` para determinar el nombre de interfaz para el dispositivo de bucle de retorno. Este mandato localiza la conexión con una descripción del adaptador de bucle de retorno de Microsoft. En el siguiente ejemplo se muestra la salida del mandato `ipconfig /all`, donde el adaptador de bucle de retorno de Microsoft es el adaptador Ethernet Conexión de área local 2, y por lo tanto, la conexión es Conexión de área local 2.

Configuración IP de Windows

```
Nombre de sistema principal. . . . : ndserv10
Sufijo DNS primario . . . . . : rtp.raleigh.ibm.com
Tipo de nodo . . . . . : Desconocido
Direccionamiento IP habilitado . : No
Proxy WINS habilitado . . . . . : No
Lista búsqueda sufijo DNS . . . . : rtp.raleigh.ibm.com
```

Adaptador Ethernet Conexión de área local 2:

```
Sufijo DNS específico conexión . :
Descripción . . . . . : Adaptador de bucle de retorno de Microsoft
Dirección física . . . . . : 02-00-4C-4F-4F-50
DHCP habilitado . . . . . : No
Dirección IP . . . . . : 9.42.92.158
Máscara de subred . . . . . : 255.255.252.0
Dirección IP . . . . . : 9.42.92.159
Máscara de subred . . . . . : 255.255.252.0
Dirección IP . . . . . : 2002:92a:8f7a:162:9:42:92:160
Dirección IP . . . . . : 2002:92a:8f7a:162:9:42:92:159
Dirección IP . . . . . : fe80::4cff:fe4f:4f50%4
Pasarela por omisión . . . . . :
Servidores DNS . . . . . : 127.0.0.1
                          fec0:0:0:ffff::1%1
                          fec0:0:0:ffff::2%1
                          fec0:0:0:ffff::3%1
```

2. Añada la dirección del clúster al bucle de retorno mediante el mandato `netsh`. Por ejemplo:

```
netsh interface ipv6 add address "Conexión de área local 2"
2002:92a:8f7a:162:9:42:92:161
```

3. Emita de nuevo el mandato `ipconfig /all` y verá la dirección añadida al adaptador de bucle de retorno. Por ejemplo:

Adaptador Ethernet Conexión de área local 2:

```
Sufijo DNS específico conexión . :
```



```

Descripción . . . . . : Adaptador de bucle de retorno de Microsoft
Dirección física . . . . . : 02-00-4C-4F-4F-50
DHCP habilitado . . . . . : No
Dirección IP . . . . . : 9.42.92.158
Máscara de subred . . . . . : 255.255.252.0
Dirección IP . . . . . : 9.42.92.159
Máscara de subred . . . . . : 255.255.252.0
Dirección IP . . . . . : 2002:92a:8f7a:162:9:42:92:161
Dirección IP . . . . . : 2002:92a:8f7a:162:9:42:92:160
Dirección IP . . . . . : 2002:92a:8f7a:162:9:42:92:159
Dirección IP . . . . . : fe80::4cff:fe4f:4f50%4
Pasarela por omisión . . . . . :
Servidores DNS . . . . . : 127.0.0.1
                             fec0:0:0:ffff::1%1
                             fec0:0:0:ffff::2%1
                             fec0:0:0:ffff::3%1

```

- Habilite el reenvío para todas las interfaces de la máquina mediante el mandato `netsh interface ipv6 show interface`. Todas las interfaces listadas con el nombre Conexión de área local deben tener habilitado el reenvío IP. Por ejemplo:

```

netsh interface ipv6>show interface
Consultando estado activo...

```

Idx	Met	MTU	Estado	Nombre
6	2	1280	Desconectada	Pseudointerfaz de transmisión por túneles Teredo
5	0	1500	Conectada	Conexión de área local
4	0	1500	Conectada	Conexión de área local 2
3	1	1280	Conectada	Pseudointerfaz 6to4
2	1	1280	Conectada	Pseudointerfaz de transmisión por túneles automática
1	0	1500	Conectada	Pseudointerfaz de bucle de retorno

```

netsh interface ipv6>set interface "Conexión de área local"
forwarding=enabled
Ok.

```

```

netsh interface ipv6>set interface "Conexión de área local 2"
forwarding=enabled
Ok.

```

En sistemas OS/2:

- Para direcciones IPv6 e IPv4: no hay cambios. Consulte la Tabla 5 en la página 73 para poner un alias al dispositivo de bucle de retorno en servidores a los que se está equilibrando la carga.

Pasos de configuración de clúster requeridos para Linux en zSeries

Para Linux en zSeries, para configurar Load Balancer es necesario llevar a cabo los siguientes pasos de configuración adicionales:

- Configure la dirección de clúster mediante el mandato `ip` o `ifconfig`.

Para direcciones IPv6 o IPv4:

```
ip -versión addr add dirección_clúster/longitud_prefijo dev dispositivo
```

Por ejemplo:

```
ip -4 addr add 12.42.38.125/24 dev eth0
ip -6 addr add 3ffe:34::24:45/64 dev eth0
```

- Añada una norma iptables para eliminar los paquetes entrantes destinados a la dirección de clúster:

Para direcciones IPv4:

```
iptables -t filter -A INPUT -d dirección_clúster -j DROP
```

Para direcciones IPv6:

```
ip6tables -t filter -A INPUT -d dirección_clúster -j DROP
```

Por ejemplo:

```
iptables -t filter -A INPUT -d 12.42.38.125 -j DROP  
ip6tables -t filter -A INPUT -d 3ffe:34::24:45 -j DROP
```

Para deshacer la configuración anterior, utilice los siguientes mandatos:

```
ip -versión addr del dirección_clúster/longitud_prefijo dev dispositivo  
iptables -t filter -D INPUT -d dirección_clúster -j DROP  
ip6tables -t filter -D INPUT -d dirección_clúster -j DROP
```

Mandatos de Dispatcher (dscontrol) para Load Balancer para IPv4 y IPv6

Dado que Load Balancer para IPv4 y IPv6 no admite todas las características del componente, los mandatos `dscontrol` válidos para esta instalación son un subconjunto de los mandatos `dscontrol` para instalaciones de Load Balancer que sólo admiten IPv4. En este apartado se describen las diferencias de sintaxis de mandato y se enumeran todos los mandatos `dscontrol` admitidos para el componente Dispatcher en Load Balancer para IPv4 y IPv6.

Diferencias de sintaxis de mandato

Con la instalación de Load Balancer para IPv4 y IPv6, la sintaxis del mandato de Dispatcher (`dscontrol`) es idéntica a la de una excepción importante. El delimitador de mandatos `dscontrol` es un símbolo arroba (@), en lugar de dos puntos (:), cuando se utiliza Load Balancer para IPv4 y IPv6.

Ha sido necesario definir un delimitador distinto de dos puntos (:) porque el formato IPv6 utiliza dos puntos dentro de su esquema de direccionamiento.

A continuación se ilustra el mandato `dscontrol` utilizando un delimitador de arroba (@):

- Para añadir un servidor IPv6 (30::200) en el puerto 80, bajo un clúster IPv6 (30::100)
`dscontrol server add 30::100@80@30::200`
- Para añadir un servidor IPv4 (192.4.40.35) en el puerto 80, bajo un clúster IPv4 (192.4.40.30)
`dscontrol server add 192.4.40.30@80@192.4.20.35`

IMPORTANTE: cuando se hace referencia a mandatos en este documento, recuerde sustituir (@) por (:) como el delimitador dentro de mandatos `dscontrol`.

Mandatos dscontrol admitidos

Para obtener información detallada y ejemplos de la sintaxis de todos los mandatos `dscontrol`, consulte el Capítulo 27, “Referencia de mandatos para Dispatcher y CBR”, en la página 347.

A continuación figura un resumen de todos los mandatos admitidos para Dispatcher en la instalación de Load Balancer para IPv4 y IPv6

- `dscontrol advisor`
 - Son válidos todos los argumentos y sus valores de clave.
 - Si desea una descripción detallada de la sintaxis de mandato, consulte el apartado “`dscontrol advisor` — controlar el asesor” en la página 349.

- `dscontrol binlog`
 - Son válidos todos los argumentos y sus valores de clave.
 - Si desea una descripción detallada de la sintaxis de mandato, consulte el apartado “`dscontrol binlog` — controlar el archivo de anotaciones cronológicas binario” en la página 354.
- `dscontrol cluster`
 - Son válidos todos los argumentos. Los únicos valores de clave válidos son: `address` y `proportions`.
 - Si desea una descripción detallada de la sintaxis de mandato, consulte el apartado “`dscontrol cluster` — configurar clústeres” en la página 355.
- `dscontrol executor`
 - Son válidos todos los argumentos. Para el argumento `set`, los únicos valores de clave válidos son `nfa`, `hatimeout` y `hasyncntimeout`.

Para los sistemas que se ejecutan en espacio de usuario, como los sistemas Linux:

- Todos los argumentos son válidos, excepto `configure` y `unconfigure`. Es importante tener en cuenta que en la pila del sistema nunca se deben utilizar alias para las direcciones del clúster.
- Para el argumento `set`, los únicos valores de clave válidos son `nfa` y `hatimeout`.
- Para el argumento `configure`, debe sustituir *longitud_prefijo* en lugar de *máscara-red*.

Para IPv6, la longitud del prefijo representa el número de bits de la parte de red de la dirección IPv6. La longitud del prefijo delinea la dirección de red de la dirección del sistema principal.

Para IPv4, determine la longitud de prefijo como se indica a continuación: si la máscara de subred es 255.255.252.0, el equivalente hexadecimal es FF.FF.FC.0. En binario, el valor es 11111111 11111111 11111100 00000000. El recuento de los 1 de la máscara de subred determina la longitud de prefijo. Si hay 22 unos en la máscara de subred, el prefijo es 22.

La sintaxis de `executor configure` es:

```
dscontrol executor configure dirección_interfaz nombre_interfaz longitud_prefijo
```

Ejemplo con el direccionamiento IPv6:

```
dscontrol executor configure 2002:092a:8f7a:4226:9:37:240:99 en0 112
```

Ejemplo con el direccionamiento IPv4, si la máscara de subred es 255.255.252.0:

```
dscontrol e config 191.60.20.20 en1 22
```

Es importante observar que el mandato `executor configure` no se utiliza para sistemas que se ejecutan en espacio de usuario, como los sistemas Linux, en instalaciones de Load Balancer para IPv4 y IPv6.

- Si desea una descripción detallada de la sintaxis de mandato, consulte el apartado “`dscontrol executor` — control del ejecutor” en la página 359.
- `dscontrol file`
 - Son válidos todos los argumentos y sus valores de clave.
 - Si desea una descripción detallada de la sintaxis de mandato, consulte el apartado “`dscontrol file` — gestionar archivos de configuración” en la página 364.
- `dscontrol help`

- Todos los argumentos son válidos, excepto `host` (configurar una máquina remota), `rule` (configurar normas) y `subagent` (configurar el subagente SNMP). No se admiten los mandatos `host`, `rule` y `subagent`.
- Si desea una descripción detallada de la sintaxis de mandato, consulte el apartado “`dscontrol help` — mostrar o imprimir ayuda para este mandato” en la página 366.
- `dscontrol highavailability`
 - Son válidos todos los argumentos. Todos los valores clave son válidos, excepto `both` porque no se admite la alta disponibilidad mutua.
 - Si desea una descripción detallada de la sintaxis de mandato, consulte el apartado “`dscontrol highavailability` — controlar alta disponibilidad” en la página 367.
- `dscontrol logstatus`
 - Son válidos todos los argumentos y sus valores de clave.
 - Si desea una descripción detallada de la sintaxis de mandato, consulte el apartado “`dscontrol logstatus` — mostrar valores de anotaciones cronológicas de servidor” en la página 372.
- `dscontrol manager`
 - Todos los argumentos son válidos, excepto `version`. Todos los valores clave son válidos
 - Si desea una descripción detallada de la sintaxis de mandato, consulte el apartado “`dscontrol manager` — controlar el gestor” en la página 373.
- `dscontrol metric`
 - Son válidos todos los argumentos y sus valores de clave.
 - Si desea una descripción detallada de la sintaxis de mandato, consulte el apartado “`dscontrol metric` — configurar métrica del sistema” en la página 379.
- `dscontrol port`
 - Todos los argumentos son válidos, excepto `halfopenaddressreport`, que no se admite.

Los valores clave siguientes son válidos para los argumentos `add` y `set` en el mandato `dscontrol port`:

- `staletimeout`
- `weightbound`
- `stickymask`

Para los sistemas que se ejecutan en espacio de usuario, como los sistemas Linux: Los valores clave siguientes son válidos para los argumentos `add` y `set` en el mandato `dscontrol port`:

- `staletimeout`
- `weightbound`
- `selectionalgorithm`

Las opciones de `selectionalgorithm` (algoritmo de selección de servidor) son:

- `connection`: la selección de servidor se basa en la selección por turno rotativo simple (valor por omisión)
- `affinity`: la selección de servidor se basa en la afinidad del cliente.

Por ejemplo:

```
dscontrol port add clúster@puerto selectionalgorithm affinity
```

- Si desea una descripción detallada de la sintaxis de mandato, consulte el apartado “dscontrol port — configurar puertos” en la página 380.
- dscontrol server
 - Son válidos todos los argumentos.
Los valores clave siguientes son válidos para el argumento add del mandato dscontrol server:
 - dirección
 - advisorrequest
 - advisorresponse
 - collocated
La palabra clave collocated está disponible en los sistemas operativos admitidos, excepto en Windows y en sistemas que se ejecutan en espacio de usuario, como los sistemas Linux.
 - fixedweight
 - weight
Los valores clave siguientes son válidos para el argumento set del mandato dscontrol server:
 - advisorrequest
 - advisorresponse
 - collocated
La palabra clave collocated está disponible en los sistemas operativos admitidos, excepto en Windows y en sistemas que se ejecutan en espacio de usuario, como los sistemas Linux.
 - fixedweight
 - weight
 - Si desea una descripción detallada de la sintaxis de mandato, consulte el apartado “dscontrol server — configurar servidores” en la página 392.
- dscontrol set
 - Son válidos todos los argumentos y sus valores de clave.
 - Si desea una descripción detallada de la sintaxis de mandato, consulte el apartado “dscontrol set — configurar anotaciones cronológicas de servidor” en la página 398.
- dscontrol status
 - Son válidos todos los argumentos y sus valores de clave.
 - Si desea una descripción detallada de la sintaxis de mandato, consulte el apartado “dscontrol status — mostrar si el gestor y los asesores se están ejecutando” en la página 399.

Mandatos dscontrol no admitidos

Los mandatos que se detallan a continuación *no* están disponibles para Dispatcher en la instalación de Load Balancer para IPv4 y IPv6:

- dscontrol host (configurar una máquina remota)
- dscontrol rule (configurar normas)
- dscontrol subagent (configurar el subagente SNMP)

Parte 3. Componente CBR (Content Based Routing)

Esta parte proporciona información sobre la configuración de inicio rápido, consideraciones de planificación y describe los métodos para configurar el componente CBR de Load Balancer. Contiene los capítulos siguientes:

- Capítulo 9, “Configuración de inicio rápido”, en la página 99
- Capítulo 10, “Planificación de CBR (Content Based Routing)”, en la página 105
- Capítulo 11, “Configuración de CBR (Content Based Routing)”, en la página 109

Capítulo 9. Configuración de inicio rápido

Este ejemplo de inicio rápido muestra cómo configurar tres estaciones de trabajo conectadas localmente utilizando CBR junto con Caching Proxy para equilibrar la carga del tráfico Web entre dos servidores Web. (Para simplicidad, este ejemplo ilustra servidores en el mismo segmento LAN, no obstante, con CBR no hay restricción para utilizar servidores en la misma LAN).



Figura 16. Configuración local sencilla de CBR

Qué necesita

Para el ejemplo de inicio rápido, necesitará tres estaciones de trabajo y cuatro direcciones IP. Se utiliza una estación de trabajo como máquina CBR; las otras dos se utilizarán como servidores Web. Cada servidor Web requiere una dirección IP. La estación de trabajo CBR requiere una dirección real y una dirección donde se va a equilibrar la carga.

Nota: El componente CBR (Content Based Routing) está disponible en todas las plataformas excepto donde se ejecuta la JVM de 64 bits. De modo alternativo, puede utilizar el método de reenvío cbr del componente Dispatcher de Load Balancer para proporcionar direccionamiento basado en contenido sin utilizar Caching Proxy. Si desea más información, consulte el apartado "Direccionamiento basado en contenido de Dispatcher (método de reenvío cbr)" en la página 55.

Para utilizar CBR, Caching Proxy debe estar instalado en el mismo servidor. Para configurar Caching Proxy para CBR, consulte el apartado "Paso 1. Configurar Caching Proxy para que pueda utilizar CBR" en la página 113.

Preparativos

1. Para este ejemplo, configure las estaciones de trabajo en el mismo segmento de la LAN. Asegúrese de que el tráfico de red entre las tres máquinas no tenga que pasar por direccionadores o puentes.

2. Configure los adaptadores de red de las tres estaciones de trabajo. Para este ejemplo, suponga que tiene la configuración de red siguiente:

Estación de trabajo	Nombre	Dirección IP
1	servidor1.misitoWeb.com	9.27.27.101
2	servidor2.misitoWeb.com	9.27.27.102
3	servidor3.misitoWeb.com	9.27.27.103
Máscara de red = 255.255.255.0		

Cada una de las estaciones de trabajo sólo contiene una tarjeta de interfaz de red Ethernet estándar.

3. Asegúrese de que servidor1.misitoWeb.com puede ejecutar el mandato ping de servidor2.misitoWeb.com y de servidor3.misitoWeb.com.
4. Asegúrese de que servidor2.misitoWeb.com y servidor3.misitoWeb.com pueden ejecutar el mandato ping de servidor1.misitoWeb.com.
5. Asegúrese de que funcionan los servidores Web en servidor2.misitoWeb.com y servidor3.misitoWeb.com. Utilice el navegador Web para solicitar páginas directamente de **http://servidor2.misitoWeb.com** (por ejemplo, .../member/index.html) y **http://servidor3.misitoWeb.com** (por ejemplo, .../guest/index.html).
6. Obtenga otra dirección IP válida para este segmento de la LAN. Esta será la dirección del clúster que proporcionará a los clientes que deseen acceder a su sitio. Para este ejemplo utilizará:

Nombre= www.misitoWeb.com
IP=9.27.27.104

Configuración del componente CBR

Con CBR, puede crear una configuración mediante la línea de mandatos, el asistente de configuración o la GUI (Interfaz gráfica de usuario). Para este ejemplo de inicio rápido, los pasos de configuración se demuestran utilizando la línea de mandatos.

Nota: Los valores de los parámetros deben escribirse en caracteres del idioma inglés. Las únicas excepciones son los valores de parámetros para los nombres de sistemas principales y de archivos.

Configuración con la línea de mandatos

Desde un indicador de mandatos, siga estos pasos:

1. Inicie cbrserver. Ejecute este mandato como usuario root o Administrador:
cbrserver

Nota: En la plataforma Windows: Inicie cbrserver (Content Based Routing) desde el Panel de control: **Inicie > Configuración** (para Windows 2000) > **Panel de control > Herramientas administrativas > Servicios**.

2. Inicie la función de ejecutor de CBR:
cbrcontrol executor start
3. Inicie Caching Proxy. (Se puede iniciar Caching Proxy en cualquier momento después de iniciar la función de ejecutor):
ibmproxy

Nota: Para la plataforma Windows: también puede iniciar Caching Proxy desde el panel Servicios: **Inicio > Configuración** (para Windows 2000)> **Panel de control > Herramientas administrativas > Servicios.**

- Añada el clúster (el nombre de sistema principal, el sitio Web, al que se conectan los clientes) a la configuración de CBR:

```
cbrcontrol cluster add www.misitioWeb.com
```

- Añada la dirección del clúster (9.27.27.104) para el sitio Web a la tarjeta de interfaz de red en la máquina de CBR. Si desea más información, consulte el apartado “Paso 5. Crear un alias para la tarjeta de interfaz de red (opcional)” en la página 115.

- Añada el puerto de protocolo http a la configuración de CBR:

```
cbrcontrol port add www.misitioWeb.com:80
```

- Añada cada uno de los servidores Web a la configuración de CBR:

```
cbrcontrol server add www.misitioWeb.com:80:servidor2.misitioWeb.com
```

```
cbrcontrol server add www.misitioWeb.com:80:servidor3.misitioWeb.com
```

- Añada normas de contenido a la configuración de CBR. (Una norma de contenido define cómo se distinguirá y enviará una petición de URL a uno de los servidores o conjuntos de servidores):

```
cbrcontrol rule add www.misitioWeb.com:80:memberRule type content  
pattern uri=*/member/*
```

```
cbrcontrol rule add www.misitioWeb.com:80:guestRule type content pattern  
uri=*/guest/*
```

En este ejemplo, utilizando la norma de contenido, las peticiones del cliente al sitio Web `www.misitioWeb.com` se envían a un servidor distinto según un directorio en su vía de acceso de la petición del URI. Si desea más información, consulte el Apéndice B, “Sintaxis de la norma de contenido (patrón)”, en la página 475.

- Añada servidores a las normas:

```
cbrcontrol rule useserver www.misitioWeb:80:memberRule  
servidor2.misitioWeb.com
```

```
cbrcontrol rule useserver www.misitioWeb:80:guestRule  
servidor3.misitioWeb.com
```

CBR ahora equilibrará la carga según la norma basada en contenido. Los clientes con peticiones de URL que contengan `/member/` se dirigirán a `servidor2.misitioWeb.com`. Los clientes con peticiones de URL que contengan `/guest/` se dirigirán a `servidor3.misitioWeb.com`.

- Inicie la función de gestor de CBR:

```
cbrcontrol manager start
```

- Inicie la función de asesor de CBR:

```
cbrcontrol advisor start http 80
```

Ahora CBR se asegurará de que las peticiones del cliente no se envíen a un servidor Web que haya dado un error.

Ya se ha completado la configuración básica con los servidores conectados localmente.

Prueba de la configuración

Compruebe si la configuración funciona:

1. Con un navegador Web, vaya a la ubicación **http://www.mywebsite.com/member/index.htm**. Si se visualiza una página, significa que la configuración funciona.
2. Vuelva a cargar la página en el navegador Web.
3. Busque los resultados del mandato siguiente:
cbrcontrol server report www.misitioweb.com:80:

La columna de conexiones totales de los dos servidores debería sumarse a "2."

Configuración con la interfaz gráfica de usuario (GUI)

Si desea información sobre cómo utilizar la GUI de CBR, consulte el apartado "GUI" en la página 111 y el Apéndice A, "GUI: instrucciones generales", en la página 467.

Configuración con el asistente de configuración

Si desea información sobre cómo utilizar el asistente de CBR, consulte el apartado "Asistente de configuración" en la página 113.

Tipos de configuraciones de clúster, puerto y servidor

Hay muchos modos de configurar CBR para dar soporte a su sitio. Si sólo tiene un nombre de sistema principal para el sitio al que se conectarán todos sus clientes, puede definir un solo clúster de servidores. Para cada uno de estos servidores, configure el puerto a través del que CBR se comunica. Consulte la Figura 9 en la página 48.

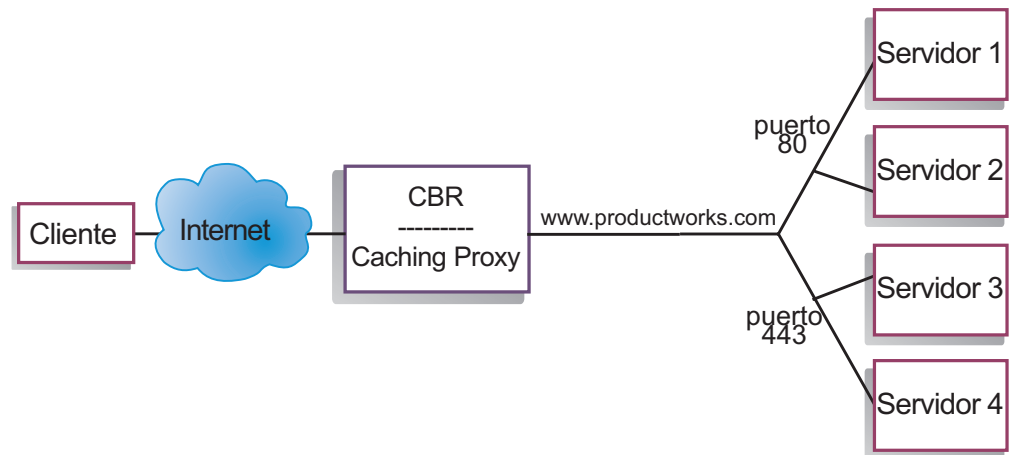


Figura 17. Ejemplo de CBR configurado con un solo clúster y 2 puertos

En este ejemplo del componente CBR, se define un clúster en **www.productworks.com**. Este clúster tiene dos puertos: el puerto 80 para HTTP y el puerto 443 para SSL. Un cliente que solicita **http://www.productworks.com** (puerto 80) va a un servidor distinto que un cliente que solicita **https://www.productworks.com** (puerto 443).

Podría resultar adecuado otro modo de configurar CBR si tiene un sitio de un tamaño muy grande con muchos servidores dedicados a cada protocolo admitido.

En este caso, quizá desee definir un clúster para cada protocolo con un solo puerto pero con muchos servidores, como se muestra en la Figura 10 en la página 49.

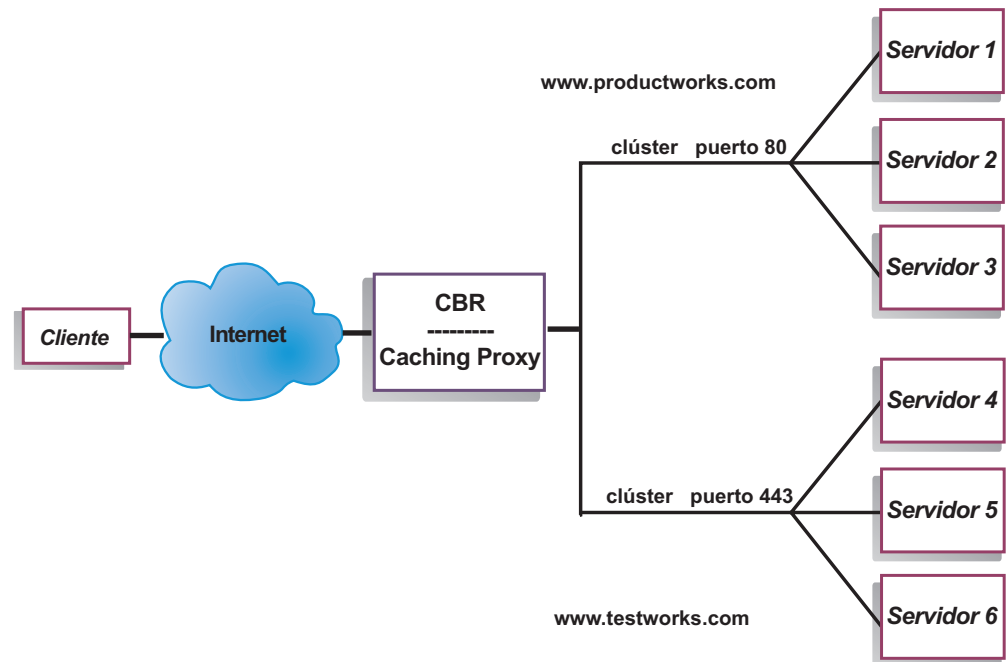


Figura 18. Ejemplo de CBR configurado con dos clústeres, cada uno con un puerto

En este ejemplo del componente CBR, se definen dos clústeres: `www.productworks.com` para el puerto 80 (HTTP) y `www.testworks.com` para el puerto 443 (SSL).

Podría ser necesario un tercer modo de configurar CBR si el sitio alberga el contenido de varias empresas o departamentos, en el que cada uno entra al sitio con un URL distinto. En este caso, quizá desee definir un clúster para cada empresa o departamento y luego definir los puertos en los que va a recibir conexiones en ese URL, como se muestra en la Figura 11 en la página 50.

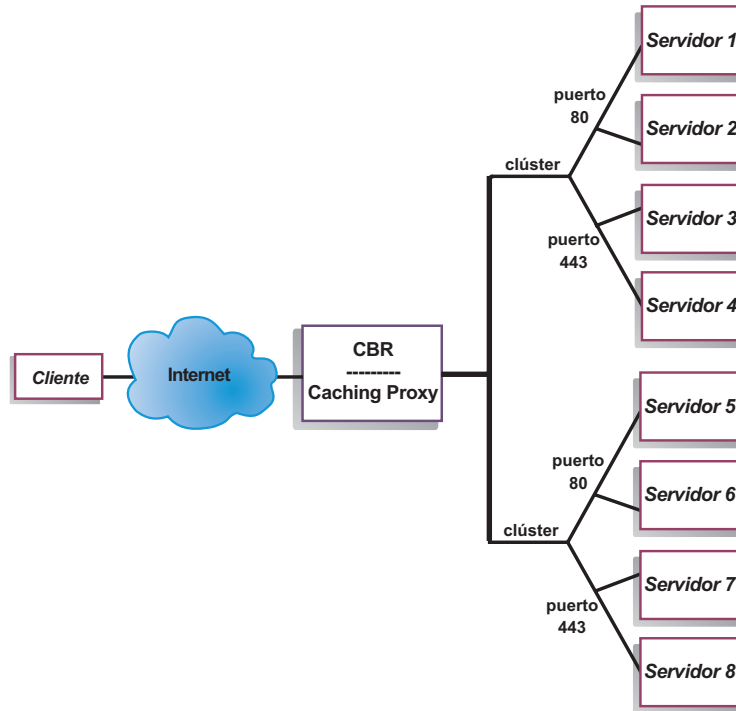


Figura 19. Ejemplo de CBR configurado con 2 clústeres, cada uno con 2 puertos

En este ejemplo del componente CBR, se definen dos clústeres con el puerto 80 (HTTP) y el puerto 443 (SSL) para cada uno de los sitios en www.productworks.com y www.testworks.com.

Capítulo 10. Planificación de CBR (Content Based Routing)

En este capítulo se describe lo que debería tener en cuenta el planificador de la red antes de instalar y configurar el componente CBR con Caching Proxy.

- Si desea obtener una visión general de características que están disponibles para gestionar la red consulte el Capítulo 3, “Gestión de la red: determinación de las características de Load Balancer que se van a utilizar”, en la página 19.
- Si desea información sobre cómo configurar parámetros de equilibrio de carga de CBR, consulte el Capítulo 11, “Configuración de CBR (Content Based Routing)”, en la página 109.
- Si desea información sobre cómo configurar Load Balancer para obtener funciones más avanzadas, consulte el Capítulo 22, “Características avanzadas para Dispatcher, CBR y Site Selector”, en la página 201.
- Si desea información sobre administración autenticada remota, archivos de anotaciones cronológicas de Load Balancer y el uso de los componentes de Load Balancer consulte el Capítulo 24, “Operación y gestión de Load Balancer”, en la página 261.

Este capítulo incluye los siguientes apartados:

- “Consideraciones de planificación”
- “Utilización de equilibrio de carga basado en normas con CBR” en la página 107
- “Equilibrio de carga entre conexiones completamente seguras (SSL)” en la página 107
- “Equilibrio de carga de cliente a proxy en SSL y de proxy a servidor en HTTP” en la página 108

Consideraciones de planificación

El componente CBR permite equilibrar la carga de tráfico HTTP y SSL con Caching Proxy para dirigir mediante proxy la petición. Con CBR, puede equilibrar la carga de servidores que puede configurar desde el archivo de configuración de CBR utilizando mandatos `cbrcontrol`.

Nota: El componente CBR (Content Based Routing) está disponible en todas las plataformas excepto donde se ejecuta la JVM de 64 bits. De modo alternativo, puede utilizar el método de reenvío `cbr` del componente Dispatcher de Load Balancer para proporcionar direccionamiento basado en contenido sin utilizar Caching Proxy. Si desea más información, consulte el apartado “Direccionamiento basado en contenido de Dispatcher (método de reenvío `cbr`)” en la página 55.

CBR es muy similar a Dispatcher en su estructura de componentes. CBR consta de las funciones siguientes:

- **cbrserver** gestiona las peticiones de la línea de mandatos al ejecutor, el gestor y los asesores.
- El **ejecutor** admite el equilibrio de carga de peticiones de cliente. Se debe iniciar el ejecutor para utilizar el componente CBR.
- El **gestor** establece los pesos que utiliza el ejecutor basándose en:
 - Contadores internos del ejecutor

- Información de retorno de los servidores proporcionada por los asesores
- Información de retorno de un programa de supervisión del sistema, como Metric Server.

La utilización del gestor es opcional. No obstante, si no se utiliza el gestor, se realiza el equilibrio de carga utilizando la planificación de turno rotativo sopesado según los pesos del servidor actual y no estarán disponibles los asesores.

- Los **asesores** consultan los servidores y analizan los resultados por protocolo antes de llamar al gestor para establecer pesos según corresponda. Quizá no tenga sentido utilizar algunos de estos asesores en una configuración típica. También tiene la opción de escribir sus propios asesores. El uso de asesores es opcional, pero se recomienda. Load Balancer proporciona un asesor de Caching Proxy (cachingproxy). Si desea más información, consulte el apartado “Asesores” en la página 185.
- Para configurar y gestionar el ejecutor, los asesores y el gestor, utilice la línea de mandatos (**cbrcontrol**) o la interfaz gráfica de usuario (**lbadmin**).

Las tres funciones clave de CBR (ejecutor, gestor y asesores) actúan conjuntamente para equilibrar y entregar las peticiones entrantes entre servidores. Junto con las peticiones de equilibrio de carga, el ejecutor supervisa el número de conexiones nuevas y de conexiones activas y suministra esta información al gestor.

Peticiones de equilibrio de carga para distintos tipos de contenido

El componente CBR proporciona la posibilidad de especificar un conjunto de servidores que gestionarán peticiones basándose en expresiones regulares comparadas con el contenido de la petición de cliente. CBR permite particionar el sitio de modo que conjuntos de servidores distintos pueden atender contenidos o servicios de aplicaciones distintos. Este particionamiento es transparente a clientes que acceden a su sitio.

División del contenido del sitio para obtener un mejor tiempo de respuesta

Un modo de dividir su sitio sería asignar algunos servidores para gestionar sólo peticiones cgi y otro conjunto de servidores para gestionar todas las demás peticiones. Esto impide que el cálculo intensivo de scripts cgi ralentice los servidores para el tráfico de HTML normal, lo que permite a los clientes obtener un mejor tiempo de respuesta global. Con el uso de este esquema, también podría asignar estaciones de trabajo más completas para peticiones normales. Esto proporcionaría a los clientes un mejor tiempo de respuesta sin los gastos de actualizar todos los servidores. También podría asignar estaciones de trabajo más completas para peticiones cgi.

Otra posibilidad para particionar su sitio podría ser dirigir a los clientes que acceden a las páginas que requieren registrarse a un conjunto de servidores y todas las demás peticiones a un segundo conjunto de servidores. Esto impediría que navegadores eventuales de su sitio acapararan recursos que podrían utilizarlos clientes que se hayan comprometido con su registro. También le permitiría utilizar estaciones de trabajo más completas para atender a los clientes que se han registrado.

Podría por supuesto combinar los métodos anteriores para obtener aún más flexibilidad y un servicio mejorado.

Provisión de una copia de seguridad del contenido del servidor Web

Dado que CBR permite especificar varios servidores para cada tipo de petición, se puede equilibrar la carga de los servidores para obtener una respuesta al cliente óptima. Si permite que se asignen varios servidores a cada tipo de contenido, estará protegido si una estación de trabajo o un servidor da un error. CBR reconocerá el error y seguirá equilibrando la carga de peticiones de cliente con los otros servidores del conjunto.

Utilización de varios procesos Caching Proxy para mejorar la utilización de la CPU

Caching Proxy comunica con un proceso CBR mediante esta interfaz del plug-in. Para que esto funcione, CBR debe ejecutarse en la máquina local. Dado que estos son dos procesos aparte, puede haber varias instancias de Caching Proxy ejecutándose y trabajando con una sola instancia de CBR. Se podría establecer esta configuración con el fin de segregar direcciones o funcionalidad entre Caching Proxies o para mejorar la utilización de recursos de la máquina teniendo varios Caching Proxies gestionando el tráfico de clientes. Las instancias del proxy se pueden detectar en puertos distintos o enlazarse a direcciones IP únicas en el mismo puerto, en función de lo que mejor se ajuste a los requisitos de tráfico.

Utilización de equilibrio de carga basado en normas con CBR

CBR junto con Caching Proxy examina las peticiones HTTP utilizando los tipos de normas especificados. Cuando se ejecuta, Caching Proxy acepta peticiones de cliente y consulta al componente CBR cuál es el mejor servidor. En esta consulta, CBR compara la petición con un conjunto de normas con prioridades. Cuando se cumple una norma, se selecciona el servidor adecuado entre un conjunto de servidores preconfigurados. Finalmente, CBR informa a Caching Proxy del servidor que ha seleccionado y la petición se dirige mediante el proxy ahí.

Después de definir un clúster para el equilibrio de carga, debe asegurarse de que todas las peticiones a ese clúster tienen una norma que seleccionará un servidor. Si no se ha encontrado ninguna norma que cumpla una petición en particular, el cliente recibirá una página de error del Caching Proxy. El modo más sencillo de asegurarse de que todas las peticiones cumplirán alguna norma es crear una norma "siempre cierta" con un número de prioridad muy alto. Asegúrese de que los servidores utilizados por esta norma puedan gestionar todas las peticiones no gestionadas explícitamente por las normas que tienen una prioridad con un número inferior. (Nota: las normas con un número de prioridad inferior se evalúan primero).

Para obtener más información consulte el apartado "Configuración de equilibrio de carga basado en normas" en la página 212.

Equilibrio de carga entre conexiones completamente seguras (SSL)

CBR con Caching Proxy puede recibir la transmisión SSL del cliente al proxy (en el sentido del cliente al proxy) así como dar soporte a la transmisión del proxy al servidor SSL (en el sentido del proxy al servidor). Si define un puerto SSL en un servidor en la configuración de CBR para recibir la petición SSL del cliente, tiene la posibilidad de mantener un sitio completamente seguro, utilizando CBR para equilibrar la carga entre servidores seguros (SSL).

Además de otros cambios en el archivo `ibmproxy.conf` para CBR, es necesario añadir otra sentencia de configuración al archivo `ibmproxy.conf` para Caching Proxy con el fin de habilitar el cifrado SSL en el sentido del proxy al servidor. El formato debe ser:

```
proxy patrón_uri patrón_url dirección
```

donde *patrón_uri* es un patrón de coincidencia (por ejemplo: `/secure/*`), *patrón_url* es una URL de sustitución (por ejemplo: `https://clusterA/secure/*`) y *dirección* es la dirección de clúster (por ejemplo: `clusterA`).

Equilibrio de carga de cliente a proxy en SSL y de proxy a servidor en HTTP

CBR con Caching Proxy también puede recibir la transmisión SSL del cliente y a continuación descifrar la petición SSL antes de dirigir mediante proxy la petición a un servidor HTTP. Para que CBR proporcione soporte de cliente a proxy en SSL y de proxy a servidor en HTTP, hay una palabra clave opcional **mapport** en el mandato `cbrcontrol server`. Utilice esta palabra clave cuando necesite indicar que el puerto en el servidor es distinto del puerto de entrada del cliente. A continuación figura un ejemplo para añadir un puerto utilizando la palabra clave `mapport`, donde el puerto del cliente es 443 (SSL) y el puerto del servidor es 80 (HTTP):

```
cbrcontrol server add cluster:443 mapport 80
```

El número de puerto de `mapport` puede ser cualquier valor entero positivo. El valor por omisión es el número de puerto del puerto de entrada del cliente.

Puesto que CBR debe ser capaz de asesorar sobre una petición HTTP de un servidor configurado en el puerto 443 (SSL), se proporciona un asesor especial *ssl2http*. Este asesor comienza en el puerto 443 (el puerto de entrada del cliente) y asesora sobre el servidor o los servidores configurados para ese puerto. Si hay dos clústeres configurados y cada clúster tiene el puerto 443, además los servidores están configurados con un `mapport` distinto, entonces una sola instancia del asesor puede abrir el puerto adecuado de modo correspondiente. A continuación figura un ejemplo de esta configuración:

```
Executor
  Cluster1
    Port:443
      Server1 mapport 80
      Server2 mapport 8080
  Cluster2
    Port:443
      Server3 mapport 80
      Server4 mapport 8080
  Manager
    Advisor ssl2http 443
```

Capítulo 11. Configuración de CBR (Content Based Routing)

Antes de llevar a cabo los pasos de este capítulo, consulte el Capítulo 10, “Planificación de CBR (Content Based Routing)”, en la página 105. En este capítulo se explica cómo crear una configuración básica para el componente CBR de Load Balancer.

- En el Capítulo 21, “Funciones del gestor, asesores y Metric Server para Dispatcher, CBR y Site Selector”, en la página 179 y el Capítulo 22, “Características avanzadas para Dispatcher, CBR y Site Selector”, en la página 201 encontrará configuraciones más complejas de Load Balancer.
- En el Capítulo 24, “Operación y gestión de Load Balancer”, en la página 261 encontrará información sobre la administración autenticada remota, las anotaciones cronológicas de Load Balancer y el uso de los componentes de Load Balancer.

Visión general de las tareas de configuración

Antes de empezar a realizar los pasos de configuración indicados en esta tabla, asegúrese de que la máquina CBR y todas las máquinas de servidores están conectadas a la red, tienen direcciones IP válidas y que pueden enviar una sonda de paquetes Internet entre sí.

Nota: El componente CBR (Content Based Routing) está disponible en todas las plataformas excepto donde se ejecuta la JVM de 64 bits. De modo alternativo, puede utilizar el método de reenvío cbr del componente Dispatcher de Load Balancer para proporcionar direccionamiento basado en contenido sin utilizar Caching Proxy. Si desea más información, consulte el apartado “Direccionamiento basado en contenido de Dispatcher (método de reenvío cbr)” en la página 55.

Tabla 7. Tareas de configuración para el componente CBR

Tarea	Descripción	Información relacionada
Configurar la máquina CBR.	Averigua los requisitos.	“Configuración de la máquina CBR” en la página 113
Configurar máquinas en las que se va a equilibrar la carga.	Configura la configuración de equilibrio de carga.	“Paso 7. Definir máquinas servidor con equilibrio de carga” en la página 117

Métodos de configuración

Existen cuatro métodos básicos para crear una configuración básica para el componente CBR de Load Balancer:

- Línea de mandatos
- Scripts
- Interfaz gráfica de usuario (GUI)
- Asistente de configuración

Para utilizar CBR, debe instalarse Caching Proxy.

Nota: Caching Proxy es un servicio que se inicia automáticamente por omisión después de la instalación. Debe detener Caching Proxy antes de iniciar la función de servidor CBR (cbrserver) y modificar el servicio Caching Proxy de forma que se inicie manualmente en lugar de hacerlo automáticamente.

- En sistemas Linux o UNIX: detenga Caching Proxy; para ello, busque su identificador de proceso con el mandato `ps -ef | grep ibmproxy` y finalice el proceso mediante el mandato `kill id_proceso`.
- En sistemas Windows: detenga Caching Proxy desde el panel Servicios.

Línea de mandatos

Es la manera más directa de configurar CBR. Los valores de los parámetros de mandatos deben especificarse en caracteres del idioma inglés. Las únicas excepciones son los nombres de sistema principal (se utiliza, por ejemplo, en los mandatos de clúster y servidor) y los nombres de archivo.

Para iniciar CBR desde la línea de mandatos:

- En sistemas Linux o UNIX: como usuario root, emita el mandato **cbrserver** desde el indicador de mandatos. (Para detener el servicio, emita lo siguiente: **cbrserver stop**).

En sistemas Windows: pulse **Inicio > Configuración** (en Windows 2000) > **Panel de control > Herramientas administrativas > Servicios**. Pulse con el botón derecho del ratón en **IBM Content Based Routing** y seleccione **Iniciar**. Para detener el servicio, efectúe los mismos pasos y seleccione **Detener**.

- A continuación, emita los mandatos de control de CBR que desee para definir la configuración. En los procedimientos de esta publicación se da por supuesto que se utiliza la línea de mandatos. El mandato es **cbrcontrol**. Para obtener más información sobre los mandatos, consulte el Capítulo 27, “Referencia de mandatos para Dispatcher y CBR”, en la página 347.
- Inicie Caching Proxy. Emita el mandato **ibmproxy** en el indicador de mandatos. (Debe iniciar el ejecutor antes de iniciar Caching Proxy).

Nota: En plataformas Windows: inicie Caching Proxy desde el panel Servicios: **Inicio > Configuración** (para Windows 2000) > **Panel de control > Herramientas administrativas > Servicios**.

Puede entrar una versión abreviada de los parámetros del mandato **cbrcontrol**. Sólo es necesario especificar las letras exclusivas de los parámetros. Por ejemplo, para obtener ayuda sobre el mandato para guardar archivos, puede escribir **cbrcontrol he f** en lugar de **cbrcontrol help file**.

Para iniciar la interfaz de línea de mandatos, emita **cbrcontrol** para obtener un indicador de mandatos **cbrcontrol**.

Para finalizar la interfaz de línea de mandatos, emita **exit** o **quit**.

Notas:

1. en la plataforma Windows, se inicia automáticamente el dsserver del componente Dispatcher. Si sólo utiliza CBR y no emplea el componente Dispatcher, puede evitar que dsserver se inicie de forma automática haciendo lo siguiente:
 - a. En la ventana Servicios, pulse con el botón derecho del ratón en IBM Dispatcher.
 - b. Seleccione Propiedades.

- c. En el campo **Tipo de inicio**, seleccione Manual.
 - d. Pulse Aceptar y cierre la ventana Servicios.
2. Al configurar CBR (Content Based Routing) desde el indicador de mandatos del sistema operativo en lugar de hacerlo desde el indicador `cbrcontrol>>`, tenga cuidado cuando utilice estos caracteres:
- () paréntesis derecho e izquierdo
 - & ampersand
 - | barra vertical
 - ! signo de exclamación
 - * asterisco

El shell del sistema operativo puede interpretarlos como caracteres especiales y convertirlos en texto alternativo antes de que `cbrcontrol` los evalúe.

Los caracteres especiales en la lista anterior son caracteres opcionales del mandato **`cbrcontrol rule add`** y se utilizan cuando se especifica un patrón para una norma de contenido. Por ejemplo, el siguiente mandato sólo puede ser válido cuando se utiliza el indicador `cbrcontrol>>`.

```
rule add 10.1.203.4:80:cbr_prod_rule_ek type content
pattern uri=/nipoek/*
```

Para que este mismo mandato funcione en el indicador del sistema operativo, el patrón debe indicarse entre dos signos de comillas (" ") de la forma indicada a continuación:

```
cbrcontrol rule add 10.1.203.4:80:cbr_prod_rule_ek type content
pattern "uri=/nipoek/*"
```

Si no se utilizan las comillas, alguna parte del patrón puede truncarse cuando la norma se guarda en CBR. Tenga en cuenta que las comillas no están soportadas cuando se utiliza el indicador de mandatos `cbrcontrol>>`.

Scripts

Los mandatos para configurar CBR pueden especificarse y ejecutarse juntos en un archivo de script de configuración.

Nota: Para ejecutar rápidamente el contenido de un archivo de script (por ejemplo, `miscrypt`), use cualquiera de los siguientes mandatos:

- Para actualizar la configuración actual, ejecute los siguientes mandatos ejecutables desde el archivo `descript`:
`cbrcontrol file appendload miscrypt`
- Para sustituir completamente la configuración actual, ejecute los siguientes mandatos ejecutables desde el archivo de script:
`cbrcontrol file newload miscrypt`

Para guardar la configuración actual en un archivo de script (por ejemplo, `guardascript`), ejecute el siguiente mandato:

```
cbrcontrol file save guardascript
```

Este mandato guardará el archivo de script de configuración en el directorio **`...ibm/edge/lb/servers/configurations/cbr`**.

GUI

Para obtener instrucciones generales y un ejemplo de la interfaz gráfica de usuario (GUI), consulte la Figura 41 en la página 468.

Para iniciar la GUI, siga estos pasos

1. Asegúrese de que cbrserver se está ejecutando. Como usuario root o administrador, emita lo siguiente en el indicador de mandatos: **cbrserver**
2. Efectúe una de las siguientes acciones, en función del sistema operativo:
 - En sistemas AIX, HP-UX, Linux o Solaris, escriba **lbadmin**
 - En sistemas Windows: pulse **Inicie > Programas > IBM WebSphere > Edge Components > IBM Load Balancer > Load Balancer**
3. Inicie Caching Proxy. (En la GUI, primero debe conectarse al sistema principal e iniciar el ejecutor para el componente CBR antes de iniciar Caching Proxy). Realice una de las operaciones siguientes:
 - En sistemas AIX, HP-UX, Linux o Solaris: para iniciar Caching Proxy, escriba **ibmproxy**
 - En sistemas Windows: para iniciar Caching Proxy, vaya al panel Servicios: **Inicio > Configuración** (en Windows 2000) > **Panel de control > Herramientas administrativas > Servicios**

Para configurar el componente CBR desde la GUI, primero debe seleccionar **Content Based Routing** en la estructura de árbol. Inicie el gestor después de conectarse a un sistema principal. También puede crear clústeres que contengan puertos y servidores, así como iniciar asesores para el gestor.

La GUI puede utilizarse para llevar a cabo las mismas tareas que realizaría con el mandato **cbrcontrol**. Por ejemplo, para definir un clúster mediante la línea de mandatos, especifique el mandato **cbrcontrol cluster add clúster**. Para definir un clúster desde la GUI, pulse con el botón derecho del ratón en Ejecutor y, en el menú emergente, pulse **Añadir clúster**. Escriba la dirección del clúster en la ventana emergente y pulse **Aceptar**.

Los archivos de configuración de CBR preexistentes pueden cargarse con las opciones **Cargar nueva configuración** (para sustituir completamente la configuración actual) y **Añadir a la configuración actual** (para actualizar la configuración actual) que aparecen en el menú emergente **Sistema principal**. Debe guardar de forma periódica la configuración de CBR en un archivo con la opción **Guardar archivo de configuración como** que también se encuentra en el menú emergente **Sistema principal**. El menú **Archivo** situado en la parte superior de la GUI, permite guardar en un archivo las conexiones actuales del sistema principal o restaurar conexiones que se encuentran en archivos existentes en todos los componentes de Load Balancer.

Para acceder a la **Ayuda**, pulse el icono de signo de interrogación situado en la esquina superior derecha de la ventana de Load Balancer.

- **Ayuda: Nivel de campo** — describe cada campo, los valores por omisión
- **Ayuda: Cómo puedo** — lista las tareas que pueden llevarse a cabo desde esa pantalla
- **InfoCenter** — proporciona acceso centralizado a la información del producto

Para poder ejecutar un mandato desde la GUI: resalte el nodo Sistema principal en el árbol de la GUI y seleccione **Enviar mandato...** en el menú emergente Sistema principal. En el campo de entrada de mandatos, escriba el mandato que desea ejecutar, por ejemplo: **ejecutor report**. Aparecerán en la ventana proporcionada los resultados y el historial de los mandatos ejecutados en la sesión actual.

Si desea más información sobre cómo utilizar la GUI, consulte el Apéndice A, “GUI: instrucciones generales”, en la página 467.

Asistente de configuración

Si va a utilizar el asistente de configuración, siga estos pasos:

1. Inicie el `cbrserver`: emita **`cbrserver`** en el indicador de mandatos como usuario `root` o administrador.
2. Inicie la función de asistente de CBR:
Inicie este asistente desde el indicador de mandatos emitiendo **`cbrwizard`**. O bien, seleccione el Asistente de configuración desde el menú del componente CBR como se presenta en la GUI.
3. Inicie Caching Proxy para equilibrar la carga del tráfico HTTP o HTTPS (SSL).
En sistemas AIX, HP-UX, Linux o Solaris: para iniciar Caching Proxy, escriba **`ibmproxy`**
En sistemas Windows: para iniciar Caching Proxy, vaya al panel Servicios: **Inicio > Configuración** (en Windows 2000) > **Panel de control > Herramientas administrativas > Servicios**

El asistente CBR le guiará, paso a paso, a través del proceso de creación de una configuración básica para el componente CBR. Formula preguntas sobre la red y le guía mientras define un clúster que permite a CBR equilibrar la carga de tráfico entre un grupo de servidores.

Configuración de la máquina CBR

Para configurar la máquina CBR, debe ser el usuario `root` (en sistemas AIX, HP-UX, Linux o Solaris) o el administrador (en los sistemas Windows).

Es necesaria una dirección IP válida para cada clúster de servidores que se configure. Una dirección de clúster es una dirección asociada con un nombre de sistema principal (como `www.empresa.com`). El cliente utilizará esta dirección IP para conectarse a los servidores de un clúster. En concreto, esta dirección se encuentra en la petición de URL del cliente. CBR equilibra la carga de todas las peticiones realizadas en la misma dirección de clúster.

Sólo para sistemas Solaris: antes de utilizar el componente CBR, deben modificarse los valores por omisión del sistema para IPC (comunicación entre procesos). Es necesario aumentar el tamaño máximo de un segmento de memoria compartida y el número de identificadores de semáforos. Para ajustar el sistema de modo que dé soporte a CBR, edite el archivo `/etc/system` en el sistema y añada las siguientes sentencias y rearranque:

```
set shmsys:shminfo_shmmax=0x02000000
set semsys:seminfo_semmap=750
set semsys:seminfo_semmni=30
set semsys:seminfo_semmns=750
set semsys:seminfo_semmnu=30
set semsys:seminfo_semume=30
```

Si no aumenta el segmento de memoria compartida hasta los valores indicados más arriba, el mandato **`cbrcontrol executor start`** no se ejecutará correctamente.

Paso 1. Configurar Caching Proxy para que pueda utilizar CBR

Para utilizar CBR, debe instalarse Caching Proxy.

Nota: Caching Proxy es un servicio que se inicia automáticamente por omisión después de la instalación. Debe detener Caching Proxy antes de iniciar la función de servidor CBR y modificar el servicio Caching Proxy de forma que se inicie manualmente en lugar de hacerlo automáticamente.

- En sistemas AIX, HP-UX, Linux y Solaris: detenga Caching Proxy; para ello, busque su identificador de proceso con el mandato `ps -ef | grep ibmproxy` y finalice el proceso mediante el mandato `kill id_proceso`.
- En sistemas Windows: detenga Caching Proxy desde el panel Servicios.

Debe realizar las siguientes modificaciones en el archivo de configuración de Caching Proxy (`ibmproxy.conf`):

Verifique que la directiva de URL entrante **CacheByIncomingUrl** tiene el valor "off" (valor por omisión).

En la sección de normas de correlación del archivo de configuración, para cada clúster, añada una norma de correlación parecida a la siguiente:

```
Proxy /* http://cluster.domain.com/* cluster.domain.com
```

Nota: CBR establece el protocolo, el servidor y el puerto de destino más adelante.

Hay cuatro entradas que deben editarse para el plug-in de CBR:

- ServerInit
- PostAuth
- PostExit
- ServerTerm

Cada entrada debe estar en una sola línea. Hay varias instancias de "ServerInit" en el archivo `ibmproxy.conf`, una para cada plug-in. Se debe eliminar el comentario de las entradas para "CBR Plug-in".

A continuación se muestran las adiciones específicas realizadas en el archivo de configuración para cada uno de los sistemas operativos.

Figura 20. Archivo de configuración de CBR para sistemas AIX, Linux y Solaris

```
ServerInit /opt/ibm/edge/lb/servers/lib/liblbcbcr.so:ndServerInit
PostAuth /opt/ibm/edge/lb/servers/lib/liblbcbcr.so:ndPostAuth
PostExit /opt/ibm/edge/lb/servers/lib/liblbcbcr.so:ndPostExit
ServerTerm /opt/ibm/edge/lb/servers/lib/liblbcbcr.so:ndServerTerm
```

Figura 21. Archivo de configuración de CBR para sistemas HP-UX

```
ServerInit /opt/ibm/edge/lb/servers/lib/liblbcbcr.sl:ndServerInit
PostAuth /opt/ibm/edge/lb/servers/lib/liblbcbcr.sl:ndPostAuth
PostExit /opt/ibm/edge/lb/servers/lib/liblbcbcr.sl:ndPostExit
ServerTerm /opt/ibm/edge/lb/servers/lib/liblbcbcr.sl:ndServerTerm
```


Figura 22. Archivo de configuración de CBR para sistemas Windows

```
ServerInit C:\Archivos de programa\IBM\edge\lb\servers\lib\liblbcbr.dll:ndServerInit
PostAuth C:\Archivos de programa\IBM\edge\lb\servers\lib\liblbcbr.dll:ndPostAuth
PostExit C:\Archivos de programa\IBM\edge\lb\servers\lib\liblbcbr.dll:ndPostExit
ServerTerm C:\Archivos de programa\IBM\edge\lb\servers\lib\liblbcbr.dll:ndServerTerm
```

Paso 2. Iniciar la función de servidor

Para iniciar la función de servidor de CBR, escriba **cbrserver** en la línea de mandatos.

Un archivo de configuración por omisión (default.cfg) se carga de forma automática al iniciar cbrserver. Si decide guardar la configuración de CBR en default.cfg, todo lo que se guarde en este archivo se carga automáticamente la próxima vez que se inicie cbrserver.

Paso 3. Iniciar la función de ejecutor

Para iniciar la función de ejecutor, escriba el mandato **cbrcontrol executor start**. En este momento también puede cambiar varios valores del ejecutor. Consulte el apartado “dscontrol executor — control del ejecutor” en la página 359.

Paso 4. Definir un clúster y establecer opciones de clúster

CBR equilibrará las peticiones enviadas para el clúster a los servidores correspondientes configurados en los puertos para dicho clúster.

El clúster es el nombre simbólico situado en la parte del sistema principal del URL y debe coincidir con el nombre utilizado en la sentencia Proxy del archivo ibmproxy.conf.

Los clústeres definidos en CBR deben definirse de modo que coincidan con la petición entrante. Un clúster debe definirse con el mismo nombre de sistema principal o la misma dirección IP que la petición entrante que incluirá. Por ejemplo, si la petición se entra como la dirección IP, el clúster debe definirse como la dirección IP. Si hay más de un nombre de sistema principal que se resuelve en una sola dirección IP (y las peticiones pueden llegar con cualquiera de estos nombres de sistema principal), todos los nombres de sistema principal deben definirse como clústeres.

Para definir un clúster, emita el siguiente mandato:

```
cbrcontrol cluster add clúster
```

Para establecer las opciones del clúster, emita el siguiente mandato:

```
cbrcontrol cluster set clúster opción valor
```

Para obtener más información, consulte el Capítulo 27, “Referencia de mandatos para Dispatcher y CBR”, en la página 347.

Paso 5. Crear un alias para la tarjeta de interfaz de red (opcional)

Si ejecuta Caching Proxy configurado como proxy de retroceso, cuando se equilibra la carga para varios sitios Web, debe añadir la dirección del clúster para cada sitio

Web a, como mínimo, una de las tarjetas de interfaz de red de la máquina Load Balancer. De lo contrario, puede omitir este paso.

En sistemas **AIX**, **HP-UX**, **Linux** o **Solaris**: para añadir la dirección del clúster a la interfaz de red, utilice el siguiente mandato ifconfig. Utilice el mandato correspondiente a su sistema operativo tal como se muestra en la Tabla 8.

Tabla 8. Mandatos para crear alias para la NIC

AIX	ifconfig <i>nombre_interfaz</i> alias <i>dirección_clúster</i> netmask <i>máscara_red</i>
HP-UX	ifconfig <i>dirección_clúster</i> <i>nombre_interfaz</i> netmask <i>máscara_red</i> up
Linux	ifconfig <i>nombre_interfaz</i> <i>dirección_clúster</i> netmask <i>máscara_red</i> up
Solaris 8, Solaris 9 y Solaris 10	ifconfig <i>nombre_interfaz</i> addif <i>dirección_clúster</i> netmask <i>máscara_red</i> up

Nota: En sistemas Linux y HP-UX, *nombre_interfaz* debe ser un número exclusivo para cada dirección de clúster que se añade, por ejemplo: eth0:1, eth0:2, etc.

En sistemas **Windows 2000**: para añadir la dirección de clúster a la interfaz de red, haga lo siguiente:

1. Pulse **Inicio** > **Configuración** > **Panel de control**.
2. Efectúe una doble pulsación en **Conexiones de red y de acceso telefónico**.
3. Pulse con el botón derecho del ratón en **Conexión de área local**.
4. Seleccione **Propiedades**.
5. Seleccione **Protocolo de Internet (TCP/IP)** y pulse **Propiedades**.
6. Seleccione **Utilizar la siguiente dirección IP** y pulse **Avanzada**.
7. Pulse **Añadir** y luego escriba la **Dirección IP** y la **máscara de subred** para el clúster.

En sistemas **Windows 2003**: para añadir la dirección de clúster a la interfaz de red, haga lo siguiente:

1. Pulse **Inicio** > **Panel de control** > **Conexiones de red** > *Conexión de área local*
2. Pulse **Propiedades**.
3. Seleccione **Protocolo de Internet (TCP/IP)** y pulse **Propiedades**.
4. Seleccione **Utilizar la siguiente dirección IP** y pulse **Avanzada**.
5. Pulse **Añadir** y escriba la dirección IP y la máscara de subred para el clúster.

Paso 6. Definir puertos y establecer opciones de puertos

El número de puerto es el puerto en el que escuchan las aplicaciones del servidor. Para CBR con Caching Proxy ejecutando tráfico HTTP, es normalmente el puerto 80.

Para definir un puerto para el clúster definido en el paso anterior, emita el siguiente mandato:

```
cbrcontrol port add clúster:puerto
```

Para establecer las opciones del puerto, emita el siguiente mandato:

```
cbrcontrol port set clúster:puerto opción valor
```

Para obtener más información, consulte el Capítulo 27, “Referencia de mandatos para Dispatcher y CBR”, en la página 347.

Paso 7. Definir máquinas servidor con equilibrio de carga

Las máquinas servidor son las máquinas que ejecutan las aplicaciones en las que se desea realizar el equilibrio de carga. El *servidor* es el nombre simbólico o dirección decimal con puntos de la máquina servidor. Para definir un servidor en el clúster y puerto, emita el siguiente mandato:

```
cbrcontrol server add clúster:puerto:servidor
```

Debe definir más de un servidor por puerto en un clúster para llevar a cabo el equilibrio de carga.

Paso 8. Añadir normas a la configuración

Este es el paso clave en la configuración de CBR con Caching Proxy. Una norma define cómo una petición de URL se distinguirá y se enviará a un servidor del conjunto de servidores adecuado. El tipo de norma especial utilizado por CBR se denomina norma de contenido. Para definir una norma de contenido, emita el siguiente mandato:

```
cbrcontrol rule add clúster:puerto:norma type content pattern patrón
```

El valor *patrón* es la expresión regular que se compara con el URL en cada petición de cliente. Si desea más información sobre cómo configurar el patrón, consulte el Apéndice B, “Sintaxis de la norma de contenido (patrón)”, en la página 475.

En CBR también se pueden utilizar algunos otros tipos de normas definidos en Dispatcher. Para obtener más información, consulte el apartado “Configuración de equilibrio de carga basado en normas” en la página 212.

Paso 9. Añadir servidores a las normas

Cuando una norma coincide con una petición de cliente, se consulta el conjunto de servidores de la norma para saber qué servidor es el mejor. El conjunto de servidores de la norma es un subconjunto de los servidores definidos en el puerto. Para añadir servidores a un conjunto de servidores de una norma, emita el siguiente mandato:

```
cbrcontrol rule useserver clúster:puerto:servidor de normas
```

Paso 10. Iniciar la función de gestor (opcional)

La función de gestor mejora el equilibrio de carga. Para iniciar el gestor, emita el siguiente mandato:

```
cbrcontrol manager start
```

Paso 11. Iniciar la función de asesor (opcional)

Los asesores proporcionan al gestor más información sobre la capacidad que tienen de las máquinas de servidor con equilibrio de carga para responder a las peticiones. Un asesor es específico de un protocolo. Por ejemplo, para iniciar el asesor HTTP, emita el siguiente mandato:

```
cbrcontrol advisor start http puerto
```

Paso 12. Definir las proporciones del clúster según sea necesario

Si inicia asesores, puede modificar la proporción de la importancia dada a la información de asesor que se incluye en las decisiones para el equilibrio de carga. Para definir las proporciones del clúster, emita el mandato **cbrcontrol cluster set clúster proportions**. Para obtener más información, consulte el apartado “Proporción de la importancia otorgada a la información de estado” en la página 180.

Paso 13. Iniciar Caching Proxy

- Sistemas AIX: añada a la variable de entorno LIBPATH:
/opt/ibm/edge/lb/servers/lib
- Sistemas Linux, HP-UX o Solaris: añada a la variable de entorno LD_LIBRARY_PATH:
/opt/ibm/edge/lb/servers/lib
- Sistemas Windows: añada a la variable de entorno PATH:
C:\Archivos de programa\IBM\edge\lb\servers\lib

En el nuevo entorno, inicie Caching Proxy: en el indicador de mandatos, emita **ibmproxy**

Nota: En sistemas Windows: inicie Caching Proxy desde el panel Servicios:
Inicio-> Configuración-(para Windows 2000) > **Panel de control -> Herramientas administrativas -> Servicios.**

Ejemplo de configuración CBR

Para configurar CBR, siga estos pasos:

1. Inicie CBR: emita el mandato **cbrserver**.
2. Inicie la interfaz de línea de mandatos: emita el mandato **cbrcontrol**.
3. Aparecerá el indicador **cbrcontrol**. Emita los siguientes mandatos.
(*cluster(c),port(p),rule(r),server(s)*)
 - **executor start**
 - **cluster add c**
 - **port add c:p**
 - **server add c:p:s**
 - **rule add c:p:r type content pattern uri=***
 - **rule useserver c:p:r s**
4. Inicie Caching Proxy: emite el mandato **ibmproxy**. (En la plataforma Windows, inicie Caching Proxy desde el panel Servicios.
5. Elimine del navegador todas las configuraciones del proxy.
6. Cargue **http://c/** en el navegador, donde “c” es el clúster configurado anteriormente.
 - Se invoca el servidor “s”
 - Aparece la siguiente página Web **http://s/**

Parte 4. Componente Site Selector

Esta parte proporciona información sobre la configuración de inicio rápido, consideraciones de planificación y describe los métodos para configurar el componente Site Selector de Load Balancer. Contiene los capítulos siguientes:

- Capítulo 12, “Configuración de inicio rápido”, en la página 121
- Capítulo 13, “Planificación de Site Selector”, en la página 125
- Capítulo 14, “Configuración de Site Selector”, en la página 131

Capítulo 12. Configuración de inicio rápido

En este ejemplo de inicio rápido se muestra cómo crear una configuración de nombre de sitio con Site Selector para el tráfico de equilibrio de carga entre un conjunto de servidores según el nombre de dominio utilizado en una petición de cliente.

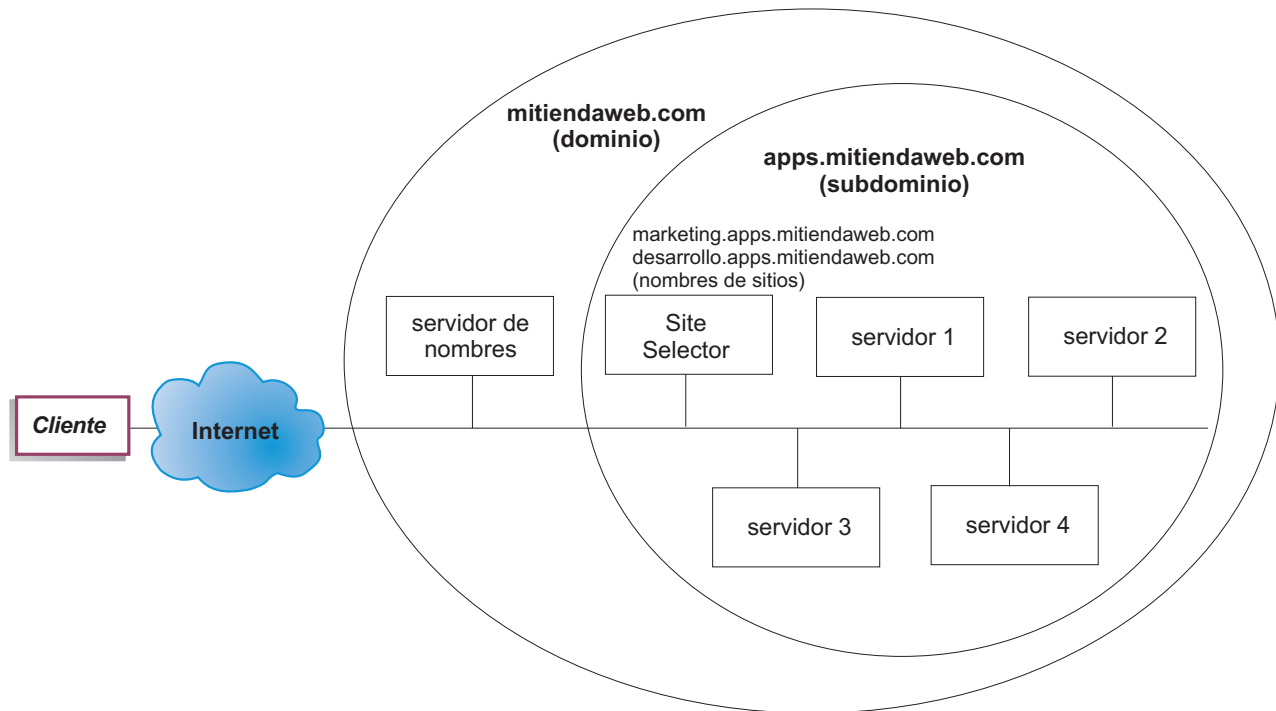


Figura 23. Configuración sencilla de Site Selector

Qué necesita

Para este ejemplo de configuración de inicio rápido, necesitará lo siguiente:

- Acceso administrativo al servidor de nombres de su sitio
- Cuatro servidores (servidor1, servidor2, servidor3, servidor4) configurados en la red y un servidor adicional con el componente Site Selector instalado

Nota: Si comparte la ubicación de Site Selector en uno de los servidores con equilibrio de carga, tendrá cuatro servidores en lugar de cinco. No obstante, la ubicación compartida influirá en el rendimiento de los servidores con equilibrio de carga.

Preparativos

Para este ejemplo de inicio rápido, el dominio del sitio de la empresa es mitiendaweb.com. Site Selector se encarga de un subdominio dentro de mitiendaweb.com. Por lo tanto, tendrá que definir un subdominio dentro de mitiendaweb.com. Por ejemplo: apps.mitiendaweb.com. Site Selector no es un DNS completamente implementado, como BIND y actúa como un nodo hoja en una

jerarquía de DNS. Site Selector tiene autoridad para el subdominio apps.mitiendaweb.com. El subdominio apps.mitiendaweb.com incluirá los nombres de sitio siguientes: marketing.apps.mitiendaweb.com y desarrollo.apps.mitiendaweb.com.

1. Actualice el servidor de nombres de dominio de la empresa (consulte la Figura 23 en la página 121). Cree un registro del servidor de nombres en el archivo de datos nombrado para el subdominio (apps.mitiendaweb.com) donde Site Selector es el servidor de nombres autorizado:
apps.mitiendaweb.com. IN NS siteselector.mitiendaweb.com
2. Asegúrese de que el nombre de sistema principal plenamente cualificado o sitio no se resuelve en el sistema de nombre de dominio actual.
3. Instale Metric Server en los servidores (servidor1, servidor2, servidor3, servidor4) de los que tiene previsto que Site Selector equilibre la carga. Si desea más información, consulte el apartado "Metric Server" en la página 196.

Configuración del componente Site Selector

Con Site Selector, puede crear una configuración mediante la línea de mandatos, el asistente de configuración o la interfaz gráfica de usuario (GUI). Para este ejemplo de inicio rápido, los pasos de configuración se demuestran utilizando la línea de mandatos.

Nota: Los valores de los parámetros deben escribirse en caracteres del idioma inglés. Las únicas excepciones son los valores de parámetros para los nombres de sistemas principales y de archivos.

Configuración con la línea de mandatos

Desde un indicador de mandatos, siga estos pasos:

1. Inicie sssserver en la máquina que alberga a Site Selector. Como usuario root o administrador, emita lo siguiente desde el indicador de mandatos: **sssserver**

Nota: Para la plataforma Windows: inicie sssserver (IBM Site Selector) desde el panel Servicios: **Inicio > Configuración** (para Windows 2000) > **Panel de control > Herramientas administrativas > Servicios**.

2. Inicie el servidor de nombres en la configuración de Site Selector:
sscontrol nameserver start
3. Configure los nombres de sitio (marketing.apps.mitiendaweb.com y desarrollo.apps.mitiendaweb.com) en Site Selector:
sscontrol sitename add marketing.apps.mitiendaweb.com
sscontrol sitename add desarrollo.apps.mitiendaweb.com
4. Añada los servidores a la configuración de Site Selector. (Configure servidor1 y servidor2 con el nombre de sitio marketing.apps.mitiendaweb.com. Configure servidor3 y servidor4 con el nombre de sitio desarrollo.apps.mitiendaweb.com):
sscontrol server add marketing.apps.mitiendaweb.com:servidor1+servidor2
sscontrol server add desarrollo.apps.mitiendaweb.com:servidor3+servidor4
5. Inicie la función de gestor de Site Selector:
sscontrol manager start
6. Inicie la función de asesor de Site Selector (asesor de HTTP para marketing.apps.mitiendaweb.com y asesor de FTP para desarrollo.apps.mitiendaweb.com):
sscontrol advisor start http marketing.apps.mitiendaweb.com:80

sscontrol advisor start ftp desarrollo.apps.mitiendaweb.com:21

Site Selector ahora se asegurará de que no se envíen las peticiones de cliente a un servidor con anomalías.

7. Asegúrese de que se ha iniciado Metric Server en cada uno de los servidores con equilibrio de carga.

Ya se ha completado la configuración básica de Site Selector.

Prueba de la configuración

Compruebe si la configuración funciona:

1. Desde un cliente, que tenga un DNS primario configurado como el servidor de nombres encargado de mitiendaweb.com, intente ejecutar ping en uno de los nombres de sitio configurados.
2. Conecte con la aplicación. Por ejemplo:
 - Abra un navegador, solicite marketing.apps.mitiendaweb.com y se servirá una página válida.
 - Abra un cliente FTP en desarrollo.apps.mitiendaweb.com y especifique un usuario y contraseña válidos.
3. Busque los resultados del mandato siguiente:

sscontrol server status marketing.apps.mitiendaweb.com:

sscontrol server status desarrollo.apps.mitiendaweb.com:

La entrada de total de aciertos de cada servidor debería sumarse al ping y a la petición de aplicación.

Configuración con la interfaz gráfica de usuario (GUI)

Si desea información sobre cómo utilizar la GUI de Site Selector, consulte el apartado “GUI” en la página 132 y el Apéndice A, “GUI: instrucciones generales”, en la página 467.

Configuración con el asistente de configuración

Si desea información sobre cómo utilizar el asistente de Site Selector, consulte el apartado “Asistente de configuración” en la página 134.

Capítulo 13. Planificación de Site Selector

En este capítulo se describe lo que debe tener en cuenta el planificador de la red antes de instalar y configurar el componente Site Selector.

- Si desea obtener una visión general de características que están disponibles para gestionar la red consulte el Capítulo 3, “Gestión de la red: determinación de las características de Load Balancer que se van a utilizar”, en la página 19.
- Si desea información sobre cómo configurar parámetros de equilibrio de carga del componente Site Selector, consulte el Capítulo 14, “Configuración de Site Selector”, en la página 131.
- Si desea información sobre cómo configurar Load Balancer para obtener funciones más avanzadas, consulte el Capítulo 22, “Características avanzadas para Dispatcher, CBR y Site Selector”, en la página 201.
- Si desea información sobre administración autenticada remota, archivos de anotaciones cronológicas de Load Balancer y el uso de los componentes de Load Balancer consulte el Capítulo 24, “Operación y gestión de Load Balancer”, en la página 261.

Este capítulo incluye los apartados siguientes:

- “Consideraciones de planificación”
- “Consideraciones de TTL” en la página 127
- “Utilización de la característica proximidad de red” en la página 128

Consideraciones de planificación

Site Selector funciona junto con un servidor de nombres de dominio para realizar el equilibrio de carga entre un grupo de servidores utilizando medidas y pesos que se recopilan. Puede crear una configuración de sitio para permitir el tráfico de equilibrio de carga entre un grupo de servidores según el nombre de dominio utilizado para una petición del cliente.

Limitaciones: Site Selector únicamente da soporte a las consultas DNS de tipo A. Cualquier otro tipo de consulta generará un código de retorno NOTIMPL (no se implementa). Si todo el dominio se delega a Site Selector, asegúrese de que el dominio sólo reciba consultas de tipo A.

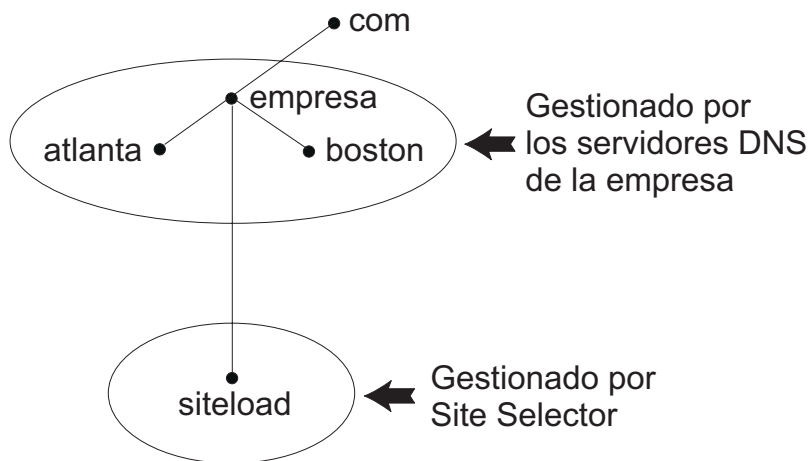


Figura 24. Ejemplo de un entorno DNS

Cuando se configura un subdominio para Site Selector dentro del entorno de DNS, Site Selector debe tener autoridad sobre su propio subdominio. Por ejemplo (consulte la Figura 24), se ha asignado a su empresa autoridad sobre el dominio **empresa.com**. Dentro de la empresa, hay varios subdominios. Site Selector tendría autoridad de **siteload.empresa.com**, mientras que el servidor o los servidores DNS seguirán manteniendo la autoridad de **atlanta.empresa.com** y **boston.empresa.com**.

Para que el servidor de nombres de la empresa reconozca que Site Selector tiene autoridad del subdominio siteload, será necesario añadir una entrada de servidor de nombres al archivo de datos nombrado. Por ejemplo, en sistemas AIX, un servidor de nombres se parecería a lo siguiente:

```
siteload.empresa.com. IN NS siteselector.empresa.com.
```

Donde **siteselector.empresa.com** es el nombre de sistema principal de la máquina Site Selector. Sería necesario crear entradas equivalentes en cualquier otro archivo de base de datos nombrado para que los servidores DNS lo utilicen.

Un cliente somete una petición de resolución de un nombre de dominio a un servidor de nombres dentro de su red. El servidor de nombres reenvía la petición a la máquina Site Selector. Site Selector luego soluciona el nombre de dominio con la dirección IP de uno de los servidores que se han configurado bajo el nombre de sitio. Site Selector devuelve la dirección IP del servidor seleccionado al servidor de nombres. El servidor de nombres devuelve la dirección IP al cliente. (Site Selector actúa como un servidor de nombres no recursivo (nodo hoja) y devolverá un error si no resuelve la petición de nombre de dominio).

Consulte la Figura 5 en la página 14 que ilustra un sitio en el que se utiliza Site Selector junto con un sistema de DNS para equilibrar la carga entre servidores locales y remotos.

Site Selector consta de estas funciones:

- **ssserver** gestiona la petición de la línea de mandatos en el servidor de nombres, el gestor y los asesores.
- La función **servidor de nombres** admite el equilibrio de carga de peticiones de servidor de nombres de entrada. Debe iniciar la función de servidor de nombres para que Site Selector empiece a proporcionar la resolución de DNS. Site Selector está a la escucha de peticiones de DNS de entrada en el puerto 53. Si se

configura el nombre de sitio solicitante, Site Selector devuelve una sola dirección de servidor (de un conjunto de direcciones de servidor) asociada al nombre de sitio.

- El **gestor** establece pesos utilizados por el servidor de nombres basándose en:
 - Información de retorno de los servidores proporcionada por los asesores
 - Información de retorno de un programa de supervisión del sistema, como Metric Server.

La utilización del gestor es opcional. No obstante, si no se utiliza el gestor, se realiza el equilibrio de carga utilizando la planificación de turno rotativo sopesado según los pesos del servidor actual y no estarán disponibles los asesores.

- **Metric Server** es un componente supervisor del sistema de Load Balancer que se instala en la máquina servidor final. (Si Load Balancer tiene una ubicación compartida en una máquina servidor donde se está equilibrando la carga, debería instalar Metric Server en la máquina Load Balancer).

Con Metric Server, Site Selector puede supervisar el nivel de actividad de un servidor, detectar si un servidor tiene la carga menos pesada o si un servidor está anómalo. La carga es una medida de cuánto está trabajando el servidor. El administrador Site Selector de sistema controla el tipo de medida utilizado para medir la carga. Puede configurar Site Selector de modo que se adapte a su entorno, teniendo en cuenta factores como la frecuencia de acceso, el número total de usuarios y los tipos de acceso (por ejemplo, consultas breves, consultas de larga ejecución o cargas con mucha utilización de la CPU).

El equilibrio de carga se realiza según los pesos del servidor. Para Site Selector, hay cuatro proporciones que el gestor utiliza para determinar pesos:

- CPU
- memoria
- puerto
- sistema

Metric Server suministra todos los valores de CPU y memoria. Por consiguiente, se *recomienda* el uso de Metric Server con el componente Site Selector.

Si desea más información, consulte el apartado “Metric Server” en la página 196.

- Los **asesores** consultan los servidores y analizan los resultados por protocolo antes de llamar al gestor para establecer pesos según corresponda. Quizá no tenga sentido utilizar algunos de estos asesores en una configuración típica. También tiene la opción de escribir sus propios asesores. El uso de asesores es opcional, pero se recomienda. Si desea más información, consulte el apartado “Asesores” en la página 185.
- Para configurar y gestionar el servidor de nombres, los asesores, Metric Server y el gestor, utilice la línea de mandatos (**sscontrol**) o la interfaz gráfica de usuario (**Ibadmin**).

Las cuatro funciones clave de Site Selector (servidor de nombres, gestor, Metric Server y asesores) interactúan para equilibrar y solucionar las peticiones de entrada entre servidores.

Consideraciones de TTL

El uso del equilibrio de carga según el DNS requiere que se inhabilite la colocación en antememoria de la resolución de nombres. El valor de TTL (tiempo de vida) determina la eficacia del equilibrio de carga según el DNS. TTL determina cuándo tiempo otro servidor de nombres colocará en antememoria la respuesta resuelta.

Valores de TTL pequeños permiten que cambios pequeños en la carga del servidor o de red se realicen de forma más ágil. No obstante, para inhabilitar la colocación en antememoria se requiere que los clientes se pongan en contacto con el servidor de nombres autorizado para todas las peticiones de resolución de nombres, así se aumenta potencialmente la latencia del cliente. Cuando se selecciona un valor de TTL, debería tenerse en cuenta el impacto que tendrá sobre el entorno la inhabilitación de la antememoria. Tenga en cuenta también que el equilibrio de carga según el DNS se puede limitar por la colocación en antememoria del cliente de las resoluciones de nombres.

Se puede configurar TTL utilizando el mandato **sscontrol sitename [add | set]** . Si desea más información, consulte el apartado “sscontrol sitename — configurar un nombre de sitio” en la página 426.

Utilización de la característica proximidad de red

La proximidad de red es el cálculo de la cercanía de cada servidor al cliente solicitante. Para determinar la proximidad de red, el agente Metric Server (que debe residir en cada servidor con equilibrio de carga) envía un ping a la dirección IP cliente y devuelve el tiempo de respuesta a Site Selector. Site Selector utiliza la respuesta de proximidad en la decisión de equilibrio de carga. Site Selector combina el valor de respuesta de proximidad de red con el peso del gestor para crear un valor de peso final combinado para el servidor.

El uso de la característica proximidad de red con Site Selector es opcional.

Site Selector proporciona estas opciones de proximidad de red que se pueden establecer por nombre de sitio:

- Duración en antememoria: la cantidad de tiempo que será válida una respuesta de proximidad y que se guardará en antememoria.
- Porcentaje de proximidad: la importancia de la respuesta de proximidad frente al estado del servidor (de entrada del peso del gestor).
- Esperar todas: determina si se va a esperar a todas las respuestas de proximidad (ping) de los servidores antes de responder a la petición del cliente.

Si se establece en **sí**, Metric Server ejecuta ping en el cliente para obtener el tiempo de respuesta de proximidad. El servidor de nombres espera a que todos los Metric Servers respondan o a que se exceda el tiempo de espera. Luego, para cada servidor, el servidor de nombres combina el tiempo de respuesta de proximidad con el peso que ha calculado del gestor para crear un valor de “peso combinado” para cada servidor. Site Selector suministrará al cliente la dirección IP del servidor con la mejor combinación de peso. (Se espera para la mayoría de servidores de nombres de cliente que tengan un tiempo de espera de 5 segundos. Site Selector intenta responder antes de que se supere el tiempo de espera).

Si se establece en **no**, se proporciona al cliente una resolución de nombres según los pesos del gestor actuales. A continuación, Metric Server ejecuta ping en el cliente para obtener el tiempo de respuesta de la proximidad. El servidor de nombres coloca en antememoria el tiempo de respuesta que recibe de Metric Server. Cuando el cliente vuelve por una segunda petición, el servidor de nombres combina el peso del gestor actual con el valor de respuesta del mandato ping colocado en antememoria para que cada servidor obtenga el servidor con el mejor “peso combinado”. Site Selector devuelve esta dirección IP del servidor al cliente para la segunda petición.

Se pueden establecer las opciones de proximidad de red en el mandato **sscontrol sitename [add | set]** . Si desea más información, consulte el Capítulo 28, “Referencia de mandatos para Site Selector”, en la página 403.

Capítulo 14. Configuración de Site Selector

Antes de llevar a cabo los pasos de este capítulo, consulte el Capítulo 13, “Planificación de Site Selector”, en la página 125. En este capítulo se explica cómo crear una configuración básica para el componente Site Selector de Load Balancer.

- En el Capítulo 21, “Funciones del gestor, asesores y Metric Server para Dispatcher, CBR y Site Selector”, en la página 179 y el Capítulo 22, “Características avanzadas para Dispatcher, CBR y Site Selector”, en la página 201 encontrará configuraciones más complejas de Load Balancer.
- En el Capítulo 24, “Operación y gestión de Load Balancer”, en la página 261 encontrará información sobre la administración autenticada remota, las anotaciones cronológicas de Load Balancer y el uso de los componentes de Load Balancer.

Visión general de las tareas de configuración

Nota: Antes de empezar a realizar los pasos de configuración indicados en esta tabla, asegúrese de que la máquina Site Selector y todas las máquinas de servidores están conectadas a la red, tienen direcciones IP válidas y que pueden enviar una sonda de paquetes Internet entre sí.

Tabla 9. Tareas de configuración para el componente Site Selector

Tarea	Descripción	Información relacionada
Configurar la máquina Site Selector.	Averigua los requisitos.	“Configuración de la máquina Site Selector” en la página 134
Configurar máquinas en las que se va a equilibrar la carga.	Configura la configuración de equilibrio de carga.	“Paso 4. Definir máquinas servidor con equilibrio de carga” en la página 135

Métodos de configuración

Para crear una configuración básica para el componente Site Selector de Load Balancer, hay cuatro métodos básicos para configurar el componente Site Selector:

- Línea de mandatos
- Scripts
- Interfaz gráfica de usuario (GUI)
- Asistente de configuración

Línea de mandatos

Es la manera más directa de configurar Site Selector. Los valores de los parámetros de mandatos deben especificarse en caracteres del idioma inglés. Las únicas excepciones son los nombres de sistema principal (se utiliza, por ejemplo, en los mandatos de nombre de sitio y servidor) y los nombres de archivo.

Para iniciar Site Selector desde la línea de mandatos:

1. Emita el mandato **sssserver** en el indicador de mandatos. Para detener el servicio, escriba **sssserver stop**

Nota: En sistemas Windows, pulse **Inicio > Configuración** (en Windows 2000) **> Panel de control > Herramientas administrativas > Servicios**. Pulse con el botón derecho del ratón en **IBM Site Selector** y seleccione **Iniciar**. Para detener el servicio, efectúe los mismos pasos y seleccione **Detener**.

2. A continuación, emita los mandatos de control de Site Selector que desee para definir la configuración. En los procedimientos de esta publicación se da por supuesto que se utiliza la línea de mandatos. El mandato es **sscontrol**. Para obtener más información sobre los mandatos, consulte el Capítulo 28, “Referencia de mandatos para Site Selector”, en la página 403.

Puede escribir una versión minimizada de los parámetros del mandato **sscontrol**. Sólo es necesario especificar las letras exclusivas de los parámetros. Por ejemplo, para obtener ayuda sobre el mandato para guardar archivos, puede escribir **sscontrol he f** en lugar de **sscontrol help file**.

Para iniciar la interfaz de línea de mandatos, emita **sscontrol** para recibir un indicador de mandatos de **sscontrol**.

Para finalizar la interfaz de línea de mandatos, emita **exit** o **quit**.

Nota: En la plataforma Windows, se inicia automáticamente el **dsserver** del componente Dispatcher. Si sólo utiliza Site Selector y no emplea el componente Dispatcher, puede evitar que **dsserver** se inicie de forma automática haciendo lo siguiente:

1. En Servicios Windows, pulse con el botón derecho del ratón en **IBM Dispatcher**.
2. Seleccione **Propiedades**.
3. En el campo **Tipo de inicio**, seleccione **Manual**.
4. Pulse **Aceptar** y cierre la ventana **Servicios**.

Scripts

Los mandatos para configurar Site Selector pueden especificarse y ejecutarse juntos en un archivo de script de configuración.

Nota: Para ejecutar rápidamente el contenido de un archivo de script (por ejemplo, **miscript**), use cualquiera de los siguientes mandatos:

- Para actualizar la configuración actual, ejecute los mandatos ejecutables del archivo de script utilizando —
sscontrol file appendload miscript
- Para sustituir completamente la configuración actual, ejecute los mandatos ejecutables del archivo de script utilizando —
sscontrol file newload miscript

Para guardar la configuración actual en un archivo de script (por ejemplo, **guardascript**), ejecute el siguiente mandato:

sscontrol file save guardascript

Este mandato guardará el archivo de script de configuración en el directorio **...ibm/edge/lb/servers/configurations/ss**.

GUI

Para obtener instrucciones y un ejemplo de la GUI, consulte la Figura 41 en la página 468.

Para iniciar la GUI, siga estos pasos

1. Asegúrese de que `ssserver` se está ejecutando. Como usuario `root` o administrador, emita lo siguiente en el indicador de mandatos: **`ssserver`**
2. A continuación, realice una de las acciones siguientes:
 - En sistemas AIX, HP-UX, Linux o Solaris, escriba **`lbadm`**
 - En sistemas Windows, pulse **Inicie > Programas IBM WebSphere > Edge Components > IBM Load Balancer > Load Balancer**

Para configurar el componente Site Selector desde la GUI, primero debe seleccionar **Site Selector** en la estructura de árbol. Una vez que se ha conectado a un `ssserver` que se ejecuta en un sistema principal, puede crear nombres de sitio que contiene servidores, iniciar el gestor e iniciar los asesores.

La GUI puede utilizarse para llevar a cabo las mismas tareas que realizaría con el mandato **`sscontrol`**. Por ejemplo, para definir un nombre de sitio con la línea de mandatos, especifique el mandato **`sscontrol sitename add nombre_sitio`**. Para definir un nombre de sitio desde la GUI, pulse con el botón derecho del ratón en Servidor de nombres y, a continuación, en el menú emergente, pulse con el botón izquierdo del ratón en **Añadir nombre de sitio**. Escriba el nombre del sitio en la ventana emergente y pulse **Aceptar**.

Los archivos de configuración de Site Selector preexistentes pueden cargarse con las opciones **Cargar nueva configuración** (para sustituir completamente la configuración actual) y **Añadir a la configuración actual** (para actualizar la configuración actual) que aparecen en el menú emergente **Sistema principal**. Debe guardar de forma periódica la configuración de Site Selector en un archivo con la opción **Guardar archivo de configuración como** que también se encuentra en el menú emergente **Sistema principal**. El menú **Archivo** situado en la parte superior de la GUI, permite guardar en un archivo las conexiones actuales del sistema principal o restaurar conexiones que se encuentran en archivos existentes en todos los componentes de Load Balancer.

Para ejecutar un mandato desde la GUI: resalte el nodo Sistema principal en el árbol de la GUI y seleccione **Enviar mandato....** en el menú emergente Sistema principal. En el campo de entrada de mandatos, escriba el mandato que desea ejecutar, por ejemplo: **`nameserver status`**. Aparecerán en la ventana proporcionada los resultados y el historial de los mandatos ejecutados en la sesión actual.

Para acceder a la **Ayuda**, pulse el icono de signo de interrogación situado en la esquina superior derecha de la ventana de Load Balancer.

- **Ayuda: Nivel de campo** — describe cada campo, los valores por omisión
- **Ayuda: Cómo puedo** — lista las tareas que pueden llevarse a cabo desde esa pantalla
- **InfoCenter** — proporciona acceso centralizado a la información del producto

Si desea más información sobre cómo utilizar la GUI, consulte el Apéndice A, “GUI: instrucciones generales”, en la página 467.

Asistente de configuración

Si va a utilizar el asistente de configuración, siga estos pasos:

1. Inicie el `sssserver` en Site Selector:

- Ejecute lo siguiente como usuario root o administrador:

sssserver

2. Inicie la función de asistente de Site Selector, **sswizard**.

Inicie este asistente desde el indicador de mandatos; para ello, emita el mandato **sswizard**. O bien, seleccione el Asistente de configuración desde el menú del componente Site Selector como se presenta en la GUI.

El asistente de Site Selector le guiará, paso a paso, a través del proceso de creación de una configuración básica para el componente Site Selector. Formula preguntas sobre la red y le guía mientras define un nombre de sitio que permite a Site Selector equilibrar la carga de tráfico entre un grupo de servidores.

Configuración de la máquina Site Selector

Para configurar la máquina Site Selector, debe ser el usuario root (en sistemas AIX, HP-UX, Linux o Solaris) o el administrador (en los sistemas Windows).

Necesitará un nombre de sistema principal que no es posible resolver para utilizarlo como nombre de sitio para el grupo de servidores que configura. El nombre de sitio es el nombre que los clientes utilizan para acceder al sitio (como `www.suempresa.com`). Site Selector equilibrará la carga del tráfico de este nombre de sitio entre el grupo de servidores mediante DNS.

Paso 1. Iniciar la función de servidor

Para iniciar la función de servidor de Site Selector, escriba **sssserver** en la línea de mandatos.

Nota: Un archivo de configuración por omisión (`default.cfg`) se carga de forma automática al iniciar `sssserver`. Si decide guardar la configuración en `default.cfg`, todo lo que se guarde en este archivo se cargará automáticamente la próxima vez que se inicie `sssserver`.

Paso 2. Iniciar el servidor de nombres

Para iniciar el servidor de nombres, escriba el mandato **sscontrol nameserver start**.

De forma opcional, inicie el servidor de nombres utilizando la palabra clave `bindaddress` para establecer el enlace únicamente con la dirección especificada.

Paso 3. Definir un nombre de sitio y establecer las opciones del nombre de sitio

Site Selector equilibrará las peticiones enviadas para el nombre de sitio a los servidores correspondientes configurados para ello.

El nombre de sitio es un nombre de sistema principal que no es posible resolver que el cliente solicitará. El nombre de sitio debe ser un nombre de dominio plenamente cualificado (por ejemplo, `www.dnsdownload.com`). Cuando un cliente solicita este nombre de sitio, se devuelve una de las direcciones IP de servidor asociadas con el nombre de sitio.

Para definir un nombre de sitio, emita el siguiente mandato:

```
sscontrol sitename add nombre_sitio
```

Para establecer las opciones del nombre de sitio, emita el siguiente mandato:

```
sscontrol sitename set nombre_sitio opción valor
```

Para obtener más información, consulte el Capítulo 28, “Referencia de mandatos para Site Selector”, en la página 403.

Paso 4. Definir máquinas servidor con equilibrio de carga

Las máquinas servidor son las máquinas que ejecutan las aplicaciones en las que se desea realizar el equilibrio de carga. El *servidor* es el nombre simbólico o dirección decimal con puntos de la máquina servidor. Para definir un servidor en el nombre de sitio desde el paso 3, emita el siguiente mandato:

```
sscontrol server add nombre_sitio:servidor
```

Para poder realizar el equilibrio de carga, debe definir más de un servidor bajo un nombre de sitio.

Paso 5. Iniciar la función de gestor (opcional)

La función de gestor mejora el equilibrio de carga. Antes de iniciar la función de gestor, asegúrese de que Metric Server está instalado en todas las máquinas con equilibrio de carga.

Para iniciar el gestor, emita el siguiente mandato:

```
sscontrol manager start
```

Paso 6. Iniciar la función de asesor (opcional)

Los asesores proporcionan al gestor más información sobre la capacidad que tienen de las máquinas de servidor con equilibrio de carga para responder a las peticiones. Un asesor es específico de un protocolo. Load Balancer ofrece muchos asesores. Por ejemplo, para iniciar el asesor HTTP para un nombre de sitio específico, emita el siguiente mandato:

```
sscontrol advisor start http nombre_sitio:puerto
```

Paso 7. Definir la métrica del sistema (opcional)

Consulte el apartado “Metric Server” en la página 196 para obtener información sobre la utilización de métrica de sistema y Metric Server.

Paso 8. Definir las proporciones del nombre de sitio según sea necesario

Si inicia asesores, puede modificar la proporción de la importancia dada a la información (puerto) de asesor que se incluye en las decisiones para el equilibrio de carga. Para definir las proporciones del nombre de sitio, emita el mandato **sscontrol sitename set *nombre_sitio* proportions**. Para obtener más información, consulte el apartado “Proporción de la importancia otorgada a la información de estado” en la página 180.

Configuración de máquinas de servidor para el equilibrio de carga

Utilice Metric Server con el componente Site Selector. Consulte el apartado “Metric Server” en la página 196 para obtener información sobre cómo configurar Metric Server en todas las máquinas de servidor en las que Site Selector está realizando el equilibrio de carga.

Parte 5. Componente Cisco CSS Controller

Esta parte proporciona información sobre la configuración de inicio rápido, consideraciones de planificación y describe los métodos para configurar el componente Cisco CSS Controller de Load Balancer. Contiene los capítulos siguientes:

- Capítulo 15, “Configuración de inicio rápido”, en la página 139
- Capítulo 16, “Planificación de Cisco CSS Controller”, en la página 143
- Capítulo 17, “Configuración de Cisco CSS Controller”, en la página 149

Capítulo 15. Configuración de inicio rápido

Este ejemplo de inicio rápido muestra cómo crear una configuración mediante el componente Cisco CSS Controller. Cisco CSS Controller proporciona información de pesos del servidor que ayuda a Conmutador Cisco CSS a determinar la selección de servidor óptima para decisiones de equilibrio de carga.

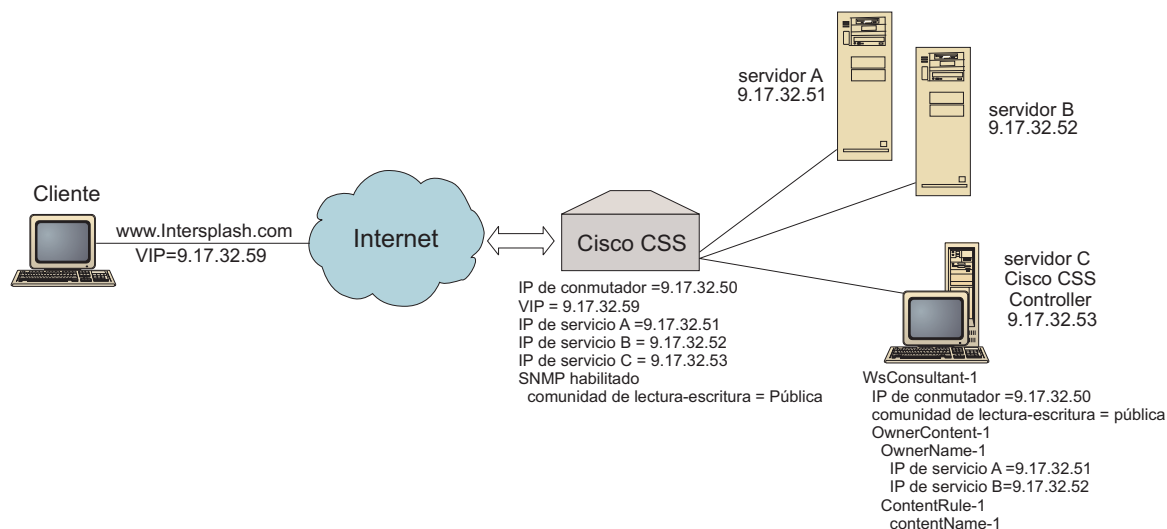


Figura 25. Configuración sencilla de Cisco CSS Controller

Qué necesita

Para este ejemplo de configuración de inicio rápido, necesitará lo siguiente:

- Conmutador Cisco CSS
- Máquina servidor con el componente Cisco CSS Controller
- Dos máquinas servidor Web
- Este ejemplo de configuración requiere cinco direcciones IP:
 - Una dirección IP que puede proporcionar a los clientes para acceder al sitio Web, www.Intersplashx.com (9.17.32.59)
 - Una dirección IP para una interfaz (pasarela) a Conmutador Cisco CSS (9.17.32.50)
 - Una dirección IP para el servidor A (9.17.32.51)
 - Una dirección IP para el servidor B (9.17.32.52)
 - Una dirección IP para el servidor C de Cisco CSS Controller (9.17.32.53)

Preparativos

Asegúrese de se completan estos pasos antes de comenzar la configuración de este ejemplo:

- Asegúrese de que el Conmutador Cisco CSS está configurado correctamente. Si desea información de configuración, consulte el manual *Cisco Content Services Switch Getting Started Guide*.

- Asegúrese de que la máquina Cisco CSS Controller puede ejecutar ping de: Conmutador Cisco CSS (9.17.32.50), el servidor A (9.17.32.51) y el servidor B (9.17.32.52).
- Asegúrese de que la máquina cliente puede ejecutar ping de VIP (9.17.32.59)

Configuración del componente Cisco CSS Controller

Con Cisco CSS Controller, puede crear una configuración mediante la línea de mandatos o la interfaz gráfica de usuario (GUI). Para este ejemplo de inicio rápido, los pasos de configuración se demuestran utilizando la línea de mandatos.

Nota: Los valores de los parámetros deben escribirse en caracteres del idioma inglés. Las únicas excepciones son los valores de parámetros para los nombres de sistemas principales y de archivos.

Configuración con la línea de mandatos

Desde un indicador de mandatos, siga estos pasos:

1. Inicie ccoserver en Load Balancer. Como usuario root o administrador, emita lo siguiente desde el indicador de mandatos: **ccoserver**
2. Añada un consultor de conmutador a la configuración de Cisco CSS Controller, especificando la dirección de la interfaz IP de Conmutador Cisco CSS y el nombre de comunidad de lectura-grabación. Estos valores deben coincidir con los atributos correspondientes en Conmutador Cisco CSS:

```
cococontrol consultant add SwConsultant-1 address 9.17.32.50 community public
```

Esto comprobará la conectividad con Conmutador Cisco CSS y verificará que el nombre de comunidad de lectura-grabación SNMP funciona correctamente.

3. Añada ownercontent (OwnerContent-1) al consultor de conmutador, especificando ownername (OwnerName-1) y contentrule (ContentRule-1):

```
cococontrol ownercontent add SwConsultant-1:OwnerContent-1 ownername OwnerName-1 contentrule ContentRule-1
```

Estos valores deben coincidir con los atributos correspondientes en Conmutador Cisco CSS.

Cisco CSS Controller puede ahora comunicarse con el conmutador en SNMP y obtendrá la información de configuración necesaria del conmutador. Después de este paso, aparecerá información en Cisco CSS Controller acerca de qué servicios están configurados en Conmutador Cisco CSS para el ownercontent especificado.

4. Configure el tipo de métricas que va a recopilar (conexión activa, velocidad de conexión, HTTP) y la proporción para cada métrica en ownercontent:

```
cococontrol ownercontent metrics SwConsultant-1:OwnerContent-1 activeconn 45 connrate 45 http 10
```

Este mandato configurará qué información de métrica y proporción desea recopilar de los servicios que se va a utilizar para el cálculo de peso. La proporción total de todas las métricas debe ser igual a 100.

5. Inicie la función de consultor de conmutador de Cisco CSS Controller:

```
cococontrol consultant start SwConsultant-1
```

Con este mandato, se iniciarán todos los recopiladores de métricas y comenzarán los cálculos de peso de servicio. Cisco CSS Controller comunica el resultado de sus cálculos de peso de servicio a Conmutador Cisco CSS mediante SNMP.

La configuración básica de Cisco CSS Controller ahora está completa.

Prueba de la configuración

Compruebe si la configuración funciona:

1. Desde el navegador Web cliente, vaya a la ubicación **http://www.Intersplashx.com**. Si se visualiza una página, significa que la configuración funciona.
2. Vuelva a cargar la página en el navegador Web.
3. Observe los resultados del mandato siguiente: **ccocontrol service report SwConsultant-1:OwnerContent-1:Service-1**. La columna de conexiones totales de los dos servidores Web debería sumarse a "2."

Configuración con la interfaz gráfica de usuario (GUI)

Si desea información sobre cómo utilizar la GUI de Cisco CSS Controller, consulte el apartado "GUI" en la página 151 y el Apéndice A, "GUI: instrucciones generales", en la página 467.

Capítulo 16. Planificación de Cisco CSS Controller

En este capítulo se describe lo que debe tener en cuenta el planificador de la red antes de instalar y configurar el componente Cisco CSS Controller.

- Si desea información sobre cómo configurar parámetros de equilibrio de carga del componente Cisco CSS Controller, consulte el Capítulo 17, “Configuración de Cisco CSS Controller”, en la página 149.
- Si desea información sobre cómo configurar Load Balancer para obtener funciones más avanzadas, consulte el Capítulo 23, “Características avanzadas de Cisco CSS Controller y Nortel Alteon Controller”, en la página 243.
- Si desea información sobre administración autenticada remota, archivos de anotaciones cronológicas de Load Balancer y el uso de los componentes de Load Balancer consulte el Capítulo 24, “Operación y gestión de Load Balancer”, en la página 261.

Este capítulo incluye:

- “Requisitos del sistema”
- “Consideraciones de planificación”
 - “Colocación del consultor en la red” en la página 144
 - “Alta disponibilidad” en la página 146
 - “Cálculo de pesos” en la página 147
 - “Determinación de problemas” en la página 147

Requisitos del sistema

Si desea obtener los requisitos de hardware y software, visite la siguiente página Web: <http://www.ibm.com/support/docview.wss?rs=180&uid=swg27006921>

También necesitará

- Sistema en el que se va a ejecutar Cisco CSS Controller.
- Conmutador Cisco CSS 11000 Series Content Services instalado y configurado

Consideraciones de planificación

Cisco CSS Controller gestiona un conjunto de consultores de conmutador. Cada consultor determina pesos para servicios a los que un solo conmutador equilibra la carga. El conmutador para el que el consultor proporciona pesos se configura para equilibrar la carga del contenido. El consultor utiliza el protocolo SNMP para enviar los pesos calculados al conmutador. El conmutador utiliza los pesos para seleccionar un servicio para la norma de contenido que está equilibrando la carga cuando el algoritmo de equilibrio de carga es de turno rotativo sopesado. Para determinar los pesos, el consultor utiliza uno o más fragmentos de información:

- Disponibilidad y tiempos de respuesta, determinados mediante el uso de **asesores** que se comunican con aplicaciones en ejecución en el servicio.
- Información de la carga del sistema, determinada al recuperar un valor de métrica de **agentes Metric Server** en ejecución en el servicio.
- Información de conexión sobre los servicios, obtenida del conmutador.
- Información de accesibilidad, obtenida de ejecutar ping en los servicios.

Si desea una descripción del equilibrio de carga del contenido o información detallada sobre cómo configurar el conmutador, consulte el manual *Cisco Content Services Switch Getting Started Guide*.

Para que un consultor obtenga la información necesaria para determinar los pesos del servicio, debe tener:

- Conectividad IP entre el consultor y los servicios para los que se calculan los pesos.
- Conectividad IP entre el consultor y el conmutador que equilibra la carga de los servidores para los que se calculan los pesos.
- SNMP habilitado en el conmutador. Deben estar habilitadas las dos posibilidades, lectura y grabación.

Colocación del consultor en la red

Como se indica en la Figura 26 en la página 145, el consultor puede conectarse a la red detrás del conmutador o los conmutadores para los que aquél proporciona pesos. Algunos parámetros deben configurarse en el conmutador y otros en el controlador para habilitar la conectividad entre el controlador, el conmutador y los servicios.

En la Figura 26 en la página 145:

- Se conecta un consultor a la red detrás de los conmutadores para los que proporciona los pesos.
- La red consta de dos VLAN.
- Para que el consultor se comuniquen con servicios en las dos redes VLAN, debe estar habilitado IP Forwarding en las interfaces a través de las que los servicios se conectan y en la interfaz a través de la que se conecta el consultor.
- La dirección IP del conmutador debe configurarse como la pasarela por omisión en el consultor y en los sistemas de servicio.

Si desea información detallada sobre cómo configurar redes VLAN y direccionamiento IP en el conmutador, consulte el manual *Cisco Content Services Switch Getting Started Guide*.

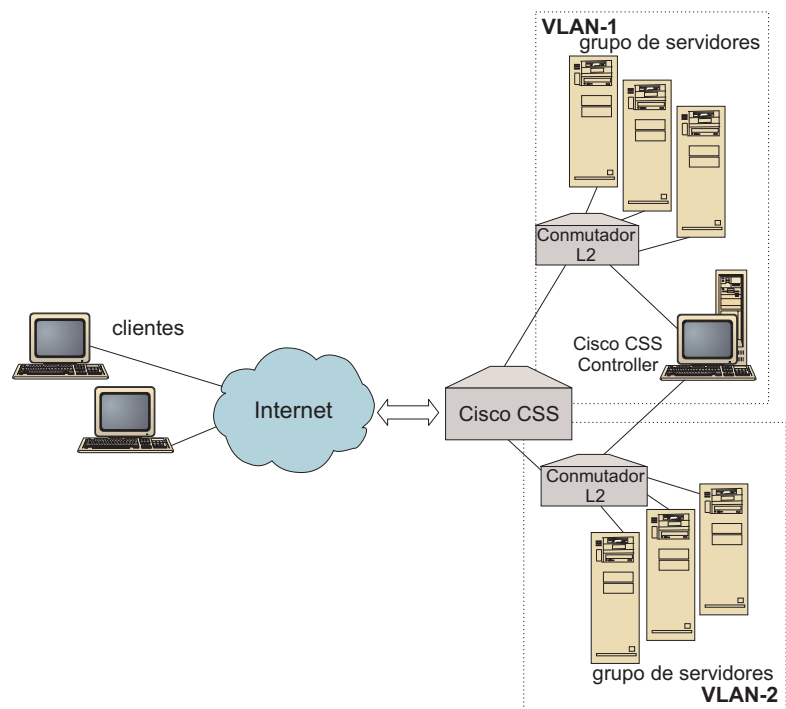


Figura 26. Ejemplo de un consultor conectado detrás de los conmutadores

Puede gestionar Cisco CSS Controller utilizando cualquiera de las interfaces siguientes:

- Navegador
- GUI (remota o local)
- Línea de mandatos (remota o local)

Para la gestión remota, en la Figura 27 en la página 146 :

- El consultor está conectado detrás del conmutador para el que proporciona pesos.
- La interfaz de usuario se ejecuta en un sistema remoto delante del conmutador.
- Se debe configurar el conmutador de modo que permita al sistema remoto comunicarse a través de éste con el sistema de controlador.

Si desea información detallada, consulte el manual *Cisco Content Services Switch Getting Started Guide*.

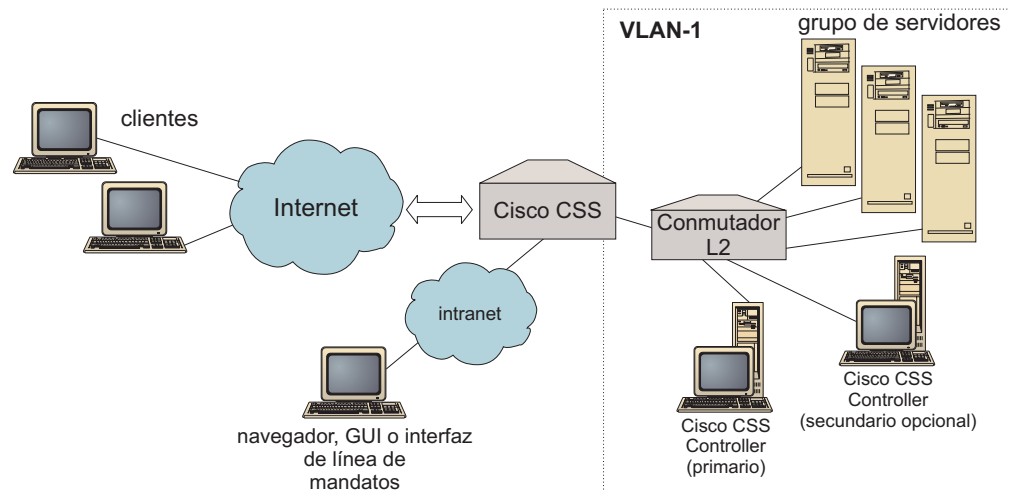


Figura 27. Ejemplo de consultor (con el asociado de alta disponibilidad opcional), configurado detrás del conmutador con la interfaz de usuario delante del conmutador

Alta disponibilidad

La alta disponibilidad del controlador mejora las posibilidades de tolerancia a errores de Load Balancer. La alta disponibilidad del controlador, diseñado teniendo en cuenta la alta disponibilidad de reenvío de paquetes, implica dos controladores en ejecución a la vez, uno con la función de maestro y el otro con la función de secundario.

Cada controlador se configura con información de conmutador idéntica y sólo un controlador está activo en un momento dado. Esto significa que, como se determina por la lógica de alta disponibilidad, sólo el controlador activo calcula y actualiza el conmutador con los nuevos pesos.

La alta disponibilidad del controlador se comunica con su asociado utilizando paquetes UDP (User Datagram Protocol) sencillos en una dirección y puerto que puede configurar. Estos paquetes se utilizan para intercambiar información entre controladores dado que pertenece a alta disponibilidad (información de alcance) y para determinar la disponibilidad del controlador de asociados (pulsos). Si el controlador en espera determina que el controlador activo ha dado un error por cualquier motivo, el controlador en espera se hace con el control del controlador activo que ha dado el error. El controlador en espera ahora pasa a ser el controlador activo y comienza a calcular y a actualizar el conmutador con nuevos pesos.

Además de la disponibilidad de los asociados, se pueden configurar destinos de alcance para alta disponibilidad. La alta disponibilidad del controlador utiliza la información de alcance para determinar qué controlador está activo y cuál está en espera. El controlador activo es el que puede ejecutar ping en más destinos y es accesible desde su asociado.

Si desea más información, consulte el apartado “Alta disponibilidad” en la página 243.

Cálculo de pesos

Si el consultor determina que un servicio no está disponible, suspenderá ese servicio en el conmutador para impedir que el conmutador tenga en cuenta el servidor cuando cargue peticiones de equilibrado. Cuando el servicio está disponible de nuevo, el consultor activa el servicio en el conmutador para que se considere en las peticiones de equilibrio de carga.

Determinación de problemas

Cisco CSS Controller envía entradas a los archivos de anotaciones cronológicas siguientes:

- server.log
- consultant.log
- highavailability.log
- metriccollector.log
- binary.log

Estos archivos de anotaciones cronológicas están ubicados en los directorios siguientes:

- En sistemas AIX, HP-UX, Linux y Solaris: `...ibm/edge/lb/servers/logs/cco/nombre_consultor`
- En sistemas Windows: `...ibm\edge\lb\servers\logs\cco\nombre_consultor`

En cada archivo de anotaciones cronológicas, puede establecer su tamaño y el nivel de anotaciones. Si desea más información, consulte el apartado “Utilización de archivos de anotaciones cronológicas de Load Balancer” en la página 265.

Capítulo 17. Configuración de Cisco CSS Controller

Antes de llevar a cabo los pasos de este capítulo, consulte el Capítulo 16, “Planificación de Cisco CSS Controller”, en la página 143. En este capítulo se explica cómo crear una configuración básica para el componente Cisco CSS Controller de Load Balancer.

- En el Capítulo 23, “Características avanzadas de Cisco CSS Controller y Nortel Alteon Controller”, en la página 243 encontrará configuraciones más complejas.
- En el Capítulo 24, “Operación y gestión de Load Balancer”, en la página 261 encontrará información sobre la administración autenticada remota, las anotaciones cronológicas y el uso del componente Cisco CSS Controller.

Visión general de las tareas de configuración

Antes de llevar a cabo los métodos de configuración descritos en este capítulo:

1. Asegúrese de que el Conmutador Cisco CSS y todas las máquinas de servidor están configuradas correctamente.
2. Configure Cisco CSS Controller, asegurándose de que la dirección de Conmutador Cisco CSS y el nombre de comunidad SNMP coinciden con los atributos correspondientes en el Conmutador Cisco CSS. Consulte el apartado “ccocontrol consultant — configurar y controlar un consultor” en la página 432 para obtener información sobre la configuración del consultor.

Tabla 10. Tareas de configuración para el componente Cisco CSS Controller

Tarea	Descripción	Información relacionada
Configurar la máquina Cisco CSS Controller	Averigua los requisitos	“Configuración de la máquina Controlador para Conmutadores Cisco CSS” en la página 152
Probar la configuración	Confirma que la configuración funciona	“Comprobación de la configuración” en la página 154

Métodos de configuración

Existen tres métodos para crear una configuración básica para el componente Cisco CSS Controller de Load Balancer:

- Línea de mandatos
- Archivo XML
- Interfaz gráfica de usuario (GUI)

Línea de mandatos

Este método es la manera más directa de configurar Cisco CSS Controller. En los procedimientos de esta publicación se da por supuesto que se utiliza la línea de mandatos. Los valores de los parámetros de mandatos deben especificarse en caracteres del idioma inglés. Las únicas excepciones son los nombres de sistema principal (se utiliza, por ejemplo, en el mandato **consultant add**) y los nombres de archivo.

Para iniciar Cisco CSS Controller desde la línea de mandatos:

1. Emita el mandato **ccoserver** en el indicador de mandatos. Para detener el servidor, escriba: **ccoserver stop**

Notas:

- a. En sistemas Windows, pulse **Inicio > Configuración** (en Windows 2000) > **Panel de control > Herramientas administrativas > Servicios**. Pulse con el botón derecho del ratón en **IBM Cisco CSS Controller** y seleccione **Iniciar**. Para detener el servicio, efectúe los mismos pasos y seleccione **Detener**.
 - b. En sistemas Windows, puede iniciar **ccoserver** automáticamente durante el arranque:
 - 1) Pulse **Inicio > Configuración > Panel de control > Herramientas administrativas > Servicios**.
 - 2) Pulse con el botón derecho del ratón en **IBM Cisco CSS Controller** y seleccione **Propiedades**.
 - 3) Pulse la flecha para el campo del tipo de **Inicio** y seleccione **Automático**.
 - 4) Pulse **Aceptar**.
2. A continuación, emita los mandatos de control de Cisco CSS Controller que desee para definir la configuración. En los procedimientos de esta publicación se da por supuesto que se utiliza la línea de mandatos. El mandato es **ccocontrol**. Para obtener más información sobre los mandatos, consulte el Capítulo 29, "Referencia de mandatos para Cisco CSS Controller", en la página 431.

Puede entrar una versión abreviada de los parámetros del mandato **ccocontrol**. Sólo es necesario especificar las letras exclusivas de los parámetros. Por ejemplo, para obtener ayuda sobre el mandato para guardar archivos, puede escribir **ccocontrol he f** en lugar de **ccocontrol help file**.

Para iniciar la interfaz de línea de mandatos, emita **ccocontrol** para recibir un indicador de mandatos de **ccocontrol**.

Para finalizar la interfaz de línea de mandatos, emita **exit** o **quit**.

Nota: En plataformas Windows, se inicia automáticamente el **dsserver** del componente Dispatcher. Si sólo utiliza Cisco CSS Controller y no emplea el componente Dispatcher, puede evitar que **dsserver** se inicie de forma automática haciendo lo siguiente:

1. En Servicios Windows, pulse con el botón derecho del ratón en **IBM Dispatcher**.
2. Seleccione **Propiedades**.
3. En el campo **Tipo de inicio**, seleccione **Manual**.
4. Pulse **Aceptar** y cierre la ventana Servicios.

XML

La configuración definida actualmente puede guardarse en un archivo XML. Esto permite cargar la configuración más adelante cuando desee volver a crear rápidamente la configuración.

Para ejecutar el contenido de un archivo XML (por ejemplo, **miscript.xml**), utilice cualquiera de los siguientes mandatos:

- Para guardar la configuración actual en un archivo XML, emita el siguiente mandatos:
ccocontrol file save *nombre_archivo_XML*
- Para cargar una configuración guardada, emita el siguiente mandato:
ccocontrol file load *nombre_archivo_XML*
Utilice el mandato load sólo si ha ejecutado anteriormente un mandato **file save**.

Los archivos XML se guardan en el directorio **...ibm/edge/lb/servers/configurations/cco/**.

GUI

Para obtener instrucciones generales y un ejemplo de la interfaz gráfica de usuario (GUI), consulte la Figura 41 en la página 468.

Para iniciar la GUI, siga estos pasos

1. Si ccoserver todavía no está en ejecución, inícielo escribiendo lo siguiente como usuario root:
ccoserver.
2. A continuación, realice una de las acciones siguientes:
 - En sistemas AIX, HP-UX, Linux o Solaris, escriba **lbadm**
 - En sistemas Windows: pulse **Inicie > Programas > IBM WebSphere > Edge Components > IBM Load Balancer > Load Balancer**

Para configurar el componente Cisco CSS Controller desde la GUI:

1. Pulse con el botón derecho del ratón en Cisco CSS Controller en la estructura de árbol.
2. Conéctese a un sistema principal.
3. Cree uno o más consultores de conmutadores que incluya el contenido de propietario que desee y la métrica asociada.
4. Inicie el consultor.

La GUI puede utilizarse para llevar a cabo las mismas tareas que realizaría con el mandato **ccocontrol**. Por ejemplo:

- Para definir un consultor mediante la línea de mandatos, escriba **ccocontrol consultant add *ID_consultor* *address* *dirección_IP* *community* *nombre***.
- Para definir un consultor desde la GUI, pulse el botón derecho del ratón en el nodo de sistema principal y pulse **Añadir un consultor de conmutador**. Escriba la dirección de conmutador y el nombre de comunidad en la ventana emergente y pulse Aceptar.
- Utilice la opción **Cargar configuración** que aparece en el menú emergente Sistema principal para cargar archivos de configuración de Cisco CSS Controller existentes previamente y añadirlos a la configuración actual.
- Seleccione **Guardar archivo de configuración como** para guardar de forma periódica la configuración de Cisco CSS Controller en un archivo.
- Seleccione **Archivo** en la barra de menús para guardar en un archivo las conexiones actuales del sistema principal o para restaurar conexiones que se encuentran en archivos existentes en todos los componentes de Load Balancer.

Para ejecutar un mandato desde la GUI:

1. Pulse con el botón derecho del ratón en el nodo **Sistema principal** y seleccione **Enviar mandato...**

2. En el campo de entrada de mandatos, escriba el mandato que desea ejecutar; por ejemplo, **consultant report**.
3. Pulse Enviar.

El resultado y el historial de los mandatos que se ejecutan en la sesión actual aparecen en el recuadro Resultado.

Para acceder a la **Ayuda** pulse el icono de signo de interrogación situado en la esquina superior derecha de la ventana de Load Balancer.

- **Ayuda: Nivel de campo** — describe cada campo, los valores por omisión
- **Ayuda: Cómo puedo** — lista las tareas que pueden llevarse a cabo desde esa pantalla
- **InfoCenter** — proporciona acceso centralizado a la información del producto

Si desea más información sobre cómo utilizar la GUI, consulte el Apéndice A, “GUI: instrucciones generales”, en la página 467.

Configuración de la máquina Controlador para Conmutadores Cisco CSS

Antes de configurar la máquina Cisco CSS Controller, debe ser usuario root (en los sistemas AIX, HP-UX, Linux o Solaris) o el administrador (en los sistemas Windows).

Consultor debe poder conectarse a Conmutador Cisco CSS como un administrador de Conmutador Cisco CSS.

Al configurar el consultor, debe configurar la dirección y el nombre de comunidad SNMP de modo que coincida con los atributos correspondientes en Conmutador Cisco CSS.

Para obtener ayuda sobre los mandatos que se utilizan en este procedimiento, consulte el Capítulo 29, “Referencia de mandatos para Cisco CSS Controller”, en la página 431.

Paso 1. Iniciar la función de servidor

Si ccoserver todavía no está en ejecución, escriba **ccoserver** como usuario root para iniciarlo.

Nota: En sistemas Windows, pulse **Inicio > Configuración** (en Windows 2000) > **Panel de control > Herramientas administrativas > Servicios**. Pulse con el botón derecho del ratón en IBM Cisco Controller y seleccione Iniciar.

Paso 2. Iniciar la interfaz de línea de mandatos

Escriba **ccocontrol** para iniciar la interfaz de línea de mandatos.

Paso 3. Configurar el consultor

Debe configurar la dirección del conmutador y el nombre de comunidad SNMP. Estos valores deben coincidir con los atributos correspondientes en Conmutador Cisco CSS.

Para añadir un consultor, escriba:

```
consultant add ID_consultor_conmutador address dirección_IP_conmutador  
community nombre_comunidad
```

Paso 3. Configurar un contenido de propietario

Un contenido de propietario es una representación de una norma de contenido para un propietario, que está definido en Conmutador Cisco CSS. El nombre del propietario y el nombre de norma de contenido debe coincidir con lo definido en el conmutador.

Para definir un contenido de propietario, escriba:

```
ownercontent add ID_consultor_conmutador:ID_contenido_propietario ownername  
nombre_propietario contentrule nombre_norma_contenido
```

Paso 4. Verificar que los servicios están definidos correctamente

Cuando se define el contenido de propietario, el consultor realiza la configuración recuperando los servicios configurado en el conmutador. Compare la configuración del conmutador con la configuración del consultor para asegurarse de que los servicios coinciden.

Paso 5. Configurar métrica

La métrica son las medidas utilizadas para determinar los pesos de servicios y las proporciones asociadas (importancia de una métrica comparada con otra), y puede ser cualquier combinación de métrica de datos de conexiones, métrica de asesor de aplicaciones y métricas de Metric Server. Las proporciones siempre deben sumar 100.

Al configurar un contenido de propietario, la métrica por omisión se define como **activeconn** y **connrate**. Si desea métricas adicionales o si desea métricas completamente distintas de los resultados, escriba:

```
ownercontent metrics ID_consultor_conmutador:ID_contenido_propietario métrica1  
proporción1 métrica2 proporción2... métricaN proporciónN
```

Paso 6. Iniciar el consultor

Para iniciar el consultor, escriba:

```
consultant start ID_consultor_conmutador
```

Así se inician los recopiladores de métricas y empieza el cálculo del peso.

Paso 7. Iniciar Metric Server (opcional)

Si se ha definido la métrica del sistema en el paso 5, se debe iniciar Metric Server en las máquinas de servicio. Consulte el apartado "Metric Server" en la página 196 para obtener información sobre la utilización de Metric Server.

Paso 8. Configurar alta disponibilidad (opcional)

Para configurar la alta disponibilidad, escriba:

```
highavailability add address dirección_IP partneraddress dirección_IP port 80  
role primario
```

En un entorno de alta disponibilidad, puede configurar varios conmutadores. Para asegurarse de que la información de peso siempre está disponible cuando un

conmutador asumen el control de otro, Cisco CSS Controller debe configurarse para proporcionar pesos para todos los conmutadores y sus reservas.

Consulte el Capítulo 23, “Características avanzadas de Cisco CSS Controller y Nortel Alteon Controller”, en la página 243 para obtener información detallada sobre cómo utilizar y configurar la alta disponibilidad del controlador.

Comprobación de la configuración

Compruebe si la configuración funciona:

1. Establezca el nivel de anotaciones cronológicas del consultor en 4.
2. Desconecte un servidor de Conmutador Cisco CSS durante un minuto o bien detenga el servidor de aplicaciones durante un minuto.
3. Vuelva a conectar el servidor o reinicie el servidor de aplicaciones.
4. Establezca el nivel de anotaciones cronológicas del consultor en el nivel que desee (1).
5. Examine el archivo `consultant.log` que se encuentra en los siguientes directorios y busque las palabras **setServerWeights setting service**:
 - En sistemas AIX, HP-UX, Linux y Solaris: `...ibm/edge/lb/servers/logs/cco/nombre_consultor`
 - En sistemas Windows: `...ibm\edge\lb\servers\logs\cco\nombre_consultor`

Parte 6. Componente Nortel Alteon Controller

Esta parte proporciona información sobre la configuración de inicio rápido, consideraciones de planificación y describe los métodos para configurar el componente Nortel Alteon Controller de Load Balancer. Contiene los capítulos siguientes:

- Capítulo 18, “Configuración de inicio rápido”, en la página 157
- Capítulo 19, “Planificación de Nortel Alteon Controller”, en la página 161
- Capítulo 20, “Configuración de Nortel Alteon Controller”, en la página 171

Capítulo 18. Configuración de inicio rápido

Este ejemplo de inicio rápido muestra cómo crear una configuración mediante el componente Nortel Alteon Controller. Nortel Alteon Controller proporciona pesos de servidor a Conmutador Nortel Alteon Web. Estos pesos se utilizan para seleccionar servidores para servicios a los que el conmutador equilibra la carga.

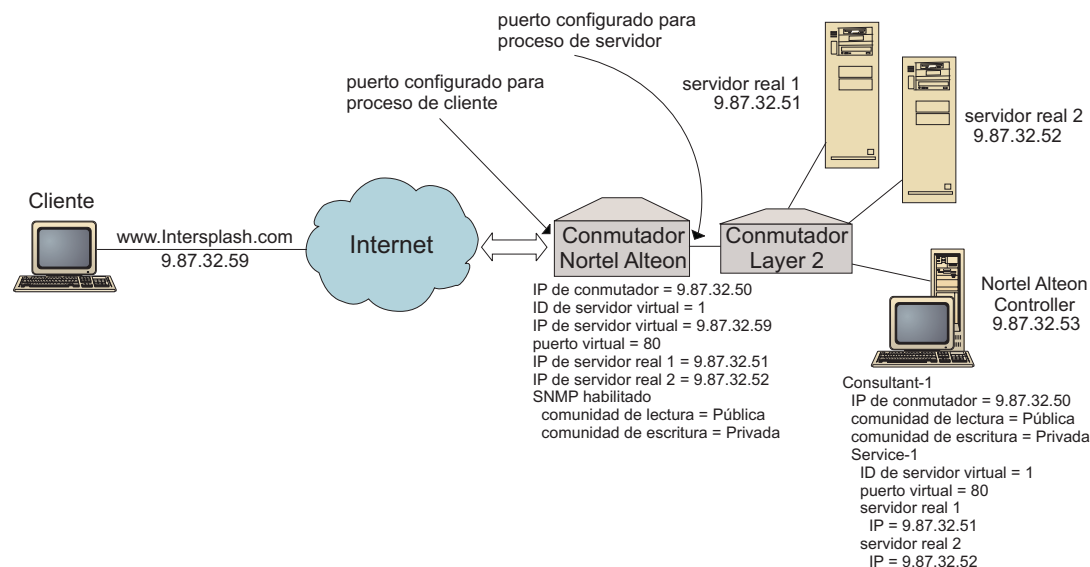


Figura 28. Configuración sencilla de Nortel Alteon Controller

Qué necesita

Para este ejemplo de configuración de inicio rápido, necesitará lo siguiente:

- Conmutador Nortel Alteon Web, que ejecuta Web OS versión 9.0 ó 10.0
- Máquina servidor con el componente Nortel Alteon Controller
- Dos máquinas servidor Web
- Conmutador Layer 2 conectado a un puerto en Conmutador Nortel Alteon Web

Nota: Si no se utiliza un Conmutador Layer 2, la máquina Nortel Alteon Controller y las máquinas servidor Web se pueden conectar directamente a puertos en Conmutador Nortel Alteon Web.

- Este ejemplo de configuración requiere cinco direcciones IP:
 - Una dirección IP que puede proporcionar a los clientes para acceder al sitio Web, www.Intersplashx.com (9.87.32.59)
 - Una dirección IP para una interfaz configurada con Conmutador Nortel Alteon Web (9.87.32.50)
 - Una dirección IP para el servidor 1 real (9.87.32.51)
 - Una dirección IP para el servidor 2 real (9.87.32.52)
 - Una dirección IP para Nortel Alteon Controller (9.87.32.53)

Preparativos

Asegúrese de se completan estos pasos antes de comenzar la configuración de este ejemplo:

- Asegúrese de que Conmutador Nortel Alteon Web esté configurado correctamente. (Si desea información de configuración más completa, consulte el manual Nortel Alteon Web OS Application Guide):
 - Habilite el equilibrio de carga del servidor de capa 4 en el conmutador.
 - Configure una interfaz IP (9.87.32.50) en Conmutador Nortel Alteon Web
 - Habilite SNMP en Conmutador Nortel Alteon Web
 - Habilite el proceso cliente de equilibrio de carga de servidor en el puerto de Conmutador Nortel Alteon Web que recibe las peticiones de cliente.
 - Habilite el proceso servidor de equilibrio de carga de servidor en el puerto de Conmutador Nortel Alteon Web al que están conectados los servidores.
 - Configure la pasarela por omisión para que sea la interfaz IP de conmutador (9.87.32.50) en el servidor 1 real, el servidor 2 real y Nortel Alteon Controller.
 - Configure Conmutador Nortel Alteon Web con el servidor 1 real y el servidor 2 real.
 - Configure Conmutador Nortel Alteon Web con un Grupo de servidores que conste del servidor 1 real y del servidor 2 real. Asigne al grupo un ID de 1.
 - Configure Conmutador Nortel Alteon Web con un servidor virtual. La dirección IP de servidor virtual es 9.87.32.59. Asigne un ID de 1 al servidor virtual.
 - Configure Conmutador Nortel Alteon Web con un servicio que utiliza el servidor virtual 80 y que lo atiende el grupo 1.
- Asegúrese de que la máquina cliente puede ejecutar ping de la dirección IP de servidor virtual 9.87.32.59.
- Asegúrese de que la máquina Nortel Alteon Controller puede ejecutar ping de la interfaz IP de Conmutador Nortel Alteon Web (9.87.32.50), el servidor real 1 (9.87.32.51) y el servidor real 2 (9.87.32.52).

Configuración del componente Nortel Alteon Controller

Con Nortel Alteon Controller, puede crear una configuración mediante la línea de mandatos o la interfaz gráfica de usuario (GUI). Para este ejemplo de inicio rápido, los pasos de configuración se demuestran utilizando la línea de mandatos.

Nota: Los valores de los parámetros deben escribirse en caracteres del idioma inglés. Las únicas excepciones son los valores de parámetros para los nombres de sistemas principales y de archivos.

Configuración con la línea de mandatos

Desde un indicador de mandatos, siga estos pasos:

1. Inicie nalserver en Nortel Alteon Controller. Como usuario root o administrador, emita lo siguiente desde el indicador de mandatos: **nalserver**
2. Añada un consultor a la configuración de Nortel Alteon Controller, especificando la dirección de la interfaz IP de Conmutador Nortel Alteon Web. (Sólo especifique la comunidad de lectura y la de grabación si es distinta de la que toma por omisión (pública, privada):
nalcontrol consultant add Consultant-1 address 9.87.32.50

Esto comprobará la conectividad con Conmutador Nortel Alteon Web y verificará que los nombres de comunidad SNMP funcionan correctamente.

3. Añada un servicio (Service-1) al consultor (Consultant-1), especificando el identificador de servidor virtual (1) y el número de puerto virtual (80) para el servicio:

nalcontrol service add Consultant-1:Service-1 vsid 1 vport 80

Nortel Alteon Controller se comunicará con el conmutador en SNMP y obtendrá la información de configuración necesaria del conmutador. Después de este paso, aparecerá información en Nortel Alteon Controller acerca de qué servidores están configurados en Conmutador Nortel Alteon Web para el servicio.

4. Configure las medidas que se van a recopilar para el conjunto de servidores asociados al servicio:

nalcontrol service metrics Consultant-1:Service-1 http 40 activeconn 30 connrate 30

Este mandato configurará qué información de métrica desea recopilar de los servidores y la importancia relativa de esas métricas durante el cálculo del peso.

5. Inicie la función de consultor de Nortel Alteon Controller:

nalcontrol consultant start Consultant-1

Con este mandato, se iniciarán todos los recopiladores de métricas y comenzarán los cálculos de peso de servidor. Nortel Alteon Controller comunica el resultado de sus cálculos del peso del servidor a Conmutador Nortel Alteon Web mediante SNMP.

La configuración básica de Nortel Alteon Controller ahora está completa.

Prueba de la configuración

Compruebe si la configuración funciona:

1. Desde el navegador Web cliente, vaya a la ubicación **http://www.Intersplashx.com**. Si se visualiza una página, significa que la configuración funciona.
2. Vuelva a cargar la página en el navegador Web.
3. Observe los resultados del mandato siguiente: **nalcontrol service report Consultant-1:Service-1**. La columna de conexiones totales de los dos servidores Web debería sumarse a "2."

Configuración con la interfaz gráfica de usuario (GUI)

Si desea información sobre cómo utilizar la GUI de Nortel Alteon Controller, consulte el apartado "GUI" en la página 173 y el Apéndice A, "GUI: instrucciones generales", en la página 467.

Capítulo 19. Planificación de Nortel Alteon Controller

En este capítulo se describe lo que debe tener en cuenta el planificador de la red antes de instalar y configurar el componente Nortel Alteon Controller.

- Si desea información sobre cómo configurar parámetros de equilibrio de carga del componente Nortel Alteon Controller, consulte el Capítulo 20, “Configuración de Nortel Alteon Controller”, en la página 171.
- Si desea información sobre cómo configurar asesores y Metric Servers, consulte el Capítulo 23, “Características avanzadas de Cisco CSS Controller y Nortel Alteon Controller”, en la página 243.
- Si desea información sobre administración autenticada remota, archivos de anotaciones cronológicas de Load Balancer y el uso de los componentes de Load Balancer consulte el Capítulo 24, “Operación y gestión de Load Balancer”, en la página 261.

Este capítulo incluye:

- “Requisitos del sistema”
- “Consideraciones de planificación”
 - “Colocación del consultor en la red” en la página 162
 - “Atributos de servidor en el conmutador (establecidos por el controlador)” en la página 165
 - “Configuración de servidores de reserva” en la página 165
 - “Configuración de grupos” en la página 166
 - “Alta disponibilidad” en la página 167
 - “Ajuste” en la página 169
 - “Determinación de problemas” en la página 169

Requisitos del sistema

Si desea obtener los requisitos de hardware y software, visite la siguiente página Web: <http://www.ibm.com/support/docview.wss?rs=180&uid=swg27006921>

También necesitará

- Sistema en el que se va a ejecutar Nortel Alteon Controller.
- Conmutador Nortel Alteon Web instalado y configurado. Las plataformas de hardware de conmutador Web son AD3, AD4, 180e, 184 y la parte 4/7 de la capa para Passport 8600.

Consideraciones de planificación

Nortel Alteon Controller gestiona un conjunto de consultores de conmutador. Cada consultor determina pesos para servidores a los que un solo conmutador equilibra la carga. El conmutador para el que el consultor proporciona pesos se configura para equilibrar la carga del servidor. El consultor utiliza el protocolo SNMP para enviar los pesos calculados al conmutador. El conmutador utiliza los pesos para seleccionar un servidor para el servicio al que está equilibrando la carga. Para determinar los pesos, el consultor utiliza uno o más fragmentos de información:

- Disponibilidad y tiempos de respuesta, determinados mediante el uso de **asesores** que se comunican con aplicaciones en ejecución en servidores.

- Información de la carga del sistema, determinada al recuperar un valor de métrica de **agentes Metric Server** en ejecución en los servidores.
- Información de conexión sobre los servidores, obtenida del conmutador.
- Información de accesibilidad, obtenida de ejecutar ping en los servidores.

Si desea una descripción del equilibrio de carga del servidor o información detallada sobre cómo configurar el conmutador, consulte el manual Nortel Alteon Web OS Application Guide.

Para que un consultor obtenga la información necesaria para determinar los pesos del servidor, debe tener:

- Conectividad IP entre el consultor y los servidores para los que se calculan los pesos.
- Conectividad IP entre el consultor y el conmutador que equilibra la carga de los servidores para los que se calculan los pesos.
- SNMP habilitado en el conmutador. Deben estar habilitadas las dos posibilidades, lectura y grabación.

Colocación del consultor en la red

El consultor puede conectarse a la red delante o detrás del conmutador o los conmutadores para los que proporciona pesos. Algunos parámetros deben configurarse en el conmutador y otros en el controlador para habilitar la conectividad entre el controlador, el conmutador y los servidores.

En la Figura 29 en la página 163:

- Se conecta un consultor a la red detrás de los conmutadores para los que proporciona los pesos.
- La red consta de dos VLAN.
- Para que el consultor se comunique con servidores en las dos VLAN, debe estar habilitado IP Forwarding en las interfaces a través de las que los servidores se conectan y en la interfaz a través de la que se conecta el consultor.
- La dirección IP del conmutador debe configurarse como la pasarela por omisión en el consultor y en los sistemas servidor.

Consulte el manual Nortel Alton Web OS Application Guide o Command Reference para obtener información detallada sobre cómo configurar las VLAN y el direccionamiento IP en el conmutador.

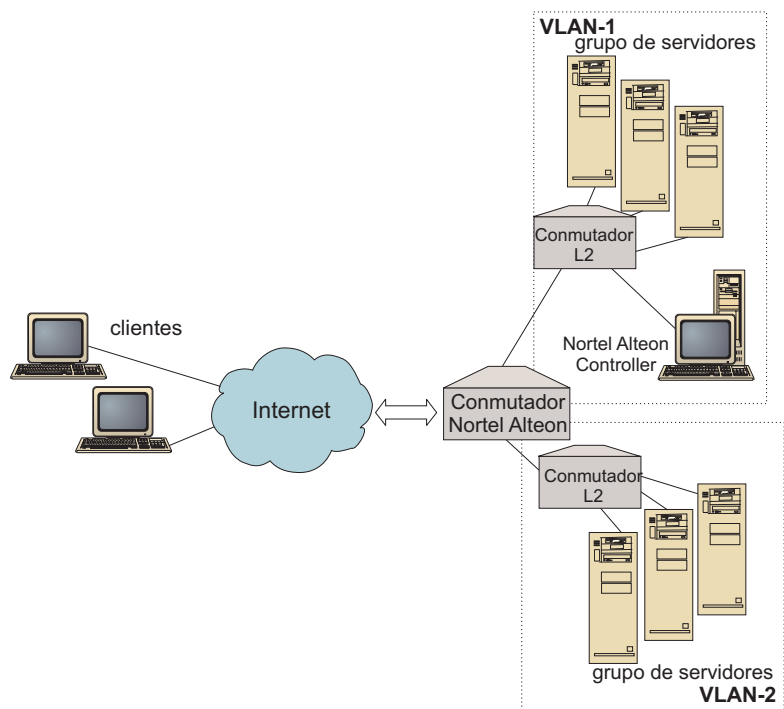


Figura 29. Ejemplo de un consultor conectado detrás del conmutador

En la Figura 30 en la página 164:

- El consultor se conecta al conmutador delante de éste mediante una intranet.
- Debe estar habilitada la modalidad de acceso directo de equilibrio de carga del servidor en el conmutador para permitir que el consultor se comunique con el conmutador y con los servidores.

- Con la modalidad de acceso directo de equilibrio de carga del servidor, cualquier cliente puede enviar tráfico directamente a cualquier servidor. Para limitar el acceso directo del servidor a únicamente el consultor, puede especificar el equilibrio de carga *mnet* y *mmask* en el conmutador. Consulte el manual Nortel Alteon Web OS Application Guide o Command Reference para obtener información detallada sobre cómo configurar el equilibrio de carga del servidor y la interacción del servidor en directo.

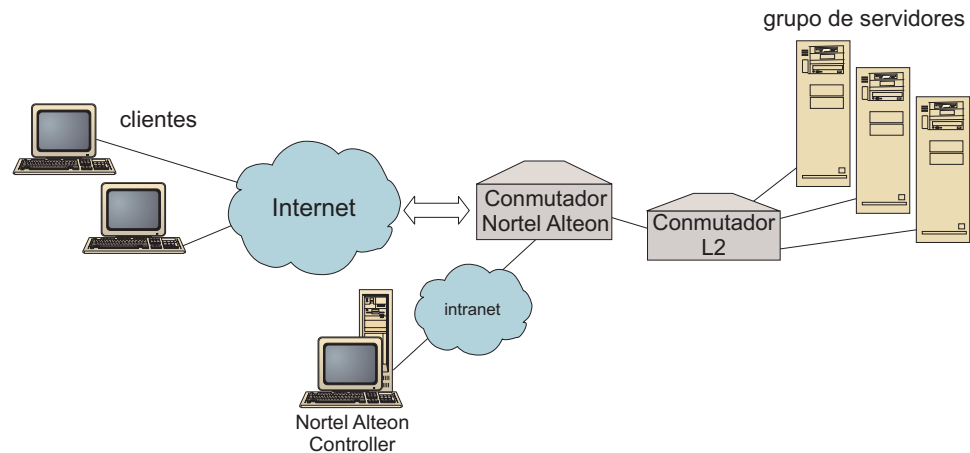


Figura 30. Ejemplo de consultor conectado mediante una intranet delante de un conmutador

Puede gestionar Nortel Alteon Controller utilizando cualquiera de las interfaces siguientes:

- Navegador
- GUI
- Línea de mandatos remota

En la Figura 31 en la página 165:

- El consultor está conectado detrás del conmutador para el que proporciona pesos.
- La interfaz de usuario se ejecuta en un sistema remoto delante del conmutador.

- La red debe configurarse para que la interfaz de usuario pueda comunicarse con el controlador.

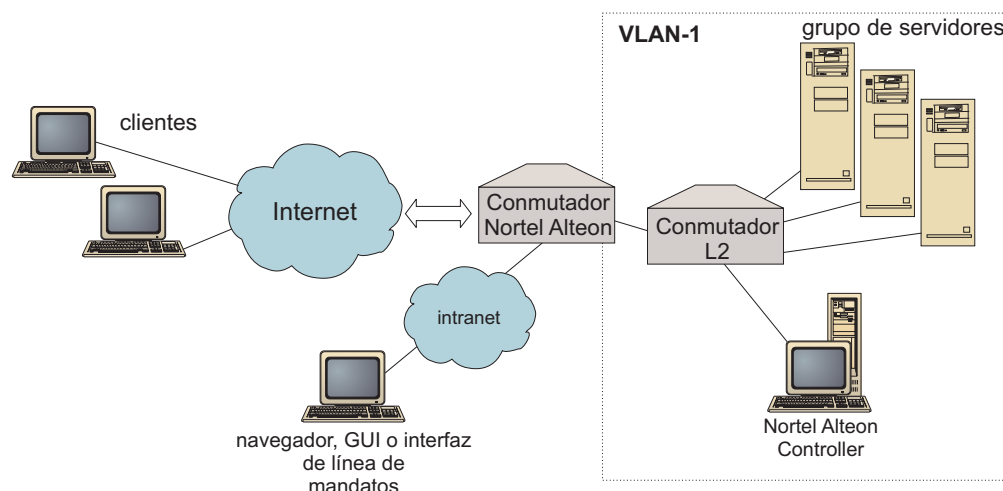


Figura 31. Ejemplo de consultor detrás del conmutador e interfaz de usuario delante del conmutador

Atributos de servidor en el conmutador (establecidos por el controlador)

Cuando un consultor calcula los pesos para servidores que proporcionan un servicio al que el conmutador equilibra la carga, el consultor inhabilita la comprobación normal de estado del servidor en el conmutador para reducir el tráfico innecesario en los servidores. El consultor vuelve a habilitar la comprobación de estado cuando deja de proporcionar pesos para el servicio. El intervalo de comprobación de estado del servidor corresponde a la variable MIB `slbNewCgRealServerPingInterval`.

Si el consultor determina que un servidor no está disponible, el consultor establece el número máximo de conexiones del servidor en cero para impedir que el conmutador tenga en cuenta el servidor cuando cargue peticiones de equilibrado. Cuando se pone de nuevo disponible el servidor, el número máximo de conexiones se restaura a su valor original. El valor máximo de conexiones del servidor corresponde a la variable MIB `slbNewCgRealServerMaxCons`.

Cuando se calcula un peso para un servidor real, se establece el peso para el servidor. El valor de peso del servidor corresponde a la variable MIB `slbNewCgRealServerWeight`.

Configuración de servidores de reserva

El conmutador permite la configuración de varios servidores de reserva de otros. Si el conmutador determina que un servidor que tiene otro de reserva no está disponible, el conmutador debería empezar a enviar peticiones al de reserva. Cuando el consultor calcula pesos para un servicio con un servidor de reserva, calcula los pesos para los dos servidores, el de reserva y el primario y, posteriormente tiene pesos que va a utilizar para la selección de servidor cuando se requiera el de reserva.

El peso para el servidor de reserva podría ser mayor que el peso para un servidor primario. Esto es porque no se le reenvía ninguna petición, de modo que tiene pocas cargas hasta que el conmutador determina utilizarlo.

Para impedir que los recursos del servidor estén desocupados, es una práctica común que los servidores asignados a un servicio se utilicen de reserva de servidores asignados a un servicio distinto. Cuando implementa una configuración de este tipo, no asigne los mismos servidores reales a varios servicios activos a la vez. Si esto sucede, el consultor sobrescribirá el peso para el servidor para cada servicio del que es parte el servidor.

Cada servidor real se identifica por un entero y tiene un peso y un atributo de dirección IP. Dos servidores reales podrían tener la misma dirección IP. En este caso, se asocian dos servidores reales a la misma máquina servidor física. Los servidores reales identificados como reserva sólo deberían configurarse como reserva para un único servicio. Si las mismas máquinas servidor físicas harán de servidores de reserva asignadas a varios servicios, deberán configurarse una vez para cada servicio y se les dará una identificación de servidor que es única para cada servicio. Esto permite que los servidores de reserva tengan un único peso asignado a ellos para cada servicio del que hacen de reserva.

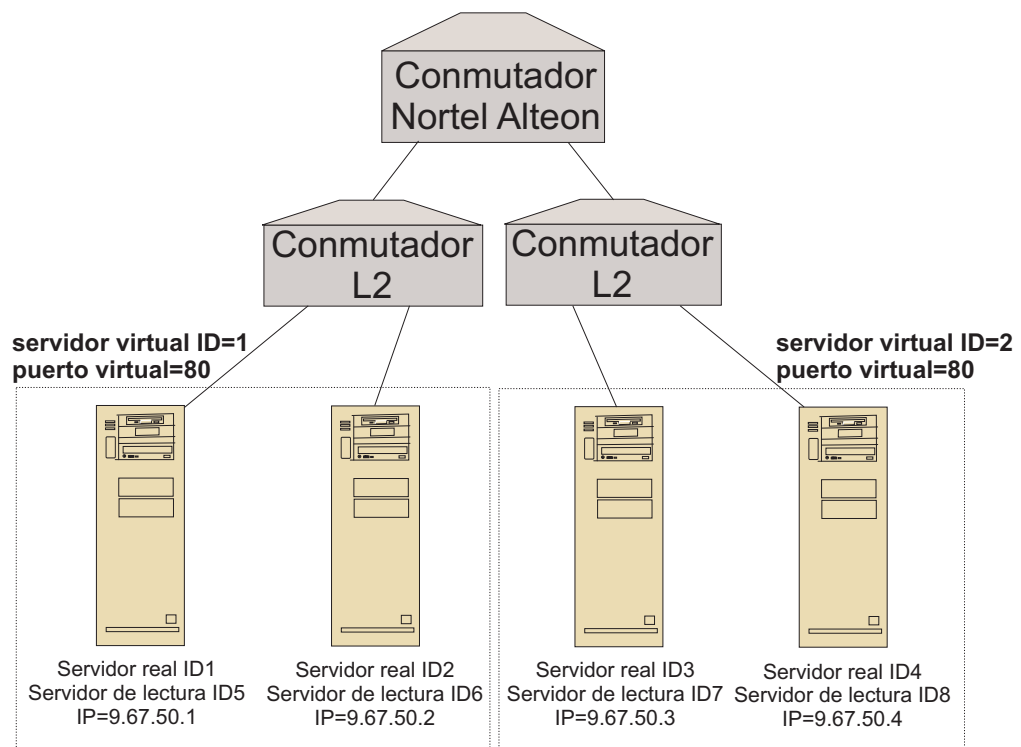


Figura 32. Ejemplo de consultor configurado con servidores de reserva

Configuración de grupos

Los servidores en un conmutador se pueden configurar como parte de varios grupos y los grupos en el conmutador se pueden configurar con servicios de varios servicios.

Dado que se puede configurar el mismo servidor para varios servicios, el peso se calcula para cada servicio del que el servidor forma parte. Es posible, por lo tanto, que el peso sea incorrecto porque se desconoce en un momento dado el peso destinado al servicio.

Además, si el consultor determina pesos para un servicio y no para otro, es posible que el servicio para el que el consultor no calcula pesos tenga inhabilitada la comprobación de estado del servidor. En este caso, quizá el conmutador no equilibre correctamente la carga de ese servicio.

Debido a estas posibilidades, debe asegurarse de que no se asigna un servidor real a varios servicios de los que se está equilibrando la carga. Esto no significa que la misma máquina servidor no pueda atender peticiones de varios servicios. Significa que debe configurarse un servidor real con un identificador único en el conmutador para cada servicio para el que la máquina servidor gestionará peticiones.

Alta disponibilidad

Tanto Nortel Alteon Controller como Conmutador Nortel Alteon Web tienen posibilidades de alta disponibilidad.

Puede configurar dos controladores para ejecutarse en sistemas distintos en una configuración de reposo dinámico.

Dos o más conmutadores pueden volver a activarse entre sí cuando los configura para actuar como VIR (direccionador de interfaz de IP virtual) o como VSR (direccionador de servidor IP virtual).

Un consultor (gestionado por el controlador) proporciona pesos para un conmutador únicamente. Debido a que un conmutador de reserva podría hacerse con el control del maestro, debe configurar el controlador con un consultor para cada conmutador que tenga la posibilidad de ser maestro. De este modo, cuando un conmutador pasa a ser maestro, se asegura que se le proporcionan pesos.

Además, cuando los controladores se conectan a un VIR, se asegura que tienen comunicación con los servidores, los conmutadores y el controlador de reserva, en caso de que se perdiera la conectividad con uno de los conmutadores.

Consulte el manual Nortel Alteon Web OS Application Guide para obtener información sobre alta disponibilidad en el conmutador.

La alta disponibilidad del controlador mejora las posibilidades de tolerancia a errores de Load Balancer. La alta disponibilidad del controlador, diseñado teniendo en cuenta la alta disponibilidad de reenvío de paquetes clásica, implica dos controladores en ejecución a la vez, uno con la función de maestro y el otro con la función de secundario.

Cada controlador se configura con información de conmutador idéntica. Similar a la alta disponibilidad clásica, sólo un controlador está activo en un momento dado. Esto significa que, como se determina por la lógica de alta disponibilidad, sólo el controlador activo calcula y actualiza el conmutador con los nuevos pesos.

La alta disponibilidad del controlador se comunica con su asociado utilizando paquetes UDP (User Datagram Protocol) sencillos en una dirección y puerto que puede configurar. Estos paquetes se utilizan para intercambiar información entre

controladores dado que pertenece a alta disponibilidad (información de alcance) y para determinar la disponibilidad del controlador de asociados (pulsos). Si el controlador en espera determina que el controlador activo ha dado un error por cualquier motivo, el controlador en espera se hace con el control del controlador activo que ha dado el error. El controlador en espera ahora pasa a ser el controlador activo y comienza a calcular y a actualizar el conmutador con nuevos pesos.

Además de la disponibilidad de los asociados, se pueden configurar destinos de alcance para alta disponibilidad. Como con la alta disponibilidad clásica, la alta disponibilidad del controlador utiliza la información de alcance para determinar qué controlador está activo y cuál está en espera. El controlador activo es el que puede ejecutar ping en más destinos y es accesible desde su asociado.

Si desea más información, consulte el apartado “Alta disponibilidad” en la página 243.

En la Figura 33 en la página 169:

- Dos Nortel Alteon Controller están conectados detrás de los conmutadores.
- Un controlador es primario y proporciona activamente a los conmutadores los pesos de servidor; el otro controlador está de reserva.
- Los controladores deben tener comunicación TCP/IP para que el de reserva reconozca cuándo debe asumir la responsabilidad del primario.
- Se configuran dos Conmutador Nortel Alteon Web, como VIR y VSR.
- El VIR proporciona alta disponibilidad para conexiones con los servidores.
- El VSR proporciona alta disponibilidad para acceder a los servidores virtuales configurados en los conmutadores.
- Uno de los conmutadores es el maestro y el otro es el de reserva.
- El controlador primario proporciona pesos para los dos conmutadores.
- El controlador de reserva envía pulsos al primario para determinar cuándo va a hacerse con el control.

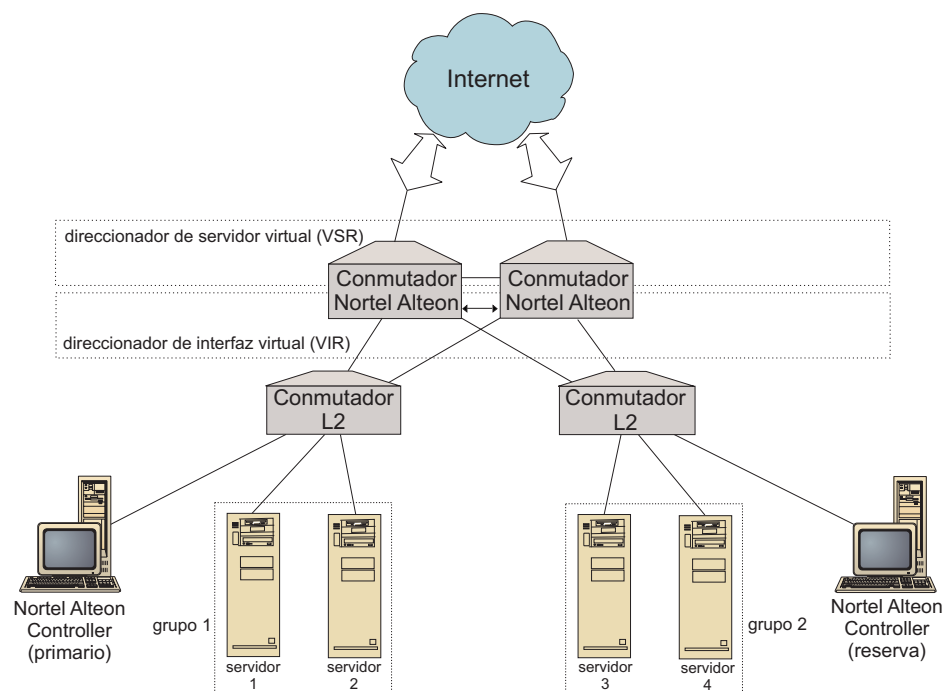


Figura 33. Ejemplo de alta disponibilidad de Nortel Alteon Controller y Conmutador Nortel Alteon Web

Ajuste

Para impedir que el cambio de pesos se produzca muy a menudo, puede configurar el consultor con un umbral de sensibilidad. El umbral de sensibilidad especifica la cantidad de cambios que deben tener lugar entre los pesos antiguos y los nuevos antes de que el peso pueda cambiar. Si desea más información, consulte el apartado “Umbral de sensibilidad” en la página 248.

Si el conmutador pasa a estar demasiado ocupado actualizando pesos, puede aumentar el tiempo de inactividad del consultor para reducir el tráfico entre el controlador y los servidores y el conmutador. El tiempo de inactividad establece el número de segundos de inactividad entre ciclos de establecimiento del peso.

Si los servidores gestionan demasiadas peticiones de supervisión del consultor, puede modificar el tiempo de inactividad de los recopiladores de métricas. Si desea una descripción detallada, consulte el apartado “Tiempos de inactividad en el cálculo de pesos” en la página 247.

Determinación de problemas

Cisco CSS Controller envía entradas a los archivos de anotaciones cronológicas siguientes:

- server.log
- consultant.log
- highavailability.log
- metriccollector.log
- binary.log

Estos archivos de anotaciones cronológicas están ubicados en los directorios siguientes:

- En sistemas AIX, HP-UX, Linux y Solaris: ...ibm/edge/lb/servers/logs/nal/*nombre_consultor*
- En sistemas Windows: ...ibm\edge\lb\servers\logs\nal*nombre_consultor*

En cada archivo de anotaciones cronológicas, puede establecer su tamaño y el nivel de anotaciones. Si desea más información, consulte el apartado “Utilización de archivos de anotaciones cronológicas de Load Balancer” en la página 265.

Capítulo 20. Configuración de Nortel Alteon Controller

Antes de llevar a cabo los pasos de este capítulo, consulte el Capítulo 19, “Planificación de Nortel Alteon Controller”, en la página 161. En este capítulo se explica cómo crear una configuración básica para el componente Nortel Alteon Controller de Load Balancer.

- En el Capítulo 23, “Características avanzadas de Cisco CSS Controller y Nortel Alteon Controller”, en la página 243 encontrará configuraciones más complejas.
- En el Capítulo 24, “Operación y gestión de Load Balancer”, en la página 261 encontrará información sobre la administración autenticada remota, las anotaciones cronológicas y el uso del componente Nortel Alteon Controller.

Visión general de las tareas de configuración

Antes de llevar a cabo los métodos de configuración descritos en este capítulo, asegúrese de que Conmutador Nortel Alteon Web y todas las máquinas de servidor se han configurado correctamente.

Tabla 11. Tareas de configuración para el componente Nortel Alteon Controller

Tarea	Descripción	Información relacionada
Configurar Conmutador Nortel Alteon Web y los servidores	Configura el conmutador.	Configurar el conmutador, en la página 174
Configurar la máquina Nortel Alteon Controller	Configura el controlador.	“Paso 1. Iniciar la función de servidor” en la página 174
Probar la configuración	Confirma que la configuración funciona	“Comprobación de la configuración” en la página 176

Métodos de configuración

Existen tres métodos para crear una configuración básica para el componente Nortel Alteon Controller de Load Balancer:

- Línea de mandatos
- Archivo XML
- Interfaz gráfica de usuario (GUI)

Línea de mandatos

Es la manera más directa de configurar Nortel Alteon Controller. En los procedimientos de esta publicación se da por supuesto que se utiliza la línea de mandatos.

Para iniciar Nortel Alteon Controller desde la línea de mandatos:

1. Emita el mandato **nalserver** en el indicador de mandatos. Para detener el servicio, escriba **nalserver stop**

Notas:

- a. En sistemas Windows, pulse **Inicio > Configuración** (en Windows 2000) > **Panel de control > Herramientas administrativas > Servicios**. Pulse con el

botón derecho del ratón en IBM Nortel Alteon Controller y seleccione **Iniciar**. Para detener el servicio, efectúe los mismos pasos y seleccione **Detener**.

- b. En sistemas Windows, puede iniciar nalservice automáticamente durante el arranque:
 - 1) Pulse **Inicio** > **Configuración** (en Windows 2000) > **Panel de control** > **Herramientas administrativas** > **Servicios**.
 - 2) Pulse con el botón derecho del ratón en IBM Nortel Alteon Controller y seleccione **Propiedades**.
 - 3) Pulse la flecha del campo **Tipo de inicio** y seleccione **Automático**.
 - 4) Pulse **Aceptar**.
2. A continuación, emita los mandatos de control de Nortel Alteon Controller que desee para definir la configuración. En los procedimientos de esta publicación se da por supuesto que se utiliza la línea de mandatos. El mandato es **nalcontrol**. Para obtener más información sobre los mandatos, consulte el Capítulo 30, "Referencia de mandatos para Nortel Alteon Controller", en la página 449.

Puede utilizar una versión abreviada de los parámetros del mandato **nalcontrol** escribiendo las letras exclusivas de los parámetros. Por ejemplo, para obtener ayuda sobre el mandato para guardar archivos, puede escribir **nalcontrol he f** en lugar de **nalcontrol help file**.

Para finalizar la interfaz de línea de mandatos, escriba **exit** o **quit**.

Notas:

1. Debe utilizar caracteres del idioma inglés en todos los valores de parámetros de mandatos. Las únicas excepciones son los nombres de sistema principal (que se utilizan en los mandatos del servidor) y los nombres de archivo (que se utilizan en los mandatos de archivo).
2. En sistemas Windows, se inicia automáticamente el dsservice del componente Dispatcher. Si sólo utiliza Nortel Alteon Controller y no el componente Dispatcher, puede evitar que ndservice se inicie automáticamente de la forma siguiente:
 - a. En Servicios de Windows, pulse con el botón derecho del ratón en IBM Dispatcher.
 - b. Seleccione **Propiedades**.
 - c. En el campo **Tipo de inicio**, seleccione **Manual**.
 - d. Pulse **Aceptar** y cierre la ventana **Servicios**.

XML

La configuración definida actualmente puede guardarse en un archivo XML. Esto permite cargar la configuración más adelante cuando desee volver a crear rápidamente la configuración.

Para ejecutar el contenido de un archivo XML (por ejemplo, **miscript.xml**), utilice los siguientes mandatos:

- Para guardar la configuración actual en un archivo XML, emita el siguiente mandato:
nalcontrol file save nombre_archivo_XML
Utilice el mandato **load** sólo si ha ejecutado anteriormente un mandato **file save**.
- Para cargar una configuración guardada, emita el siguiente mandato:

nalcontrol file load *nombre_archivo_XML*

Utilice el mandato load sólo si ha ejecutado anteriormente un mandato **file save**.

Los archivos XML se guardan en el directorio **...ibm/edge/lb/servers/configurations/nal/**.

GUI

Para ver un ejemplo de la interfaz gráfica de usuario (GUI), consulte la Figura 41 en la página 468.

Para iniciar la GUI:

1. Si nalservice todavía no está en ejecución, inícielo escribiendo **nalservice** como usuario root.
2. A continuación, realice una de las acciones siguientes:
 - En sistemas AIX, HP-UX, Linux o Solaris, escriba **lbadm**
 - En sistema Windows: pulse Inicio > **Programas** > **IBM WebSphere** > **Edge Components** > **IBM Load Balancer** > **Load Balancer**

Para configurar el componente Nortel Alteon Controller desde la GUI:

1. Pulse con el botón derecho del ratón en Nortel Alteon Controller en la estructura de árbol.
2. Conéctese a un sistema principal.
3. Cree uno o más consultores de conmutadores que contengan los servicios que desee y la métrica asociada.
4. Inicie el consultor.

La GUI puede utilizarse para llevar a cabo las mismas tareas que realizaría con el mandato **nalcontrol**. Por ejemplo:

- Para definir un destino de alcance con la línea de mandatos, escriba **nalcontrol highavailability usereach dirección**. Para definir un destino de alcance desde la GUI, pulse el botón derecho del ratón en Alta disponibilidad > Añadir destino de alcance... Escriba la dirección de alcance en la ventana emergente y pulse Aceptar.
- Utilice la opción **Cargar configuración** que aparece en el menú emergente Sistema principal para añadir a la configuración que se ejecuta la configuración almacenada en un archivo. Si desea cargar una *nueva* configuración, debe detener y reiniciar el servidor antes de cargar el archivo.
- Pulse con el botón derecho del ratón en el nodo Sistema principal y seleccione **Guardar archivo de configuración como** para guardar de forma periódica la configuración de Nortel Alteon Controller en un archivo.
- Seleccione **Archivo** en la barra de menús para guardar en un archivo las conexiones actuales del sistema principal o para restaurar conexiones que se encuentran en archivos existentes en todos los componentes de Load Balancer.

Para ejecutar un mandato desde la GUI:

1. Pulse con el botón derecho del ratón en el nodo **Sistema principal** y seleccione **Enviar mandato....**
2. En el campo de entrada de mandatos, escriba el mandato que desea ejecutar; por ejemplo, **consultant report**.
3. Pulse Enviar.

El resultado y el historial de los mandatos que se ejecutan en la sesión actual aparecen en el recuadro Resultado.

Para acceder a la Ayuda, pulse el icono de signo de interrogación situado en la esquina superior derecha de la ventana de Load Balancer.

- **Ayuda: Nivel de campo** — describe cada campo, los valores por omisión
- **Ayuda: Cómo puedo** — lista las tareas que pueden llevarse a cabo desde esa pantalla
- **InfoCenter** — proporciona acceso centralizado a la información del producto

Si desea más información sobre cómo utilizar la GUI, consulte el Apéndice A, “GUI: instrucciones generales”, en la página 467.

Configuración de Nortel Alteon Controller

Para obtener ayuda sobre los mandatos que se utilizan en este procedimiento, consulte el Capítulo 30, “Referencia de mandatos para Nortel Alteon Controller”, en la página 449.

Antes de configurar la máquina Nortel Alteon Controller:

- Debe ser el usuario root (en sistemas AIX, HP-UX, Linux y Solaris) o el administrador (en sistemas Windows).
- Nortel Alteon Controller debe tener conectividad IP con un Conmutador Nortel Alteon Web y con todos los servidores para los que se calculan los pesos.
- Conmutador Nortel Alteon Web debe configurarse de la forma indicada a continuación:
 1. Habilite el equilibrio de carga del servidor de capa 4 en el conmutador.
 2. Configure una interfaz IP.
 3. Habilite SNMP.
 4. Habilite el cliente de equilibrio de carga del servidor que procesa en el puerto que recibe las peticiones de clientes.
 5. Habilite el servidor que realiza el equilibrio de carga del servidor que procesa en el puerto a través del que se conectan los servidores reales.
 6. Configure servidores reales para las máquinas servidor Web.
 7. Configure un grupo de servidores reales formado por los servidores reales que ejecutan el servidor de aplicaciones.
 8. Configure un servidor virtual.
 9. Configure un servicio en un puerto virtual y asígnele el grupo de servidores reales que le darán servicio.

Paso 1. Iniciar la función de servidor

Si nalservice todavía no está en ejecución, escriba **nalservice** como usuario root para iniciarlo.

Nota: En sistemas Windows, pulse **Inicio > Configuración** (en Windows 2000) > **Panel de control > Herramientas administrativas > Servicios**. Pulse con el botón derecho del ratón en IBM Nortel Alteon Controller y seleccione Iniciar.

Paso 2. Iniciar la interfaz de línea de mandatos

Escriba **nalcontrol** para iniciar la interfaz de línea de mandatos.

Paso 3. Definir un consultor de Conmutador Nortel Alteon Web

Para añadir un consultor de conmutador, escriba:

```
consultant add ID_consultor_conmutador address dirección_IP_conmutador
```

Paso 4. Añadir un servicio al consultor de conmutador

Para añadir un servicio, escriba:

```
service add ID_consultor_conmutador:ID_servicio vsid ID_servidor_virtual vport  
número_puerto_virtual
```

Un servicio se identifica por identificador de servidor virtual (VSID) y un número de puerto virtual (VPORT). Los dos están asociados a un servidor virtual configurado anteriormente en el conmutador.

Paso 5. Configurar métrica

La métrica es la información utilizada para determinar los pesos de los servidores. A cada métrica se le asigna una proporción para indicar su importancia relativa a otra métrica. Puede configurarse cualquier combinación de métricas: métrica de datos de conexiones, métrica de asesor de aplicaciones y métrica de Metric Server. Las proporciones siempre deben sumar 100.

Al configurar un servicio, la métrica por omisión se define como **activeconn** y **connrate**. Si desea métricas adicionales o si desea métricas completamente distintas de los resultados, escriba:

```
service metrics ID_consultor_conmutador0:ID_servicio nombre_métrica 50  
nombre_métrica2 50
```

Paso 6. Iniciar el consultor

Para iniciar el consultor, escriba:

```
consultant start ID_consultor_conmutador
```

Así se inician los recopiladores de métricas y empieza el cálculo del peso.

Paso 7. Configurar alta disponibilidad (opcional)

Para configurar la alta disponibilidad, escriba:

```
highavailability add address dirección_IP partneraddress dirección_IP port 80  
role primario
```

Consulte el Capítulo 23, “Características avanzadas de Cisco CSS Controller y Nortel Alteon Controller”, en la página 243 para obtener información detallada sobre cómo utilizar y configurar la alta disponibilidad del controlador.

Paso 8. Iniciar Metric Server (opcional)

Si se ha definido la métrica del sistema en el paso 5, se debe iniciar Metric Server en las máquinas de servicio. Consulte el apartado “Metric Server” en la página 253 para obtener información sobre la utilización de Metric Server.

Paso 9. Renovar la configuración de Nortel Alteon Controller

Si modifica la configuración de Conmutador Nortel Alteon Web, puede renovar la configuración del controlador. Escriba:

```
service refresh
```

Antes de renovar la configuración, detenga el consultor. Una vez que el mandato de renovación actualiza la configuración, reinicie el consultor.

Comprobación de la configuración

Compruebe si la configuración funciona:

1. Establezca el nivel de anotaciones cronológicas del consultor en 4.
2. Desconecte un servidor de Conmutador Nortel Alteon Web durante un minuto o bien detenga el servidor de aplicaciones durante un minuto.
3. Vuelva a conectar el servidor o reinicie el servidor de aplicaciones.
4. Establezca el nivel de anotaciones cronológicas del consultor en el nivel que desee (1).
5. Examine el archivo `consultant.log` que se encuentra en los siguientes directorios y busque las palabras **setServerWeights setting service**. Esto significa que se ha realizado un intento de enviar pesos al conmutador.
 - En sistemas AIX, HP-UX, Linux y Solaris: `...ibm/edge/lb/servers/logs/cco/nombre_consultor`
 - En sistemas Windows: `...ibm\edge\lb\servers\logs\cco\nombre_consultor`
6. Visualice los pesos de servidores en el conmutador y verifique que estos pesos coincidan con los pesos que se muestran en el informe del controlador.

Parte 7. Funciones y características avanzadas de Load Balancer

Esta parte proporciona información sobre funciones y características de configuración avanzada que están disponibles para Load Balancer. Contiene los capítulos siguientes:

- Capítulo 21, “Funciones del gestor, asesores y Metric Server para Dispatcher, CBR y Site Selector”, en la página 179
- Capítulo 22, “Características avanzadas para Dispatcher, CBR y Site Selector”, en la página 201
- Capítulo 23, “Características avanzadas de Cisco CSS Controller y Nortel Alteon Controller”, en la página 243

Capítulo 21. Funciones del gestor, asesores y Metric Server para Dispatcher, CBR y Site Selector

En este capítulo se explica cómo configurar los parámetros de equilibrio de carga y cómo configurar las funciones del gestor, de los asesores y de Metric Server de Load Balancer.

Nota: Al leer este capítulo, si *no* está utilizando el componente Dispatcher, sustituya "dscontrol" por lo siguiente:

- Para CBR, utilice **cbrcontrol**
- En Site Selector, utilice **sscontrol** (consulte el Capítulo 28, "Referencia de mandatos para Site Selector", en la página 403)

IMPORTANTE: si utiliza la instalación de Load Balancer para IPv4 y IPv6 consulte el Capítulo 8, "Despliegue de Dispatcher en Load Balancer para IPv4 y IPv6", en la página 81 para obtener las limitaciones y diferencias de configuración antes de consultar el contenido de este apartado.

Tabla 12. Tareas de configuración avanzada para Load Balancer

Tarea	Descripción	Información relacionada
Si se desea, se pueden cambiar los valores del equilibrio de carga	Puede cambiar los siguientes valores de equilibrio de carga: <ul style="list-style-type: none">• Proporción de la importancia otorgada a la información de estado La proporción por omisión es 50-50-0-0. Si emplea el valor por omisión, no se utilizará la información de asesores, Metric Server y WLM.• Pesos• Pesos fijados por el gestor• Intervalos del gestor• Umbral de sensibilidad• Índice de suavizado	"Optimización del equilibrio de carga que proporciona Load Balancer" en la página 180
Utilizar scripts para generar una alerta o anotar anomalía de servidor cuando el gestor marca los servidores como inactivos o activos	Load Balancer proporciona salidas de usuario que desencadenan scripts que puede personalizar cuando el gestor marca los servidores como inactivos o activos	"Utilización de scripts para generar una alerta o anotar anomalías en el servidor" en la página 184
Utilizar asesores	Describe y lista los asesores, que informan sobre estados concretos de los servidores	"Asesores" en la página 185
Utilizar la opción de petición y respuesta (URL) del asesor HTTP o HTTPS	Define una serie de URL HTTP de cliente exclusiva, específica de un servicio que desea examinar en la máquina	"Configuración del asesor HTTP o HTTPS utilizando la opción de petición y respuesta (URL)" en la página 190
Utilizar el asesor automático	Proporciona estado de carga del servidor de programa de fondo en una configuración WAN de dos niveles de Load Balancer	"Utilización del asesor automático en una configuración WAN de dos niveles" en la página 192
Crear asesores personalizados	Describe cómo escribir sus propios asesores personalizados	"Crear asesores personalizados (personalizables)" en la página 192

Tabla 12. Tareas de configuración avanzada para Load Balancer (continuación)

Tarea	Descripción	Información relacionada
Utilizar agente de Metric Server	Metric Server proporciona información de carga del sistema a Load Balancer	"Metric Server" en la página 196
Utilizar el asesor del gestor de carga de trabajo (WLM)	El asesor WLM proporciona información de carga del sistema a Load Balancer	"Asesor del gestor de carga de trabajo" en la página 198

Optimización del equilibrio de carga que proporciona Load Balancer

La función de gestor de Load Balancer lleva a cabo el equilibrio de carga basándose en los siguientes valores:

- "Proporción de la importancia otorgada a la información de estado"
- "Pesos" en la página 181
- "Intervalos del gestor" en la página 183
- "Intervalos de asesor" en la página 187
- "Tiempo de espera de informe del asesor" en la página 187
- "Umbral de sensibilidad" en la página 183
- "Índice de suavizado" en la página 183

Si lo desea, modifique estos valores para optimizar el equilibrio de carga para la red.

Proporción de la importancia otorgada a la información de estado

El gestor puede tener en cuenta algunos de los siguientes factores externos o todos cuando se sopesan las decisiones:

- *Conexiones activas*: el número de conexiones activas en cada máquina servidor con equilibrio de carga (detectadas por el ejecutor). Esta proporción no se aplica a Site Selector.
○ —
CPU: el porcentaje de la CPU en uso en cada máquina servidor con equilibrio de carga (entrada del agente de Metric Server). En Site Selector, esta proporción aparece en lugar de la columna de proporción de conexiones activas.
- *Conexiones nuevas*: el número de conexiones nuevas en cada máquina servidor con equilibrio de carga (detectadas por el ejecutor). Esta proporción no se aplica a Site Selector.
○ —
Memoria: el porcentaje de la memoria en uso (entrada del agente de Metric Server) en cada servidor con equilibrio de carga. En Site Selector, esta proporción aparece en lugar de la columna de proporción de conexiones nuevas.
- *Específico del puerto*: la entrada de los asesores que escuchan en el puerto.
- *Métrica de sistema*: la entrada de las herramientas de supervisión del sistema, como Metric Server o WLM.

Junto con el peso actual para cada servidor y alguna otra información necesaria para sus cálculos, el gestor obtiene los dos primeros valores (conexiones activas y nuevas) del ejecutor. Estos valores se basan en la información generada y almacenada internamente en el ejecutor.

Nota: En el caso de Site Selector, el gestor obtiene los dos primeros valores (CPU y memoria) para Metric Server.

Puede cambiar la proporción de importancia relativa de los cuatro valores clúster por clúster (o nombre de sitio). Piense en las proporciones como si fueran porcentajes; la suma de las proporciones relativas debe ser 100%. La proporción por omisión es 50/50/0/0, que ignora la información del asesor y del sistema. En el entorno, es posible que sea necesario probar distintas proporciones hasta encontrar la combinación que ofrezca el mejor rendimiento.

Nota: Al añadir un asesor (distinto de WLM), si la **proporción del puerto** es cero, el gestor aumenta este valor hasta 1. Puesto que la suma de las proporciones relativas debe ser 100, se restará 1 al valor más alto.

Al añadir el asesor WLM, si la **proporción de métrica del sistema** es cero, el gestor aumenta este valor hasta 1. Puesto que la suma de las proporciones relativas debe ser 100, se restará 1 al valor más alto.

El número de conexiones activas depende del número de clientes así como del periodo de tiempo necesario para utilizar los servicios proporcionados por las máquinas de servidor con equilibrio de carga. Si las conexiones de cliente son rápidas (como páginas Web pequeñas servidas mediante HTTP GET), el número de conexiones activas será bastante bajo. Si las conexiones de cliente son más lentas (como una consulta a una base de datos), el número de conexiones activas será más alto.

Debe evitar establecer demasiado bajos los valores de las proporciones de conexiones activas y nuevas. Debe inhabilitar el equilibrio de carga y el suavizado, a menos que estos dos valores estén establecidos como mínimo en 20 cada uno.

Para definir la proporción de los valores de importancia, emita el mandato **dscontrol cluster set *clúster* proportions**. Consulte el apartado “dscontrol cluster — configurar clústeres” en la página 355 para obtener más información.

Pesos

Los pesos los establece la función de gestor basándose en contadores internos del ejecutor, información procedente de los asesores e información procedente de un programa de supervisión del sistema, como Metric Server. Si desea establecer pesos manualmente mientras ejecuta el gestor, especifique la opción **fixedweight** en el mandato **dscontrol server**. Para obtener una descripción de la opción **fixedweight**, consulte el apartado “Pesos fijos del gestor” en la página 182.

Los pesos se aplican a todos los servidores de un puerto. Para cualquier puerto concreto, las peticiones se distribuyen entre los servidores en función del peso relativo que dichos servidores tienen entre sí. Por ejemplo, si el peso de un servidor se establece en 10 y el de otro en 5, el servidor establecido en 10 debería recibir el doble de peticiones que el servidor establecido en 5.

Para especificar el límite máximo de peso que un servidor puede tener, utilice el mandato **dscontrol port set *puerto* weightbound *peso***. Este mandato afecta a la diferencia permitida entre la cantidad de peticiones que cada servidor obtendrá. Si establece el valor máximo de ponderación en 1, todos los servidores podrán tener el peso 1, 0 si están desactivados temporalmente o -1 si se han marcado como inactivos. Cuando se incrementa este número, aumentará la diferencia entre el peso que se puede otorgar a los servidores. Si establece el valor máximo de ponderación

en 2, un servidor podría obtener el doble de peticiones que otro. Si establece el valor máximo de ponderación en 10, un servidor podría obtener diez veces más peticiones que otro. El valor máximo por omisión de ponderación es 20.

Si un asesor encuentra que un servidor ha concluido, lo comunica al gestor y éste establecerá el peso para el servidor en cero. Como resultado, el ejecutor no enviará ninguna conexión adicional a dicho servidor siempre que dicho peso permanezca en cero. En el caso de que hubiera alguna conexión activa con dicho servidor antes de cambiar el peso, se dejará que finalice normalmente.

Si todos los servidores están inactivos, el gestor establece los pesos a la mitad de la ponderación.

Pesos fijos del gestor

Sin el gestor, los asesores no se pueden ejecutar y no pueden detectar si un servidor está inactivo. Si opta por ejecutar los asesores, pero *no* desea que el gestor actualice el peso establecido para un servidor concreto, utilice la opción **fixedweight** en el mandato **dscontrol server**. Por ejemplo:

```
dscontrol server set clúster:puerto:servidor fixedweight yes
```

Una vez que **fixedweight** se establece en **yes**, utilice el mandato **dscontrol server set weight** para establecer el peso en el valor que desee. El valor de peso del servidor permanece fijo mientras el gestor se está ejecutando hasta que se emite otro mandato **dscontrol server** con la opción **fixedweight** establecida en **no**. Para obtener más información, consulte el apartado “**dscontrol server** — configurar servidores” en la página 392.

Envío de una restauración TCP a un servidor inactivo (sólo componente Dispatcher)

Si se activa una **restauración TCP**, Dispatcher enviará una restauración TCP al cliente cuando éste tenga una conexión con un servidor con un peso 0. El peso de un servidor puede ser 0 si se ha configurado 0 o si un asesor lo marca como inactivo. Una restauración TCP hará que la conexión se cierre inmediatamente. Esta característica es útil para conexiones de larga duración donde acelera la capacidad el cliente para renegociar una conexión anómala. Para activar la restauración TCP, utilice el mandato **dscontrol port add | set puerto reset yes**. El valor por omisión para **reset** es **no**.

Nota: La restauración TCP se aplica a todos los métodos de reenvío de Dispatcher. No obstante, para utilizar la característica de restauración TCP, la opción **clientgateway** en el mandato **dscontrol executor** debe establecerse en una dirección de direccionador. .

Una característica que será de gran utilidad configurar, junto con la restauración TCP, es **advisor retry**. Con esta característica, un asesor tiene la capacidad de volver a intentar una conexión antes de marcar un servidor como inactivo. Esto ayudara a impedir que el asesor marque prematuramente el servidor como inactivo, lo que podría provocar problemas en la restauración de la conexión. Es decir, sólo porque el asesor haya fallado en el primer intento, no significa necesariamente que las conexiones existentes también están sufriendo anomalías. Consulte el apartado “Reintento del asesor” en la página 188 para obtener más información.

Intervalos del gestor

Para optimizar el rendimiento general, se restringe la frecuencia con la que el gestor puede interactuar con el ejecutor. Puede realizar cambios en este intervalo emitiendo los mandatos **dscontrol manager interval** y **dscontrol manager refresh**.

El intervalo del gestor especifica la frecuencia con la que el gestor actualizará los pesos del servidor que el ejecutor utiliza en el direccionamiento de conexiones. Si el intervalo del gestor es demasiado bajo, puede suponer un bajo rendimiento como resultado de que el gestor interrumpe constantemente al ejecutor. Si el valor de intervalo del gestor es demasiado alto, puede indicar que el direccionamiento de peticiones del ejecutor no se basará en información actualizada y precisa.

Por ejemplo, para establecer el intervalo en 1 segundo, escriba el siguiente mandato:

```
dscontrol manager interval 1
```

El ciclo de renovación del gestor especifica con qué frecuencia el gestor solicitará información de estado al ejecutor. El ciclo de renovación se basa en el intervalo de tiempo.

Por ejemplo, para establecer el ciclo de renovación del gestor en 3, escriba el siguiente mandato:

```
dscontrol manager refresh 3
```

Esto hará que el gestor espere 3 intervalos antes de solicitar el estado al ejecutor.

Umbral de sensibilidad

Hay otros métodos disponibles para optimizar el equilibrio de carga para los servidores. Para trabajar a máxima velocidad, sólo se actualizan los pesos de los servidores si dichos pesos han cambiado de una manera significativa. Si se actualizan constantemente los pesos cuando no se produce ningún cambio en el estado del servidor o dicho cambio es muy pequeño, supondrá una carga adicional innecesaria. Cuando el cambio en el porcentaje del peso para el peso total de todos los servidores de un puerto es mayor que el umbral de sensibilidad, el gestor actualiza los pesos utilizados por el ejecutor para distribuir las conexiones. Por ejemplo, suponga que el total de los cambios de pesos pasa de 100 a 105. El cambio es del 5%. Con el umbral de sensibilidad por omisión 5, el gestor no actualizará los pesos utilizados por el ejecutor, porque el cambio del porcentaje no está **por encima** del umbral. Sin embargo, si el peso total pasa de 100 a 106, el gestor actualizará los pesos. Para establecer el umbral de sensibilidad el gestor en un valor distinto del valor por omisión (por ejemplo, 6), especifique el siguiente mandato:

```
dscontrol manager sensitivity 6
```

En la mayoría de los casos, no es necesario cambiar este valor.

Índice de suavizado

El gestor calcula los pesos de servidores de forma dinámica. En consecuencia, un peso actualizado puede ser muy distinto de uno anterior. En la mayoría de casos, esto no será un problema. Sin embargo, en algunas ocasiones puede causar un efecto de fluctuación en la forma en que se realiza el equilibrio de carga en las peticiones. Por ejemplo, un servidor puede acabar recibiendo la mayoría de las peticiones debido a un peso alto. El gestor verá que el servidor tiene un elevado número de conexiones activas y que el servidor responde muy lentamente.

Entonces pasará el peso a los servidores libres, lo que producirá el mismo efecto y provocará una utilización de recursos ineficaz.

Para aliviar este problema, el gestor utiliza un índice de suavizado. El índice de suavizado limita la cantidad que el peso de un servidor puede cambiar, mitigando el cambio en la distribución de peticiones. Un índice de suavizado más alto hará que los pesos de servidores cambien menos radicalmente. Un índice más bajo hará que los pesos de servidores cambien de forma más radical. El valor por omisión para el índice de suavizado es 1,5. Con un índice de 1,5, los pesos de servidores pueden ser bastante dinámicos. Si se especifica un índice de 4 o 5, los pesos serán más estables. Por ejemplo, para establecer el índice de suavizado en 4, escriba el siguiente mandato:

```
dscontrol manager smoothing 4
```

En la mayoría de los casos, no es necesario cambiar este valor.

Utilización de scripts para generar una alerta o anotar anomalías en el servidor

Load Balancer proporciona salidas de usuario que desencadenan scripts que se pueden personalizar. Puede crear los scripts para realizar acciones automatizadas, como avisar a un administrador cuando el gestor ha marcado que los servidores están inactivos o simplemente anotar el suceso de la anomalía. Los scripts de ejemplo, que puede personalizar, están en el directorio de instalación `...ibm/edge/lb/servers/samples`. Para ejecutar los archivos, debe ponerlos en el directorio `...ibm/edge/lb/servers/bin` y eliminar la extensión de archivo "sample". Se proporcionan los siguientes scripts de ejemplo:

- **serverDown**: el gestor marca un servidor como inactivo.
- **serverUp**: el gestor marca un servidor como inactivo.
- **managerAlert**: todos los servidores de un determinado puerto se marcan como inactivos.
- **managerClear**: como mínimo hay un servidor activo, después de que todos se marcaran como inactivos para un puerto determinado.

Si todos los servidores de un clúster se marcan como inactivos (por el usuario o por los asesores), se inicia **managerAlert** (si está configurado) y Load Balancer intenta direccionar el tráfico a los servidores utilizando una técnica de turno rotativo. El script **serverDown** no se inicia cuando se ha detectado que el último servidor del clúster está fuera de línea.

Load Balancer se ha diseñado de modo que intente continuar direccionando el tráfico en caso de que un servidor vuelva a estar en línea y responda a la petición. Si en lugar de esto, Load Balancer dejara de direccionar todo el tráfico, el cliente no recibiría ninguna respuesta.

Cuando Load Balancer detecta que el primer servidor de un clúster vuelve a estar en línea, se inicia el script **managerClear** (si está configurado), aunque el script **serverUp** (si está configurado) no se ejecutará hasta que no vuelva a estar en línea un servidor adicional.

Factores que deben tenerse en cuenta cuando se utilizan los scripts **serverUp** y **serverDown**:

- Si define el ciclo del gestor en un valor inferior al 25% del tiempo del asesor, pueden generarse falsos informes de servidores activos o inactivos. Por omisión, el gestor se ejecuta cada 2 segundos, pero el asesor se ejecuta cada 7 segundos.

Por lo tanto, el gestor espera nueva información de asesor cada 4 ciclos. Sin embargo, si se elimina esta restricción (es decir, definir el ciclo de gestor de forma que tenga un valor superior al 25% del tiempo del asesor) se disminuirá de forma significativa el rendimiento porque varios asesores pueden asesorar sobre un solo servidor.

- Cuando un servidor pasa a estar inactivo, se inicia el script `serverDown`. Sin embargo, si emite un mandato `serverUp`, se da por supuesto que el servidor está activo hasta que el gestor obtiene nueva información del ciclo del asesor. Si el servidor sigue estando inactivo, el script `serverDown` se ejecutará de nuevo.

Asesores

Los asesores son agentes incluidos en Load Balancer. Su finalidad es evaluar el estado y la carga de las máquinas servidor. Esto lo llevan a cabo con un intercambio parecido a los clientes proactivos con los servidores. Los asesores se consideran como clientes ligeros de los servidores de aplicaciones.

El producto proporciona varios asesores específicos de protocolo para la mayoría de los protocolos más utilizados. No obstante, no tiene sentido utilizar todos los asesores proporcionados con cada componente de Load Balancer. (Por ejemplo, no utilice el asesor Telnet con el componente CBR). Load Balancer también da soporte al concepto de un “asesor personalizado” que permite a los usuarios escribir sus propios asesores.

Limitación en la utilización de aplicaciones de servidor específicas del enlace:

Para poder utilizar asesores en servidores específicos del enlace, inicie dos instancias del servidor: una instancia para enlazar el clúster:puerto y la otra instancia para enlazar en servidor:puerto. Para determinar si el servidor es específico del enlace, emita el mandato `netstat -an` y busque `server:port`. Si el servidor no es específico del enlace, el resultado del mandato será `0.0.0.0:80`. Si el servidor es específico del enlace, verá una dirección parecida a `192.168.15.103:80`.

En sistemas HP-UX y Solaris existe una limitación en la utilización de aplicaciones de servidor específicas del enlace: Si utiliza el mandato `arp publish` en lugar del mandato `ifconfig alias`, Load Balancer *dará* soporte al uso de asesores cuando los servidores que realizan el equilibrio de carga con aplicaciones de servidores específicos del enlace (incluidos otros componentes de Load Balancer, como CBR o Site Selector) cuando están enlazados a la dirección IP del clúster. Sin embargo, cuando se utilicen asesores para la aplicación de servidor específico del enlace, Load Balancer no puede compartir la misma ubicación en la misma máquina con la aplicación de servidor.

Nota: Cuando Load Balancer se está ejecutando en un sistema con varias tarjetas de adaptador de red y desea que el tráfico del asesor circule por un adaptador concreto, puede forzar la dirección IP de origen de los paquetes de forma que sea una dirección concreta. Para forzar que la dirección de origen de paquetes del asesor sea una dirección concreta, añada la siguiente línea `java...SRV_XXXConfigServer...` en el archivo script (`dssserver`, `cbrserver` o `ssserver`) de inicio de Load Balancer adecuado.

`-DLB_ADV_SRC_ADDR=dirección_IP`

Cómo funcionan los asesores

Los asesores abren periódicamente una conexión TCP con cada servidor y envían un mensaje de petición al servidor. El contenido del mensaje es específico para el protocolo que se ejecuta en el servidor. Por ejemplo, el asesor HTTP envía una petición HTTP “HEAD” al servidor.

Los asesores están a la escucha de la respuesta del servidor. Después de obtener la respuesta, el asesor realiza una evaluación del servidor. Para calcular este valor de “carga”, la mayoría de los asesores calculan el tiempo que el servidor tarda en responder y luego utilizan este valor (en milisegundos) como carga.

A continuación, los asesores notifican el valor de la carga a la función de gestor, donde aparece en el informe del gestor en la columna “Puerto”. Luego, el gestor calcula los valores de peso total de todas las fuentes, según sus proporciones y establece estos valores en la función del ejecutor. El ejecutor utilizará estos valores para realizar el equilibrio de carga de nuevas conexiones de cliente entrantes.

Si el asesor determina que un servidor está activo y funciona, notificará al gestor un número de carga positivo distinto de cero. Si el asesor determina que un servidor no está activo, devolverá un valor de carga especial de uno negativo (-1). El gestor y el ejecutor no reenviará más conexiones a dicho servidor hasta que el servidor no vuelva a estar en funcionamiento.

Nota: Antes de enviar el mensaje de petición inicial, el asesor emitirá el mandato ping al servidor. Esto proporcionará rápidamente el estado para determinar si la máquina está en línea. Una vez que el servidor responda al mandato ping, no se enviarán más mandatos ping. Para inhabilitar el envío de mandatos ping, añada -DLB_ADV_NB_PING al archivo script de inicio de Load Balancer.

Inicio y detención de un asesor

Si lo desea, puede iniciar un asesor para un puerto concreto de todos los clústeres (asesor de grupo). O bien, puede optar por ejecutar distintos asesores en el mismo puerto, pero en distintos clústeres (asesor específico del clúster/sitio). Por ejemplo, si ha definido Load Balancer con tres clústeres (*clusterA*, *clusterB*, *clusterC*), cada uno con el puerto 80, puede hacer lo siguiente:

- Asesor específico del clúster/sitio: para iniciar un asesor en el puerto 80 para *clusterA*, especifique el clúster y el puerto:

```
dscontrol advisor start http clusterA:80
```

Este mandato iniciará el asesor HTTP en el puerto 80 para *clusterA*. El asesor HTTP asesorará sobre todos los servidores conectados al puerto 80 para *clusterA*.

- Asesor de grupo: para iniciar un asesor personalizado en el puerto 80 para todos los demás clústeres, simplemente especifique el puerto:

```
dscontrol advisor start ADV_personalizado 80
```

Este mandato iniciará el asesor *ADV_personalizado* en el puerto 80 para *clusterB* y *clusterC*. El asesor personalizado asesorará sobre todos los servidores conectados al puerto 80 para *clusterB* y *clusterC*. (Para obtener más información sobre asesores personalizados, consulte el apartado “Crear asesores personalizados (personalizables)” en la página 192).

Nota: El asesor de grupo asesorará sobre todos los clústeres/sitios que actualmente no tienen un asesor específico de clúster/sitio.

Si utiliza el ejemplo de configuración anterior para el asesor de grupo, puede decidir detener el asesor personalizado *ADV_personalizado* para el puerto 80 en sólo uno de los clústeres o en ambos (*clusterB* y *clusterC*).

- Para detener el asesor personalizado para el puerto 80 únicamente en *clusterB*, especifique el clúster y el puerto:

```
dscontrol advisor stop ADV_personalizado  
clusterB:80
```

- Para detener el asesor personalizado para el puerto 80 en *clusterB* y *clusterC*, especifique sólo el puerto:

```
dscontrol advisor stop ADV_personalizado 80
```

Intervalos de asesor

Nota: Los valores por omisión del asesor deben funcionar de forma eficaz para la gran mayoría de casos posibles. Tenga cuidado al especificar valores distintos a los valores por omisión.

El intervalo del asesor establece la frecuencia con la que un asesor solicita el estado de los servidores en el puerto que está supervisando y, a continuación, notifica los resultados al gestor. Si el intervalo del asesor es demasiado bajo, puede suponer un bajo rendimiento como resultado de que el asesor interrumpe constantemente a los servidores. Si el valor de intervalo del asesor es demasiado alto, puede indicar que las decisiones del gestor sobre la ponderación no se basan en información actualizada y precisa.

Por ejemplo, para establecer el intervalo en 3 segundos para el asesor HTTP para el puerto 80, escriba el siguiente mandato:

```
dscontrol advisor interval http 80 3
```

No tiene sentido especificar un intervalo de asesor más pequeño que el intervalo del gestor. El valor por omisión del intervalo del asesor son siete segundos.

Tiempo de espera de informe del asesor

Para asegurarse de que el gestor no utiliza información desfasada en sus decisiones de equilibrio de carga, el gestor no utilizará información procedente del asesor cuya indicación de la hora sea anterior a la hora establecida en el tiempo de espera de informe del asesor. El tiempo de espera de informe del asesor debe ser mayor que el intervalo de sondeo del asesor. Si el tiempo de espera es más pequeño, el asesor ignorará informes que en buena lógica deberían utilizarse. Por omisión, los informes del asesor no exceden el tiempo de espera; el valor por omisión es unlimited.

Por ejemplo, para establecer el tiempo de espera de informe del asesor en 30 segundos para el asesor HTTP para el puerto 80, escriba el siguiente mandato:

```
dscontrol advisor timeout http 80 30
```

Si desea más información sobre cómo establecer el tiempo de espera de informe del asesor, consulte el apartado “dscontrol advisor — controlar el asesor” en la página 349.

Tiempo de espera de conexión y recepción del asesor para los servidores

En Load Balancer, puede establecer los valores de tiempo de espera del asesor en el que detecta que un puerto particular en el servidor (un servicio) ha sufrido una anomalía. Los valores de tiempo de espera del servidor anómalo (connecttimeout y receivetimeout) determinan cuánto tiempo espera un asesor antes de informar que se ha producido una anomalía en una conexión o recepción.

Para obtener la detección más rápida del servidor anómalo, establezca los tiempos de espera de conexión y recepción en el valor más pequeño (un segundo) y establezca el tiempo de intervalo del gestor y asesor en el valor más pequeño (un segundo).

Nota: Si el volumen de tráfico de la red oscila entre moderado a alto y la respuesta del servidor aumenta, no establezca los valores timeoutconnect y timeoutreceive demasiado bajos o el asesor podría marcar prematuramente un servidor ocupado como anómalo.

Por ejemplo, para establecer connecttimeout y receivetimeout en 9 segundos para el asesor HTTP en el puerto 80, escriba el siguiente mandato:

```
dscontrol advisor connecttimeout http 80 9
dscontrol advisor receivetimeout http 80 9
```

El valor por omisión para el tiempo de espera de conexión y recepción es 3 veces el valor especificado para el tiempo de intervalo del asesor.

Reintento del asesor

Los asesores tienen la capacidad de reintentar una conexión antes de marcar un servidor como inactivo. El asesor no marcará un servidor como inactivo hasta que la consulta del servidor haya fallado el número de reintentos más 1. El valor de **retry** no debe ser mayor que 3. El siguiente mandato establece un valor de reintento de 2 para el asesor LDAP en el puerto 389:

```
dscontrol advisor retry ldap 389 2
```

Lista de asesores

- El asesor **HTTP** abre una conexión, por omisión envía una petición HEAD, espera una conexión de respuesta y devuelve el tiempo transcurrido como carga. Consulte el apartado “Configuración del asesor HTTP o HTTPS utilizando la opción de petición y respuesta (URL)” en la página 190 para obtener más información sobre cómo cambiar el tipo de petición enviada por el asesor HTTP.
- El **HTTPS** asesor es un asesor esencial para las conexiones SSL. Establece una conexión de socket SSL completa con el servidor. El asesor HTTPS abre una conexión SSL, envía una petición HTTPS, espera una respuesta, cierra la conexión y devuelve el tiempo transcurrido como carga. (Consulte también el asesor SSL, que es un asesor de poca importancia para las conexiones SSL).

Nota: El asesor HTTPS no depende de la clave de servidor ni del contenido de certificado, aunque éstos no pueden haber caducado.

- El asesor **SIP** abre una conexión, envía una petición OPTIONS, espera una respuesta, cierra la conexión y devuelve el tiempo transcurrido como carga. El asesor SIP que recibe soporte sólo se ejecuta en TCP y requiere que haya instalada una aplicación en un servidor que responda a una petición OPTIONS.

- El asesor **FTP** abre una conexión, envía una petición SYST, espera una respuesta, cierra la conexión y devuelve el tiempo transcurrido como carga.
- El asesor **LDAP** abre una conexión, envía una petición BIND anónima, espera una respuesta, cierra la conexión y devuelve el tiempo transcurrido como carga.
- El asesor **Telnet** abre una conexión, espera un mensaje inicial del servidor, cierra la conexión y devuelve el tiempo transcurrido como carga.
- El asesor **NNTP** abre una conexión, espera un mensaje inicial del servidor, envía un mandato quit, cierra la conexión y devuelve el tiempo transcurrido como carga.
- El asesor **IMAP** abre una conexión, espera un mensaje inicial del servidor, envía un mandato quit, cierra la conexión y devuelve el tiempo transcurrido como carga.
- El asesor **POP3** abre una conexión, espera un mensaje inicial del servidor, envía un mandato quit, cierra la conexión y devuelve el tiempo transcurrido como carga.
- El asesor **SMTP** abre una conexión, espera un mensaje inicial del servidor, envía un mandato quit, cierra la conexión y devuelve el tiempo transcurrido como carga.
- El asesor **SSL** es un asesor de poca importancia para las conexiones SSL. No establece una conexión de socket SSL completa con el servidor. El asesor SSL abre una conexión, envía una petición SSL CLIENT_HELLO, espera una respuesta, cierra la conexión y devuelve el tiempo transcurrido como carga. (Consulte también el asesor HTTPS, que es un asesor esencial para las conexiones SSL).

Nota: El asesor SSL no depende de la gestión de claves ni de los certificados.

- El **ssl2http** asesor se inicia y asesora a los servidores enumerados bajo el puerto 443, pero el asesor abrirá un socket para “mapport” para las peticiones HTTP. Sólo debe utilizar el asesor ssl2http para CBR si el protocolo de cliente a proxy es SSL y el protocolo de proxy a servidor es HTTP. Consulte el apartado “Equilibrio de carga de cliente a proxy en SSL y de proxy a servidor en HTTP” en la página 108 para obtener más información
- El asesor Caching Proxy (cachingproxy) abre una conexión, envía una petición HTTP GET específica de Caching Proxy e interpreta la respuesta como carga de Caching Proxy.

Nota: Al utilizar el asesor Caching Proxy, Caching Proxy necesita estar en ejecución en todos los servidores en los que se realiza el equilibrio de carga. La máquina en la que reside Load Balancer no necesita tener instalado Caching Proxy a menos que esté en una ubicación compartida de la misma máquina en la que realiza el equilibrio de carga.

- El asesor **DNS** abre una conexión, envía una consulta de puntero para DNS, espera una respuesta, cierra la conexión y devuelve el tiempo transcurrido como carga.
- El asesor **connect** no intercambia ningún dato específico de protocolo con el servidor. Simplemente calcula el tiempo que tarda en abrir y cerrar una conexión TCP con el servidor. Este asesor es útil para las aplicaciones de servidor que utilizan TCP, pero con un protocolo de alto nivel para el que no está disponible un asesor personalizado o proporcionado por IBM.
- El asesor **ping** no abre una conexión TCP con los servidores, sino que en su lugar informa de si el servidor responde a un mandato ping. Mientras el asesor ping puede utilizarse en cualquier puerto, también se ha diseñado para configuraciones que utilizan el puerto comodín, en el que puede circular tráfico

con varios protocolos. También es útil para configuraciones que utilizan protocolos que no son TCP con sus servidores, como UDP.

- El asesor de **alcance** emite mandatos ping a sus máquinas de destino. Este asesor también está diseñado para que los componentes de alta disponibilidad de Dispatcher determinen la accesibilidad de sus destinos de alcance. Los resultados se dirigen al componente de alta disponibilidad y *no* aparecen en el informe del gestor. A diferencia de otros asesores, el asesor de alcance lo inicia automáticamente la función de gestor del componente Dispatcher.
- El asesor **DB2** funciona junto con los servidores DB2. Dispatcher tiene una función incorporada para comprobar el estado de servidores DB2 sin que sea necesario que los clientes escriban sus propios asesores personalizados. El asesor DB2 sólo se comunica con el puerto de conexión DB2, no con el puerto de conexión Java.
- El asesor **automático** recopila información sobre el estado de carga de los servidores de programa de fondo. Puede usar el asesor automático cuando utiliza Dispatcher en una configuración de dos niveles, en donde Dispatcher facilita información del asesor automático a Load Balancer de nivel superior. El asesor automático mide automáticamente el índice de conexiones por segundo en los servidores de programa de fondo de Dispatcher en el nivel del ejecutor. Consulte el apartado “Utilización del asesor automático en una configuración WAN de dos niveles” en la página 192 para obtener más información.
- El asesor **WLM** (Gestor de carga de trabajo) se ha diseñado para funcionar junto con servidores en sistemas principales OS/390 que ejecutan el componente Gestor de carga de trabajo (WLM) de MVS. Para obtener más información, consulte el apartado “Asesor del gestor de carga de trabajo” en la página 198.
- Dispatcher permite que un cliente escriba un asesor *personalizado* (personalizable). Esto permite el soporte de protocolos con marca registrada (encima de TCP) para los que IBM no ha desarrollado un asesor específico. Para obtener más información, consulte el apartado “Crear asesores personalizados (personalizables)” en la página 192.
- El asesor **WAS** (WebSphere Application Server) funciona junto con los servidores de aplicaciones de WebSphere. En el directorio de instalación encontrará archivos de ejemplo personalizables para este asesor. Para obtener más información, consulte el apartado “Asesor WAS” en la página 194.

Configuración del asesor HTTP o HTTPS utilizando la opción de petición y respuesta (URL)

La opción URL para el asesor HTTP o HTTPS está disponible para los componentes Dispatcher y CBR.

Después de iniciar un asesor HTTP o HTTPS, puede definir una serie URL HTTP de cliente exclusiva, específica para el servicio que desea examinar en el servidor. Esto permite que el asesor evalúe el estado de servicios individuales dentro de un servidor. Para hacerlo, defina los servidores lógicos con nombres de servidor exclusivos que tengan la misma dirección IP física. Consulte el apartado “Creación de particiones del servidor: servidores lógicos configurados con un servidor físico (dirección IP)” en la página 58 para obtener más información.

Para cada servidor lógico definido bajo el puerto HTTP, puede especificar una serie URL HTTP de cliente exclusiva, específica para el servicio que desea examinar en el servidor. El asesor HTTP o HTTPS utiliza la serie **advisorrequest** para examinar el estado de los servidores. El valor por omisión es HEAD / HTTP/1.0. La serie **advisorresponse** es la respuesta en la que el asesor busca la respuesta HTTP. El

asesor utiliza la serie **advisorresponse** y la compara con la respuesta real que se recibe del servidor. El valor por omisión es null.

Importante: si la serie URL de HTTP incluye un espacio en blanco:

- Al emitir el mandato desde el indicador del shell **dscontrol>>**, si la serie contiene un espacio en blanco, debe especificar la serie entre comillas. Por ejemplo:

```
server set clúster:puerto:servidor advisorrequest "head / http/1.0"
server set clúster:puerto:servidor advisorresponse "HTTP 200 OK"
```

- Al emitir el mandato **dscontrol** desde el indicador del sistema operativo, debe preceder el texto con `"\"` y terminarlo con `\"`. Por ejemplo:

```
dscontrol server set clúster:puerto:servidor
advisorrequest "\"head / http/1.0\""
```

```
dscontrol server set clúster:puerto:servidor advisorresponse "\"HTTP 200 OK\""
```

Cuando cree la petición que el asesor HTTP o HTTPS envía a servidores de programa de fondo para comprobar si están funcionando, escriba el comienzo de la petición HTTP y Load Balancer completará el final de la petición con lo siguiente:

```
\r\nAccept:
*/*\r\nUser-Agent:IBM_Network_Dispatcher_HTTP_Advisor\r\n\r\n
```

Si desea añadir otros campos de cabecera HTTP antes de que Load Balancer añada esta serie al final de la petición, también puede hacerlo incluyendo su propia serie `\r\n` en la petición. A continuación se muestra un ejemplo de lo que podría escribir para añadir el campo de cabecera de sistema principal HTTP a la petición:

```
GET /pub/WWW/TheProject.html HTTP/1.0 \r\nHost: www.w3.org
```

Nota: Después de iniciar un asesor HTTP o HTTPS para un número de puerto HTTP especificado, el valor de petición y respuesta del asesor se habilita para servidores bajo dicho puerto HTTP.

Consulte el apartado “dscontrol server — configurar servidores” en la página 392 para obtener más información.

Utilización del asesor automático en una configuración WAN de dos niveles

El asesor automático está disponible en el componente Dispatcher.

Para Load Balancer, en una configuración de WAN (red de área amplia) de dos niveles, Dispatcher proporciona un asesor *automático* que recopila información de estado de carga en servidores de programa de fondo.

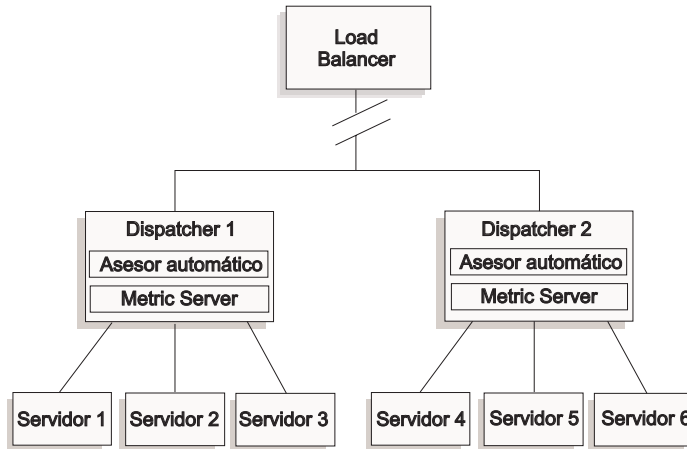


Figura 34. Ejemplo de una configuración WAN de dos niveles que utiliza el asesor automático

En este ejemplo, el asesor automático junto con Metric Server reside en las dos máquinas Dispatcher sobre las que realiza el equilibrio de carga Load Balancer de nivel superior. El asesor automático mide automáticamente el índice de conexiones por segundo en los servidores de programa de fondo de Dispatcher en el nivel del ejecutor.

El asesor automático escribe los resultados en el archivo dsloadstat. Load Balancer también proporciona una métrica externa denominada dsload. El agente de Metric Server de cada máquina Dispatcher ejecuta su configuración que llama al dsload de métrica externa. El script dsload extrae una serie del archivo dsloadstat y la devuelve al agente de Metric Server. Posteriormente, cada uno de los agentes de Metric Server (de cada uno de los sistemas Dispatcher) devuelve el valor del estado de la carga a Load Balancer de nivel superior para que la utilice para determinar a qué sistema Dispatcher reenviar las peticiones de cliente.

El dsload ejecutable reside en el directorio `...ibm/edge/lb/ms/script` de Load Balancer.

Consulte el apartado “Configurar soporte de Dispatcher de área amplia” en la página 229 para más información sobre la utilización de Dispatcher en configuraciones WAN. Consulte el apartado “Metric Server” en la página 196 para obtener más información sobre Metric Server.

Crear asesores personalizados (personalizables)

El asesor personalizado (personalizable) es un trozo pequeño de código Java que se proporciona como archivo de clases y es llamado por el código base. El código base proporciona todos los servicios administrativos, como iniciar y detener una instancia del asesor personalizado, proporcionar estado e informes y anotar la información de historial en un archivo de anotaciones cronológicas. También

notifica los resultados al componente del gestor. De forma periódica, el código base lleva a cabo un ciclo de asesor, donde evalúa de forma individual todos los servidores en su configuración. Empieza abriendo una conexión con una máquina servidor. Si se abre socket, el código base llamará al método “getLoad” (función) en el asesor personalizado. A continuación, el asesor personalizado llevará a cabo los pasos necesarios para evaluar el estado del servidor. En general, enviará al servidor un mensaje definido por el usuario y luego esperará una respuesta. (Se proporciona acceso al socket abierto para el asesor personalizado). A continuación, el código base cierra el socket con el servidor y notifica la información de carga al gestor.

El código base y el asesor personalizado puede funcionar en modalidad normal o de sustitución. La selección de la modalidad de operación se especifica en el archivo de asesor personalizado como parámetro en el método del constructor.

En modalidad normal, el asesor personalizado intercambia datos con el servidor y el código del asesor base calcula la duración del intercambio y calcula el valor de carga. A continuación, el código base informa de este valor de carga al gestor. El asesor personalizado sólo necesita devolver un cero (cuando es satisfactorio) o un valor negativo (cuando es erróneo). Para especificar la modalidad normal, el distintivo de sustitución en el constructor se establece en false.

En modalidad de sustitución, el código base no lleva a cabo las mediciones de tiempo. El código del asesor personalizado realiza todas las operaciones que desee para sus requisitos exclusivos y, a continuación, devuelve un número de carga real. El código base aceptará el número y lo notificará al gestor. Para obtener los mejores resultados, normalice el número de carga entre 10 y 1000, en donde 10 representa un servidor rápido y 1000 representa un servidor lento. Para especificar la modalidad de sustitución, el distintivo de sustitución en el constructor se establece en true.

Con esta característica, puede escribir sus propios asesores de forma que proporcionen la información exacta que necesite sobre los servidores. Con el producto Load Balancer se proporciona un asesor personalizado de ejemplo, **ADV_sample.java**. Después de instalar Load Balancer, puede encontrar el código de ejemplo en el directorio de instalación
...<directorio de instalación>/servers/samples/CustomAdvisors.

El valor por omisión del *directorio de instalación* es:

- En sistemas AIX, HP-UX, Linux, Solaris: /opt/ibm/edge/lb
- En sistemas Windows: C:\Archivos de programa\IBM\edge\lb

Nota: Si añade un asesor personalizado a Dispatcher o a cualquier otro componente de Load Balancer pertinente, debe detener y, a continuación, reiniciar **dsserver** (o el servicio en sistemas Windows) para que proceso Java pueda leer los nuevos archivos de clase de asesor personalizado. Los archivos de clase de asesor personalizado sólo se cargan durante el arranque. No es necesario detener el ejecutor. El ejecutor sigue en ejecución incluso cuando se ha detenido dsserver o el servicio.

Si el asesor personalizado hace referencia a clases Java adicionales, se debe actualizar la classpath en el archivo script de inicio de Load Balancer (dsserver, cbrserver, ssserver) de forma que incluya la ubicación.

Asesor WAS

Los archivos de asesor personalizado de ejemplo para el asesor WebSphere Application Server (WAS) se proporcionan en el directorio de instalación de Load Balancer.

- ADV_was.java es el archivo que debe compilarse y ejecutarse en la máquina Load Balancer
- LBAAdvisor.java.servlet (que debe renombrarse LBAAdvisor.java) es el archivo que debe compilarse y ejecutarse en la máquina WebSphere Application Server.

Los archivos de ejemplo del asesor de WebSphere Application Server se encuentran en el mismo directorio de ejemplo que el archivo ADV_sample.java.

Convenio de denominación

El nombre del archivo de asesor personalizado debe tener el formato "ADV_miasesor.java." Debe empezar con el prefijo " ADV_" en mayúsculas. Todos los caracteres subsiguientes deben indicarse en minúsculas.

Según los convenios Java, el nombre de la clase definida dentro del archivo debe coincidir con el nombre del archivo. Si copia el código de ejemplo, asegúrese de cambiar todas las instancias de "ADV_sample" dentro del archivo por el número nombre de clase.

Compilación

Los asesores personalizados se escriben en lenguaje Java. Utilice el compilador Java que se instala con Load Balancer. Durante la compilación aparecen referenciados los siguientes archivos:

- El archivo de asesor personalizado
- El archivo de clases base, ibmlb.jar, que se encuentra en el directorio de instalación **...ibm/edge/lb/servers/lib**.

La classpath debe apuntar al archivo de asesor personalizado y el archivo de clases base durante la compilación.

En sistemas Windows, un mandato de compilación de ejemplo es:

```
dir_instalación/java/bin/javac -classpath  
dir_instalación\lb\servers\lib\ibmlb.jar ADV_fred.java
```

donde:

- El archivo del asesor se denomina ADV_fred.java
- El archivo del asesor se almacena en el directorio actual

La salida de la compilación está en un archivo de clases, por ejemplo:

ADV_fred.class

Antes de iniciar el asesor, copie el archivo de clases en el directorio de instalación **...ibm/edge/lb/servers/lib/CustomAdvisors**.

Nota: Si lo desea, los asesores personalizados pueden compilarse en un sistema operativo y ejecutarse en otro. Por ejemplo, puede compilar el asesor en sistemas Windows, copiar el archivo de clase (en binario) en una máquina AIX y ejecutar aquí el asesor personalizado.

En sistemas AIX, HP-UX, Linux y Solaris, la sintaxis es parecida.

Ejecución

Para ejecutar el asesor personalizado, primero debe copiar el archivo de clases en el directorio de instalación adecuado:

```
...ibm/edge/lb/servers/lib/CustomAdvisors/ADV_fred.class
```

Configure el componente, inicie la función de gestor y emita el mandato para iniciar el asesor personalizado:

```
dscontrol advisor start fred 123
```

donde:

- fred es el nombre del asesor, como en ADV_fred.java
- 123 es el puerto en donde funcionará el asesor

Si el asesor personalizado hace referencia a clases Java adicionales, se debe actualizar la classpath en el archivo script de inicio de Load Balancer (dssserver, cbrserver, sssserver) de forma que incluya la ubicación.

Rutinas necesarias

Como todos los asesores, un asesor personalizado amplía la función del asesor base, denominada ADV_Base. Se trata de la base del asesor que en realidad efectúa la mayoría de las funciones del asesor, como informar de las cargas al gestor para que se utilicen en el algoritmo de peso del gestor. La base del asesor también realiza operaciones de conexión y cierre de sockets, y proporciona métodos de envío y recepción para que el asesor los utilice. El asesor sólo se utiliza para enviar datos y recibir datos en el puerto del servidor que se está asesorando. Para calcular la carga, se calcula la duración de los métodos TCP incluidos en la base del asesor. Un distintivo incluido en el constructor en ADV_base escribe encima de la carga existente la nueva carga devuelta desde el asesor, si se desea.

Nota: La base del asesor proporciona la carga al algoritmo de peso a intervalos especificados en función de un valor fijado en el constructor. Si el asesor real no se ha completado y no puede devolver una carga válida, la base del asesor utiliza la carga anterior.

A continuación se indican los métodos de clase base:

- Una rutina **constructor**. El constructor llama al constructor de clase base (consulte el archivo de asesor de ejemplo)
- Un método **ADV_AdvisorInitialize**. Este método proporciona un enlace por si fuera necesario realizar pasos adicionales después de que la clase base finalice su inicialización.
- Una rutina **getload**. La clase de asesor base lleva a cabo la apertura del socket; por lo tanto, getload sólo necesita emitir las peticiones de envío y recepción para completar el ciclo del asesor.

Orden de búsqueda

Load Balancer primero busca en la lista de los asesores nativos que proporciona. Si no encuentra un determinado asesor aquí, Load Balancer lo buscará en la lista de asesores personalizados del cliente.

Denominación y vía de acceso

- La clase de asesor personalizado debe estar dentro del subdirectorio de **...ibm/edge/lb/servers/lib/CustomAdvisors/** en el directorio base de Load Balancer. Los valores por omisión para este directorio varían según el sistema operativo:
 - Sistemas AIX, HP-UX, Linux y Solaris
/opt/ibm/edge/lb/servers/lib/CustomAdvisors/
 - Sistemas Windows
C:\Archivos de programa\IBM\edge\lb\servers\lib\CustomAdvisors
- Sólo se permiten caracteres alfabéticos en minúsculas. Esto excluye la sensibilidad a mayúsculas y minúsculas cuando un operador entra los mandatos en la línea de mandatos. El nombre de archivo de asesor debe tener el prefijo **ADV_**.

Asesor de ejemplo

La lista de programas de un asesor de ejemplo se incluye en “Asesor de ejemplo” en la página 485. Después de la instalación, este asesor de ejemplo puede encontrarse en el directorio **...ibm/edge/lb/servers/samples/CustomAdvisors** .

Metric Server

Esta característica está disponible para todos los componentes de Load Balancer.

Metric Server proporciona información de carga de servidor para Load Balancer en la forma de métricas específicas del sistema que notifica el estado de los servidores. El gestor de Load Balancer examina el agente de Metric Server que reside en cada uno de los servidores y asigna pesos al proceso de equilibrio de carga utilizando la métrica recopilada desde los agentes. Los resultados también aparecen en el informe del gestor.

Nota: Cuando se recopilan y normalizan dos o más métricas para cada servidor en un solo valor de carga del sistema, pueden producirse errores de redondeo.

Para obtener información sobre el funcionamiento de Metric Server (inicio y detención) y la utilización de los archivos de anotaciones de Metric Server, consulte “Utilización del componente Metric Server” en la página 280.

Para obtener un ejemplo de configuración, consulte la Figura 5 en la página 14.

Restricción para WLM

Al igual que el asesor WLM, Metric Server informa sobre los sistemas de servidor como un conjunto, en lugar de hacerlo en daemons de servidor individuales específicos del protocolo. Tanto WLM como Metric Server colocan sus resultados en la columna de sistema del informe del gestor. Como consecuencia, no se da soporte a la ejecución simultánea del asesor WLM y de Metric Server.

Requisitos previos

El agente de Metric Server debe estar instalado y en ejecución en todos los servidores en los que se está realizando el equilibrio de carga.

Cómo utilizar Metric Server

A continuación se muestran los pasos para configurar Metric Server para Dispatcher. Para configurar Metric Server para los demás componentes de Load Balancer puede utilizar un procedimiento parecido.

- Gestor de Load Balancer (Load Balancer)

1. Inicie **dsserver**.

2. Emita el mandato: **dscontrol manager start** *manager.log puerto*

puerto es el puerto RMI seleccionado para que se ejecuten todos los agentes de Metric Server. El puerto RMI por omisión establecido en el archivo `metricserver.cmd` es 10004.

3. Emita el mandato: **dscontrol metric add** *clúster:métricaSistema*

métricaSistema es el nombre del script (que reside en el servidor de programa de fondo) que debe ejecutarse en cada uno de los servidores de la configuración bajo el clúster (o nombre de sitio) especificado. Se proporcionan dos scripts para el cliente, **cpuload** y **memload**. O si lo desea, puede crear scripts de métrica de sistema personalizados. El script contiene un mandato que debe devolver un valor numérico comprendido en el rango 0-100 o el valor -1 si el servidor está inactivo. Este valor numérico debe representar una medida de carga, no un valor de disponibilidad..

Nota: En el caso de Site Selector, **cpuload** y **memload** se ejecutan automáticamente.

Limitación: en la plataforma Windows, si la extensión del nombre del script de métrica del sistema tiene una extensión distinta de ".exe", debe especificar el nombre completo del archivo (por ejemplo, "miscriptsistema.bat"). Se debe a una limitación de Java.

4. Añada a la configuración sólo servidores que contengan un agente de Metric Server en el puerto especificado en el archivo `metricserver.cmd`. El puerto debe coincidir con el valor de puerto especificado en el mandato **manager start**.

Nota: Habilite la seguridad:

- En la máquina Load Balancer, cree un archivo de claves (con el mandato **lbkeys create**). Consulte el apartado "RMI (Remote Method Invocation)" en la página 262 para obtener más información sobre **lbkeys**.
- En la máquina servidor de programa de fondo, copie el archivo de claves obtenido, correspondiente al componente que está utilizando, en el directorio `...ibm/edge/lb/admin/keys`. Verifique que los permisos del archivo de claves permitan al usuario root leer el archivo.

- Agente de Metric Server (máquina servidor)

1. Instale el paquete de Metric Server en la instalación de Load Balancer.

2. Examine el script **metricserver** que está en el directorio `/usr/bin` para verificar que se están utilizando el puerto RMI que desee. (En sistemas Windows 2003, el directorio es `C:\WINDOWS\system32`.) El puerto RMI por omisión es 10004.

Nota: El valor de puerto RMI especificado debe ser el mismo que el valor del puerto RMI para Metric Server en la máquina de Load Balancer.

3. Para el cliente ya se proporcionan los dos scripts siguientes: **cpuload** (devuelve el porcentaje de CPU en uso que oscila entre 0 y 100) y **memload**

(devuelve el porcentaje de la memoria en uso que oscila entre 0 y 100). Estos scripts residen en el directorio **...ibm/edge/lb/ms/script**.

De manera opcional, los clientes pueden escribir sus propios archivos de script de métrica personalizados que definan el mandato que Metric Server emitirá en las máquinas de servidor. Asegúrese de que todos los script personalizados son ejecutables y que están en el directorio

...ibm/edge/lb/ms/script. Los scripts personalizados **debe** devolver un valor de carga numérico comprendido entre 0 y 100.

Nota: Un script de métrica personalizada debe ser un script o programa válido con una extensión ".bat" o ".cmd". De forma específica, en Sistemas Linux y UNIX los scripts deben empezar con la declaración del shell, de lo contrario, es posible que no se ejecuten correctamente.

4. Inicie el agente emitiendo el mandato **metricserver**.
5. Para detener el agente de Metric Server, emita el mandato **metricserver stop**.

Para que Metric Server se ejecute en una dirección distinta del sistema principal local, es necesario editar el archivo **metricserver** en la máquina servidor con equilibrio de carga. Después de la aparición de "java" en el archivo **metricserver**, inserte lo siguiente:

```
-Djava.rmi.server.hostname=OTRA_DIRECCIÓN
```

Además, añada esta línea **hostname OTRA_DIRECCIÓN** antes de las sentencias "if" en el archivo **metricserver**.

En la plataforma Windows: también es necesario crear un alias de **OTRA_DIRECCIÓN** en la pila de Microsoft de la máquina de Metric Server. Por ejemplo:

```
call netsh interface ip add address "Conexión de área local"  
addr=9.37.51.28 mask=255.255.240.0
```

Al recopilar métricas por distintos dominios, debe establecer de forma explícita **java.rmi.server.hostname** en el script del servidor (**dsserver**, **cbrserver**, etc) con el nombre de dominio completo (FQDN) de la máquina que solicita la métrica. Esto es necesario porque, en función de la configuración y del sistema operativo que utilice, es posible que **InetAddress.getLocalHost.getHostName()** no devuelva el nombre de dominio completo (FQDN).

Asesor del gestor de carga de trabajo

WLM es el código que se ejecuta en sistemas principales MVS. Puede consultarse para saber la carga de la máquina MVS.

Cuando se ha configurado la gestión de carga de trabajo de MVS en el sistema OS/390, Dispatcher puede aceptar información de capacidad de WLM y utilizarla en el proceso de carga del sistema. Con el asesor WLM, Dispatcher abre de forma periódica las conexiones a través del puerto de WLM en cada servidor de la tabla de sistemas principales de Dispatcher y aceptar los enteros de capacidad devueltos. Puesto que estos enteros representan la cantidad de capacidad que todavía está disponible y Dispatcher espera valores que representan las cargas en cada máquina, el asesor invierte los enteros de capacidad y se sistematizan en valores de carga (es decir, un entero de gran capacidad y un valor de carga pequeño representan un servidor eficaz. Las cargas obtenidas se colocan en la columna Sistema del informe del gestor.

Hay varias diferencias importantes entre el asesor WLM y los demás asesores de Dispatcher.

1. Otros asesores abren conexiones para los servidores utilizando el mismo puerto en el que circula el tráfico de cliente normal. El asesor WLM abre conexiones para los servidores utilizando un puerto distinto del que utiliza el tráfico normal. El agente de WLM en cada máquina servidor debe configurarse de modo que escuche en el mismo puerto en el que se inicia el asesor WLM de Dispatcher. El puerto por omisión de WLM es 10007.
2. Otros asesores sólo evalúan a los servidores definidos en la configuración clúster:puerto:servidor de Dispatcher para la que el puerto del servidor coincide con el puerto del asesor. El asesor WLM informa sobre *cada* servidor de la configuración de Dispatcher (independientemente del clúster:puerto). Por lo tanto, no puede definir ningún servidor que no sea WLM cuando utiliza el asesor WLM.
3. Otros asesores ponen su información de carga en el informe de gestor bajo su columna "Puerto". El asesor WLM pone su información de carga en el informe del gestor bajo la columna del sistema.
4. Junto con el asesor WLM es posible utilizar los dos asesores específicos del protocolo. Los asesores específicos de protocolo sondearán los servidores en sus puertos de tráfico normal y el asesor WLM sondeará la carga del sistema utilizando el puerto WLM.

Restricción para Metric Server

Al igual que el agente de Metric Server, el agente de WLM informa sobre los sistemas de servidor como un conjunto, en lugar de hacerlo en daemons de servidor individuales específicos del protocolo. Metric Server y WLM colocan sus resultados en la columna de sistema del informe del gestor. Como consecuencia, no se da soporte a la ejecución simultánea del asesor WLM y de Metric Server.

Capítulo 22. Características avanzadas para Dispatcher, CBR y Site Selector

En este capítulo se explica cómo configurar los parámetros de equilibrio de carga así como las funciones avanzadas de Load Balancer.

Nota: Al leer este capítulo, si *no* está utilizando el componente Dispatcher, sustituya "dscontrol" por lo siguiente:

- Para CBR, utilice **cbrcontrol**
- En Site Selector, utilice **sscontrol** (consulte el Capítulo 28, "Referencia de mandatos para Site Selector", en la página 403)

IMPORTANTE: si utiliza la instalación de Load Balancer para IPv4 y IPv6 consulte el Capítulo 8, "Despliegue de Dispatcher en Load Balancer para IPv4 y IPv6", en la página 81 para obtener las limitaciones y diferencias de configuración antes de consultar el contenido de este capítulo.

Tabla 13. Tareas de configuración avanzada para Load Balancer

Tarea	Descripción	Información relacionada
Poner en ubicación compartida Load Balancer en una máquina que tiene equilibrio de carga	Configura una máquina Load Balancer con ubicación compartida.	"Utilización de servidores con ubicación compartida" en la página 203
Configurar alta disponibilidad o alta disponibilidad mutua	Configura una segunda máquina Dispatcher para proporcionar una máquina de reserva.	"Alta disponibilidad" en la página 204
Configurar el equilibrio de carga basado en normas	Define las condiciones en las que se utiliza un conjunto de servidores.	"Configuración de equilibrio de carga basado en normas" en la página 212
Utilizar la alteración temporal de la afinidad entre puertos para proporcionar un mecanismo para que un servidor altere la característica de permanencia en memoria.	Permite a un servidor alterar el valor de permanencia en memoria en este puerto.	"Alteración temporal de la afinidad entre puertos" en la página 219
Utilizar característica de permanencia en memoria (afinidad) para configurar el puerto de un clúster para que sea permanente en memoria	Permite dirigir al mismo servidor las peticiones de cliente.	"Cómo funciona la característica de afinidad para Load Balancer" en la página 221
Utilizar afinidad entre puertos para expandir la característica de permanencia en memoria(afinidad) entre los puertos	Permite dirigir al mismo servidor las peticiones de cliente que se reciben en distintos puertos.	"Afinidad entre puertos" en la página 222
Utilizar máscara de dirección de afinidad para designar una dirección de subred IP común	Permite dirigir al mismo servidor las peticiones de cliente que se reciben en la misma subred.	"Máscara de dirección de afinidad (stickymask)" en la página 223
Utilizar afinidad de cookies activos para equilibrar la carga en servidores de CBR	Una opción de norma que permite que una sesión mantenga afinidad para un servidor concreto.	"Afinidad de cookies activos" en la página 225

Tabla 13. Tareas de configuración avanzada para Load Balancer (continuación)

Tarea	Descripción	Información relacionada
Utilizar afinidad de cookies pasivos para equilibrar la carga en servidores con direccionamiento basado en contenido de Dispatcher y el componente CBR	Una opción de norma que permite que una sesión mantenga afinidad para un servidor concreto en función del valor de cookie/nombre de cookie.	"Afinidad de cookies pasivos" en la página 227
Utilizar la afinidad de URI para equilibrar la carga en los servidores Caching Proxy con contenido exclusivo para almacenarlo en la antememoria de cada uno de ellos	Una opción de norma que permite que una sesión mantenga afinidad para un servidor concreto en función del URI.	"Afinidad de URI" en la página 228
Configurar el soporte de Dispatcher de red de área amplia	Configura un Dispatcher remoto para equilibrar la carga en toda una red de área amplia. O bien, equilibra la carga en toda una red de área amplia (sin un Dispatcher remoto) utilizando una plataforma de servidor que dé soporte a GRE.	"Configurar soporte de Dispatcher de área amplia" en la página 229
Utilizar enlace explícito	Evita que Dispatcher se pase por alto en los enlaces.	"Utilización del enlace explícito" en la página 236
Utilizar una red privada	Configura Dispatcher para equilibrar la carga en los servidores de una red privada.	"Utilización de una configuración de red privada" en la página 236
Utilizar un clúster comodín para combinar configuraciones de servidores comunes	Las direcciones que no se han configurado de forma explícita utilizarán el clúster comodín como una forma de equilibrar la carga del tráfico.	"Utilizar un clúster comodín para combinar configuraciones de servidores" en la página 237
Utilizar clúster comodín para equilibrar la carga de cortafuegos	Se equilibrará la carga de todo el tráfico en cortafuegos.	"Utilizar un clúster comodín para equilibrar la carga de cortafuegos" en la página 238
Utilizar el clúster comodín con Caching Proxy para un proxy transparente	Permite utilizar Dispatcher para habilitar un proxy transparente.	"Utilizar un clúster comodín con Caching Proxy para el proxy transparente" en la página 238
Utilizar puerto comodín para dirigir tráfico de puerto no configurado	Maneja el tráfico que no está configurado para cualquier puerto específico.	"Utilizar el puerto comodín para dirigir el tráfico de puerto no configurado" en la página 239
Utilizar la detección de "ataques para rechazo de servicio" (DoS) para notificar a los administradores (mediante una alerta) los ataques potenciales	Dispatcher analiza peticiones entrantes para una cantidad llamativa de conexiones TCP medio abiertas en servidores.	"Detección de ataques para rechazo de servicio (DoS)" en la página 239
Utilizar el registro cronológico binario para analizar estadísticas de servidor	Permite almacenar en archivos binarios la información del servidor y recuperarla.	"Utilización del registro cronológico binario para analizar estadísticas de servidor" en la página 241
Utilizar una configuración de cliente con ubicación compartida	Permite a Load Balancer residir en la misma máquina que un cliente	"Utilización de un cliente con ubicación compartida" en la página 242

Utilización de servidores con ubicación compartida

Load Balancer puede residir en la misma máquina que un servidor para el que equilibre la carga de las peticiones. Esto se conoce habitualmente como *ubicación compartida* de un servidor. La ubicación compartida se aplica a los componentes Dispatcher y Site Selector. La ubicación compartida también se admite en CBR, pero sólo cuando utiliza servidores Web específicos del enlace y Caching Proxy específico del enlace.

Nota: Un servidor con ubicación compartida compite por los recursos contra Load Balancer durante los periodos de mucho tráfico. Sin embargo, si no hay máquinas sobrecargadas, si se utiliza un servidor con ubicación compartida se reducirá el número total de máquinas necesarias para definir un sitio con equilibrio de carga.

Para el componente Dispatcher

Sistemas **Linux**: para configurar la ubicación compartida y la alta disponibilidad a la vez cuando se ejecuta el componente Dispatcher utilizando el método de reenvío MAC, consulte el apartado “Alternativas de alias de bucle de retorno de Linux cuando se utiliza el reenvío MAC de Load Balancer” en la página 78.

Sistemas Windows: para configurar la ubicación compartida y la alta disponibilidad a la vez cuando se ejecuta el componente Dispatcher utilizando el método de reenvío MAC, consulte el apartado “Configurar la ubicación compartida y la alta disponibilidad (sistemas Windows)” en la página 211.

Sistemas **Solaris**: existe una limitación; no pueden configurarse asesores WAN cuando Dispatcher de punto de entrada tiene ubicación compartida. Consulte el apartado “Utilización de asesores remotos con el soporte de área amplia de Dispatcher” en la página 230.

En releases anteriores, era necesario especificar que la dirección del servidor con ubicación compartida fuera la misma que la dirección de no reenvío (NFA) en la configuración. Esta restricción ya no existe.

Para configurar un servidor para que forme parte de una ubicación compartida, el mandato **dscontrol server** proporciona una opción llamada **collocated** que puede establecerse en *yes* o *no*. El valor por omisión es *no*. La dirección del servidor debe ser una dirección IP válida de una tarjeta de interfaz de red de la máquina. El parámetro **collocated** no debe establecerse para servidores con ubicación compartida que utilizan el método de reenvío NAT o CBR de Dispatcher.

Puede configurar un servidor con ubicación compartida de una de las siguientes maneras:

- Si utiliza la NFA como dirección de servidor con ubicación compartida: establezca la NFA utilizando el mandato **dscontrol executor set nfa dirección_IP**. Añada también el servidor que utiliza la dirección NFA con el mandato **dscontrol server add clúster:puerto:servidor**.
- Si utiliza una dirección distinta de la NFA: añada el servidor con la dirección IP que desee con el parámetro **collocated** establecido en *yes*, tal como se indica a continuación: **dscontrol server add clúster:puerto:servidor collocated yes**.

Para el reenvío NAT o CBR de Dispatcher, debe configurar (crear un alias) una dirección de adaptador no utilizada en la NFA. El servidor debe configurarse de modo que escuche en esta dirección. Configure el servidor con la siguiente sintaxis de mandato:

```
dscontrol server add clúster:puerto:nuevo_alias address nuevo_alias router  
IP_direccionador returnaddress dirección_retorno
```

Si no se configura pueden producirse errores del sistema, que no haya respuesta del servidor, o los dos.

Configuración de la ubicación compartida del servidor con el reenvío NAT de Dispatcher

Al configurar un servidor con ubicación compartida utilizando el método de reenvío nat de Dispatcher, el direccionador especificado en el mandato `dscontrol server add` debe ser una dirección de direccionador real y no la dirección IP del servidor.

El soporte para la ubicación compartida al configurar el método de reenvío NAT de Dispatcher ahora puede llevarse a cabo en todos los sistemas operativos si se llevan a cabo los siguientes pasos en la máquina Dispatcher:

- **En sistemas AIX**, el servidor con ubicación compartida se configura como cualquier otro servidor. No es necesario realizar cambios en la configuración.
- **En sistemas Linux**, el servidor con ubicación compartida se configura como cualquier otro servidor. No es necesario realizar cambios en la configuración.
- **En sistemas Solaris y HP-UX**, se crea un alias para el clúster utilizando `ifconfig` de la forma habitual; sin embargo, la dirección de retorno debe publicarse con ARP en lugar de otorgarle un alias. Para ello, ejecute el siguiente mandato:

```
arp -s hostname ether_addr pub
```

utilizando la dirección MAC local para `ether_addr`. Esto permite a la aplicación local enviar tráfico a la dirección de retorno en el kernel.

- **En plataformas Windows**, el clúster y la dirección de retorno deben configurarse con el mandato `dscontrol executor configure` y sin ponerlos en Windows Networking. Para la aplicación local debe añadir un nuevo alias IP al adaptador local en Windows Networking. En la configuración de TCP/IP, busque la opción Avanzada para añadir las direcciones IP adicionales a un adaptador. Esta segunda dirección IP se utiliza como definición de servidor en la configuración de Dispatcher.

Para el componente CBR

CBR da soporte a la ubicación compartida en todas las plataformas sin que sea necesario realizar configuraciones adicionales. No obstante, los servidores Web y Caching Proxy que utilice deben ser específicos del enlace.

Para el componente Site Selector

Site Selector da soporte a la ubicación compartida en todas las plataformas sin que sea necesario realizar configuraciones adicionales.

Alta disponibilidad

La función de alta disponibilidad (que puede configurarse con el mandato `dscontrol highavailability`) está disponible para el componente Dispatcher, pero no para el componente CBR o Site Selector.

Para mejorar la disponibilidad de Dispatcher, la función de alta disponibilidad de Dispatcher utiliza los siguientes mecanismos:

- Dos sistemas Dispatcher con conectividad a los mismos clientes y el mismo clúster de servidores, así como conectividad entre los sistemas Dispatcher. Los dos sistemas Dispatcher deben ejecutarse en el mismo tipo de sistema operativo y plataforma.
- Un mecanismo de “pulsos” entre los dos sistemas Dispatcher para detectar anomalías en Dispatcher. Como mínimo un par de pulsos debe tener las NFA del par como dirección de origen y destino.
Si es posible, al menos uno de los pares de pulsos debe estar en una subred distinta del tráfico del clúster normal. Si el tráfico de pulsos se identifica claramente se evitará que se produzcan falsas lecturas de otras señales en condiciones de cargas elevadas en la red y se mejorarán los tiempos de recuperación completos después de producirse una sustitución por anomalía.
- Una lista de destinos de alcance, direcciones que las dos máquinas Dispatcher puedan contactar para equilibrar la carga del tráfico. Para obtener más información, consulte el apartado “Capacidad de detección de anomalías utilizando pulsos y destino de alcance” en la página 207.
- La sincronización de la información de Dispatcher (es decir, las tablas de conexión, las tablas de accesibilidad y otra información).
- La lógica para elegir el sistema Dispatcher activo que se ocupa de un determinado clúster de servidores y el sistema Dispatcher en espera que se sincroniza continuamente para dicho clúster de servidores.
- Un mecanismo para llevar a cabo la toma de control IP, cuando la lógica o un operador decide conmutar entre activo y en espera.

Nota: Si desea obtener una ilustración y una descripción de una configuración de *alta disponibilidad mutua*, donde dos máquinas Dispatcher que comparten dos conjuntos de clústeres actúan como máquina de reserva entre sí, consulte el apartado “Alta disponibilidad mutua” en la página 61. La alta disponibilidad mutua es parecida a la alta disponibilidad aunque se basa específicamente en la dirección de clúster en lugar de basarse en una máquina Dispatcher como un todo. Las dos máquinas deben configurar de la misma forma sus conjuntos de clúster compartidos.

Configurar la alta disponibilidad

La sintaxis completa para **dscontrol highavailability** está en “dscontrol highavailability — controlar alta disponibilidad” en la página 367.

Para obtener una descripción completa de muchas de las tareas que se indican a continuación, consulte el apartado “Configuración de la máquina Dispatcher” en la página 66.

1. Cree archivos script de alias en cada una de las dos máquinas Dispatcher. Consulte el apartado “Utilización scripts” en la página 209.
2. Inicie el servidor en las dos máquinas servidor Dispatcher.
3. Inicie el ejecutor en las dos máquinas.
4. Asegurarse de que la dirección de no reenvío (NFA) de cada máquina Dispatcher está configurada y que es una dirección IP válida para la subred de las máquinas Dispatcher.
5. Añada la información de pulsos en las dos máquinas:
`dscontrol highavailability heartbeat add dirección_origen dirección_destino`

Nota: *dirección_origen* y *dirección_destino* son las direcciones IP (los nombres DNS o las direcciones IP) de las máquinas Dispatcher. Los valores se invertirán en cada máquina. Por ejemplo:

```
Primary - highavailability heartbeat add 9.67.111.3 9.67.186.8
Backup - highavailability heartbeat add 9.67.186.8 9.67.111.3
```

Al menos un par de pulsos debe tener las NFA del par como dirección de origen y destino.

Si es posible, al menos uno de los pares de pulsos debe estar en una subred distinta del tráfico del clúster normal. Si el tráfico de pulsos se identifica claramente se evitará que se produzcan falsas lecturas de otras señales en condiciones de cargas elevadas en la red y se mejorarán los tiempos de recuperación completos después de producirse una sustitución por anomalía.

Establezca el número de segundos que el ejecutor utiliza para indicar el tiempo de espera de los pulsos de alta disponibilidad. Por ejemplo:

```
dscontrol executor set hatimeout 3
```

El valor por omisión es 2.

6. En las dos máquinas, configure la lista de direcciones IP que Dispatcher debe poder alcanzar para garantizar un servicio completo, utilizando el mandato **reach add**. Por ejemplo:

```
dscontrol highavailability reach add 9.67.125.18
```

Los destinos de alcance son recomendables aunque no necesarios. Consulte el apartado “Capacidad de detección de anomalías utilizando pulsos y destino de alcance” en la página 207 para obtener más información.

7. Añada la información de reserva para cada máquina:

- Para la máquina **primary**:

```
dscontrol highavailability backup add primary [auto | manual] puerto
```

- Para la máquina **backup**:

```
dscontrol highavailability backup add backup [auto | manual] puerto
```

- En alta disponibilidad mutua, cada máquina Dispatcher tiene **ambos** roles, primaria y reserva.

```
dscontrol highavailability backup add both [auto | manual] puerto
```

Nota: Seleccione un puerto no utilizado en las máquinas como *puerto*. El número de puerto entrado se utilizará como clave para asegurarse de que el paquete lo recibe el sistema principal correcto.

8. Compruebe el estado de alta disponibilidad en cada máquina:

```
dscontrol highavailability status
```

Cada una de las máquinas debe tener el rol correcto (reserva, primaria o ambos), estados y subestados. La máquina primaria debe estar activa y sincronizada; la máquina de reserva debe estar en modalidad de reposo y debe sincronizarse dentro de poco tiempo. Las estrategias deben ser las mismas.

9. Establezca la información de clúster, puerto y servidor en las dos máquinas.

Nota: Para la configuración de alta disponibilidad mutua (Figura 14 en la página 61), por ejemplo, configure los conjuntos del clúster compartidos entre los dos sistemas Dispatcher tal como se indica a continuación:

- Para Dispatcher 1, emita:
`dscontrol cluster set clústerA primaryhost NFAdispatcher1`
`dscontrol cluster set clústerB primaryhost NFAdispatcher2`
- Para Dispatcher 2, emita:
`dscontrol cluster set clústerB primaryhost NFAdispatcher2`
`dscontrol cluster set clústerA primaryhost NFAdispatcher1`

10. Inicie el gestor y los asesores en las dos máquinas.

Notas:

1. Para configurar una sola máquina Dispatcher para direccionar paquetes sin una máquina de reserva, no emita ninguno de los mandatos de alta disponibilidad durante el arranque.
2. Para convertir dos máquinas Dispatcher configuradas para alta disponibilidad en una sola máquina, detenga el ejecutor en una de las máquinas y suprima las características de alta disponibilidad (los pulsos, alcance y reserva) de la otra.
3. En los dos casos anteriores, debe utilizar direcciones de clúster para crear un alias para la tarjeta de interfaz de red, según sea necesario.
4. Cuando dos máquinas Dispatcher se ejecutan en configuración de alta disponibilidad y están sincronizadas, entre primero todos los mandatos `dscontrol` (para actualizar la configuración) en la máquina en espera y después en la máquina activa.
5. Cuando se ejecutan dos máquinas Dispatcher en una configuración de alta disponibilidad, pueden producirse resultados inesperados si en las dos máquinas se establecen distintos valores en alguno de los parámetros para el ejecutor, puerto o servidor (por ejemplo, `port stickytime`).
6. Para la alta disponibilidad mutua, considere el caso en que uno de las máquinas Dispatcher debe direccionar de forma activa paquetes para su clúster primario así como tomar el control del direccionamiento de paquetes para el clúster de reserva. Asegúrese que esto no exceda la capacidad de la producción en esta máquina.
7. En sistemas Linux, al configurar la alta disponibilidad y la ubicación compartida a la vez utilizando el método de reenvío del puerto MAC del componente Dispatcher, consulte el apartado “Alternativas de alias de bucle de retorno de Linux cuando se utiliza el reenvío MAC de Load Balancer” en la página 78.
8. En sistemas Windows, al configurar la alta disponibilidad y la ubicación compartida a la vez, consulte el apartado “Configurar la ubicación compartida y la alta disponibilidad (sistemas Windows)” en la página 211.
9. Si desea sugerencias que le ayuden a reducir los problemas que pueden surgir derivados de los problemas de configuración de alta disponibilidad, como por ejemplo:
 - Conexiones desactivadas después de la toma de control
 - No se pueden sincronizar máquinas asociadas
 - Peticiones dirigidas erróneamente a la máquina asociada de reserva

Consulte “Problema: sugerencias para configurar la alta disponibilidad” en la página 319.

Capacidad de detección de anomalías utilizando pulsos y destino de alcance

Además de los criterios básicos de detección de anomalía (la pérdida de conectividad entre máquinas Dispatcher activas y en espera, que se detecta a través de los mensajes de pulso), hay otro mecanismo de detección de anomalías

denominado *criterios de accesibilidad*. Al configurar Dispatcher se puede proporcionar una lista de sistemas principales a los que cada una de las máquinas Dispatcher debe poder llegar para funcionar correctamente. Los dos socios de alta disponibilidad se comunican constantemente a través de pulsos y se actualizan mutuamente en lo que se refiere a la cantidad de destinos de alcance a los que pueden emitir mandatos ping. Si, mediante mandatos ping, la máquina en espera puede acceder a más destinos de alcance que la máquina activa, se produce una sustitución por anomalía.

Los pulsos los envía la máquina Dispatcher activa y está previsto que la máquina Dispatcher en espera los reciba cada medio segundo. Si la máquina Dispatcher en espera no puede recibir un pulso durante un intervalo de 2 segundos, se empieza un proceso de sustitución por anomalía. Para que se produzca un proceso de toma de control por parte de la máquina Dispatcher en espera, es necesario que se interrumpan todos los pulsos. Es decir, cuando hay dos pares de pulsos configurados, los dos pulsos deben interrumpirse. Para estabilizar el entorno de alta disponibilidad y para evitar que se produzca una sustitución por anomalía, añada más de un par de pulsos.

Para los destinos de alcance, debe elegir como mínimo un sistema principal para cada subred que utiliza la máquina Dispatcher. Los sistemas principales pueden ser direccionadores, servidores IP u otros tipos de sistemas principales. La accesibilidad de sistemas principales se obtiene mediante el asesor de alcance que emite el mandato ping al sistema principal. La sustitución por anomalía tiene lugar si los mensajes de pulso no pueden transmitirse o si los criterios de accesibilidad los satisface mejor la máquina Dispatcher en espera que la máquina Dispatcher activa. Para tomar una decisión basándose en toda la información disponible, la máquina Dispatcher activa envía regularmente su capacidad de accesibilidad a la máquina Dispatcher en espera. Luego la máquina Dispatcher en espera compara esta capacidad con la suya y decide si debe conmutar el control.

Nota: Al configurar el destino de alcance, también debe iniciarse el *asesor de alcance*. El asesor de alcance se inicia automáticamente al iniciar la función de gestor. Si desea más información sobre el asesor de alcance, consulte la página 190.

Estrategia de recuperación

Hay configuradas dos máquinas Dispatcher: la máquina primaria y una segunda máquina denominada *de reserva*. Durante el arranque, la máquina primaria envía todos los datos de conexión a la máquina de reserva hasta que la máquina se sincroniza. La máquina primaria pasa a estar *activa*, es decir, empieza el equilibrio de carga. Mientras tanto, la máquina de reserva supervisa el estado de la máquina primaria y se dice que está en estado *en espera*.

Si en cualquier momento la máquina de reserva detecta que la máquina primaria ha sufrido una anomalía, *tomará el control* de las funciones de equilibrio de carga de la máquina primaria y pasará a ser la máquina activa. Cuando la máquina primaria vuelve a estar en funcionamiento, las máquinas responden de acuerdo con la *estrategia* de recuperación configurada por el usuario. Existen dos tipos de estrategia:

Automática

La máquina primaria reanuda el direccionamiento de paquetes tan pronto vuelve a estar en funcionamiento.

Manual

La máquina de reserva sigue direccionando paquetes incluso después de que la primaria pase a estar en funcionamiento. Para devolver la máquina primaria al estado activo y restablecer la máquina de reserva al estado en espera es necesario realizar una intervención manual.

El parámetro `strategy` debe tener el mismo valor en ambas máquinas.

Utilizando el mandato `takeover`, la estrategia de recuperación manual permite forzar el direccionamiento de paquetes a una máquina determinada. La recuperación manual es útil cuando el mantenimiento se lleva a cabo en la otra máquina. La estrategia de recuperación automática está diseñada para operaciones desatendidas normales.

Para una configuración de alta disponibilidad mutua, no se produce ninguna anomalía por clúster. Si hay algún problema en una máquina, incluso si sólo afecta a un clúster, la otra máquina tomará el control de los dos clústeres.

Nota: Durante las situaciones de toma de control, es posible que se pierdan algunas actualizaciones de conexiones. Esto puede causar que se terminen conexiones de larga ejecución existentes (como Telnet) a las que se está accediendo cuando se lleva a cabo la toma de control.

Utilización scripts

Para que Dispatcher dirija paquetes, cada dirección de clúster debe tener un alias asociado a un dispositivo de interfaz de red.

- En una configuración de Dispatcher autónomo, cada dirección de clúster debe tener un alias asociado a una tarjeta de interfaz de red (por ejemplo, `en0`, `tr0`).
- En una configuración de alta disponibilidad:
 - En la máquina activa, cada dirección de clúster debe tener un alias asociado a una tarjeta de interfaz de red (por ejemplo, `en0`, `tr0`).
 - En una máquina en espera, cada dirección de clúster debe tener un alias asociado a un dispositivo de bucle de retorno (por ejemplo, `lo0`) si se utiliza el método de reenvío MAC con servidores con ubicación compartida.
- En cualquier máquina en la que se haya detenido el ejecutor, deben eliminarse todos los alias para evitar que se produzcan conflictos con otra máquina que pueda estar iniciada.

Para obtener información sobre la creación de un alias para la tarjeta de interfaz de red, consulte “Paso 5. Crear un alias para la tarjeta de interfaz de red” en la página 69.

Puesto que las máquinas Dispatcher cambiarán su estado cuando se detecte una anomalía, los mandatos anteriores deben emitirse automáticamente. Para ello Dispatcher ejecutará scripts creados por el usuario. Los scripts de ejemplo se encuentran en el directorio `...ibm/edge/lb/servers/samples` y deben moverse al directorio `...ibm/edge/lb/servers/bin` para que funcionen. Los scripts se ejecutarán automáticamente sólo si `dsrserver` se está ejecutando.

Notas:

1. Para una configuración de alta disponibilidad mutua, Dispatcher invoca cada script “go” con un parámetro que identifique la dirección del Dispatcher

primario. El script debe consultar este parámetro y ejecutar los mandatos **executor configure** para dichas direcciones de clúster asociadas a dicho Dispatcher primario.

2. Para configurar la alta disponibilidad para el método de reenvío NAT de Dispatcher, debe añadir a los archivos de script las direcciones de retorno.

Se pueden utilizar los siguientes scripts de ejemplo:

goActive

El script goActive se ejecuta cuando un Dispatcher pasa a estado activo y empieza el direccionamiento de paquetes.

- Si ejecuta Dispatcher en una configuración de alta disponibilidad, debe crear este script. Este script suprime alias de bucle de retorno y añade alias de dispositivo.
- Si ejecuta Dispatcher en una configuración autónoma, no es necesario crear este script.

goStandby

El script goStandby se ejecuta cuando Dispatcher pasa al estado en espera y supervisa el estado de la máquina activa, pero sin direccionar ningún paquete.

- Si ejecuta Dispatcher en una configuración de alta disponibilidad, debe crear este script. Este script debe suprimir alias de dispositivo y añadir alias de bucle de retorno.
- Si ejecuta Dispatcher en una configuración autónoma, no es necesario crear este script.

goInOp

El script goInOp se ejecuta cuando se detiene un ejecutor de Dispatcher.

- Si suele ejecutar Dispatcher en una configuración de alta disponibilidad, debería crear este script. Este script suprime todos los alias de dispositivo y bucle de retorno.
- Si suele ejecutar Dispatcher en una configuración autónoma, este script es opcional. Puede crearlo y que suprima alias de dispositivos, o puede optar por suprimirlos manualmente.

goIdle El script goIdle se ejecuta cuando un Dispatcher pasa a estado desocupado y empieza el direccionamiento de paquetes. Esto ocurre cuando no se han añadido las características de alta disponibilidad, como en una configuración autónoma. También sucede en una configuración de alta disponibilidad antes de añadir las características de alta disponibilidad o después de eliminarlas.

- Si suele ejecutar Dispatcher en una configuración de alta disponibilidad, *no* debe crear este script.
- Si suele ejecutar Dispatcher en una configuración autónoma, este script es opcional. Puede crearlo y que añada alias de dispositivos, o puede optar por añadirlos manualmente. Si no crea este script para la configuración autónoma, tendrá que utilizar el mandato **dscontrol executor configure** o configurar manualmente los alias cada vez que se inicia el ejecutor.

highavailChange

El script highavailChange se ejecuta siempre que cambia el estado de alta disponibilidad dentro de Dispatcher, como ocurre cuando se llama a los scripts "go". El parámetro único pasado a este script es el nombre del script "go" que acaba de ejecutar Dispatcher. Cree este script para utilizar

información de cambio de estado, por ejemplo, para avisar a un administrador o para anotar el suceso.

En sistemas Windows: en la configuración, si dispone de Site Selector equilibrando la carga de dos máquinas Dispatcher que están funcionando en un entorno de alta disponibilidad, será necesario añadir un alias a la pila de Microsoft para los Metric Servers. Este alias debe añadirse al script goActive. Por ejemplo:

```
call netsh interface ip add address "Conexión de área local"  
addr=9.37.51.28 mask=255.255.240.0
```

En el caso de goStandby y goInOp, será necesario suprimir el alias: Por ejemplo:

```
call netsh interface ip delete address "Conexión de área local"  
addr=9.37.51.28
```

Si hay varias NIC en la máquina, compruebe primero qué interfaz debe utilizar emitiendo el siguiente mandato en el indicador de mandatos: netsh interface ip show address. Este mandato devolverá una lista de las interfaces configuradas actualmente y asignará un número a "Conexión de área local" (por ejemplo, "Conexión de área local 2") para que pueda determinar cuál debe utilizar.

En Linux para S/390: Dispatcher emite un ARP injustificado para poder mover direcciones IP desde un Dispatcher a otro. Este mecanismo está, por lo tanto, relacionado con el tipo de red implícito. Al ejecutar Linux para S/390, Dispatcher puede hacer tomas de control de alta disponibilidad de manera nativa (completa con movimientos de la dirección IP) sólo en aquellas interfaces que pueden emitir un ARP y configurar la dirección en la interfaz local. Este mecanismo no funcionará correctamente en interfaces punto a punto como, por ejemplo, IUCV y CTC, y no funcionará correctamente en algunas configuraciones de qeth/QDIO.

Para estas interfaces y configuraciones donde la función de toma de control de IP nativa del Dispatcher no funcionará correctamente, el cliente puede colocar mandatos adecuados en los scripts go para mover las direcciones de manera manual. De esta manera también se asegurará de que dichas topologías de red se puedan beneficiar de la alta disponibilidad.

Configurar la ubicación compartida y la alta disponibilidad (sistemas Windows)

Es posible configurar tanto la alta disponibilidad como la ubicación compartida en servidores Windows. Sin embargo, para configurar estas características de Load Balancer juntas en sistemas Windows son necesarios unos pasos adicionales.

En sistemas Windows, cuando se utiliza la ubicación compartida con la alta disponibilidad, necesitará una dirección IP adicional, una especie de dirección IP ficticia, que pueda añadirse al adaptador de bucle de retorno. Es necesario instalar el adaptador de bucle de reserva tanto en la máquina primaria como en la máquina de reserva. Para instalar el dispositivo de bucle de retorno en sistemas Windows, siga los pasos descritos en "Configuración de máquinas de servidor para el equilibrio de carga" en la página 72.

Cuando los pasos indiquen que añada la dirección IP de clúster al bucle de retorno, deberá añadir una dirección IP ficticia, no la dirección del clúster. Esto se debe a que los scripts go* de alta disponibilidad para sistemas Windows necesitan suprimir y añadir la dirección de clúster al dispositivo de bucle de retorno, en función de si la máquina de Load Balancer está activa o en espera.

Los sistemas Windows no permitirán que se elimine del dispositivo de bucle de retorno la última dirección IP configurada porque el dispositivo de bucle de retorno no funciona en modalidad DHCP. La dirección ficticia permite a Load Balancer eliminar en cualquier momento su dirección de clúster. La dirección IP ficticia no se utiliza para ningún tipo de tráfico y se puede utilizar tanto en la máquina activa como en la máquina de reserva.

Actualice y traslade los scripts go* de Load Balancer de la máquina activa y en espera y, a continuación, inicie Dispatcher. La dirección del clúster se añadirá y eliminará de la interfaz de red y del dispositivos de bucle de retorno en los momentos adecuados.

Configuración de equilibrio de carga basado en normas

Utilice el equilibrio de carga basado en normas para ajustar cuándo y por qué los paquetes se envían a qué servidores. Load Balancer examina todas las normas que se añaden, desde la primera prioridad a la última, se detiene en la primera norma que es cierta y luego equilibra la carga del contenido entre todos los servidores asociados a la norma. Ya se ha equilibrado la carga basada en el destino y el puerto, pero si se utilizan normas se amplía la capacidad de distribuir conexiones.

En la mayoría de los casos, al configurar normas se debe configurar una norma **siempre cierta** para poder detectar cualquier petición pasada por otras normas de prioridad más altas. Este valor por omisión puede ser la respuesta "Lo sentimos, el sitio está inactivo actualmente, inténtelo más adelante" cuando los demás servidores no pueden aceptar la petición de cliente.

Debe utilizar el equilibrio de carga basado en normas con Dispatcher y Site Selector cuando por alguna razón desea utilizar un subconjunto de servidores. Siempre *debe* utilizar normas para el componente CBR.

Puede elegir entre los siguientes tipos de normas:

- Para Dispatcher:
 - Dirección IP de cliente
 - Puerto cliente
 - Hora del día
 - Tipo de servicio (TOS)
 - Conexiones por segundo
 - Total de conexiones activas
 - Ancho de banda reservado
 - Ancho de banda compartido
 - Siempre cierta
 - Contenido de una petición
- Para CBR:
 - Dirección IP de cliente
 - Hora del día
 - Conexiones por segundo
 - Total de conexiones activas
 - Siempre cierta
 - Contenido de una petición

- Para Site Selector:
 - Dirección IP de cliente
 - Hora del día
 - Toda la métrica
 - Media de la métrica
 - Siempre cierta

Antes de empezar a añadir normas a la configuración, planifique la lógica que desea que sigan las normas.

¿Cómo se evalúan las normas?

Todas las normas tienen un nombre, un tipo, una prioridad y pueden tener un inicio del rango y un final del rango, junto con un conjunto de servidores. Además, la norma de tipo contenido para el componente CBR tiene asociado un patrón de expresión regular coincidente. (Si desea ver ejemplos y casos de cómo utilizar la norma de contenido y la sintaxis de patrón válida para la norma de contenido, consulte el Apéndice B, “Sintaxis de la norma de contenido (patrón)”, en la página 475).

Las normas se evalúan en orden de prioridad. Es decir, una norma con prioridad 1 (número más bajo) se evalúa antes que una norma con prioridad 2 (número más alto). Se utilizará la primera norma que se satisfaga. Una vez que se ha satisfecho una norma, no se evalúan más normas.

Para que una norma se satisfaga, debe cumplir dos condiciones:

1. El predicado de la norma debe ser verdadero. Es decir, el valor que está evaluando debe estar entre los rangos de inicio y fin, o el contenido debe coincidir con la expresión regular especificada en el patrón de la norma de contenido. Para las normas de tipo “true,” el predicado siempre se satisface, independientemente de los rangos de inicio y fin.
2. Si hay servidores asociados a esta norma, como mínimo debe haber uno con un peso mayor que 0 al que reenviar paquetes.

Si una norma no tiene asociado ningún servidor, sólo es necesario que la norma cumpla la condición uno para que se satisfaga. En este caso, Dispatcher descartará la petición de conexión, Site Selector devolverá la petición del servidor de nombres con un error, y CBR causará que Caching Proxy devuelva una página de error.

Si no se satisface ninguna norma, Dispatcher seleccionará un servidor del total de servidores disponibles en el puerto, Site Selector seleccionará un servidor del total de servidores disponibles en el nombre de sitio y CBR provocará que Caching Proxy devuelva una página de error.

Utilización de normas basadas en la dirección IP de cliente

Este tipo de norma está disponible en el componente Dispatcher, CBR o Site Selector.

Utilice normas basadas en la dirección IP de cliente si desea filtrar los clientes y asignar los recursos en función del lugar de donde proceden.

Por ejemplo, si observa que hay demasiado tráfico sin pagar en la red, y por lo tanto no deseado, que procede de un grupo específico de direcciones IP. Cree una norma utilizando el mandato **dscontrol rule**, por ejemplo:

```
dscontrol rule add 9.67.131.153:80:ni type ip
beginrange 9.0.0.0 endrange 9.255.255.255
```

Esta norma "ni" filtra cualquier conexión de clientes no deseados. A continuación, añada a la norma los servidores a los que se podrá acceder, o si no añade ningún servidor a la norma, los servidores no atenderán las peticiones que procedan de las direcciones 9.x.x.x.

Utilización de normas basadas en el puerto de cliente

Este tipo de norma sólo está disponible en el componente Dispatcher.

Utilice normas basadas en el puerto de cliente, si los clientes utilizan algún tipo de software que solicita un puerto específico de TCP/IP cuando realiza peticiones.

Por ejemplo, cree una norma que indique que todas las peticiones que tengan el puerto de cliente 10002 podrán utilizar un conjunto de servidores rápidos especiales porque sabe que todas las peticiones de cliente con dicho puerto proceden de un grupo selecto de clientes.

Utilización de normas basadas en la hora del día

Este tipo de norma está disponible en el componente Dispatcher, CBR o Site Selector.

Utilice normas basadas en la hora del día por razones de planificación de capacidad. Por ejemplo, si se accede al sitio Web mayormente durante el mismo grupo de horas cada día, puede dedicar cinco servidores adicionales durante el periodo de hora punta.

Otra razón por la que puede utilizar una norma basada en la hora del día es cuando desea apagar algunos de los servidores para realizar su mantenimiento cada día a medianoche, por lo que puede establecer una norma que excluya estos servidores durante el periodo de mantenimiento necesario.

Utilización de normas basadas en el tipo de servicio (TOS)

Este tipo de norma sólo está disponible en el componente Dispatcher.

Utilice normas basadas en el contenido del campo de "tipo de servicio" (TOS) en la cabecera IP. Por ejemplo, si una petición de cliente llega con un valor TOS que indica servicio normal, puede direccionarse a un conjunto de servidores. Si una petición de cliente diferente llega con un valor de TOS distinto que indica una prioridad de servicio más alta, puede direccionarse a un grupo de servidores distinto.

La norma TOS permite configurar completamente cada bit del byte TOS utilizando el mandato **dscontrol rule**. Para bits significativos que desee hacer coincidir en el byte TOS, utilice 0 o 1. Si no, utilice el valor x. A continuación se muestra un ejemplo de adición de una norma TOS:

```
dscontrol rule add 9.67.131.153:80:tsr type service tos 0xx1010x
```

Utilización de normas basadas en las conexiones por segundo

Este tipo de norma está disponible en los componentes Dispatcher y CBR.

Nota: El gestor debe estar en ejecución para que lo siguiente funcione.

Utilice normas basadas en conexiones por segundo si necesita compartir algunos de los servidores con otras aplicaciones. Por ejemplo, puede establecer dos normas:

1. Si el número de conexiones por segundo en el puerto 80 oscila entre 0 y 2000, utilice estos 2 servidores
2. Si el número de conexiones por segundo en el puerto 80 es superior a 2000, utilice estos 10 servidores

O, puede utilizar Telnet y reservar dos de los cinco servidores para Telnet, excepto cuando las conexiones por segundo superen un determinado nivel. De esta forma, Dispatcher equilibrará la carga en todos los cinco servidores durante las horas punta.

Si establece la opción de evaluación de normas "upserversonrule" junto con la norma de tipo "conexión": cuando se utiliza la norma de tipo conexión y se establece la opción **upserversonrule**, si algunos de los servidores del conjunto de servidores están inactivos, puede garantizar que no se sobrecargarán los servidores restantes. Consulte el apartado "Opción de evaluación del servidor para normas" en la página 220 para obtener más información.

Utilización de normas basadas en el total de conexiones activas

Este tipo de norma está disponible en el componente Dispatcher o CBR.

Nota: El gestor debe estar en ejecución para que lo siguiente funcione.

Utilice normas basadas en el total de conexiones activas en un puerto si los servidores se sobrecargan y empiezan a descartar paquetes. Determinados servidores Web seguirán aceptando conexiones incluso cuando no tengan suficientes hebras para responder a la petición. Como resultado, las peticiones de cliente excederán el tiempo de espera y no se atenderá al cliente procedente del sitio Web. Utilice normas basadas en conexiones activas para equilibrar la capacidad dentro de una agrupación de servidores.

Por ejemplo, sabe por experiencia que los servidores dejarán de dar servicio una vez que han aceptado 250 conexiones. Cree una norma utilizando el mandato **dscontrol rule** o el mandato **cbrcontrol rule**, por ejemplo:

```
dscontrol rule add 130.40.52.153:80:pool2 type active
beginrange 250 endrange 500
```

o

```
cbrcontrol rule add 130.40.52.153:80:pool2 type active
beginrange 250 endrange 500
```

A continuación, añada a la norma los servidores actuales y a algunos servidores adicionales, que si no se utilizarán para otro proceso.

Utilización de normas basadas en ancho de banda reservado y ancho de banda compartido

Las normas de ancho de banda reservado y ancho de banda compartido sólo están disponibles en el componente Dispatcher.

Para las normas de ancho de banda, Dispatcher calcula el ancho de banda como la velocidad a la que un conjunto de servidores entregan los datos a los clientes. Dispatcher realiza un seguimiento de la capacidad en los niveles de servidor, norma, puerto, clúster y ejecutor. Para cada uno de estos niveles, hay un campo de contador de bytes: kilobytes transferidos por segundo. Dispatcher calcula estas velocidades a un intervalo de 60 segundos. Puede ver estas velocidades en la GUI o en la salida de un informe de línea de mandatos.

Norma de ancho de banda reservado

La norma de ancho de banda reservado permite controlar el número de kilobytes por segundos que entregan un conjunto de servidores. Si se establece un umbral (asignando un rango de ancho de banda específico) para cada conjunto de servidores en toda la configuración, puede controlar y garantizar la cantidad de ancho de banda que utiliza cada combinación de clúster-puerto.

A continuación se muestra un ejemplo de adición de una norma de ancho de banda reservado:

```
dscontrol rule add 9.67.131.153:80:rbw type reservedbandwidth  
beginrange 0 endrange 300
```

El inicio del rango y el final del rango se especifican en kilobytes por segundo.

Norma de ancho de banda compartido

Antes de configurar la norma de ancho de banda compartido, debe especificar la cantidad máxima de ancho de banda (kilobytes por segundo) que puede compartirse en el nivel de ejecutor o clúster utilizando el mandato **dscontrol executor** o **dscontrol cluster** con la opción `sharedbandwidth`. El valor de `sharedbandwidth` no debe exceder el ancho de banda total (capacidad total de la red) disponible. Si se utiliza el mandato **dscontrol** para establecer el ancho de banda compartido sólo se proporciona un límite superior para la norma.

A continuación se muestran ejemplos de la sintaxis de mandato:

```
dscontrol executor set sharedbandwidth tamaño  
dscontrol cluster [add | set] 9.12.32.9 sharedbandwidth tamaño
```

El *tamaño* para `sharedbandwidth` es un valor entero (kilobytes por segundo). El valor por omisión es cero. Si el valor es cero, el ancho de banda no puede compartirse.

El ancho de banda compartido en el nivel de clúster permite que el clúster utilice el máximo ancho de banda especificado. Mientras el ancho de banda utilizado por el clúster esté por debajo de la cantidad especificada, esta norma se evaluará como `true`. Si el ancho de banda total utilizado es superior a la cantidad especificada, esta norma se evaluará como `false`.

Si se comparte el ancho de banda en el nivel de ejecutor, se permitirá que toda la configuración de Dispatcher comparta una cantidad máxima de ancho de banda. Mientras el ancho de banda utilizado en el nivel de ejecutor esté por debajo de la cantidad especificada, esta norma se evaluará como `true`. Si el ancho de banda total utilizado es superior al definido, esta norma se evaluará como `false`.

A continuación se muestran ejemplos de la adición o definición de una norma de ancho de banda compartido:

```
dscontrol rule add 9.20.30.4:80:shbw type sharedbandwidth sharelevel valor  
dscontrol rule set 9.20.34.11:80:shrule sharelevel valor
```

El *valor* para sharelevel es executor o cluster. Sharelevel es un parámetro necesario en la norma de ancho de banda compartido.

Utilización de normas de ancho de banda reservado y compartido

Dispatcher permite asignar un ancho de banda específico a conjuntos de servidores dentro de la configuración mediante la norma de *ancho de banda reservado*. Si especifica un inicio y un final del rango puede controlar el rango de kilobytes entregados por un conjunto de servidores a los clientes. Cuando la norma ya no se evalúa como true (se excede el final del rango), se evaluará la norma con prioridad más baja siguiente. Si la norma de prioridad más baja siguiente es una norma "siempre cierta", se podría seleccionar un servidor para responder al cliente con una respuesta de "sitio ocupado".

Por ejemplo, suponga un grupo de tres servidores en el puerto 2222. Si el ancho de banda reservado se establece en 300, la cantidad máxima de kbytes por segundo es de 300, en un periodo de 60 segundos. Cuando esta velocidad se excede, la norma ya no se evaluará como true. Si ésta fuera la única norma, Dispatcher seleccionaría uno de los tres servidores para manejar la petición. Si hubiera una norma "siempre cierta" con prioridad más baja, la petición podría dirigirse a otro servidor y responderse con "sitio ocupado".

La norma de ancho de banda compartido puede proporcionar a los clientes acceso a servidores adicionales. En concreto, cuando se utiliza como una norma de prioridad más baja después de una norma de ancho de banda reservado, un cliente seguirá pudiendo acceder a un servidor incluso si se ha excedido el ancho de banda reservado.

Por ejemplo, si utiliza una norma de ancho de banda compartido después de una norma de ancho de banda reservado, puede permitir a los clientes que accedan a los tres servidores de una forma controlada. Mientras haya un ancho de banda compartido para utilizarse, la norma se evaluará como true y se otorgará el acceso. Si no hay ningún ancho de banda compartido disponible, la norma no es true y se evalúa la norma siguiente. Si a continuación hay una norma "siempre cierta", la petición puede redirigirse según sea necesario.

Si utiliza el ancho de banda reservado y compartido tal como se describe en el ejemplo anterior, se podrá ejercer una mayor flexibilidad al otorgar (o denegar) acceso a los servidores. Los servidores de un puerto específico pueden limitarse al uso de un ancho de banda, mientras que otros pueden utilizar un ancho de banda adicional mientras esté disponible.

Nota: Dispatcher realiza un seguimiento del ancho de banda midiendo el tráfico del cliente, como "acks" de datos, que circulan hacia un servidor. Si por alguna razón Dispatcher no detecta este tráfico, al utilizar las normas de ancho de banda los resultados son imprevisibles.

Norma de toda la métrica

Este tipo de norma sólo está disponible en el componente Site Selector.

Para la norma de toda la métrica, elija una métrica del sistema (cpuload, memload, o su propio script de métrica de sistema personalizado) y el Site Selector compara el valor de métrica del sistema (devuelto por el agente de Metric Server que reside en cada servidor con equilibrio de carga) con el inicio y el final del rango que se especifica en la norma. El valor de métrica del sistema actual para todos los servidores del conjunto de servidores debe estar dentro del rango para que se active la norma.

Nota: El script de métrica de sistema elegido debe estar en cada uno de los servidores con equilibrio de carga.

A continuación se muestra un ejemplo de adición a la configuración de una norma de toda la métrica:

```
sscontrol rule add dnsload.com:allrule1 type metricall  
metricname cpuload beginrange 0 endrange 100
```

Norma de media de la métrica

Este tipo de norma sólo está disponible en el componente Site Selector.

Para la norma de media de la métrica, elija una métrica del sistema (cpuload, memload, o su propio script de métrica de sistema personalizado) y el Site Selector compara el valor de métrica del sistema (devuelto por el agente de Metric Server que reside en cada servidor con equilibrio de carga) con el inicio y el final del rango que se especifica en la norma. La *media* de los valores de métrica del sistema actuales para todos los servidores del conjunto de servidores debe estar dentro del rango para que se active la norma.

Nota: El script de métrica de sistema elegido debe estar en cada uno de los servidores con equilibrio de carga.

A continuación se muestra un ejemplo de adición a la configuración de una norma de media de la métrica:

```
sscontrol rule add dnsload.com:avgrule1 type metricavg  
metricname cpuload beginrange 0 endrange 100
```

Utilización de normas que son siempre ciertas

Este tipo de norma está disponible en el componente Dispatcher, CBR o Site Selector.

Puede crearse una norma que sea “siempre cierta.” Dicha norma siempre estará seleccionada, a menos que los servidores asociados estén inactivos. Por esta razón, habitualmente debe tener una prioridad más baja que las otras normas.

También puede tener varias normas “siempre cierta”, con un conjunto de servidores asociado a cada una de ellas. Se selecciona la primera norma true que tenga un servidor disponible. Por ejemplo, suponga que tiene seis servidores. Desea que dos de ellos controlen el tráfico en todas las circunstancias, a menos los dos estén inactivos. Si los dos primeros servidores están inactivos, se recomienda disponer de un segundo conjunto de servidores que controle el tráfico. Si los cuatro servidores están inactivos, se utilizarán los dos últimos servidores para manejar el tráfico. Puede establecer hasta tres normas “siempre cierta”. Así pues siempre se seleccionará el primer conjunto de servidores siempre y cuando haya uno activo como mínimo. Si los dos están inactivos, se optará por uno del segundo conjunto y así sucesivamente.

Otro ejemplo sería si deseara una norma “siempre cierta” para asegurarse de que no se atenderá a los clientes entrantes si estos no coinciden con ninguna de las normas establecidas. Puede crear una norma utilizando el mandato **dscontrol rule** como la siguiente:

```
dscontrol rule add 130.40.52.153:80:jamais type true priority 100
```

Entonces no añadiría ningún servidor a la norma, lo que provocaría que los paquetes de clientes se dejaran sin respuesta.

Nota: Al crear una norma siempre cierta no es necesario establecer un inicio de rango ni un final de rango.

Puede definir más de una norma “siempre cierta” y, a partir de ahí, ajustar cuál se ejecuta cambiando los niveles de prioridad.

Utilización de normas basadas en el contenido de peticiones

Este tipo de norma está disponible en el componente CBR o el componente Dispatcher (cuando se utiliza el método de reenvío CBR de Dispatcher).

Se recomienda utilizar normas de tipo de contenido para enviar peticiones a conjuntos de servidores establecidos específicamente para manejar algún subconjunto del tráfico del sitio. Por ejemplo, si desea utilizar un conjunto de servidores para manejar todas las peticiones *cgi-bin*, otro conjunto para manejar todas las peticiones de audio de modalidad continua y un tercer conjunto para manejar las demás peticiones. Añada una norma con un patrón que coincida con la vía de acceso al directorio *cgi-bin*, otra que coincida con el tipo de archivo de los archivos de audio de modalidad continua y una tercera norma siempre cierta para manejar el resto del tráfico. A continuación, añada los servidores adecuados a cada una de las normas.

Importante: si desea ver ejemplos y casos de cómo utilizar la norma de contenido y la sintaxis de patrón válida para la norma de contenido, consulte el Apéndice B, “Sintaxis de la norma de contenido (patrón)”, en la página 475.

Alteración temporal de la afinidad entre puertos

Con la alteración temporal de afinidad entre puertos, puede alterar temporalmente la permanencia en memoria de un puerto para un servidor específico. Por ejemplo, si utiliza una norma para limitar la cantidad de conexiones para cada servidor de aplicaciones y tiene un servidor de desbordamiento con una norma siempre cierta que indica “por favor, inténtelo más adelante” para dicha aplicación. El puerto tiene un valor de permanencia en memoria de 25 minutos, por lo tanto no desea que el cliente sea permanente en memoria para dicho servidor. Con la alteración temporal de afinidad entre puertos, puede cambiar el servidor de desbordamiento para alterar temporalmente la afinidad que normalmente está asociada a dicho puerto. La próxima vez que el cliente emite una petición al clúster, se equilibra su carga con el mejor servidor de aplicaciones disponible, no el servidor de desbordamiento.

Consulte el apartado “dscontrol server — configurar servidores” en la página 392, para obtener información detallada sobre la sintaxis del mandato de alteración temporal de afinidad entre puertos, utilizando la opción **sticky** del servidor .

Adición de normas a la configuración

Para añadir normas mediante el mandato **dscontrol rule add**, edite el archivo de configuración de ejemplo o utilice la interfaz gráfica de usuario (GUI). Puede añadir una o más normas a cada puerto definido.

Es un proceso de dos pasos: añadir la norma y definir qué servidores la atenderán si la norma es cierta. Por ejemplo, el administrador del sistema desea realizar un seguimiento del uso de los servidores proxy que realiza cada una de las secciones del sitio. Se han otorgado direcciones IP a cada sección. Cree el primer conjunto de normas basándose en la dirección IP de cliente para separar la carga de cada sección:

```
dscontrol rule add 130.40.52.153:80:div1 type ip b 9.1.0.0 e 9.1.255.255
dscontrol rule add 130.40.52.153:80:div2 type ip b 9.2.0.0 e 9.2.255.255
dscontrol rule add 130.40.52.153:80:div3 type ip b 9.3.0.0 e 9.3.255.255
```

A continuación, añada un servidor distinto para cada norma y mida la carga en cada uno de los servidores para poder facturar correctamente a la sección por los servicios que está utilizando. Por ejemplo:

```
dscontrol rule useserver 130.40.52.153:80:div1 207.72.33.45
dscontrol rule useserver 130.40.52.153:80:div2 207.72.33.63
dscontrol rule useserver 130.40.52.153:80:div3 207.72.33.47
```

Opción de evaluación del servidor para normas

La opción de evaluación del servidor sólo está disponible en el componente Dispatcher.

En el mandato **dscontrol rule** hay una opción de evaluación del servidor para normas. Utilice la opción *evaluate* para optar por evaluar la condición de la norma en todos los servidores del puerto o evaluar la condición de la norma sólo en los servidores incluidos en la norma. (En versiones anteriores de Load Balancer, sólo se podía medir la condición de cada norma en todos los servidores del puerto).

Notas:

1. La opción de evaluación del servidor sólo es válida para las normas que toman las decisiones basándose en las características de los servidores: norma de total de conexiones (por segundo), norma de conexiones activas y norma de ancho de banda reservado.
2. La norma de tipo "conexión" tiene una opción de evaluación adicional que puede elegir, **upserversonrule**. Consulte el apartado "Utilización de normas basadas en las conexiones por segundo" en la página 215 para obtener más información.

A continuación se muestran ejemplos de la adición o definición de la opción de evaluación en una norma de ancho de banda reservado:

```
dscontrol rule add 9.22.21.3:80:rbweval type reservedbandwidth evaluate nivel
dscontrol rule set 9.22.21.3:80:rbweval evaluate nivel
```

El *nivel* de la evaluación puede establecerse en port, rule o upserversonrule. El valor por omisión es port.

Evaluar servidores a los que se aplica la norma

La opción de medir la condición de la norma en todos los servidores a los que se aplica le permite configurar dos normas con las siguientes características:

- La primera norma que se evalúa contiene todos los servidores que mantienen el contenido del sitio Web y la opción de evaluación se establece en *rule* (evaluar la condición de la norma en todos los servidores a los que se aplica la norma).
- La segunda norma es una norma siempre cierta que contiene un solo servidor que responde con una respuesta de tipo “sitio ocupado”.

El resultado es que cuando el tráfico excede el umbral de los servidores a los que se aplica la primera norma, el tráfico se envía al servidor “sitio ocupado” al que se aplica la segunda norma. Cuando el tráfico es inferior al umbral de los servidores a los que se aplica la primera norma, el nuevo tráfico vuelve a dirigirse otra vez a los servidores a los que se aplica la primera norma.

Evaluar servidores en el puerto

Si utiliza las dos normas del ejemplo anterior, si establece la opción de evaluación en *port* para la primera norma (evaluar condición de la norma en todos los servidores del puerto), cuando el tráfico excede el umbral de dicha norma, se envía al servidor “sitio ocupado” asociado a la segunda norma.

La primera norma mide todo el tráfico del servidor (incluido el servidor “sitio ocupado”) en el puerto para determinar si el tráfico excede el umbral. Cuando la congestión disminuye en todos los servidores asociados a la primera norma, puede producirse un resultado involuntario en el que el tráfico sigue dirigiéndose al servidor “sitio ocupado” porque el tráfico en el puerto todavía supera el umbral de la primera norma.

Cómo funciona la característica de afinidad para Load Balancer

Para los componentes Dispatcher y CBR: habilite la característica de afinidad cuando configure un puerto de clúster para que sea permanente en memoria. Si configura el puerto de un clúster de modo que sea permanente en memoria, permite que las peticiones de cliente subsiguientes se direccionen al mismo servidor. Esto se lleva a cabo estableciendo **stickytime** en el nivel de ejecutor, clúster o puerto en algunos segundos. Esta característica se inhabilita estableciendo el tiempo de permanencia en memoria (stickytime) en el valor cero.

Si está habilitando la afinidad entre puertos, los valores de tiempo de permanencia en memoria (stickytime) de los puertos compartidos deben ser valores iguales (no cero). Consulte el apartado “Afinidad entre puertos” en la página 222 para obtener más información.

Para el componente Site Selector: habilite la característica de afinidad cuando configure un nombre de sitio para que sea permanente en memoria. Si configura un nombre de sitio para que sea permanente en memoria, el cliente podrá utilizar el mismo servidor para varias peticiones del servicio de nombres. Esto se lleva a cabo estableciendo **stickytime** del nombre del sitio en algunos segundos. Esta característica se inhabilita estableciendo el tiempo de permanencia en memoria (stickytime) en el valor cero.

El período de permanencia en memoria es el intervalo entre el cierre de una conexión y la apertura de una conexión nueva, durante el cual un cliente se volverá a enviar al mismo servidor utilizado durante la primera conexión. Cuando caduca el tiempo de permanencia en memoria, el cliente puede enviarse a un servidor distinto del primero. El valor de tiempo de permanencia en memoria para un servidor se configura mediante los mandatos *dscontrol*, *executor*, *port* o *cluster*. Cuando se utiliza un mandato *server down* (*dscontrol server down*) para poner un servidor fuera de línea, si el valor de tiempo de permanencia en memoria (stickytime)

no es cero para dicho servidor, ese servidor seguirá atendiendo los clientes existentes hasta que caduque el tiempo de permanencia en memoria. El servidor pasará a estar inactivo una vez que caduque el valor de tiempo de permanencia en memoria (sticky).

Comportamiento cuando la afinidad está inhabilitada

Cuando la característica de afinidad se inhabilita, siempre que se recibe una nueva conexión TCP de un cliente, Load Balancer elige el servidor más adecuado para dicho momento y le remite los paquetes. Si llega una conexión subsiguiente procedente del mismo cliente, Load Balancer la trata como si fuera una nueva conexión no relacionada y vuelve a elegir el servidor más apropiado para dicho momento.

Comportamiento cuando la afinidad está habilitada

Con la característica de afinidad habilitada, si se recibe una petición subsiguiente del mismo cliente, la petición se dirige al mismo servidor.

Con el tiempo, el cliente terminará el envío de transacciones y el registro de afinidad desaparecerá. De ahí el significado de "tiempo de permanencia en memoria." Cada registro de afinidad existe durante el "tiempo de permanencia en memoria" en segundos. Cuando se reciben conexiones subsiguientes dentro del tiempo de permanencia en memoria, el registro de afinidad seguirá siendo válido y la petición se dirigirá al mismo servidor. Si no se recibe una conexión subsiguiente dentro del tiempo de permanencia en memoria, el registro se depura; una conexión que se recibe después de dicho tiempo tendrá un nuevo servidor seleccionado para la misma.

El mandato `server down (dscontrol server down)` se utiliza para poner un servidor fuera de línea. El servidor pasará a estar inactivo una vez que caduque el valor de tiempo de permanencia en memoria (stickytime).

Afinidad entre puertos

La afinidad entre puertos sólo se aplica a los métodos de reenvío MAC y NAT/NATP del componente Dispatcher.

La afinidad entre puertos es la característica de permanencia en memoria que se ha ampliado para cubrir varios puertos. Por ejemplo, si una petición de cliente se recibe primero en un puerto y la siguiente se recibe en otro puerto, la afinidad entre puertos permite a Dispatcher enviar la petición de cliente al mismo servidor. Para utilizar esta característica, los puertos deben:

- compartir la misma dirección de clúster
- compartir los mismos servidores
- tener el mismo valor de permanencia en memoria (**stickytime**) no cero valor
- tener el mismo valor de máscara de permanencia en memoria (**stickymask**) valor

Más de un puerto puede enlazar con el mismo **crossport**. Cuando llegan conexiones subsiguientes del mismo cliente al mismo puerto o a un puerto compartido, se accederá al mismo servidor. A continuación se muestra un ejemplo de cómo configurar varios puertos con una afinidad entre puertos para el puerto 10:

```
dscontrol port set clúster:20 crossport 10
dscontrol port set clúster:30 crossport 10
dscontrol port set clúster:40 crossport 10
```

Una vez que se ha establecido la afinidad entre puertos, tiene la flexibilidad de modificar el valor de tiempo de permanencia en memoria para el puerto. No obstante, se recomienda cambiar los valores de tiempo de permanencia en memoria para todos los puertos compartidos por el mismo valor; de lo contrario, pueden producirse resultados inesperados.

Para eliminar la afinidad entre puertos, establezca el valor de `crossport` de nuevo en el número de su propio puerto. Consulte el apartado “`dscontrol port` — configurar puertos” en la página 380, para obtener información detallada sobre la sintaxis de mandato para la opción **crossport**.

Máscara de dirección de afinidad (**stickymask**)

La máscara de dirección de afinidad sólo se aplica al componente Dispatcher.

La máscara de dirección de afinidad es una mejora de la característica de permanencia en memoria para agrupar clientes basándose en las direcciones de subred comunes. Si especifica **stickymask** en el mandato **dscontrol port** se podrán ocultar los bits de orden superior comunes de la dirección IP de 32 bits. Si se configura esta característica, la primera vez que una petición de cliente realiza una conexión con el puerto, todas las peticiones subsiguientes procedentes de clientes con la misma dirección de subred (representada por la parte de la dirección que está enmascarada) se dirigirán al mismo servidor.

Nota: Para poder habilitar **stickymask**, el valor **stickytime** debe ser un valor no cero.

Por ejemplo, si desea que todas las peticiones de clientes entrantes con la misma dirección de Clase A de red se dirijan al mismo servidor, establezca el valor de **stickymask** en 8 (bits) para el puerto. Para agrupar peticiones de clientes con la misma dirección de Clase B de red, establezca el valor de **stickymask** en 16 (bits). Para agrupar peticiones de clientes con la misma dirección de Clase C de red, establezca el valor de **stickymask** en 24 (bits).

Para obtener los mejores resultados, establezca el valor **stickymask** la primera vez que inicie Load Balancer. Si cambia el valor de **stickymask** de forma dinámica, los resultados pueden ser imprevisibles.

Interacción con afinidad entre puertos: si está habilitando la afinidad entre puertos, los valores de **stickymask** de los puertos compartidos deben ser los mismos. Consulte el apartado “Afinidad entre puertos” en la página 222 para obtener más información.

Para habilitar la máscara de dirección de afinidad, emita un mandato **dscontrol port** parecido al siguiente:

```
dscontrol port set clúster:puerto stickytime 10 stickymask 8
```

Los posibles valores de **stickymask** son 8, 16, 24 y 32. El valor 8 especifica los 8 primeros bits de orden superior de la dirección IP (dirección de Clase A de red) se ocultará. El valor 16 especifica los 16 primeros bits de orden superior de la dirección IP (dirección de Clase B de red) se ocultará. El valor 24 especifica los 24 primeros bits de orden superior de la dirección IP (dirección de Clase C de red) se ocultará. Si especifica el valor 32, está ocultando toda la dirección IP que inhabilita de hecho la característica de máscara de dirección de afinidad. El valor por omisión de **stickymask** es 32.

Consulte el apartado “dscontrol port — configurar puertos” en la página 380, para obtener información detallada sobre la sintaxis de mandato para stickymask (característica de máscara de dirección de afinidad).

Desactivar temporalmente el manejo de conexiones de servidor

Desactivar temporalmente el manejo se aplica a Dispatcher y componentes CBR.

Para eliminar un servidor de la configuración de Load Balancer por cualquier razón (actualizaciones, ampliaciones, servicio, etc.), puede utilizar el mandato **dscontrol manager quiesce**. El submandato quiesce permite que las conexiones existentes finalicen (sin ser atendidas) y sólo remite las nuevas conexiones posteriores del cliente al servidor desactivado temporalmente si la conexión se ha designado como de permanencia en memoria y el tiempo de permanencia en memoria no ha caducado. El submandato quiesce no deja que se realicen otras conexiones nuevas al servidor.

Desactivar temporalmente el manejo de conexiones de permanencia en memoria

Utilice la opción quiesce “now” si ha fijado el tiempo de permanencia en memoria y desea enviar nuevas conexiones a otro servidor (en lugar de enviarlas al servidor desactivado temporalmente) antes de que caduque el tiempo de espera. A continuación se muestra un ejemplo de utilización de la opción now para desactivar temporalmente el servidor 9.40.25.67:

```
dscontrol manager quiesce 9.40.25.67 now
```

La opción now determina cómo se manejarán las conexiones de permanencia en memoria:

- Si *no* se especifica “now,” se dejará que terminen las conexiones existentes y las nuevas conexiones posteriores se remitirán al servidor desactivado temporalmente desde aquellos clientes con conexiones existentes que se han diseñado como de permanencia en memoria, siempre y cuando el servidor desactivado temporalmente reciba la nueva petición antes de que caduque el tiempo de espera. (No obstante, si no ha habilitado la característica de permanencia en memoria (afinidad), el servidor desactivado temporalmente no puede recibir más conexiones nuevas).

Esta es la forma progresiva y menos brusca de desactivar temporalmente los servidores. Por ejemplo, puede desactivar temporalmente un servidor de forma progresiva y luego esperar el momento en el que haya la mínima cantidad de tráfico (quizás de madrugada) para eliminar completamente el servidor de la configuración.

- Si se especifica “now,” se desactiva temporalmente el servidor de forma que permite que se completen las conexiones existentes aunque rechaza que se establezcan nuevas conexiones, incluidas las nuevas conexiones posteriores de aquellos clientes con conexiones existentes que se han diseñado como de permanencia en memoria. Esta es la forma más brusca de desactivar temporalmente los servidores, que era la única forma de gestionarse en versiones anteriores del Load Balancer.

Opción de afinidad de la norma basada en el contenido de la petición de cliente

Puede especificar los siguientes tipos de afinidad en el mandato **dscontrol rule**:

- **Cookie activo:** habilita el equilibrio de carga del tráfico Web con afinidad para el mismo servidor basándose en los cookies generados por Load Balancer.
La afinidad de cookies activos sólo se aplica al componente CBR.
- **Cookie pasivo:** habilita el equilibrio de carga del tráfico Web con afinidad para el mismo servidor basándose en los cookies que se identifican a sí mismos generados por los servidores. Junto con la afinidad de cookies pasivos, también debe especificar el parámetro cookienam en el mandato rule.
Cookie pasivo se aplica al componente CBR y al método de reenvío CBR del componente Dispatcher.
- **URI:** habilita el equilibrio de carga en el tráfico Web para los servidores Caching Proxy de forma que aumente de manera eficaz la capacidad de la antememoria.
La afinidad de URL se aplica al componente CBR y al método de reenvío CBR del componente Dispatcher.

El valor por omisión para la opción affinity es "none." La opción **stickytime** en el mandato port debe ser cero (no habilitado) para poder establecer la opción **affinity** en el mandato rule para el cookie activo, cookie pasivo o URI. Cuando se establece la función de afinidad en la norma, no se puede habilitar el tiempo de permanencia en memoria en el puerto.

Afinidad de cookies activos

El función de afinidad de cookies activos sólo se aplica al componente CBR.

Proporciona una forma para hacer que los clientes sean "permanentes" para un servidor particular. Esta función se habilita estableciendo la opción **stickytime** de una norma en un número positivo y estableciendo la opción affinity en "activecookie." Esto puede llevarse a cabo cuando se añade la norma o se utiliza el mandato rule set. Consulte el apartado "dscontrol rule — configurar normas" en la página 386 para obtener información detallada sobre la sintaxis del mandato.

Cuando se habilita una norma para la afinidad de cookies activos, se equilibra la carga de nuevas peticiones de clientes utilizando algoritmos CBR estándar, mientras que las peticiones sucesivas del mismo cliente se envían al servidor elegido al principio. El servidor elegido se almacena en forma de cookie en la respuesta al cliente. Siempre y cuando las peticiones futuras del cliente contengan el cookie y lleguen dentro del intervalo de permanencia en memoria, el cliente mantendrá afinidad con el servidor inicial.

La afinidad de cookies activos se utiliza para asegurar que un cliente siga realizando el equilibrio de carga en el mismo servidor durante un periodo de tiempo. Esto se lleva a cabo enviando un cookie para que se almacene en el navegador de los clientes. El cookie contiene los valores `clúster:puerto:norma` que se utilizaron para tomar una decisión, el servidor en el que se realizó el equilibrio de carga y una indicación de la hora del tiempo de espera excedido para cuando la afinidad ya no es válida. El cookie tiene el siguiente formato:

IBMCBR=clúster:puerto:norma+servidor-hora! La información `clúster:puerto:norma` y `servidor` está codificada para que no muestre la configuración de CBR.

Cómo funciona la afinidad de cookies activos

Siempre que una norma indique que tiene activada la afinidad de cookies activos, se examinará el cookie enviado por el cliente.

- Si se encuentra un cookie que contenga el identificador para el clúster:puerto:norma que provocó la activación, se extraerán del cookie el servidor sobre el que se ha realizado el equilibrio de carga y la indicación de la hora de caducidad.
- Si el servidor sigue en el conjunto utilizado por la norma y su peso es positivo o es un servidor desactivado temporalmente, y la indicación de la hora de caducidad es posterior a ahora, se opta por realizar el equilibrio de carga sobre el servidor del cookie.
- Si no se cumple alguna de las condiciones especificadas en el punto anterior, se selecciona un servidor mediante el algoritmo normal.
- Una vez que se ha seleccionado un servidor (utilizando cualquiera de los dos métodos), se crea un nuevo cookie que contiene la información IBMCBR, clúster:puerto:norma, servidor_seleccionado y una indicación de la hora. La indicación de la hora es la hora en que caduca la afinidad. La información de “clúster:puerto:norma y servidor_seleccionado” está codificada para que no muestre la configuración de CBR.
- También se inserta en el cookie un parámetro “expires”. Este parámetro está en un formato que el navegador puede entender y hace que el cookie pase a ser no válido siete días después de la indicación de la hora de caducidad. De esta forma la base de datos de cookies del cliente no se llena demasiado.

Este nuevo cookie se insertará en las cabecera que se devuelven al cliente, y si el navegador del cliente se configura de forma que acepte cookies, devolverá peticiones subsiguientes.

Cada instancia de afinidad del cookie tiene una longitud de 65 bytes y termina con un signo de exclamación. Como resultado, un cookie de 4096 bytes puede mantener aproximadamente 60 normas de cookies activos individuales por dominio. Si el cookie se rellena completamente, se depuran todas las instancias de afinidad caducadas. Si todas las instancias siguen siendo válidas, se elimina la más antigua y se añaden las nuevas instancias para la norma actual.

Nota: CBR sustituirá todas las apariciones de los cookies de IBMCBR con el formato antiguo a medida que aparezcan en el proxy.

La opción affinity de cookies activos, para el mandato rule, sólo puede establecerse en activecookie si la opción port stickytime es cero (no habilitada). Una vez que la afinidad de cookies activos está activa en una norma, no se puede habilitar el tiempo de permanencia en memoria en el puerto.

Cómo habilitar la afinidad de cookies activos

Para habilitar la afinidad de cookies activos para una norma concreta, utilice el mandato rule set:

```
rule set clúster:puerto:norma stickytime 60
rule set clúster:puerto:norma affinity activecookie
```

Por qué se utiliza la afinidad de cookies activos

Hacer que una norma sea permanente en memoria normalmente se utiliza para CGI o servlets que almacenan estado de cliente en el servidor. El estado lo identifica un ID de cookie (estos son cookies de servidor). El estado del cliente sólo está en el servidor seleccionado, de modo que el cliente necesita el cookie de dicho servidor para mantener dicho estado entre peticiones.

Alteración temporal de la hora de caducidad de la afinidad de cookies activos

La afinidad de cookies activos tiene una hora de caducidad del servidor actual por omisión, más el intervalo de tiempo de permanencia en memoria, más veinticuatro horas. Si las horas de los sistemas clientes (aquellos que envían peticiones a la máquina CBR) son incorrectas (por ejemplo, van un día por delante de la hora del servidor), los sistemas de estos clientes ignorarán los cookies de CBR porque el sistema dará por supuesto que los cookies ya han caducado. Para fijar una hora de caducidad posterior, modifique el script `cbrserver`. En el archivo script, edite la línea `javaw` añadiendo el siguiente parámetro después de `LB_SERVER_KEYS`: `-DCOOKIEEXPIREINTERVAL=X` donde `X` es el número de días que desea añadir a la hora de caducidad.

En sistemas AIX, Solaris y Linux, el archivo `cbrserver` está en el directorio `/usr/bin`.

En sistemas Windows, el archivo `cbrserver` está en el directorio `\winnt\system32`.

Afinidad de cookies pasivos

La afinidad de cookies pasivos se aplica al método de reenvío de CBR (Content Based Routing) del componente Dispatcher y al componente CBR. Consulte el apartado “Direccionamiento basado en contenido de Dispatcher (método de reenvío cbr)” en la página 55 para obtener información sobre cómo configurar el método de reenvío de CBR de Dispatcher.

La afinidad de cookies pasivos proporcionan una forma para que los clientes sean permanentes en memoria para un servidor concreto. Cuando habilita la afinidad de una norma para “`passivecookie`”, la afinidad de cookies pasivos le permite equilibrar la carga del tráfico Web con afinidad al mismo servidor, basándose en cookies que se identifican a sí mismos generados por los servidores. La afinidad de cookies pasivos se configura en el nivel de normas.

Cuando se activa la norma, si la afinidad de cookies pasivos está habilitada, Load Balancer seleccionará el servidor basándose en el nombre de cookie de la cabecera HTTP de la petición del cliente. Load Balancer empieza a comparar el nombre de cookie de la cabecera HTTP del cliente con el valor de cookie configurado para cada servidor.

La primera vez que Load Balancer encuentre un servidor cuyo valor de cookie *contenga* el nombre de cookie del cliente, Load Balancer selecciona dicho servidor para la petición.

Nota: Load Balancer proporciona esta flexibilidad para manejar casos en los que el servidor podría generar un valor de cookie al que se ha añadido una parte estática a una parte variable. Por ejemplo, el valor de cookie del servidor podría ser el nombre de servidor (un valor estático) al que se ha añadido una indicación de la hora (un valor variable).

Si el nombre de cookie en la petición de cliente no se encuentra o no coincide con ningún contenido de los valores de cookie de los servidores, el servidor se selecciona utilizando la selección del servidor existente o la técnica de turno rotativo sopesado.

Para configurar **afinidad de cookies pasivos**:

- Para Dispatcher, primero configure el método de reenvío CBR de Dispatcher. (Consulte el apartado “Direccionamiento basado en contenido de Dispatcher (método de reenvío cbr)” en la página 55). Este paso se omite para el componente CBR.
- Establezca el parámetro **affinity** en “passivecookie” en el mandato **dscontrol rule [add | set]**. Además, el parámetro **cookievalue** debe establecerse en el nombre del cookie que Load Balancer debe buscar en la petición de cabecera HTTP de cliente.
- Establezca el parámetro **cookievalue**, para cada servidor del conjunto de servidores de la norma, en el mandato **dscontrol server [add | set]**.

La opción affinity de cookies pasivos, para el mandato rule, sólo puede establecerse en passivecookie si la opción port stickytime es cero (no habilitada). Una vez que la afinidad de cookies pasivos está activa en una norma, no se puede habilitar el tiempo de permanencia en memoria en el puerto.

Afinidad de URI

La afinidad de URI se aplica al método de reenvío CBR de Dispatcher y el componente CBR. Consulte el apartado “Direccionamiento basado en contenido de Dispatcher (método de reenvío cbr)” en la página 55 para obtener información sobre cómo configurar el método de reenvío CBR.

La afinidad de URI permite equilibrar la carga del tráfico Web para servidores Caching Proxy, lo que permitirá que el contenido exclusivo se almacene en la antememoria de cada servidor individual. Como resultado, se aumentará eficazmente la capacidad de la antememoria del sitio y se eliminará el almacenamiento en antememoria redundante de contenido en varias máquinas. Configure la afinidad de URI en el nivel de normas. Una vez que la norma se activa, la afinidad de URI se habilita y el mismo conjunto de servidores están activos y responden, Load Balancer remitirá nuevas peticiones de cliente entrantes con el mismo URI al mismo servidor.

Normalmente, Load Balancer puede distribuir peticiones a varios servidores que sirven contenido idéntico. Al utilizar Load Balancer con un grupo de servidores de antememoria, llegará un momento en que el contenido al que se suele acceder habitualmente estará almacenado en la antememoria de todos los servidores. Esto da soporte a una carga muy alta de clientes duplicando en varias máquinas el contenido idéntico almacenado en antememoria. Esto es de gran utilidad para sitios Web de alto volumen.

Sin embargo, si el sitio Web da soporte a un volumen moderado de tráfico de cliente para un contenido muy diverso, y si prefiere tener una antememoria más grande a lo largo de varios servidores, el sitio tendrá un mejor rendimiento si cada servidor de antememoria incluye contenido exclusivo y Load Balancer sólo distribuye la petición al servidor de antememoria con dicho contenido.

Con la afinidad de URI, Load Balancer le permite distribuir el contenido almacenado en antememoria a servidores individuales y elimina el almacenamiento en antememoria redundante del contenido en varias máquinas. Con esta mejora aumenta el rendimiento de sitios de servidores de contenido diverso que utilizan servidores Caching Proxy. Se enviarán peticiones idénticas al mismo servidor y de esta forma sólo se almacenará en antememoria el contenido en servidores individuales. El tamaño real de la antememoria irá aumentando con cada nueva máquina servidor añadida a la agrupación.

Para configurar la **afinidad de URI**:

- Para Dispatcher, primero configure el método de reenvío CBR de Dispatcher. (Consulte el apartado “Direccionamiento basado en contenido de Dispatcher (método de reenvío cbr)” en la página 55). Este paso se omite para el componente CBR.
- Establezca el parámetro **affinity** en “uri” en el mandato **dscontrol rule [add | set]** o **cbrcontrol rule [add | set]**.

La opción de afinidad de URI, para el mandato rule, sólo puede establecerse en URI si la opción port stickytime es cero (no habilitada). Cuando la afinidad de URI está activa en una norma, no se puede habilitar el tiempo de permanencia en memoria en el puerto.

Configurar soporte de Dispatcher de área amplia

Esta característica sólo está disponible para el componente Dispatcher.

Si no utiliza el soporte de área amplia de Dispatcher y no utiliza el método de reenvío NAT de Dispatcher, una configuración de Dispatcher requiere que la máquina Dispatcher y todos sus servidores estén conectados al mismo segmento de LAN (consulte la Figura 35). La petición de un cliente llega a la máquina Dispatcher y se envía al servidor. Desde el servidor la respuesta se envía directamente al cliente.

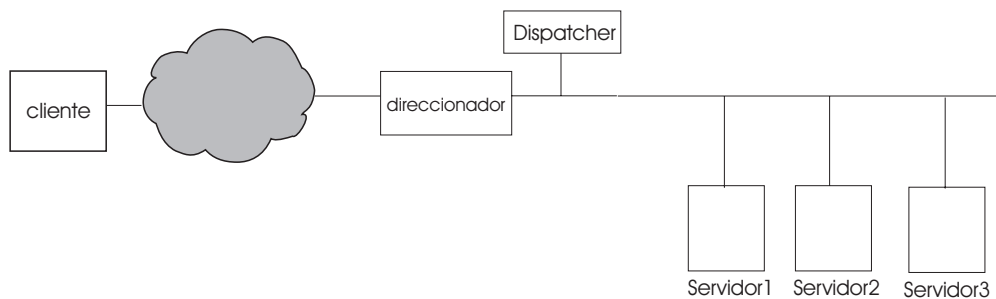


Figura 35. Ejemplo de una configuración que consta de un único segmento LAN

La característica Dispatcher de área amplia añade soporte para servidores que están en otros sitios, llamados *servidores remotos* (consulte la Figura 36 en la página 230). Si no se da soporte a GRE en el sitio remoto y no está utilizando el método de reenvío NAT de Dispatcher, el sitio remoto debe constar de una máquina Dispatcher remota (Dispatcher 2) y de sus servidores conectados localmente (ServidorG, ServidorH y ServidorI). Se transferirán los paquetes del cliente desde Internet a la máquina Dispatcher inicial. Desde la máquina Dispatcher inicial, se transferirá entonces el paquete a una máquina Dispatcher remota geográficamente y a uno de sus servidores conectados localmente.

Todas las máquinas Dispatcher (local y remota) deben estar en el mismo tipo de sistema operativo y plataforma para ejecutar configuraciones de área amplia.

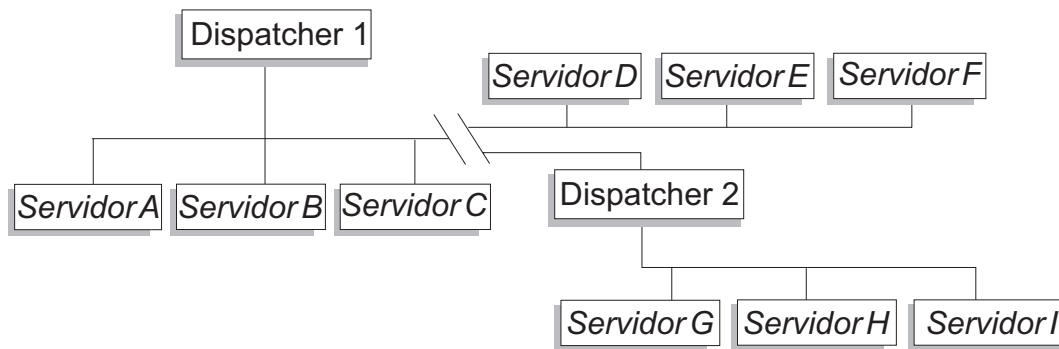


Figura 36. Ejemplo de configuración mediante servidores locales y remotos

Esto permite que una dirección de clúster dé soporte a todas las peticiones de cliente mundiales a la vez que distribuye la carga por servidores situados en todo el mundo.

La máquina Dispatcher que recibe inicialmente el paquete aún puede tener conectados servidores locales y puede distribuir la carga entre sus servidores locales y los servidores remotos.

Sintaxis de mandatos

Para configurar el soporte del área amplia:

1. Añada los servidores. Al añadir un servidor a un sistema Dispatcher, debe definir si el servidor es local o remoto (vea arriba). Para añadir un servidor y definirlo como local, emita el mandato **dscontrol server add** sin especificar un direccionador. Es el valor por omisión. Para definir el servidor como remoto, debe especificar el direccionador a través del que Dispatcher debe enviar el paquete para llegar al servidor remoto. El servidor debe ser otro sistema Dispatcher y la dirección del servidor debe ser una dirección de no reenvío del sistema Dispatcher. Por ejemplo, en la Figura 37 en la página 232, si añade *LB 2* como servidor remoto bajo *LB 1*, debe definir *direccionador 1* como la dirección del direccionador. Sintaxis general:

```
dscontrol server add clúster:puerto:servidor router dirección
```

Si desea más información sobre la palabra clave *router*, consulte el apartado “dscontrol server — configurar servidores” en la página 392.

2. Configure los alias. En la primera máquina Dispatcher (donde llega la petición de cliente desde Internet), debe crearse un alias de la dirección de clúster con el mandato **executor configure**. (En sistemas Linux o UNIX, puede utilizar el mandato **executor configure** o **ifconfig**). Sin embargo, en las máquinas Dispatcher remotas la dirección del clúster *no* tienen ningún alias asociado a la tarjeta de interfaz de red.

Utilización de asesores remotos con el soporte de área amplia de Dispatcher

En Dispatchers de punto de entrada:

Los Dispatchers de punto de entrada que se ejecutan en plataformas AIX, Linux (con GRE) o Solaris mostrarán correctamente cargas del asesor de visualización. Otras plataformas tendrán que confiar en el equilibrio de carga mediante el algoritmo de turno rotativo o utilizar los métodos de reenvío nat/cbr de Dispatcher en lugar de la red de área amplia.

Sistemas AIX

- No es necesario llevar a cabo ningún paso especial de configuración.

Sistemas HP-UX

- En una configuración WAN, cuando se utiliza un sistema Dispatcher de punto de entrada que se ejecuta en una plataforma HP-UX, existe una limitación en la utilización de asesores remotos. Con el método de reenvío MAC de Dispatcher, los asesores de HP-UX siempre se dirigirán directamente a la dirección del servidor en lugar de al clúster. Puesto que no tienen el clúster como destino, el sistema Dispatcher remoto no equilibrará la carga de la petición del asesor para los servidores remotos. Sin embargo, los asesores remotos funcionarán correctamente cuando utilicen el reenvío CBR o NAT.

Sistemas Linux

- En una configuración WAN, cuando se utiliza un sistema Dispatcher de punto de entrada que se ejecuta en una plataforma Linux, existe una limitación en la utilización de asesores remotos. Con el método de reenvío MAC de Dispatcher, los asesores de Linux siempre se dirigirán directamente a la dirección del servidor en lugar de al clúster. Puesto que no tienen el clúster como destino, el sistema Dispatcher remoto no equilibrará la carga de la petición del asesor para los servidores remotos. Sin embargo, los asesores remotos funcionarán correctamente cuando utilicen el reenvío CBR o NAT.
- Si utiliza GRE (encapsulamiento genérico de direccionamiento) para enviar tráfico a un servidor remoto sin que exista un sistema Dispatcher remoto en la configuración, no hay ninguna limitación en la utilización de asesores cuando se ejecuta el método de reenvío MAC, NAT o CBR de Dispatcher en una plataforma Linux. Si desea más información sobre GRE, consulte el apartado “Soporte de GRE (Encapsulamiento genérico de direccionamiento)” en la página 234.

Sistemas Solaris

- En una configuración WAN, si utiliza un Dispatcher de punto de entrada que se ejecuta en una plataforma Solaris, debe utilizar el método de configuración ARP en lugar de los métodos de configuración ifconfig o dscontrol executor. Por ejemplo:

```
arp -s mi_dirección_clúster> mi_dirección_MAC pub
```
- A continuación se indican las limitaciones para la plataforma Solaris:
 - Los asesores WAN sólo funcionan con el método ARP de configuración de clúster.
 - Los asesores para servidores específicos del enlace sólo funcionan con el método ARP de configuración de clúster.
 - Los asesores para servidores específicos del enlace sólo funcionan con el método ARP de configuración de clúster. Al utilizar asesores para servidores específicos del enlace, no ponga Load Balancer en el mismo servidor compartiendo ubicación con la aplicación específica del enlace.

Sistemas Windows

- En una configuración WAN, cuando se utiliza un sistema Dispatcher de punto de entrada que se ejecuta en una plataforma Windows, existe una limitación en la utilización de asesores remotos. Con el método de reenvío MAC de Dispatcher, los asesores de Windows siempre se dirigirán directamente a la dirección del servidor en lugar de al clúster. Puesto que no tienen el clúster como destino, el sistema Dispatcher remoto no equilibrará la carga de la petición

del asesor para los servidores remotos. Sin embargo, los asesores remotos funcionarán correctamente cuando utilicen el reenvío CBR o NAT.

En sistemas Dispatcher remotos: realice los siguientes pasos de configuración para cada dirección de clúster remoto. Para una configuración de alta disponibilidad en la ubicación del sistema Dispatcher remoto, debe llevar a cabo estos pasos en las dos máquinas.

Sistemas AIX

- Dispatcher debe tener cada clúster configurado en la interfaz con una máscara de red 255.255.255.255 para que los asesores funcionen correctamente. Utilice uno de los siguientes formatos de sintaxis para configurar un clúster:
 - `ifconfig nombre_interfaz alias dirección_clúster netmask 255.255.255.255`. Por ejemplo,
`ifconfig en0 alias 10.10.10.99 netmask 255.255.255.255`
 - `dscontrol executor configure dirección_interfaz nombre_interfaz máscara_red`. Por ejemplo,
`dscontrol executor configure 204.67.172.72 en0 255.255.255.255`

Nota: Los asesores que se ejecutan en las máquinas Dispatcher locales y remotas son necesarios.

Sistemas HP-UX, Linux, Solaris y Windows

- No es necesario llevar a cabo más pasos de configuración.

Ejemplo de configuración

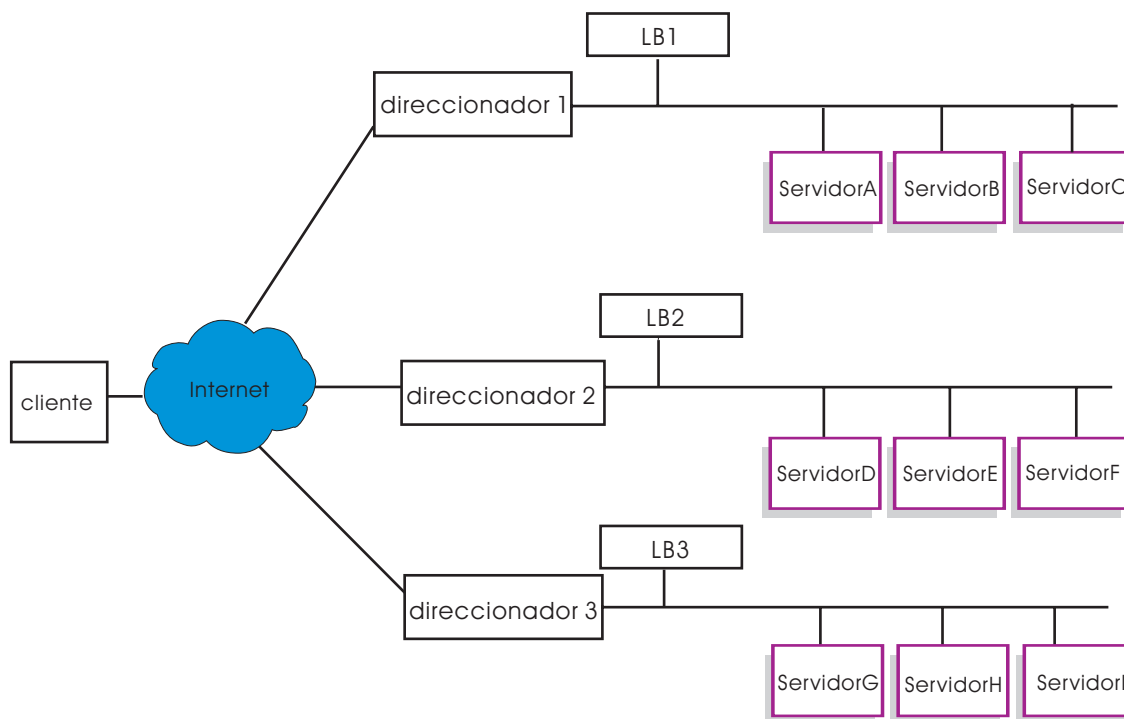


Figura 37. Configuración del ejemplo de área amplia con varios Load Balancer remotos

Este ejemplo se aplica a la configuración que se muestra en la Figura 37.

Aquí se muestra cómo configurar las máquinas Dispatcher para dar soporte a la dirección de clúster xebec en el puerto 80. LB1 se define como Load Balancer de “punto de entrada”. Se da por supuesto una conexión Ethernet. Tenga en cuenta que LB1 tiene definidos cinco servidores: tres locales (ServidorA, ServidorB, ServidorC) y dos remotos (LB2 y LB3). Cada uno de los servidores LB2 y LB3 remotos tiene definido tres servidores locales.

En la consola de la primera máquina Dispatcher (LB1):

1. Inicie el ejecutor.
dscontrol executor start
2. Establezca la dirección de no reenvío de la máquina Dispatcher.
dscontrol executor set nfa LB1
3. Defina el clúster.
dscontrol cluster add xebec
4. Defina el puerto.
dscontrol port add xebec:80
5. Defina los servidores.
 - a. **dscontrol server add xebec:80:ServidorA**
 - b. **dscontrol server add xebec:80:ServidorB**
 - c. **dscontrol server add xebec:80:ServidorC**
 - d. **dscontrol server add xebec:80:LB2 router Direccionador1**
 - e. **dscontrol server add xebec:80:LB3 router Direccionador1**
6. Configure la dirección de clúster.
dscontrol executor configure xebec

En la consola de la segunda máquina Dispatcher (LB2):

1. Inicie el ejecutor.
dscontrol executor start
2. Establezca la dirección de no reenvío de la máquina Dispatcher.
dscontrol executor set nfa LB2
3. Defina el clúster.
dscontrol cluster add xebec
4. Defina el puerto.
dscontrol port add xebec:80
5. Defina los servidores.
 - a. **dscontrol server add xebec:80:ServidorD**
 - b. **dscontrol server add xebec:80:ServidorE**
 - c. **dscontrol server add xebec:80:ServidorF**

En la consola de la tercera máquina Dispatcher (LB3):

1. Inicie el ejecutor.
dscontrol executor start
2. Establezca la dirección de no reenvío de la máquina Dispatcher.
dscontrol executor set nfa LB3
3. Defina el clúster.
dscontrol cluster add xebec
4. Defina el puerto.

dscontrol port add xebec:80

5. Defina los servidores.
 - a. **dscontrol server add xebec:80:ServidorG**
 - b. **dscontrol server add xebec:80:ServidorH**
 - c. **dscontrol server add xebec:80:ServidorI**

Notas

1. En todos los servidores (A-I), cree el alias de la dirección de clúster con el bucle de retorno.
2. Los clústeres y los puertos se añaden con dscontrol a todas las máquinas Dispatcher implicadas: el sistema Dispatcher de punto de entrada y todas las máquinas remotas.
3. Consulte el apartado “Utilización de asesores remotos con el soporte de área amplia de Dispatcher” en la página 230 para obtener ayuda sobre cómo utilizar asesores remotos con soporte de área amplia.
4. El soporte de área amplia no permite utilizar bucles de direccionamiento infinito. (Si una máquina Dispatcher recibe un paquete desde otra máquina Dispatcher, no se reenviará a una tercera máquina Dispatcher). El área amplia sólo da soporte a un nivel de sistemas remotos.
5. El área amplia da soporte a UDP y a TCP.
6. El área amplia funciona junto con alta disponibilidad: se puede hacer una copia de seguridad de cada sistema Dispatcher en una máquina en espera adyacente (en el mismo segmento LAN).
7. El gestor y los asesores funcionan con red de área amplia y, si se utiliza, debe iniciarse en todas las máquinas Dispatcher implicadas.
8. Load Balancer da soporte a WAN sólo en sistemas operativos iguales.

Soporte de GRE (Encapsulamiento genérico de direccionamiento)

El encapsulamiento genérico de direccionamiento (GRE) es un Internet Protocolo especificado en RFC 1701 y RFC 1702. Si utiliza GRE, Load Balancer puede encapsular paquetes IP del cliente dentro de paquetes IP/GRE y remitirlos a plataformas de servidor como OS/390 que dan soporte a GRE. El soporte de GRE permite al componente Dispatcher equilibrar la carga de paquetes en varias direcciones de servidores asociadas a una dirección MAC.

Load Balancer implementa GRE como parte de su característica WAN. Esto permite que Load Balancer proporcione equilibrio de carga de área local directamente a todos los sistemas de servidor que puedan abrir los paquetes GRE. No es necesario que Load Balancer esté instado en el sitio remoto, si los servidores remotos dan soporte a paquetes GRE encapsulados. Load Balancer encapsula paquetes WAN con el campo clave GRE establecido en un valor decimal 3735928559.

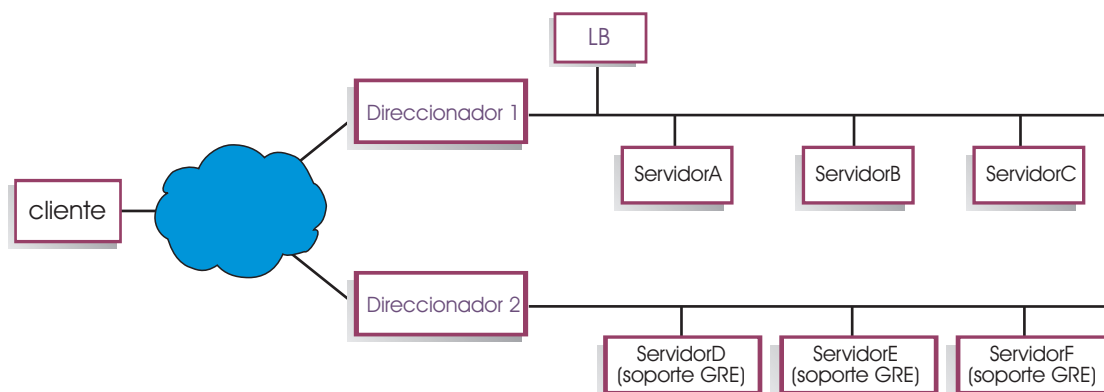


Figura 38. Configuración del ejemplo de área amplia con una plataforma de servidor que da soporte a GRE

En este ejemplo (Figura 38), para añadir el ServidorD remoto, que da soporte a GRE, defínalo dentro de la configuración de Load Balancer como si estuviera definiendo un servidor de WAN en la jerarquía clúster:puerto:servidor:

```
dscontrol server add clúster:puerto:ServidorD router Direcciónador1
```

En sistemas Linux, configuración del excapsulamiento de GRE para WAN

Los sistemas Linux tienen la capacidad nativa para excapsular GRE que permite a Load Balancer equilibrar la carga en las imágenes del servidor Linux para s/390, donde muchas imágenes de servidor comparten una dirección MAC. Esto permite que Load Balancer de punto de entrada equilibre la carga directamente en servidores WAN de Linux WAN, sin pasar a través de un sistema Load Balancer en el sitio remoto. También permite que los asesores del sistema Load Balancer de punto de entrada operen directamente con cada servidor remoto.

En el sistema Load Balancer de punto de entrada, configúrelo para WAN tal como se describe.

Para configurar cada servidor del programa de fondo Linux, emita los siguientes mandatos como usuario root. (Estos mandatos se pueden añadir al recurso de inicio del sistema para que los cambios se mantengan en los rearranques).

```
# modprobe ip_gre
# ip tunnel add gre-nd mode gre ikey 3735928559
# ip link set gre-nd up
# ip addr add dirección_clúster dev gre-nd
```

Nota: El servidor Linux configurado utilizando estas instrucciones *no puede* estar en el mismo elemento físico que el sistema Load Balancer de punto de entrada. Esto se debe a que el servidor Linux responderá a las peticiones "ARP who-has" para la dirección del clúster, lo que provocará que un estado de competición que llevará a un posible "corto circuito" en el que todo el tráfico de la dirección del clúster sólo se dirige al ganador de la competición ARP.

Utilización del enlace explícito

En general, las funciones de equilibrio de carga de Dispatcher funcionan independientemente del contenido de los sitios en los que se utiliza el producto. No obstante, existe un área en la que el contenido del sitio puede ser importante y donde las decisiones que se han tomado respecto al contenido pueden tener un impacto significativo en la eficacia de Dispatcher. Se trata del área de direccionamiento de enlaces.

Si las páginas especifican enlaces que apuntan a servidores individuales del sitio, en realidad está forzando a un cliente a que vaya a una máquina específica y, por lo tanto, omitirá cualquier función de equilibrio de carga que podría estar aplicándose. Por esta razón, utilice siempre la dirección de Dispatcher en todos los enlaces contenidos en las páginas. Tenga en cuenta que es posible que el tipo de direccionamiento utilizado no sea siempre evidente, si el sitio utiliza programación automatizada que crea código HTML de forma dinámica. Para maximizar el equilibrio de carga, debe conocer bien todo el direccionamiento explícito y evitarlo cuando sea posible.

Utilización de una configuración de red privada

Puede configurar las máquinas Dispatcher y del servidor TCP utilizando una red privada. Esta configuración puede reducir el conflicto sobre la red pública o externa que puede afectar al rendimiento.

En sistemas AIX, esta configuración también puede beneficiarse de las velocidades rápidas del conmutador de alto rendimiento de SP, si está ejecutando las máquinas Dispatcher y del servidor TCP en nodos que están en una trama SP.

Para crear una red privada, cada máquina debe tener como mínimo dos tarjetas de LAN y una de las tarjetas está conectada a la red privada. También debe configurar la segunda tarjeta de LAN en una subred distinta. La máquina Dispatcher enviará las peticiones de cliente a las máquinas servidor TCP a través de la red privada.

Sistemas Windows: configure la dirección de no reenvío con el mandato `executor configure`.

Los servidores añadidos con el mandato **`dscontrol server add`** deben añadirse utilizando las direcciones de la red privada; por ejemplo, si nos remitimos al ejemplo del servidor Apple en la Figura 39 en la página 237, el mandato debería codificarse en la forma:

```
dscontrol server add dirección_clúster:80:10.0.0.1
```

no

```
dscontrol server add dirección_clúster:80:9.67.131.18
```

Si utiliza Site Selector para proporcionar información de carga en Dispatcher, debe configurar Site Selector de modo que notifique las cargas en las direcciones privadas.

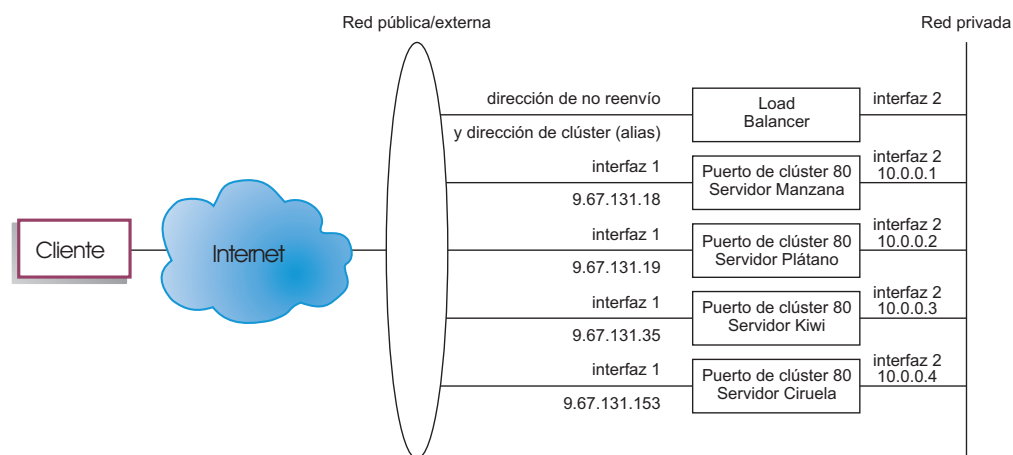


Figura 39. Ejemplo de una red privada que utiliza Dispatcher

La utilización de la configuración de red privada sólo se aplica al componente Dispatcher.

Utilizar un clúster comodín para combinar configuraciones de servidores

La utilización de clúster comodín para combinar configuraciones de servidor sólo se aplica al componente Dispatcher.

La palabra “comodín” hace referencia a la capacidad del clúster para emparejar varias direcciones IP (es decir, actúa como un comodín). La dirección del clúster 0.0.0.0 se utiliza para especificar un clúster comodín.

Si tiene muchas direcciones de clúster en las que se debe equilibrar la carga y las configuraciones de puerto/servidor son idénticas en todos los clústeres, puede combinar todos los clústeres en una configuración de clúster comodín.

Deberá configurar de forma explícita cada dirección de clúster en uno de los adaptadores de la red de la estación de trabajo de Dispatcher. Sin embargo, no debe añadir ninguna de las direcciones de clúster a la configuración de Dispatcher utilizando el mandato dscontrol cluster add.

Únicamente añada un clúster comodín (dirección = 0.0.0.0) y configure los puertos y servidores como se requiere para el equilibrio de carga. Se equilibra la carga de todo el tráfico que se dirija a cualquiera de las direcciones configuradas del adaptador utilizando la configuración del clúster comodín.

Una ventaja de este método es que, al determinar cuál es el mejor servidor al que dirigirse, se toma en cuenta el tráfico dirigido a todas las direcciones del clúster. Si un clúster recibe mucho tráfico y ha creado muchas conexiones activas en uno de los servidores, con esta información se equilibra la carga del tráfico que se dirige a otras direcciones del clúster.

Si tiene algunas direcciones de clúster con configuraciones de puerto/servidor exclusivas y algunas con configuraciones comunes, puede combinar el clúster comodín con clústeres reales. Se debe asignar cada una de las configuraciones exclusivas a una dirección de clúster real. Todas las configuraciones comunes pueden asignarse al clúster comodín.

Utilizar un clúster comodín para equilibrar la carga de cortafuegos

La utilización de clúster comodín para equilibrar la carga de cortafuegos sólo se aplica al componente Dispatcher. La dirección del clúster 0.0.0.0 se utiliza para especificar un clúster comodín.

El clúster comodín puede utilizarse para equilibrar la carga del tráfico en direcciones que no están configuradas de forma explícita en ningún adaptador de red de la estación de trabajo de Dispatcher. Para que esto funcione, Dispatcher como mínimo debe poder ver todo el tráfico en el que se va a equilibrar la carga. La estación de trabajo de Dispatcher no verá el tráfico que se dirige a las direcciones que no se han configurado de forma explícita en uno de sus adaptadores de red, a menos que se configure como la ruta por omisión para algún conjunto de tráfico.

Después de configurar Dispatcher como una ruta por omisión, la carga de todo el tráfico TCP o UDP que pase por la máquina Dispatcher se equilibra utilizando la configuración de clúster comodín.

Esto se aplica para equilibrar la carga de cortafuegos. Puesto que los cortafuegos pueden procesar paquetes para cualquier dirección de destino y cualquier puerto de destino, es necesario poder equilibrar la carga del tráfico independientemente de la dirección y el puerto de destino.

Los cortafuegos se utilizan para manejar el tráfico de clientes no seguros a servidores seguros, y las respuestas de los servidores seguros, así como el tráfico de clientes que están en el lado seguro a servidores que están en el lado no seguro y las respuestas.

Debe configurar dos máquinas Dispatcher, una para equilibrar la carga del tráfico no seguro dirigido a las direcciones de cortafuegos no seguro y otra para equilibrar la carga del tráfico seguro dirigido a las direcciones del cortafuegos seguro. Puesto que los dos sistemas Dispatcher deben utilizar el clúster comodín y el puerto comodín con distintos conjuntos de direcciones de servidores, los dos sistemas Dispatcher deben estar en dos estaciones de trabajo separadas.

Utilizar un clúster comodín con Caching Proxy para el proxy transparente

La utilización del clúster comodín con Caching Proxy para el proxy transparente sólo se aplica al componente Dispatcher. La dirección del clúster 0.0.0.0 se utiliza para especificar un clúster comodín.

La función de clúster comodín también permite que Dispatcher se utilice para habilitar una función de proxy transparente para un servidor Caching Proxy que resida en la misma máquina que Dispatcher. Esta característica sólo es de AIX, porque debe haber comunicación entre el componente Dispatcher y el componente TCP del sistema operativo.

Para habilitar esta característica, debe iniciar Caching Proxy escuchando peticiones de cliente en el puerto 80. A continuación, configure un clúster comodín (0.0.0.0). En el clúster comodín, configure el puerto 80. En el puerto 80, configure la NFA de la máquina Dispatcher como el único servidor. Ahora, todo el tráfico de cliente dirigido a cualquier dirección del puerto 80 se entrega al servidor Caching Proxy que se ejecuta en la estación de trabajo de Dispatcher. La petición de cliente se

dirigirán a través del proxy de la forma habitual y la respuesta se devuelve de Caching Proxy al cliente. En esta modalidad, el componente Dispatcher no realiza ningún equilibrio de carga.

Utilizar el puerto comodín para dirigir el tráfico de puerto no configurado

Se puede utilizar un puerto comodín para manejar el tráfico que no está destinado a ningún puerto configurado de forma explícita. Un uso de lo anterior es para el equilibrio de carga de cortafuegos. Un segundo uso es para asegurar que el tráfico destinado a un puerto no configurado se maneja de forma adecuada. Mediante la definición de un puerto comodín sin servidores, garantizará que se descarte cualquier petición destinada a un puerto que no se haya configurado en lugar de devolverse al sistema operativo. El número de puerto 0 (cero) se utiliza para especificar el puerto comodín, por ejemplo:

```
dscontrol port add clúster:0
```

Puerto comodín para manejar el tráfico FTP

Cuando se configura un clúster para manejar el FTP pasivo y el puerto comodín, el FTP pasivo por omisión utiliza el rango completo de puertos TCP sin privilegios para las conexiones de datos. Esto significa que un cliente, con una conexión existente a través de un clúster de equilibrio de carga a un puerto de control FTP, tendrá conexiones de control y conexiones de puertos altos (puerto >1023) subsiguientes al mismo clúster direccionadas automáticamente por Load Balancer al mismo servidor que el de la conexión de control FTP.

Si el puerto comodín y el puerto FTP, en el mismo clúster, no tienen el mismo conjunto de servidores, entonces es posible que las aplicaciones de puertos altos (puerto >1023) fallen cuando un cliente tenga una conexión de control FTP. Por lo tanto, no se recomienda configurar distintos conjuntos de servidores para los puertos FTP y comodín en el mismo clúster. Si se desea este escenario, se debe configurar el rango de puertos pasivos del daemon de FTP en la configuración de Load Balancer.

Detección de ataques para rechazo de servicio (DoS)

Esta característica sólo está disponible para el componente Dispatcher.

Dispatcher proporciona la capacidad de detectar ataques para "rechazo de servicio" (DoS) potenciales y notifica a los administradores mediante una alerta. Dispatcher lo lleva a cabo analizando las peticiones entrantes para una cantidad llamativa de conexiones TCP medio abiertas en servidores, un rasgo común de los ataques simples para rechazo de servicio (DoS). En un ataque para rechazo de servicio (DoS), un sitio recibe una gran cantidad de paquetes SYN fabricados procedentes de un gran número de direcciones IP de origen y números de puerto de origen, pero el sitio no recibe paquetes posteriores para estas conexiones TCP. Esto resulta en un gran número de conexiones TCP medio abiertas en los servidores y, con el tiempo, los servidores pueden funcionar muy lentamente y no aceptar nuevas conexiones entrantes.

Nota: Debe haber tráfico entrante a través del clúster y del puerto a los que se ataca para que Dispatcher pueda determinar el fin del ataque para rechazo de servicio (DoS). Dispatcher no puede detectar que el ataque se ha detenido hasta que el tráfico empieza a circular de nuevo.

Load Balancer proporciona salidas de usuario que desencadenan scripts que se pueden personalizar y que avisan al administrador de un posible ataque para rechazo de servicio (DoS). Dispatcher proporciona el siguiente script de ejemplo en el directorio `...ibm/edge/lb/servers/samples`:

- `halfOpenAlert`: se ha detectado un probable ataque para rechazo de servicio (DoS)
- `halfOpenAlertDone`: el ataque DoS ha finalizado

Para ejecutar los archivos, debe ponerlos en el directorio `...ibm/edge/lb/servers/bin` y eliminar la extensión de archivo `".sample"`.

Para implementar la detección del ataque DoS, establezca el parámetro **maxhalfopen** en el mandato **dscontrol port** tal como se indica a continuación:

```
dscontrol port set 127.40.56.1:80 maxhalfopen 1000
```

En el ejemplo anterior, Dispatcher comparará el número total actual de conexiones medio abiertas (para todos los servidores que residen en el clúster 127.40.56.1 en el puerto 80) con el valor de umbral 1000 (especificado por el parámetro `maxhalfopen`). Si el número de conexiones medio abiertas actuales excede el umbral, se realiza una llamada al script de alerta (`halfOpenAlert`). Cuando el número de conexiones medio abiertas es inferior al umbral, se realiza una llamada a otro script de alerta (`halfOpenAlertDone`) para indicar que el ataque ha terminado.

Para determinar cómo establecer el valor `maxhalfopen`: ejecute periódicamente (quizás cada 10 minutos) un informe de conexiones medio abiertas (**dscontrol port halfopenaddressreport *clúster:puerto***) cuando la cantidad de tráfico del sitio oscile de normal a elevada. El informe de conexiones medio abiertas devolverá el "total de conexiones medio abiertas recibidas" actuales. Debe establecer `maxhalfopen` en un valor entre un 50 y un 200% mayor que el número más alto de conexiones medio abiertas que se producen en el sitio.

Además de los datos estadísticos reportados, `halfopenaddressreport` también genera entradas en las anotaciones cronológicas (`..ibm/edge/lb/servers/logs/dispatcher/halfOpen.log`) para todas las direcciones de cliente (hasta aproximadamente 8000 pares de direcciones) que han accedido a servidores que han resultado en conexiones medio abiertas.

Nota: Existe una condición de excepción SNMP correspondiente a los scripts `halfOpenAlert` y `halfOpenAlertDone`. Si el subagente SNMP está configurado y en ejecución, las correspondientes condiciones de excepción se envían en las mismas condiciones que desencadenaron los scripts. Si desea más información sobre el subagente SNMP, consulte el apartado "Utilización de Simple Network Management Protocol con el componente Dispatcher" en la página 269.

Para proporcionar protección adicional de los ataques para rechazo de servicio (DoS) para servidores de programas de fondo, puede configurar puertos y clústeres comodín. En concreto, añada un puerto comodín sin servidores bajo cada clúster configurado. Añada también un clúster comodín con un puerto comodín y sin servidores. Esto provocará que se descarten todos los paquetes que no se dirijan a un clúster y puerto que no sea comodín. Para obtener información sobre clústeres comodín y puertos comodín, consulte el apartado "Utilizar un clúster comodín para combinar configuraciones de servidores" en la página 237 y "Utilizar el puerto comodín para dirigir el tráfico de puerto no configurado" en la página 239.

Utilización del registro cronológico binario para analizar estadísticas de servidor

Nota: La característica de registro cronológico en binario se aplica al componente Dispatcher y CBR.

La característica de registro cronológico en binario permite almacenar información de servidor en archivos binarios. Estos archivos pueden procesarse para analizar la información de servidor que se ha recopilado con el tiempo.

La siguiente información se ha almacenado en las anotaciones cronológicas en binario para cada servidor definido en la configuración.

- dirección del clúster
- número de puerto
- ID de servidor
- dirección de servidor
- peso del servidor
- total de conexiones de servidor
- conexiones activas de servidor
- carga de puerto de servidor
- carga de servidor de sistema

Parte de esta información se recupera del ejecutor como parte del ciclo del gestor. Por lo tanto, para que la información se pueda anotar cronológicamente en las anotaciones cronológicas en binario, el gestor debe estar en ejecución.

Utilice el mandato **dscontrol binlog** establecido para configurar el registro cronológico en binario.

- binlog start
- binlog stop
- binlog set interval <segundo>
- binlog set retention <horas>
- binlog status

La opción start inicia el registro cronológico de la información de servidor en anotaciones cronológicas en binario en el directorio logs. Al inicio de cada hora se crea un archivo con la fecha y la hora como el nombre del archivo.

La opción stop detiene el registro cronológico de la información de servidor en las anotaciones cronológicas en binario. Por omisión, el servicio de anotaciones cronológicas está detenido.

La opción set interval controla la frecuencia con la que información se escribe en las anotaciones cronológicas. Cada intervalo del gestor, éste enviará información de servidor al servidor de anotaciones cronológicas. La información se graba en las anotaciones cronológicas sólo cuando hayan transcurrido los segundos especificados en el intervalo de anotaciones cronológicas después de anotarse el último registro en las anotaciones cronológicas. Por omisión, el intervalo de anotaciones cronológicas se establece en 60 segundos. Los valores del intervalo del gestor y del intervalo de anotaciones cronológicas están relacionados. Puesto que al servidor de anotaciones cronológicas se le proporciona información cómo máximo

a la velocidad indicada por los segundos del intervalo del gestor, si se establece el intervalo de anotaciones cronológicas en un valor inferior al valor del intervalo del gestor en realidad se establece en el mismo valor que el intervalo del gestor. Esta técnica de registro cronológico permite captar información de servidor en cualquier granularidad. Puede captar todos los cambios realizados en la información del servidor detectados por el gestor para calcular pesos de servidor. No obstante, esta cantidad de información probablemente no es necesaria para analizar tendencias y utilización del servidor. Si se registra información del servidor cada 60 segundos, con el tiempo dispondrá de instantáneas de información del servidor. Si establece el intervalo de anotaciones cronológicas muy bajo puede generar enormes cantidades de datos.

La opción `set retention` controla cuánto tiempo se mantienen los archivos. El servidor de anotaciones cronológicas elimina los archivos de anotaciones cronológicas anteriores a las horas de retención especificadas. Esto sólo sucederá si el gestor está llamando al servidor de anotaciones cronológicas, por lo tanto, si detiene el gestor no se suprimirán los archivos de anotaciones cronológicas antiguos.

La opción de estado devuelve los valores actuales del servicio de anotaciones cronológicas. Estos valores indican si el servicio se ha iniciado, el intervalo y las horas de retención.

Se proporciona un archivo de mandatos y un programa Java de ejemplo en el directorio `...ibm/edge/lb/servers/samples/BinaryLog`. Este ejemplo muestra cómo recuperar toda la información de los archivos de anotaciones cronológicas e imprimirla en la pantalla. Puede personalizar realizar cualquier tipo de análisis que desea con los datos. Un ejemplo de la utilización del script proporcionado y el programa para Dispatcher sería:

```
dslogreport 2001/05/01 8:00 2001/05/01 17:00
```

para obtener un informe con la información de servidor del componente Dispatcher para el día 1 de mayo de 2001, de las 8:00 a las 17:00. (Para CBR, utilice `cbrlogreport`).

Utilización de un cliente con ubicación compartida

Sólo los sistemas Linux dan soporte a configuraciones en las que el cliente se encuentra en la misma máquina que Load Balancer.

Las configuraciones de cliente con ubicación compartida pueden no funcionar correctamente en otras plataformas porque Load Balancer utiliza distintas técnicas para examinar los paquetes de entrada en los diversos sistemas operativos a los que da soporte. En la mayoría de los casos, en sistemas que no sean Linux, Load Balancer no recibe paquetes que proceden de la máquina local. Sólo recibe paquetes que proceden de la red. Debido a ello, Load Balancer no recibirá las peticiones realizadas desde la máquina local a la dirección de clúster y no podrá atenderlas.

Capítulo 23. Características avanzadas de Cisco CSS Controller y Nortel Alteon Controller

Este capítulo incluye los siguientes apartados:

- “Ubicación compartida”
- “Alta disponibilidad”
- “Optimización del equilibrio de carga que proporciona Load Balancer” en la página 246
- “Asesores” en la página 248
- “Metric Server” en la página 253
- “Utilización del registro cronológico binario para analizar estadísticas de servidor” en la página 256
- “Utilización de scripts para generar una alerta o anotar anomalías en el servidor” en la página 257

Nota: En este capítulo **xxxcontrol** indica **ccocontrol** para Cisco CSS Controller y **nalcontrol** para Nortel Alteon Controller.

Ubicación compartida

Cisco CSS Controller o Nortel Alteon Controller puede residir en la misma máquina como servidor para el que se está equilibrando la carga de peticiones. Esto se conoce habitualmente como *ubicación compartida* de un servidor. No es necesario llevar a cabo más pasos de configuración.

Nota: Un servidor con ubicación compartida compite por los recursos contra Load Balancer durante los periodos de mucho tráfico. Sin embargo, si no hay máquinas sobrecargadas, si se utiliza un servidor con ubicación compartida se reducirá el número total de máquinas necesarias para definir un sitio con equilibrio de carga.

Alta disponibilidad

La característica de alta disponibilidad está ahora disponible para Cisco CSS Controller y Nortel Alteon Controller.

Para mejorar la tolerancia de errores del controlador, la función de alta disponibilidad contiene estas funciones:

- Un mecanismo de pulsos para determinar la disponibilidad de los controladores asociados. Los pulsos se intercambian entre las direcciones configuradas en el mandato **xxxcontrol highavailability add**. Puede configurar el intervalo durante el que se intercambian los pulsos y el intervalo durante el que un controlador asume el control del socio.
- Una lista de destinos que cada controlador debe poder alcanzar para calcular pesos y actualizar el conmutador. Consulte el apartado “Detección de anomalías” en la página 245 para obtener más información.
- Lógica para elegir el controlador activo basándose en la información de disponibilidad y de alcance.
- La estrategia de toma de control configurable utilizada para determinar cómo un controlador asume el control de su socio.

- Un mecanismo de toma de control manual para el mantenimiento de controladores activos.
- Informes que muestran el rol, el estado, la sincronización, etc. del controlador actual.

Configuración

Consulte los apartados “ccocontrol highavailability — controlar alta disponibilidad” en la página 439 y “nalcontrol highavailability — controlar alta disponibilidad” en la página 457 para obtener la sintaxis completa para **xxxcontrol highavailability**.

Para configurar la alta disponibilidad del controlador:

1. Inicie el servidor del controlador en las dos máquinas del controlador.
2. Configure cada controlador con configuraciones idénticas.
3. Configure el rol de alta disponibilidad local, dirección y dirección de socio tal como se indica a continuación:

```
xxxcontrol highavailability add address 10.10.10.10  
partneraddress 10.10.10.20 port 143 role primary
```

4. Configure el rol de alta disponibilidad de socio, dirección y dirección de socio tal como se indica a continuación:

```
xxxcontrol highavailability add address 10.10.10.20  
partneraddress 10.10.10.10 port 143 role secondary
```

Los parámetros address y partneraddress se invierten en las máquinas primaria y secundaria.

5. Si lo desea, configure los parámetros de alta disponibilidad en los controladores local y asociado; por ejemplo:

```
xxxcontrol highavailability set beatinterval 1000
```

6. Si lo desea, configure los destinos de alcance en los controladores local y asociado como se indica a continuación:

```
xxxcontrol highavailability usereach  
10.20.20.20
```

Debe configurarse el mismo número de destinos de alcance en los controladores local y asociado.

7. Inicie el componente de alta disponibilidad y defina la estrategia de recuperación en los controladores local y asociado como se indica a continuación:

```
xxxcontrol highavailability start auto
```

8. De manera opcional, puede mostrar la información de alta disponibilidad de los controladores local y asociado como se indica a continuación:

```
xxxcontrol highavailability report
```

9. De manera opcional, especifique la toma de control sobre el controlador en espera para asumir el control desde el controlador activo como se indica a continuación:

```
xxxcontrol highavailability takeover
```

Esto sólo es necesario para realizar el mantenimiento.

Notas:

1. Para configurar un solo controlador sin alta disponibilidad, no emita ningún mandato de alta disponibilidad.

2. Para convertir dos controladores de una configuración de alta disponibilidad en un solo controlador, primero detenga la alta disponibilidad en el controlador en espera y, si lo desea, después detenga la alta disponibilidad en el controlador activo.
3. Cuando ejecuta dos controladores en una configuración de alta disponibilidad, pueden producirse resultados imprevistos si algunas de las propiedades del controlador son distintas entre los conmutadores; por ejemplo, el identificador de consultor de conmutador, la dirección de conmutador, etc. También puede obtener resultados imprevistos si las propiedades de alta disponibilidad del controlador no coinciden; por ejemplo, el puerto, el rol, los destinos de alcance, el intervalo de pulsos, el intervalo de toma de control y la estrategia de recuperación.

Detección de anomalías

Además de la pérdida de conectividad entre controladores activos y en espera, que se detecta a través de los mensajes de pulsos, *accesibilidad* proporciona otro mecanismo de detección de anomalías.

Al configurar la alta disponibilidad del controlador, puede proporcionar una lista de los sistemas principales a los que deben acceder los controladores para funcionar correctamente. Debe haber como mínimo un sistema principal para cada subred que utiliza la máquina del controlador. Estos sistemas principales pueden ser direccionadores, servidores IP o otros tipos de sistemas principales.

La accesibilidad de sistemas principales se obtiene mediante el asesor de alcance que emite el mandato ping al sistema principal. Tiene lugar la conmutación si los mensajes de pulso no pueden transmitirse o si los criterios de accesibilidad los satisface mejor el controlador en espera que el controlador activo. Para tomar esta decisión basándose en toda la información disponible, el controlador activo envía regularmente al controlador en espera su capacidad de accesibilidad y viceversa. Los controladores comparan su información de accesibilidad con la información de su socio y deciden quién debe estar activo.

Estrategia de recuperación

Los roles de las dos máquinas de controlador se configuran como primario y secundario. Durante el arranque, los controladores intercambian información hasta que se sincroniza cada máquina. En este punto, el controlador primario pasa al estado activo y empieza a calcular pesos y a actualizar el conmutador, mientras que la máquina secundaria pasa a estado de espera y supervisa la disponibilidad de la máquina primaria.

Si en cualquier momento la máquina en espera detecta que la máquina activa ha sufrido una anomalía, la máquina en espera asumirá el control de las funciones de equilibrio de carga de la máquina activa (anómala) y pasará a ser la máquina activa. Cuando la máquina primaria vuelve a estar operativa, las dos máquinas determinan qué controlador estará activo según cómo se haya configurado la estrategia de recuperación.

Hay dos tipos de estrategia de recuperación:

Recuperación automática

El controlador primario pasa al estado activo y empieza a calcular y actualizar pesos tan pronto vuelve a estar operativo. La máquina secundaria pasa al estado en espera una vez que la máquina primaria está activa.

Recuperación manual

El controlador secundario activo permanece en estado activo, incluso después de que el controlador primario sea operativo.

El controlador primario pasa al estado en espera y requiere intervención manual para pasar al estado activo.

El parámetro `strategy` debe tener el mismo valor en ambas máquinas.

Ejemplos

Para obtener ejemplos de configuración de alta disponibilidad de Cisco CSS Controller, consulte el apartado “Ejemplos” en la página 441.

Para obtener ejemplos de configuración de alta disponibilidad de Nortel Alteon Controller, consulte el apartado “Ejemplos” en la página 459.

Optimización del equilibrio de carga que proporciona Load Balancer

La función de controlador de Load Balancer lleva a cabo el equilibrio de carga basándose en los siguientes valores:

- “Importancia dada a la información métrica”
- “Pesos” en la página 247
- “Tiempos de inactividad en el cálculo de pesos” en la página 247
- “Tiempos de inactividad del asesor” en la página 249
- “Umbral de sensibilidad” en la página 248

Si lo desea, modifique estos valores para optimizar el equilibrio de carga para la red.

Importancia dada a la información métrica

El controlador puede utilizar algunos de los siguientes recopiladores de métricas o todos cuando se sopesan las decisiones:

- *Conexiones activas*: el número de conexiones activas en cada máquina servidor con equilibrio de carga, que se ha recuperado del conmutador.
- *Velocidad de conexión*: el número de nuevas conexiones establecidas desde la última consulta sobre cada máquina servidor con equilibrio de carga que se ha recuperado del conmutador.
- *CPU*: el porcentaje de la CPU en uso en cada máquina servidor con equilibrio de carga (entrada del agente de Metric Server).
- *Memoria*: el porcentaje de la memoria en uso (entrada del agente de Metric Server) en cada servidor con equilibrio de carga.
- *Métrica de sistema*: la entrada de las herramientas de supervisión del sistema, como Metric Server o WLM.
- *Específico de la aplicación*: la entrada de los asesores que escuchan en el puerto.

La métrica por omisión es `activeconn` y `connrate`.

Puede cambiar la proporción de importancia relativa de los valores de métrica. Piense en las proporciones como si fueran porcentajes; la suma de las proporciones relativas debe ser 100%. Por omisión, se utilizan las conexiones activas y la nueva métrica de conexiones y sus proporciones se fijan en 50/50. Es posible que sea

necesario probar distintas combinaciones de proporciones de métrica en su entorno hasta encontrar la combinación que ofrezca el mejor rendimiento.

Para establecer los valores de proporción:

En Cisco CSS Controller

```
cococontrol ownercontent metrics nombre_métrica1 proporción1  
nombre_métrica2 proporción2
```

En Nortel Alteon Controller

```
nalcontrol service metrics nombre_métrica1 proporción1 nombre_métrica2  
proporción2
```

Pesos

Los pesos se establecen en función del tiempo de respuesta de la aplicación, información procedente de los asesores e información procedente de un programa de supervisión del sistema, como Metric Server. Si desea establecer pesos manualmente, especifique la opción **fixedweight** para el servidor. Para obtener una descripción de la opción **fixedweight**, consulte el apartado “Pesos fijos de controlador”.

Los pesos se aplican a todos los servidores que proporcionan un servicio. Para cualquier servicio concreto, las peticiones se distribuyen entre servidores en función del peso que dichos servidores tienen entre sí. Por ejemplo, si el peso de un servidor se establece en 10 y el de otro en 5, el servidor establecido en 10 debería recibir el doble de peticiones que el servidor establecido en 5.

Si un asesor encuentra que un servidor ha concluido, el peso para el servidor se establece en -1. En Cisco CSS Controller y Nortel Alteon Controller, se informa al conmutador que el servidor no está disponible y el conmutador deja de asignar conexiones al servidor.

Pesos fijos de controlador

Sin el controlador, los asesores no se pueden ejecutar y no pueden detectar si un servidor está inactivo. Si opta por ejecutar los asesores, pero *no* desea que el controlador actualice el peso establecido para un servidor concreto, utilice la opción **fixedweight** en el mandato **cococontrol service** en Cisco CSS Controller o el mandato **nalcontrol server** en Nortel Alteon Controller.

Utilice el mandato **fixedweight** para establecer el peso en el valor que desee. El valor de peso del servidor permanece fijo mientras el controlador se está ejecutando hasta que se emite otro mandato con la opción **fixedweight** establecida en no.

Tiempos de inactividad en el cálculo de pesos

Para optimizar el rendimiento general, puede restringir la frecuencia con la que se recopila la métrica.

El tiempo de inactividad del consultor especifica la frecuencia con la que el consultor actualiza los pesos del servidor. Si el valor de tiempo de inactividad del consultor es demasiado bajo, puede suponer un bajo rendimiento como resultado de que el consultor interrumpe constantemente al conmutador. Si el valor de tiempo de inactividad del consultor es demasiado alto, puede significar que el equilibrio de carga del conmutador no se basará en información actualizada y precisa.

Por ejemplo, para establecer el tiempo de inactividad del consultor en 1 segundo:

```
xxxcontrol consultant set ID_consultor sleeptime intervalo
```

Umbral de sensibilidad

Hay otros métodos disponibles para optimizar el equilibrio de carga para los servidores. Para trabajar a máxima velocidad, sólo se actualizan los pesos de los servidores si dichos pesos han cambiado de una manera significativa. Si se actualizan constantemente los pesos cuando no se produce ningún cambio en el estado del servidor o dicho cambio es muy pequeño, supondrá una carga adicional innecesaria. Cuando el cambio en el porcentaje del peso para el peso total de todos los servidores que proporcionan un servicio es mayor que el umbral de sensibilidad, se actualizan los pesos utilizados por Load Balancer para distribuir las conexiones. Por ejemplo, suponga que el total de los cambios de pesos pasa de 100 a 105. El cambio es del 5%. Con el umbral de sensibilidad por omisión 5, los pesos utilizados por Load Balancer no se actualizan, porque el cambio del porcentaje no está **por encima** del umbral. Sin embargo, si el peso total pasa de 100 a 106, los pesos se actualizan. Para establecer el umbral de sensibilidad del consultor en un valor distinto del valor por omisión, escriba el siguiente mandato:

```
xxxcontrol consultant set ID_consultor sensitivity porcentaje_cambio
```

En la mayoría de los casos, no es necesario cambiar este valor.

Asesores

Los asesores son agentes incluidos en Load Balancer. Su finalidad es evaluar el estado y la carga de las máquinas servidor. Esto lo llevan a cabo con un intercambio parecido a los clientes proactivos con los servidores. Piense en los asesores como clientes ligeros de los servidores de aplicaciones.

Nota: Para obtener una lista detallada de asesores, consulte el apartado “Lista de asesores” en la página 188.

Cómo funcionan los asesores

Los asesores abren periódicamente una conexión TCP con cada servidor y envían un mensaje de petición al servidor. El contenido del mensaje es específico para el protocolo que se ejecuta en el servidor. Por ejemplo, el asesor HTTP envía una petición HTTP “HEAD” al servidor.

Los asesores están a la escucha de la respuesta del servidor. Después de obtener la respuesta, el asesor realiza una evaluación del servidor. Para calcular este valor de *carga*, la mayoría de los asesores calculan el tiempo que el servidor tarda en responder y luego utilizan este valor (en milisegundos) como carga.

A continuación, los asesores notifican el valor de la carga a la función de consultor donde aparece en el informe del consultor. Luego, el consultor calcula los valores de peso total de todas las fuentes, según sus proporciones y envía estos valores del peso al conmutador. El conmutador utiliza estos valores para realizar el equilibrio de carga de nuevas conexiones de cliente entrantes.

Si el asesor determina que un servidor está activo y funciona, notifica al consultor un número de carga positivo distinto de cero. Si el asesor determina que un servidor no está activo, devuelve el valor de carga especial uno negativo (-1) para notificar al conmutador que el servidor está inactivo. Posteriormente, el conmutador no enviará más conexiones a dicho servidor hasta que el servidor no vuelva a estar en funcionamiento.

Tiempos de inactividad del asesor

Nota: Los valores por omisión del asesor funcionan de forma eficaz para la gran mayoría de casos posibles. Preste atención cuando especifique valores distintos a los valores por omisión.

El tiempo de inactividad del asesor establece la frecuencia con la que un asesor solicita el estado de los servidores en el puerto que está supervisando y, a continuación, notifica los resultados al consultor. Si el valor de tiempo de inactividad del asesor es demasiado bajo, puede dar como resultado un bajo rendimiento porque el asesor interrumpe constantemente a los servidores. Si el valor de tiempo de inactividad del asesor es demasiado alto, puede significar que la ponderación de decisiones del consultor no se basa en información actualizada y precisa.

Por ejemplo, para establecer el intervalo en 3 segundos para el asesor HTTP, escriba el siguiente mandato:

```
xxxcontrol metriccollector set ID_consultor:HTTP sleeptime 3
```

Tiempo de espera de conexión y recepción del asesor para los servidores

Puede establecer la cantidad de tiempo que un asesor tarda en detectar que un puerto concreto del servidor o servicio ha sufrido una anomalía. Los valores de tiempo de espera del servidor anómalo, connecttimeout y receivetimeout, determinan cuánto tiempo espera un asesor antes de informar que se ha producido una anomalía en una conexión o recepción.

Para obtener la detección más rápida del servidor anómalo, establezca los tiempos de espera de conexión y recepción en el valor más pequeño (un segundo) y establezca el tiempo de inactividad del consultor y asesor en el valor más pequeño (un segundo).

Nota: Si el volumen de tráfico de la red oscila entre moderado a alto y la respuesta del servidor aumenta, no establezca los valores timeoutconnect y timeoutreceive demasiado bajos. Si estos valores son demasiado pequeños, el asesor puede marcar prematuramente como anómalo un servidor ocupado.

Para establecer timeoutconnect en 9 segundos para el asesor HTTP, escriba el siguiente mandato:

```
xxxcontrol metriccollector set ID_consultor:HTTP timeoutconnect 9
```

El valor por omisión para el tiempo de espera de conexión y recepción es 3 veces el valor especificado para el tiempo de inactividad del asesor.

Reintento del asesor

Los asesores tienen la capacidad de reintentar una conexión antes de marcar un servidor como inactivo. El asesor no marcará un servidor como inactivo hasta que la consulta del servidor haya fallado el número de reintentos más 1. Si no se establece, el valor de reintento toma el valor por omisión que es cero.

En Cisco CSS Controller, especifique el valor **retry** utilizando el mandato **ccocontrol ownercontent set**. Para obtener más información, consulte el apartado “ccocontrol ownercontent — controlar el nombre de propietario y la norma de contenido” en la página 444.

En Nortel Alteon Controller, especifique el valor **retry** utilizando el mandato **nalcontrol service set**. Para obtener más información, consulte el apartado “nalcontrol service — configurar un servicio” en la página 464.

Crear asesores personalizados (personalizables)

Nota: En este apartado **servidor** se utiliza como término genérico para hacer referencia a un servicio de Cisco CSS Controller o a un servidor de Nortel Alteon Controller.

El asesor personalizado (personalizable) es un trozo pequeño de código Java que se proporciona como archivo de clases y es llamado por el código base. El código base proporciona todos los servicios administrativos, como:

- Inicio y detención de una instancia del asesor personalizado
- Suministro de estado e informes
- Registro de información histórica en un archivo de anotaciones cronológicas

También notifica los resultados al consultor. De forma periódica, el código base lleva a cabo un ciclo de asesor, donde evalúa de forma individual todos los servidores en su configuración. Empieza abriendo una conexión con una máquina servidor. Si se abre el socket, el código base llama al método `getLoad` (función) en el asesor personalizado. A continuación, el asesor personalizado llevará a cabo los pasos necesarios para evaluar el estado del servidor. En general, envía al servidor un mensaje definido por el usuario y luego espera una respuesta. (Se proporciona acceso al socket abierto para el asesor personalizado). A continuación, el código base cierra el socket con el servidor y notifica la información de carga al consultor.

El código base y el asesor personalizado puede funcionar en modalidad normal o de sustitución. La selección de la modalidad de operación se especifica en el archivo de asesor personalizado como parámetro en el método del constructor.

En modalidad normal, el asesor personalizado intercambia datos con el servidor y el código del asesor base calcula la duración del intercambio y calcula el valor de carga. A continuación, el código base informa de este valor de carga al consultor. El asesor personalizado sólo necesita devolver un cero (cuando es satisfactorio) o un valor negativo (cuando es erróneo). Para especificar la modalidad normal, el distintivo de sustitución en el constructor se establece en `false`.

En modalidad de sustitución, el código base no lleva a cabo las mediciones de tiempo. El código del asesor personalizado realiza todas las operaciones que desee para sus requisitos exclusivos y, a continuación, devuelve un número de carga real. El código base aceptará el número y lo notificará al consultor. Para obtener los mejores resultados, normalice el número de carga entre 10 y 1000, en donde 10 representa un servidor rápido y 1000 representa un servidor lento. Para especificar la modalidad de sustitución, el distintivo de sustitución en el constructor se establece en `true`.

Con esta característica, puede escribir sus propios asesores de forma que proporcionen la información exacta que necesite sobre los servidores. Se proporciona un asesor personalizado de ejemplo para los controladores, **ADV_ctlrsample.java**. Después de instalar Load Balancer, puede encontrar el código de ejemplo en el directorio de instalación `...ibm/edge/lb/servers/samples/CustomAdvisors`.

Los directorios de instalación por omisión son:

- Sistemas AIX, HP-UX, Linux, Solaris: /opt/ibm/edge/lb
- Sistemas Windows: C:\Archivos de programa\IBM\ibm\edge\lb

Nota: Si añade un asesor personalizado a Cisco CSS Controller o Nortel Alteon Controller, debe detener y después reiniciar **ccoserver** o **nalserver** (en sistemas Windows, utilice Servicios) para que el proceso Java pueda leer los nuevos archivos de clase de asesor personalizado. Los archivos de clase de asesor personalizado sólo se cargan durante el arranque.

Convenio de denominación

El nombre de archivo de asesor personalizado debe tener el formato *ADV_miasesor.java*. Debe empezar con el prefijo *ADV_* en mayúsculas. Todos los caracteres subsiguientes deben indicarse en minúsculas.

Según los convenios Java, el nombre de la clase definida dentro del archivo debe coincidir con el nombre del archivo. Si copia el código de ejemplo, asegúrese de cambiar todas las instancias de *ADV_ctrlsample* dentro del archivo por el nuevo nombre de clase.

Compilación

Los asesores personalizados se escriben en lenguaje Java. Utilice el compilador Java que se instala con Load Balancer. Durante la compilación aparecen referenciados los siguientes archivos:

- El archivo de asesor personalizado
- El archivo de clases base, *ibmlb.jar*, que se encuentra en el directorio de instalación **...ibm/edge/lb/servers/lib**.

La classpath debe apuntar al archivo de asesor personalizado y el archivo de clases base durante la compilación.

En la plataforma Windows, un mandato de compilación puede ser parecido al siguiente:

```
dir_instalación/java/bin/javac -classpath  
dir_instalación\lb\servers\lib\ibmlb.jar ADV_pam.java
```

donde:

- El archivo del asesor se denomina *ADV_pam.java*
- El archivo del asesor se almacena en el directorio actual

La salida de la compilación está en un archivo de clases; por ejemplo:

ADV_pam.class

Antes de iniciar el asesor, copie el archivo de clases en el directorio de instalación **...ibm/edge/lb/servers/lib/CustomAdvisors**.

Nota: Si lo desea, los asesores personalizados pueden compilarse en un sistema operativo y ejecutarse en otro. Por ejemplo, puede compilar el asesor en sistemas Windows, copiar el archivo de clase (en binario) en una máquina AIX y ejecutar aquí el asesor personalizado.

En sistemas AIX, HP-UX, Linux y Solaris, la sintaxis es parecida.

Ejecución

Para ejecutar el asesor personalizado, primero debe copiar el archivo de clases en el directorio de instalación adecuado:

```
...ibm/edge/lb/servers/lib/CustomAdvisors/ADV_pam.class
```

Inicie el consultor y luego emita este mandato para iniciar el asesor personalizado:

En Cisco CSS Controller

```
cococontrol ownercontent metrics ID_consultor:ID_contenido_propietario pam  
100
```

En Nortel Alteon Controller

```
nalcontrol service metrics ID_consultor:ID_servicio pam 100
```

donde:

- pam es el nombre del asesor, como en ADV_pam.java
- 100 es la proporción del peso dado a este asesor

Rutinas necesarias

Como todos los asesores, un asesor personalizado amplía la función del asesor base, denominada ADV_Base. Se trata de la base del asesor que en realidad efectúa la mayoría de las funciones del asesor, como informar de las cargas al consultor para que se utilicen en el algoritmo de peso del consultor. La base del asesor también realiza operaciones de conexión y cierre de sockets, y proporciona métodos de envío y recepción para que el asesor los utilice. El asesor sólo se utiliza para enviar datos y recibir datos en el puerto del servidor que se está asesorando. Para calcular la carga, se calcula la duración de los métodos TCP incluidos en la base del asesor. Un distintivo incluido en el constructor en ADV_base escribe encima de la carga existente la nueva carga devuelta desde el asesor, si se desea.

Nota: La base del asesor proporciona la carga al algoritmo de peso a intervalos especificados en función de un valor fijado en el constructor. Si el asesor real no se ha completado y no puede devolver una carga válida, la base del asesor utiliza la carga anterior.

A continuación se indican los métodos de clase base:

- Una rutina **constructor**. El constructor llama al constructor de clase base (consulte el archivo de asesor de ejemplo)
- Un método **ADV_AdvisorInitialize**. Este método proporciona un enlace por si fuera necesario realizar pasos adicionales después de que la clase base finalice su inicialización.
- Una rutina **getLoad**. La clase de asesor base lleva a cabo la apertura del socket; por lo tanto, getLoad sólo necesita emitir las peticiones de envío y recepción para completar el ciclo del asesor.

Orden de búsqueda

En primer lugar, los controladores examinan la lista de asesores nativos que se proporciona; si no encuentran un asesor específico en la lista, consultarán la lista de asesores personalizados.

Denominación y vía de acceso

- La clase de asesor personalizado debe estar dentro del subdirectorio de **...ibm/edge/lb/servers/lib/CustomAdvisors/** en el directorio base de Load Balancer. Los valores por omisión para este directorio varían según el sistema operativo:
 - Sistemas AIX, HP-UX, Linux o Solaris
`/opt/ibm/edge/lb/servers/lib/CustomAdvisors/`
 - Sistemas Windows
`C:\Archivos de programa\IBM\edge\lb\servers\lib\CustomAdvisors`
- Sólo se permiten caracteres alfabéticos en minúsculas. Esto excluye la sensibilidad a mayúsculas y minúsculas cuando un operador entra los mandatos en la línea de mandatos. El nombre de archivo de asesor debe tener el prefijo **ADV_**.

Asesor de ejemplo

La lista de programas de un asesor de ejemplo del controlador se incluye en “Asesor de ejemplo” en la página 485. Después de la instalación, este asesor de ejemplo puede encontrarse en el directorio **...ibm/edge/lb/servers/samples/CustomAdvisors** .

Metric Server

Metric Server proporciona información de carga de servidor para Load Balancer en la forma de métricas específicas del sistema que notifica el estado de los servidores. El consultor de Load Balancer consulta el agente de Metric Server que residen en cada uno de los servidores, asignado pesos al proceso de equilibrio de carga utilizando la métrica recopilada desde los agentes. Los resultados también aparecen en el informe de servicio de Cisco CSS Controller o en el informe de servidor de Nortel Alteon Controller.

Requisitos previos

El agente de Metric Server debe estar instalado y en ejecución en todos los servidores en los que se está realizando el equilibrio de carga.

Cómo utilizar Metric Server

A continuación se muestran los pasos para configurar Metric Server para los controladores.

- En el controlador
 1. Inicie **ccoserver** o **nalserver**.
 2. En Cisco CSS Controller, añada un consultor de conmutador y añada el contenido de propietario.
En Nortel Alteon Controller, añada un consultor de conmutador y añada un servicio.
 3. Especifique el puerto en el que escucha el agente de Metric Server. Éste debe coincidir con la información especificada en el archivo `metricserver.cmd`. El valor por omisión es 10004. Utilice el siguiente mandato:

En Cisco CSS Controller

```
cctocontrol service set ID_consultor:ID_contenido_propietario:ID_servidor  
metricserverport número_puerto
```

En Nortel Alteon Controller

```
nalcontrol server set ID_consultor:ID_servicio:ID_servidor  
metricserverport número_puerto
```

4. Emita el mandato de métrica del sistema:

En Cisco CSS Controller

```
ccocontrol ownercontent metrics ID_consultor:ID_contenido_propietario  
nombre_métrica importancia
```

En Nortel Alteon Controller

```
nalcontrol service metrics ID_consultor:ID_servicio nombre_métrica  
importancia
```

donde *nombre_métrica* es el nombre del script de Metric Server.

El script de métrica del sistema reside en el servidor de programa de fondo y se ejecuta en cada uno de los servidores que se encuentran en la configuración bajo el servicio o contenido de propietario especificado. Se proporcionan dos scripts, **cpuload** y **memload** o puede crear scripts de métrica de sistema personalizados. El script contiene un mandato que debe devolver un valor numérico. Este valor numérico representa una medida de carga, no un valor de disponibilidad.

Limitación: en sistemas Windows, si la extensión del nombre del script de métrica del sistema es distinta de .exe, debe especificar el nombre completo del archivo; por ejemplo, miScriptSistema.bat. Se trata de una limitación del código Java.

5. Emita el mandato para el controlador como se indica a continuación:

En Cisco CSS Controller

```
ccocontrol consultant start
```

En Nortel Alteon Controller

```
nalcontrol consultant start
```

Nota: Habilite la seguridad:

- En la máquina del controlador, cree archivos de claves con el mandato **lbkeys create**. Consulte el apartado “RMI (Remote Method Invocation)” en la página 262 para obtener más información sobre lbkeys.
 - En la máquina servidor, copie el archivo de claves resultante en el directorio **...ibm/edge/lb/admin/key**. Verifique que los permisos del archivo de claves permitan al usuario root leer el archivo.
- Agente de Metric Server (máquina servidor)
 1. Instale el paquete de Metric Server en la instalación de Load Balancer.
 2. Examine el script **metricserver** que está en el directorio **/usr/bin** para verificar que se están utilizando el puerto RMI que desee. (En sistemas Windows, el directorio C:\WINNT\SYSTEM32). El puerto RMI por omisión es 10004.

Nota: El valor de puerto RMI especificado debe ser el mismo que el valor del puerto RMI para Metric Server en la máquina de controlador.

3. Se proporcionan los dos scripts siguientes: **cpuload** (devuelve el porcentaje de CPU en uso que oscila entre 0 y 100) y **memload** (devuelve el porcentaje de la memoria en uso que oscila entre 0 y 100). Estos scripts residen en el directorio **...ibm/edge/lb/ms/script**.

De manera opcional, puede escribir sus propios archivos de script de métrica personalizados que definan el mandato que Metric Server emitirá en las

máquinas de servidor. Asegúrese de que todos los script personalizados son ejecutables y que están en el directorio **...ibm/edge/lb/ms/script**. Los scripts personalizados **deben** devolver un valor de carga numérico.

Nota: Un script de métrica personalizada debe ser un script o programa válido con una extensión **.bat** o **.cmd**. De forma específica, en Sistemas Linux y UNIX los scripts deben empezar con la declaración del shell; de lo contrario, es posible que no se ejecuten correctamente.

4. Inicie el agente emitiendo el mandato **metricserver**.
5. Para detener el agente de Metric Server, escriba **metricserver stop**.

Para que Metric Server se ejecute en una dirección distinta del sistema principal local, edite el archivo **metricserver** en la máquina servidor con equilibrio de carga. En el archivo **metricserver**, inserte lo siguiente después de **java**:

```
-Djava.rmi.server.hostname=OTRA_DIRECCIÓN
```

Además, añada **hostname OTRA_DIRECCIÓN** antes de las sentencias **"if"** en el archivo **metricserver**.

En sistemas Windows: cree un alias de **OTRA_DIRECCIÓN** en la pila de Microsoft. Para crear un alias para un dirección en la pila de Microsoft, consulte la página 211.

Asesor del gestor de carga de trabajo

WLM es el código que se ejecuta en sistemas principales MVS. Puede consultarse para saber la carga de la máquina MVS.

Cuando se ha configurado la gestión de carga de trabajo de MVS en el sistema OS/390, los controladores pueden aceptar información de capacidad de WLM y utilizarla en el proceso de carga del sistema. Con el asesor WLM, los controladores abren de forma periódica las conexiones a través del puerto de WLM en cada servidor de la tabla de sistema principal de consultor y aceptar los enteros de capacidad devueltos. Puesto que estos enteros representan la cantidad de capacidad que todavía está disponible y los consultores esperan valores que representan las cargas en cada máquina, el asesor invierte los enteros de capacidad y se sistematizan en valores de carga (por ejemplo, un entero de gran capacidad y un valor de carga pequeño representan un servidor eficaz. Hay varias diferencias importantes entre el asesor WLM y los demás asesores de controlador.

1. Otros asesores abren conexiones para los servidores utilizando el mismo puerto en el que circula el tráfico de cliente normal. El asesor WLM abre conexiones para los servidores utilizando un puerto distinto del que utiliza el tráfico normal. El agente de WLM en cada máquina servidor debe configurarse de modo que escuche en el mismo puerto en el que se inicia el asesor WLM del controlador. El puerto por omisión de WLM es 10007.
2. Junto con el asesor WLM es posible utilizar los dos asesores específicos del protocolo. Los asesores específicos de protocolo sondearán los servidores en sus puertos de tráfico normal y el asesor WLM sondeará la carga del sistema utilizando el puerto WLM.

Utilización del registro cronológico binario para analizar estadísticas de servidor

La característica de registro cronológico en binario permite almacenar información de servidor en archivos binarios. Estos archivos pueden procesarse para analizar la información de servidor que se ha recopilado con el tiempo.

La siguiente información se ha almacenado en las anotaciones cronológicas en binario para cada servidor definido en la configuración.

- padre (ID_contenido_propietario para Cisco CSS Controller; ID_servicio para Nortel Alteon Controller)
- ID de servidor
- dirección de servidor
- puerto de servidor
- peso del servidor
- número de métricas configuradas para este servidor
- lista de valores de métrica

El consultor debe estar en ejecución para anotar información en las anotaciones cronológicas en binario.

Utilice el conjunto de mandatos **xxxcontrol consultant binarylog** para configurar el registro cronológico en binario.

- `binarylog start`
- `binarylog stop`
- `binarylog report`
- `binarylog set interval <segundos>`
- `binarylog set retention <horas>`

La opción `start` inicia el registro cronológico de la información de servidor en anotaciones cronológicas en binario en el directorio `logs`. Al inicio de cada hora se crea un archivo con la fecha y la hora como el nombre del archivo.

La opción `stop` detiene el registro cronológico de la información de servidor en las anotaciones cronológicas en binario. Por omisión, el servicio de anotaciones cronológicas está detenido.

La opción `set interval` controla la frecuencia con la que información se escribe en las anotaciones cronológicas. Cada intervalo del consultor, éste enviará información de servidor al servidor de anotaciones cronológicas. La información se graba en las anotaciones cronológicas sólo cuando hayan transcurrido los segundos especificados en el intervalo de anotaciones cronológicas después de anotarse el último registro en las anotaciones cronológicas. Por omisión, el intervalo de anotaciones cronológicas se establece en 60 segundos.

Los valores del intervalo del consultor y el intervalo de anotaciones cronológicas están relacionados. Puesto que al servidor de anotaciones cronológicas se le proporciona información como máximo a la velocidad indicada por los segundos del intervalo del consultor, si se establece el intervalo de anotaciones cronológicas en un valor inferior al valor del intervalo del consultor en realidad se establece en el mismo valor que el intervalo del consultor.

Esta técnica de registro cronológico permite captar información de servidor en cualquier granularidad. Puede captar todos los cambios realizados en la información del servidor detectados por el consultor para calcular pesos de servidor; sin embargo, es probable que esta cantidad de información no sea necesaria para analizar las tendencias y el uso del servidor. Si se registra información del servidor cada 60 segundos, con el tiempo dispondrá de instantáneas de información del servidor. Si establece el intervalo de anotaciones cronológicas muy bajo puede generar enormes cantidades de datos.

La opción `set retention` controla cuánto tiempo se mantienen los archivos. El servidor de anotaciones cronológicas elimina los archivos de anotaciones cronológicas anteriores a las horas de retención especificadas. Esto sólo sucede si el consultor llama al servidor de anotaciones cronológicas, ya que si se detiene el consultor, no se suprimirán los archivos de anotaciones cronológicas antiguos.

Se proporciona un archivo de mandato y un programa Java en el directorio `...ibm/edge/lb/servers/samples/BinaryLog`. Este ejemplo muestra cómo recuperar toda la información de los archivos de anotaciones cronológicas e imprimirla en la pantalla. Puede personalizar realizar cualquier tipo de análisis que desea con los datos.

A continuación se proporciona un ejemplo de la utilización del programa y script suministrados:

```
xxxlogreport 2002/05/01 8:00 2002/05/01 17:00
```

Esto genera un informe de la información de servidor del controlador para el día 1 de mayo de 2002, de las 8:00 a las 17:00.

Utilización de scripts para generar una alerta o anotar anomalías en el servidor

Load Balancer proporciona salidas de usuario que desencadenan scripts que se pueden personalizar. Puede crear los scripts para realizar acciones automatizadas, como avisar a un administrador cuando se marca que los servidores están inactivos o simplemente anotar el suceso de la anomalía. Los scripts de ejemplo, que puede personalizar, están en el directorio de instalación `...ibm/edge/lb/servers/samples`. Para ejecutar los archivos, cópielos en el directorio `...ibm/edge/lb/servers/bin` y, a continuación, cambie el nombre de cada archivo de acuerdo con las instrucciones incluidas en el script.

Se proporcionan los siguientes scripts de ejemplo, donde **xxx** es **cco** para Cisco CSS Controller y **nal** para Nortel Alteon Controller:

- **xxxserverdown**: el controlador marca un servidor como inactivo.
- **xxxserverUp**: el controlador marca un servidor como activo.
- **xxxallserversdown**: un servicio concreto marca todos los servidores como inactivos.

Parte 8. Administración y resolución de problemas de Load Balancer

Esta parte proporciona información sobre cómo administrar y resolver problemas de Load Balancer. Contiene los capítulos siguientes:

- Capítulo 24, “Operación y gestión de Load Balancer”, en la página 261
- Capítulo 25, “Resolución de problemas”, en la página 281

Capítulo 24. Operación y gestión de Load Balancer

Nota: Cuando lea este capítulo, en los apartados generales que no son específicos de un componente, si *no* utiliza el componente Dispatcher, sustituya "dscontrol" y "dsserver" por lo que se detalla a continuación:

- Para CBR, utilice **cbrcontrol** y **cbrserver**
- Para Site Selector, utilice **sscontrol** y **ssserver**
- Para Cisco CSS Controller, utilice **ccocontrol** y **ccoserver**
- Para Nortel Alteon Controller, utilice **nalcontrol** y **nalserver**

IMPORTANTE: si utiliza la instalación de Load Balancer para IPv4 y IPv6 consulte el Capítulo 8, "Despliegue de Dispatcher en Load Balancer para IPv4 y IPv6", en la página 81 para obtener las limitaciones y diferencias de configuración antes de consultar el contenido de este capítulo.

En este capítulo se describe cómo operar y gestionar Load Balancer e incluye estos apartados:

- "Administración remota de Load Balancer"
 - "RMI (Remote Method Invocation)" en la página 262
 - "Administración basada en la Web" en la página 263
- "Utilización de archivos de anotaciones cronológicas de Load Balancer" en la página 265
 - "Para Dispatcher, CBR y Site Selector" en la página 265
 - "Para Cisco CSS Controller y Nortel Alteon Controller" en la página 267
- "Utilización del componente Dispatcher" en la página 268
 - "Utilización de Simple Network Management Protocol con el componente Dispatcher" en la página 269
- "Utilización del componente CBR (Content Based Routing)" en la página 277
- "Utilización del componente Site Selector" en la página 278
- "Utilización del componente Cisco CSS Controller" en la página 278
- "Utilización del componente Nortel Alteon Controller" en la página 279

Administración remota de Load Balancer

Load Balancer proporciona dos modos distintos de ejecutar los programas de configuración en una máquina aparte de aquella en la que reside Load Balancer. La comunicación entre los programas de configuración (dscontrol, cbrcontrol, sscontrol, ccocontrol, nalcontrol) y el servidor (dsserver, cbrserver, etc.) se puede realizar utilizando uno de estos métodos:

- Java RMI (Remote Method Invocation)
- Administración basada en la Web

La ventaja de la administración remota utilizando RMI es que el rendimiento es más rápido que la administración basada en la Web.

Las ventajas de utilizar la administración basada en la Web es que proporciona administración remota, autenticada y segura y se puede comunicar con la máquina Load Balancer aún cuando esté presente un cortafuegos. Además, este método de

administración *no* requiere la instalación y el uso de claves de autenticación (lbkeys) en la máquina cliente remota que se comunica con la máquina Load Balancer.

RMI (Remote Method Invocation)

Para RMI, el mandato para conectar con una máquina de Load Balancer para la administración remota es **dscontrol host:sistema_principal_remoto**.

Si la llamada a RMI procede de una máquina que no sea la máquina local, debe producirse una secuencia de autenticación de clave pública/privada antes de que sea aceptado el mandato de configuración.

La comunicación entre los programas de control que se ejecutan en la misma máquina que los servidores del componente no se autentica.

Utilice este mandato para generar claves públicas y privadas que se van a utilizar para autenticación remota:

lbkeys [create | delete]

Este mandato se ejecuta sólo en la misma máquina que Load Balancer.

El uso de la opción **create** crea una clave privada en el subdirectorio key del directorio servers (...**ibm/edge/lb/servers/key/**) y crea claves públicas en el subdirectorio keys del directorio admin (...**ibm/edge/lb/admin/keys/**) para cada uno de los componentes de Load Balancer. El nombre de archivo para la clave pública es: *componente-DirecciónServidor-puertoRMI*. Estas claves públicas deben transportarse entonces a los clientes remotos y colocarse en el subdirectorio keys del directorio admin.

Para una máquina de Load Balancer con la dirección de nombre de sistema principal 10.0.0.25 que utiliza el puerto RMI por omisión para cada componente, el mandato **lbkeys create** genera estos archivos:

- La clave privada: ...**ibm/edge/lb/servers/key/authorization.key**
- Las claves públicas:
 - ...**ibm/edge/lb/admin/keys/dispatcher-10.0.0.25-10099.key**
 - ...**ibm/edge/lb/admin/keys/cbr-10.0.0.25-11099.key**
 - ...**ibm/edge/lb/admin/keys/ss-10.0.0.25-12099.key**
 - ...**ibm/edge/lb/admin/keys/cco-10.0.0.25-13099.key**
 - ...**ibm/edge/lb/admin/keys/na1-10.0.0.25-14099.key**

El conjunto de archivos de administración se ha instalado en otra máquina. Los archivos de clave pública deben ubicarse en el directorio ...**ibm/edge/lb/admin/keys** de la máquina cliente remota.

Ahora se autorizará al cliente remoto para configurar Load Balancer en 10.0.0.25.

Se deben utilizar estas mismas claves en todos los clientes remotos que desea autorizar para configurar Load Balancer en 10.0.0.25.

Si fuera a ejecutar de nuevo el mandato **lbkeys create**, se generaría un nuevo conjunto de claves públicas/privadas. Esto significaría que todos los clientes

remotos que intentaran conectar con las claves anteriores no serían autorizados. La nueva clave tendría que ubicarse en el directorio correcto de los clientes a los que deseara volver a autorizar.

El mandato **lbkeys delete** suprime las claves privadas y públicas en la máquina servidor. Si se suprimen estas claves, no se autorizará a ningún cliente remoto para conectarse con los servidores.

Para los dos mandatos: lbkeys create y lbkeys delete, hay una opción **force**. La opción force suprime las indicaciones del mandato que solicitan si desea sobrescribir o suprimir las claves existentes.

Después de establecer la conexión RMI, puede comunicar entre los programas de configuración utilizando los mandatos: dscontrol, cbrcontrol, sscontrol, ccocontrol, nalcontrol, dswizard, cbrwizard y sswizard desde un indicador de mandatos. También puede configurar Load Balancer mediante la GUI escribiendo lbadm en un indicador de mandatos.

Nota: Debido a cambios en los paquetes de seguridad de la versión Java, las claves de Load Balancer generadas para releases anteriores a v5.1.1 quizá no sean compatibles con las claves del release actual, de modo que debe volver a generar las claves cuando instale un nuevo release.

Administración basada en la Web

Requisitos

Para utilizar administración basada en la Web, se necesita lo siguiente en la **máquina cliente** que realiza la administración remota:

- JRE 1.3.0 (o superiores)
- Si desea información sobre los navegadores soportados, visite la siguiente página Web: <http://www.ibm.com/support/docview.wss?rs=180&uid=swg27006921>

Nota: Si utiliza Netscape, no cambie el tamaño (Minimizar, Maximizar, Restaurar minimizando, etc.) de la ventana del navegador Netscape en la que aparece la GUI de Load Balancer. Dado que Netscape vuelve a cargar una página cada vez que se cambia el tamaño de la ventana del navegador, esto provocará una desconexión del sistema principal. Tendrá que volver a conectar con el sistema principal cada vez que cambie el tamaño de la ventana.

Se necesita lo siguiente en la **máquina de sistema principal** a la que accede para realizar la administración remota basada en la Web:

- Caching Proxy V6
- Perl 5.5 (o superior)

Configuración de Caching Proxy

- Para Caching Proxy, se necesita el programa de utilidad IBM Key Management (iKeyman) u otro programa de utilidad para crear certificados de servidor SSL. (Consulte el manual *Guía de administración de Caching Proxy* para obtener información sobre cómo crear los certificados).
- En la sección "Load Balancer Web-based administration" del archivo de configuración de Caching Proxy (ibmproxy.conf), añada estas directivas después de las definiciones de dominios de protección, pero antes de las normas de correlación:

En sistemas Windows —

```
Protect /lb-admin/lbwebaccess PROT-ADMIN
Exec /lb-admin/lbwebaccess C:\ARCHIV~1\IBM\edge\lb\admin\lbwebaccess.pl
Pass /lb-admin/help/* C:\ARCHIV~1\IBM\edge\lb\admin\help\*
Pass /lb-admin/*.jar C:\ARCHIV~1\IBM\edge\lb\admin\lib\*.jar
Pass /lb-admin/* C:\ARCHIV~1\IBM\edge\lb\admin\*
Pass /documentation/idioma/* C:\ARCHIV~1\IBM\edge\lb\documentation\idioma*
```

donde *idioma* es el subdirectorio de idioma (por ejemplo, en_US)

Para Sistemas Linux y UNIX —

```
Protect /lb-admin/lbwebaccess PROT-ADMIN
Exec /lb-admin/lbwebaccess /opt/ibm/edge/lb/admin/lbwebaccess.pl
Pass /lb-admin/help/* /opt/ibm/edge/lb/admin/help/*
Pass /lb-admin/*.jar /opt/ibm/edge/lb/admin/lib/*.jar
Pass /lb-admin/* /opt/ibm/edge/lb/admin/*
Pass /documentation/idioma/* /opt/ibm/edge/lb/documentation/idioma*
```

Nota: En sistemas HP-UX, en el script lbwebaccess.pl se supone que el binario Perl se ubica en el directorio /usr/bin/. (La primera línea del script contiene #!/usr/bin/perl). Actualice esta vía de acceso al directorio donde esté ubicada la aplicación Perl. Otra opción es crear un enlace simbólico. Por ejemplo, si se instala Perl en /opt/perl/bin/perl, ejecute el mandato:

```
ln -s /opt/perl/bin/perl /usr/bin/perl
```

Ejecución y acceso a la administración basada en la Web

Para ejecutar la administración basada en la Web, debe iniciarse ésta en la máquina de sistema principal de Load Balancer: emita **lbwebaccess** en el indicador de mandatos de la máquina de sistema principal.

También se necesita el ID de usuario y la contraseña para la máquina de sistema principal a la que va a acceder de forma remota. El ID de usuario y la contraseña son los mismos que para la administración de Caching Proxy.

Para presentar la administración basada en la Web de Load Balancer, acceda a esta dirección URL en el navegador Web de la ubicación remota:

```
http://nombre_sistema_principal/lb-admin/lbadmin.html
```

Donde *nombre_sistema_principal* es el nombre de la máquina a la que va a acceder para comunicarse con Load Balancer.

Una vez que se ha cargado la página Web, aparecerá la GUI de Load Balancer en la ventana del navegador para que realice la administración remota basada en la Web.

Desde la GUI de Load Balancer, también puede emitir mandatos de control de configuración. Para emitir un mandato desde la GUI:

1. Resalte el nodo de sistema principal en el árbol de la GUI
2. Seleccione **Enviar mandato...** en el menú emergente del sistema principal
3. En el campo de entrada de mandatos, escriba el mandato que desea ejecutar. Por ejemplo: **executor report**. El resultado y el historial de los mandatos que se ejecutan en la sesión actual aparece en la ventana que se proporciona.

Renovación de la configuración de forma remota

Con la administración remota basada en la Web, si hay varios administradores actualizando la configuración de Load Balancer desde otras ubicaciones, tendrá que renovar la configuración para consultar (por ejemplo) el clúster, el puerto o el servidor que otro administrador ha añadido (o suprimido). La GUI de administración remota basada en la Web proporciona una función de **Renovar configuración** y **Renovar todas las configuraciones**.

Desde la GUI basada en la Web, para renovar la configuración

- De un sistema principal: pulse con el botón derecho del ratón en un nodo de **sistema principal** de la estructura de árbol de la GUI y seleccione **Renovar configuración**
- De todos los sistemas principales: seleccione **Archivo** del menú y a continuación **Renovar todas las configuraciones**

Utilización de archivos de anotaciones cronológicas de Load Balancer

Para Dispatcher, CBR y Site Selector

Load Balancer envía entradas a un archivo de anotaciones cronológicas de: el servidor, el gestor y el supervisor de métrica (que anota las comunicaciones con agentes Metric Server) así como a un archivo de anotaciones cronológicas para cada asesor que utiliza.

Nota: De forma adicional, sólo para el componente Dispatcher, se pueden realizar las entradas a un archivo de anotaciones cronológicas de subagente (SNMP).

Nota: El componente CBR (Content Based Routing) está disponible en todas las plataformas excepto donde se ejecuta la JVM de 64 bits. De modo alternativo, puede utilizar el método de reenvío cbr del componente Dispatcher de Load Balancer para proporcionar direccionamiento basado en contenido sin utilizar Caching Proxy. Si desea más información, consulte el apartado “Direccionamiento basado en contenido de Dispatcher (método de reenvío cbr)” en la página 55.

Puede establecer el nivel de anotaciones para definir la expansividad de los mensajes grabados en el archivo de anotaciones cronológicas. En el nivel 0, se anotan los errores y Load Balancer también anota las cabeceras y los registros de sucesos que suceden sólo una vez (por ejemplo, un mensaje sobre un asesor que se empieza a grabar en el archivo de anotaciones cronológicas del gestor). El nivel 1 incluye la información en curso y, así sucesivamente, con el nivel 5 incluyendo todos los mensajes producidos para ayudar a depurar un problema si es necesario. El valor por omisión de los archivos de anotaciones cronológicas de: el gestor, el asesor, el servidor o el subagente es 1.

También puede establecer el tamaño máximo de un archivo de anotaciones cronológicas. Cuando se establece un tamaño máximo para el archivo de anotaciones cronológicas, el texto del archivo vuelve al principio; es decir, cuando el archivo alcanza el tamaño especificado, las entradas subsiguientes se anotarán al principio del archivo y se grabarán encima de las entradas de anotaciones cronológicas anteriores. No puede establecer el tamaño de archivo de anotaciones cronológicas en un valor que sea menor que el actual. Las entradas del archivo de anotaciones cronológicas llevarán la indicación de la hora, para que pueda indicar el orden en el que se han grabado.

Cuanto más alto establezca el nivel de anotaciones, debería escoger con más cuidado el tamaño de archivo de anotaciones cronológicas. En el nivel 0, probablemente sea seguro dejar el tamaño de archivo de anotaciones cronológicas con el valor por omisión de 1 MB; no obstante, cuando realiza las anotaciones a nivel 3 y superior, limite el tamaño sin hacerlo demasiado pequeño para que resulte de utilidad.

- Para configurar el nivel de anotaciones o el tamaño máximo de archivo de anotaciones cronológicas de un archivo de anotaciones cronológicas del servidor, utilice el mandato **dscontrol set**. (Para mostrar los valores del archivo de anotaciones cronológicas del servidor, utilice el mandato **dscontrol logstatus**).
- Para configurar el nivel de anotaciones o el tamaño máximo de archivo de anotaciones cronológicas de un archivo de anotaciones cronológicas del gestor, utilice el mandato **dscontrol manager**.
- Para configurar el nivel de anotaciones o el tamaño máximo de archivo de anotaciones cronológicas de un archivo de anotaciones cronológicas del supervisor de métrica que anota la comunicación con agentes Metric Server, utilice el mandato **dscontrol manager metric set**.
- Para configurar el nivel de anotaciones o el tamaño máximo de archivo de anotaciones cronológicas de un archivo de anotaciones cronológicas del asesor, utilice el mandato **dscontrol advisor**.
- Para configurar el nivel de anotaciones o el tamaño máximo de archivo de anotaciones cronológicas de un archivo de anotaciones cronológicas del subagente, utilice el mandato **dscontrol subagent**. (Sólo el componente Dispatcher utiliza el subagente SNMP).

Cambio de las vías de acceso del archivo de anotaciones cronológicas

Por omisión, los archivos de anotaciones cronológicas generados por Load Balancer se almacenan en el directorio logs de la instalación de Load Balancer. Para cambiar esta vía de acceso, establezca la variable *lb_logdir* en el script dsserver.

Sistemas AIX, HP-UX, Linux y Solaris: el script dsserver se encuentra en el directorio /usr/bin. En este script, la variable *lb_logdir* está establecida en el directorio por omisión. Puede modificar esta variable para especificar su directorio de archivo de anotaciones cronológicas. Ejemplo:

```
LB_LOGDIR=/víaAcceso/a/mis/anotaciones/
```

Sistemas Windows: el archivo dsserver se encuentra en el directorio del sistema Windows C:\WINNT\SYSTEM32, para Windows 2003. En el archivo dsserver, la variable *lb_logdir* está establecida en el directorio por omisión. Puede modificar esta variable para especificar su directorio de archivo de anotaciones cronológicas. Ejemplo:

```
set LB_LOGDIR=c:\víaAcceso\A\mis\anotaciones\
```

Para todos los sistemas operativos, asegúrese de que no haya espacios a ambos lados del signo igual y que la vía de acceso finaliza con una barra inclinada o invertida ("/" o "\") según sea adecuado.

Anotaciones en binario

Nota: Las anotaciones cronológicas binarias no se aplican al componente Site Selector.

La característica de anotaciones cronológicas binarias de Load Balancer utiliza el mismo directorio de anotaciones cronológicas que los demás archivos de anotaciones cronológicas. Consulte el apartado “Utilización del registro cronológico binario para analizar estadísticas de servidor” en la página 241.

Para Cisco CSS Controller y Nortel Alteon Controller

Puede establecer el nivel de anotaciones para definir la expansividad de los mensajes grabados en el archivo de anotaciones cronológicas. En el nivel 0, se anotan los errores y Load Balancer anota también las cabeceras y los registros de sucesos que suceden sólo una vez (por ejemplo, un mensaje sobre un asesor que se empieza a grabar en el archivo de anotaciones cronológicas del consultor). El nivel 1 incluye la información en curso y, así sucesivamente, con el nivel 5 incluyendo todos los mensajes producidos para ayudar a depurar un problema si es necesario. El valor por omisión para los archivos de anotaciones cronológicas es 1.

También puede establecer el tamaño máximo de un archivo de anotaciones cronológicas. Si establece un tamaño máximo para el archivo de anotaciones cronológicas, el archivo se envolverá; cuando el archivo alcance el tamaño especificado, las entradas subsiguientes se grabarán al principio del archivo, sobrescribiendo las entradas del archivo de anotaciones cronológicas anteriores. No puede establecer el tamaño de archivo de anotaciones cronológicas en un valor que sea menor que el actual. Las entradas del archivo de anotaciones cronológicas llevarán la indicación de la hora, para que pueda indicar el orden en el que se han grabado.

Cuanto más alto establezca el nivel de anotaciones, debería escoger con más cuidado el tamaño de archivo de anotaciones cronológicas. En el nivel 0, probablemente sea seguro dejar el tamaño de archivo de anotaciones cronológicas con el valor por omisión de 1MB; no obstante, cuando realiza las anotaciones a nivel 3 y superior, limite el tamaño sin hacerlo demasiado pequeño para que resulte de utilidad.

Archivo de anotaciones cronológicas del controlador

Cisco CSS Controller y Nortel Alteon Controller tienen anotaciones cronológicas como se detalla a continuación:

- Anotaciones cronológicas controller (mandato **controller set**)
- Anotaciones cronológicas consultant (mandato **consultant set**)
- Anotaciones cronológicas highavailability (mandato **highavailability set**)
- Anotaciones cronológicas metriccollector (mandato **metriccollector set**)
- Anotaciones cronológicas binary (mandato **consultant binarylog**)

A continuación figura un ejemplo de cómo configurar el nivel de anotaciones y el tamaño máximo de las anotaciones cronológicas para el archivo de anotaciones cronológicas del supervisor de métrica que anota las comunicaciones con agentes Metric Server:

```
xxxcontrol metriccollector set IDconsultor:IDservicio:nombreMétrica  
loglevel x logsize y
```

Cambio de las vías de acceso del archivo de anotaciones cronológicas

Por omisión, las anotaciones cronológicas generadas por los controladores se almacenarán en el directorio logs de la instalación del controlador. Para cambiar esta vía de acceso, establezca la variable `xxx_logdir` en el script `xxxserver`.

Sistemas AIX, HP-UX, Linux y Solaris: el script `xxxserver` se encuentra en el directorio `/usr/bin`. En este script, la variable `xxx_logdir` está establecida en el directorio por omisión. Puede modificar esta variable para especificar su directorio de archivo de anotaciones cronológicas. Ejemplo:

```
xxx_LOGDIR=/víaAcceso/a/mis/anotaciones/
```

Sistemas Windows: el archivo `xxxserver` se encuentra en el directorio del sistema Windows, normalmente `C:\WINNT\SYSTEM32`. En el archivo `xxxserver`, la variable `xxx_logdir` está establecida en el directorio por omisión. Puede modificar esta variable para especificar su directorio de archivo de anotaciones cronológicas. Ejemplo:

```
set xxx_LOGDIR=c:\víaAcceso\mis\anotaciones\
```

Para todos los sistemas operativos, asegúrese de que no haya espacios a ambos lados del signo igual y que la vía de acceso finaliza con una barra inclinada o invertida ("`/`" o "`\`") según sea adecuado.

Anotaciones en binario

La característica de anotaciones cronológicas binarias de Load Balancer utiliza el mismo directorio de anotaciones cronológicas que los demás archivos de anotaciones cronológicas. Consulte el apartado "Utilización del registro cronológico binario para analizar estadísticas de servidor" en la página 241.

Utilización del componente Dispatcher

En este apartado se describe cómo operar y gestionar el componente Dispatcher.

Inicio y detención de Dispatcher

- Escriba **`dsserver`** en la línea de mandatos para iniciar Dispatcher.
- Escriba **`dsserver stop`** en la línea de mandatos para detener Dispatcher.

Utilización del valor de tiempo de espera sin actividad

Para Load Balancer, se considera que las conexiones están inactivas cuando no ha habido actividad en esa conexión durante el número de segundos especificado en el tiempo de espera sin actividad. Cuando se supere el número de segundos sin actividad, Load Balancer eliminará ese registro de conexión de sus tablas y se descartará el tráfico subsiguiente para esa conexión.

A nivel de puerto, por ejemplo, puede especificar el valor de tiempo de espera sin actividad en el mandato **`dscontrol port set staletimeout`**.

El tiempo de espera sin actividad se puede establecer a nivel de ejecutor, clúster y puerto. A nivel de ejecutor y de clúster, el valor por omisión son 300 segundos y se filtra hasta el puerto. A nivel de puerto, el valor por omisión depende del puerto. Algunos puertos bien definidos tienen valores distintos de tiempo de espera sin actividad. Por ejemplo, el puerto telnet 23 tiene un valor por omisión de 259,200 segundos.

Algunos servicios también pueden tener valores de tiempo de espera sin actividad propios. Por ejemplo, LDAP (Lightweight Directory Access Protocol) tiene un parámetro de configuración denominado `idletimeout`. Cuando se han superado

idletimeout segundos, se forzará el cierre de una conexión de cliente desocupado. También se puede establecer idletimeout en 0, lo que significa que nunca se forzará el cierre de la conexión.

Se pueden producir problemas de conectividad si el valor de tiempo de espera sin actividad de Load Balancer es menor que el valor de tiempo de espera del servicio. En el caso de LDAP, el valor de tiempo de espera sin actividad de Load Balancer toma por omisión 300 segundos. Si no hay actividad en la conexión durante 300 segundos, Load Balancer eliminará el registro de conexión de sus tablas. Si el valor de idletimeout es mayor que 300 segundos (o está establecido en 0), el cliente todavía cree que tiene una conexión con el servidor. Cuando el cliente envía paquetes, Load Balancer los descartará. Esto provocará que se cierre la comunicación de LDAP cuando se realice una petición al servidor. Para evitar este problema, establezca el idletimeout de LDAP en un valor que no sea cero, que sea igual o menor que el valor de tiempo de espera sin actividad de Load Balancer.

Utilización del tiempo de espera de conexiones finalizadas y del tiempo de espera sin actividad con el fin de controlar la limpieza de registros de conexión

Un cliente envía un paquete FIN después de que ha enviado todos sus paquetes, para que el servidor sepa que ha finalizado la transacción. Cuando Dispatcher recibe el paquete FIN, marca la transacción de estado activo a estado FIN. Cuando una transacción se marca como FIN, se puede borrar la memoria reservada para la conexión.

Con el fin de mejorar el rendimiento de la asignación y reutilización del registro de conexión, utilice el mandato **executor set fintimeout** para controlar el período durante el cual Dispatcher conservará conexiones en el estado FIN, activas en las tablas de Dispatcher y aceptando tráfico. Cuando una conexión en el estado FIN supera el **tiempo de espera de conexiones finalizadas**, se eliminará de las tablas de Dispatcher y estará preparada para reutilizarse. Puede cambiar el tiempo de espera de FIN utilizando el mandato **dscontrol executor set fincount**.

Utilice el mandato **dscontrol executor set staletimeout** con el fin de controlar el período durante el que Dispatcher debería conservar conexiones en el estado de establecidas, cuando no se haya visto tráfico activo en las tablas de Dispatcher ni aceptar tráfico. Si desea más información, consulte el apartado “Utilización del valor de tiempo de espera sin actividad” en la página 268.

Informe a la GUI — la opción de menú Supervisar

Se pueden mostrar distintos diagramas según la información del ejecutor y transmitirse al gestor. (La opción de menú Supervisar de la GUI requiere que la función de gestor esté en ejecución):

- Conexiones por segundo por servidor (se podrían mostrar varios servidores en el mismo diagrama)
- Los valores de pesos relativos por servidor en un puerto en particular
- Promedio de duración de la conexión por servidor en un puerto en particular

Utilización de Simple Network Management Protocol con el componente Dispatcher

Un sistema de gestión de red es un programa que se ejecuta continuamente y se utiliza para supervisar, reflejar el estado y controlar una red. El conocido protocolo SNMP (Protocolo simple de gestión de red) para comunicarse con dispositivos en

red, es el estándar de gestión de red actual. Los dispositivos de red normalmente tienen un *agente* SNMP y uno o más subagentes. El agente SNMP se comunica con la *estación de gestión de red* o responde a las peticiones SNMP de línea de mandatos. El *subagente* SNMP recupera y actualiza datos y proporciona esos datos al agente SNMP para comunicarse de nuevo con el solicitante.

Dispatcher proporciona una *Management Information Base* (ibmNetDispatcherMIB) SNMP y un subagente SNMP. Esto permite utilizar cualquier sistema de gestión de red, como — Tivoli NetView, Tivoli Distributed Monitoring o HP OpenView — para supervisar el estado, el rendimiento y la actividad de Dispatcher. Los datos MIB describen el Dispatcher que se va a gestionar y reflejan el estado actual de Dispatcher. MIB se instala en el subdirectorio `..lb/admin/MIB`.

Nota: MIB, ibmNetDispatcherMIB.02, no se cargará con el programa Tivoli NetView xnmloadmib2. Para corregir este problema, ponga como comentario la sección NOTIFICATION-GROUP del MIB. Es decir, inserte "-" delante de la línea "indMibNotifications Group NOTIFICATION-GROUP" y de las 6 líneas que siguen.

El sistema de gestión de red utiliza mandatos GET SNMP para detectar valores de MIB en otras máquinas. Luego el sistema puede notificarle si se han superado los valores de umbral especificados. Usted puede entonces influir en el rendimiento de Dispatcher, modificando los datos de configuración de Dispatcher, para ajustar de forma proactiva o corregir problemas de Dispatcher antes de que se conviertan en caídas de Dispatcher o del servidor Web.

Mandatos y protocolo SNMP

El sistema suele proporcionar un agente SNMP para cada estación de gestión de red. El usuario envía un mandato GET al agente SNMP. A cambio, este agente SNMP envía un mandato GET para recuperar los valores de la variable MIB especificada de un subagente encargado de esas variables MIB.

Dispatcher proporciona un subagente que actualiza y recupera datos MIB. El subagente responde con los datos MIB adecuados cuando el agente SNMP envía un mandato GET. El agente SNMP comunica los datos a la estación de gestión de red. La estación de gestión de red puede notificarle si se han superado los valores de umbral especificados.

El soporte SNMP de Dispatcher incluye un subagente SNMP que utiliza la posibilidad DPI (Distributed Program Interface). DPI es una interfaz entre un agente SNMP y sus subagentes. El sistema operativo Windows utiliza el agente de ampliación de Windows como una interfaz entre el agente SNMP y sus subagentes.

Habilitación de SNMP en sistemas AIX, HP-UX, Linux y Solaris

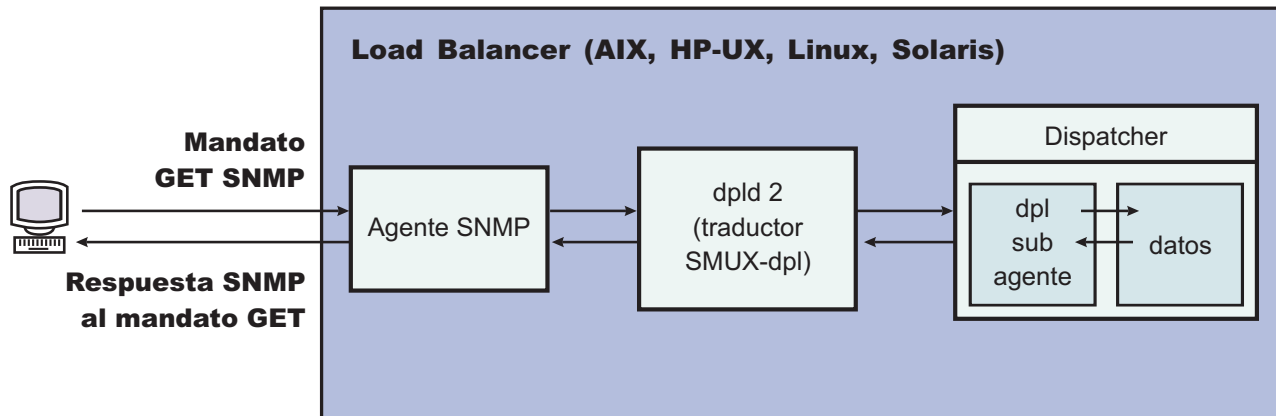


Figura 40. Mandatos SNMP para Sistemas Linux y UNIX

Los sistemas AIX proporcionan un agente SNMP que utiliza el protocolo SMUX (SNMP Multiplexer) y proporciona DPID2, que es un ejecutable adicional que funciona como un conversor entre DPI y SMUX.

En sistemas HP-UX, debe obtener un agente SNMP que sea compatible con SMUX puesto que HP-UX no proporciona ninguno. Load Balancer proporciona DPID2 para sistemas HP-UX.

Los sistemas Linux proporcionan un agente SNMP que utiliza SMUX. La mayoría de las versiones Linux (por ejemplo, Red Hat) vienen con un paquete UCD SNMP. UCD SNMP versión 4.1 o posteriores tienen agentes compatibles con SMUX. Load Balancer proporciona DPID2 para sistemas Linux.

Nota: En sistemas SuSE Linux, debe obtener un agente SNMP que sea compatible con SMUX puesto que SuSE no proporciona ninguno.

En sistemas Solaris, debe obtener un agente SNMP que sea compatible con SMUX puesto que Solaris no proporciona ninguno. Load Balancer proporciona DPID2 para sistemas Solaris. en el directorio /opt/ibm/edge/lb/servers/samples/SNMP.

El agente DPI debe ejecutarse como un usuario root. Antes de ejecutar el daemon de DPID2, actualice el archivo /etc/snmpd.peers y /etc/snmpd.conf como se detalla a continuación:

En sistemas AIX y Solaris:

- En el archivo /etc/snmpd.peers, añada esta entrada para dpid:


```
"dpid2" 1.3.6.1.4.1.2.3.1.2.2.1.1.2 "dpid_password"
```
- En /etc/snmpd.conf, añada esta entrada para dpid:


```
smux 1.3.6.1.4.1.2.3.1.2.2.1.1.2 dpid_password #dpid
```

En sistemas Linux:

- En el archivo /etc/snmpd.peers (si no existe en el sistema cree uno), añada esta entrada para dpid:


```
"dpid2" 1.3.6.1.4.1.2.3.1.2.2.1.1.2 "dpid_password"
```
- En /etc/snmp/snmpd.conf, añada esta entrada para dpid:


```
smuxpeer .1.3.6.1.4.1.2.3.1.2.2.1.1.2 dpid_password
```

Además, debe poner como comentario todas las líneas del archivo `snmpd.conf` que comienzan por estas palabras: `com2sec`, `group`, `view` o `access`.

Habilitar SNMP en sistemas HP-UX

Para instalar el soporte de SNMP de HP-UX:

1. Si no tiene instalada una versión de GNU SED, obténgala del sitio Web de HP, <http://www.hp.com>.
2. Obtenga `ucd-snmp-4.2.4.tar.gz` de la siguiente página Web, http://sourceforge.net/project/showfiles.php?group_id=12694.
3. Asegúrese de que tiene instalado "gcc" y "gmake o make" en su máquina. Si no, deberá instalarlos.
4. Descomprima (`unzip`) el archivo `ucd-snmp-4.2.4.tar.gz` file y, después, desempaquete (`untar`) todos los archivos fuentes en el directorio.
5. Vaya al directorio donde se guardan los archivos fuentes y haga lo siguiente:
 - a. ejecute `./configure --with-mib-modules=smux`
 - b. `make`
 - c. Ejecute los dos mandatos siguientes como root:
 - 1) `umask 022`
 - 2) `make install`
 - d. `export SNMPCONFPATH=/etc/snmp`
 - e. `start /usr/local/sbin/snmpd -s` (Esto inicia el agente SNMP)
 - f. `start dpid2` (Esto inicia el conversor DPI)
 - g. `dscontrol subagent start` (Esto inicia el subagente Dispatcher)

Habilitar SNMP en sistemas SuSE Linux

Para utilizar SNMP de Load Balancer con sistemas SuSE Linux, debe realizar lo siguiente:

1. Quite el `ucd-snmp rpm` instalado de la máquina SuSE.
2. Obtenga `ucd-snmp-4.2.4.tar.gz` de http://sourceforge.net/project/showfiles.php?group_id=12694.
3. Asegúrese de que tiene instalado "gcc" y "gmake o make" en la máquina SuSE (debe instalarlos si no están ahí).
4. Descomprima (`unzip`) el archivo `ucd-snmp-4.2.4.tar.gz` file y, después, desempaquete (`untar`) todos los archivos fuentes en el directorio.
5. Vaya al directorio donde se guardan los archivos fuentes y haga lo siguiente:
 - a. `run ./configure --with-mib-modules=smux`
 - b. `make`
 - c. Ejecute los dos mandatos siguientes como root:
 - 1) `umask 022 #`
 - 2) `make install`
 - d. `export SNMPCONFPATH=/etc/snmp`
 - e. `start /usr/local/sbin/snmpd -s`
 - f. `start dpid2`

Renueve `snmpd` (si aún está en ejecución) para que vuelva a leer el archivo `snmpd.conf`:

```
refresh -s snmpd
```

Inicie el DPID SMUX del igual:

dpid2

Los daemons deben iniciarse en el orden siguiente:

1. Agente SNMP
2. Conversor DPI
3. Subagente Dispatcher

Habilitación de SNMP en sistemas Solaris

Para instalar el soporte de SNMP de Solaris:

1. Elimine el daemon de Solaris SNMP en ejecución (snmpdx y snmpXdmid).
2. Renombre archivos como se detalla a continuación:
`/etc/rc3.d/S76snmpdx` por `/etc/rc3.d/K76snmpdx`
`/etc/rc3.d/S77dmi` por `/etc/rc3.d/K77dmi`
3. Bájese los paquetes siguientes de <http://www.sunfreeware.com/>:
 - libgcc-3.0.3-sol8-sparc-local (SMClibgcc)
 - openssl-0.9.6c-sol8-sparc-local (SMCssl)
 - poprt-1.6.3-sol8-sparc-local (SMCpoprt)
4. Instale los paquetes bajados utilizando pkgadd.
5. Bájese ucd-snmp-4.2.3-solaris8.tar.gz de http://sourceforge.net/project/showfiles.php?group_id=12694
6. Ejecute Gunzip y untar de ucd-snmp-4.2.3-solaris8.tar.gz en el directorio raíz (/)
7. Emita estos mandatos:

```
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH: /usr/local/lib:/usr/local/ssl/lib:/usr/lib
export PATH=/usr/local/sbin:/usr/local/bin:$PATH
export SNMPCONFPATH=/etc/snmp
export MIBDIRS=/usr/local/share/snmp/mibs
cp /opt/ibm/edge/lb/servers/samples/SNMP/dpid2 /usr/local/sbin/dpid2
```
8. Si todavía no existe, cree /etc/snmpd.peers. Inserte lo siguiente en snmpd.peers:

```
"dpid2" 1.3.6.1.4.1.2.3.1.2.2.1.1.2      "dpid_password"
```
9. Si todavía no existe, cree /etc/snmp/snmpd.conf. Inserte lo siguiente en snmpd.conf:

```
smuxpeer      1.3.6.1.4.1.2.3.1.2.2.1.1.2      dpid_password
```
10. Inicie /usr/local/sbin/snmpd.
11. Inicie /usr/local/sbin/dpid2.

Notas:

1. Los paquetes siguientes están en formato de paquete.
 - libgcc-3.0.3-sol8-sparc-local (SMClibgcc)
 - openssl-0.9.6c-sol8-sparc-local (SMCssl)
 - poprt-1.6.3-sol8-sparc-local (SMCpoprt)

En el sitio Web <http://sunfreeware.com/>, los nombres tienen una extensión de .gz, por lo tanto no utilice gunzip/untar con éstos. En su lugar, utilice pkgadd *nombrePaquete*.

2. Cuando añada la entrada smuxpeer en /etc/snmp/snmpd.conf, asegúrese de que no se incluye ningún espacio en la serie **dpid_password**.
3. La característica SNMP de Load Balancer se prueba con ucd-snmp para smux versión 4.2.3. Futuros releases de ucd-snmp con smux deberían funcionar con una configuración similar.

Habilitación de SNMP en el sistema operativo Windows

Para instalar el soporte de SNMP de Windows:

1. Pulse Inicio > Configuración (Windows 2000) > Panel de control > Agregar o quitar programas.
2. Pulse **Agregar o quitar componentes de Windows**.
3. En el Asistente para componentes de Windows, pulse **Herramientas de administración y supervisión** (pero no seleccione ni anule la selección de este recuadro de selección), luego pulse **Detalles**
4. Active el recuadro de selección **SNMP (Protocolo simple de gestión de red)** y pulse Aceptar.
5. Pulse Siguiente.

Provisión de un nombre de comunidad para SNMP

Con el ejecutor en ejecución, utilice el mandato **dscontrol subagent start [nombrecomunidad]** para definir el nombre de comunidad utilizado entre el agente de extensión del SO Windows y el agente SNMP.

IMPORTANTE: En Windows 2003, por omisión SNMP no responde a ningún nombre de comunidad presentado. En tal caso, el subagente SNMP no responderá a ninguna petición SNMP. Para asegurarse de que el subagente SNMP responderá al nombre de comunidad, debe establecer las propiedades del servicio SNMP con el nombre de comunidad adecuado y el sistema o los sistemas principales de destino. Configure las propiedades de seguridad SNMP como se detalla a continuación:

1. Abra Administración de equipos
2. En el árbol de la consola, pulse **Servicios**
3. En el panel de detalles, pulse **Servicio SNMP**
4. En el menú de acción, pulse **Propiedades**
5. En la pestaña Seguridad, bajo Nombres de comunidad aceptados, pulse **Agregar**
6. Bajo Derechos de comunidad, seleccione un nivel de permiso para que este sistema principal procese peticiones SNMP de la comunidad seleccionada (al menos el permiso de **Sólo lectura**)
7. En Nombre de la comunidad, escriba un nombre de comunidad sensible a mayúsculas y minúsculas, el mismo que ha proporcionado al subagente de Load Balancer (nombre de comunidad por omisión: public) y pulse **Agregar**
8. Especifique si va a aceptar o no paquetes SNMP de un sistema principal. Seleccione una de estas opciones:
 - Para aceptar peticiones SNMP de un sistema principal en la red, independientemente de la identidad: pulse **Aceptar paquetes SNMP de cualquier host**. (Con esta opción, una persona o entidad debe verificarse por medio de la autenticación, según unos criterios como la contraseña o el certificado).

- Para limitar la aceptación de paquetes SNMP: pulse **Aceptar paquetes SNMP de estos hosts**, a continuación pulse **Agregar**. Escriba el nombre de sistema principal adecuado, dirección IP o IPX y pulse **Agregar**, después de cada entrada.

9. Reinicie el Servicio SNMP para que el cambio entre en vigor

Condiciones de excepción

SNMP se comunica enviando y recibiendo *condiciones de excepción*, mensajes enviados por dispositivos gestionados para informar de condiciones de excepción o de la aparición de sucesos significativos, como un umbral alcanzado.

El subagente utiliza estas condiciones de excepción:

- indHighAvailStatus
- indSrvrGoneDown
- indDOSAttack
- indDOSAttackDone

La condición de excepción **indHighAvailStatus** anuncia que el valor de la variable de estado de alta disponibilidad (hasState) ha cambiado. Los valores posibles de hasState son:

- idle** Esta máquina equilibra la carga y no intenta establecer contacto con su Dispatcher asociado.
- listen** Acaba de iniciarse la alta disponibilidad y Dispatcher está a la escucha de su asociado.
- active** Esta máquina está equilibrando la carga.
- standby**
Esta máquina está supervisando la máquina activa.
- preempt**
Esta máquina está en un estado transitorio durante el cambio de primaria a reserva.
- elect** Dispatcher está negociando con su asociado respecto a cuál será la primaria o la reserva.
- no_exec**
El ejecutor no está en ejecución

La condición de excepción **indSrvrGoneDown** anuncia que el peso del servidor especificado por la parte csID (ID de clúster), psNum (número de puerto) y ssID (ID de servidor) del identificador de objeto ha alcanzado cero. El último número conocido de conexiones activas del servidor se envía en la condición de excepción. Esta condición de excepción indica que, en lo que puede determinar Dispatcher, se ha quedado inactivo el servidor especificado.

La condición de excepción **indDOSAttack** indica que numhalfopen, el número de conexiones medio abiertas que constan sólo de paquetes SYN, ha superado el umbral maxhalfopen del puerto especificado por la parte csID (ID de clúster) y psNum (número de puerto) del identificador de objeto. El número de servidores configurados en el puerto se envía en la condición de excepción. Esta condición de excepción indica que Load Balancer puede estar experimentando un ataque para rechazo de servicio.

La condición de excepción **indDOSAttackDone** indica que numhalfopen, el número de conexiones medio abiertas que constan sólo de paquetes SYN, ha caído por debajo del umbral maxhalfopen del puerto especificado por la parte csID y psNum del identificador de objeto. El número de servidores configurados en el puerto se envía en la condición de excepción. Cuando Load Balancer determina que ha finalizado el posible ataque para rechazo de servicio, se enviará esta condición de excepción después de que se envíe una condición de excepción indDOSAttack.

Para Sistemas Linux y UNIX, debido a una limitación en la API de SMUX, el identificador de empresa del que se informa en condiciones de excepción del subagente ibmNetDispatcher podría ser el identificador de empresa de dpid2, en lugar del identificador de empresa de ibmNetDispatcher, 1.3.6.1.4.1.2.6.144. No obstante, los programas de utilidad de gestión de SNMP podrán determinar el origen de la condición de excepción porque los datos contendrán un identificador de objeto desde dentro del MIB de ibmNetDispatcher.

Activación y desactivación del soporte de SNMP desde el mandato dscontrol

El mandato **dscontrol subagent start** activa el soporte de SNMP. El mandato **dscontrol subagent stop** desactiva el soporte de SNMP.

Si desea más información sobre el mandato dscontrol, consulte el apartado “dscontrol subagent — configurar subagente SNMP” en la página 400.

Utilización de ipchains o tablas ip para rechazar todo el tráfico con el fin de proteger la máquina de Load Balancer (sistemas Linux)

En el kernel Linux hay incorporado un recurso de cortafuegos llamado ipchains. Cuando Load Balancer e ipchains se ejecutan a la vez, los paquetes los detecta primero Load Balancer y luego los detecta ipchains. Esto permite el uso de ipchains para proteger una máquina de Load Balancer Linux, que podría ser, por ejemplo, una máquina de Load Balancer que se utiliza para equilibrar la carga de los cortafuegos.

Cuando se configuran ipchains o tablas ip restringidas completamente (no se permite el tráfico de entrada ni de salida), la parte de reenvío de paquetes de Load Balancer sigue funcionando normalmente.

Recuerde que *no pueden* utilizarse ipchains y tablas ip para filtrar el tráfico de entrada antes de que se equilibre de carga.

Debe permitirse algún tráfico adicional para que todo el Load Balancer funcione correctamente. Algunos ejemplos de esta comunicación son:

- Los asesores se comunican entre la máquina Load Balancer y los servidores finales.
- Load Balancer ejecuta el mandato ping de las máquinas servidores finales, destinos de alcance y máquinas de Load Balancer de asociados de alta disponibilidad.
- Las interfaces de usuario (interfaz gráfica de usuario, línea de mandatos y asistentes) utilizan RMI.
- Los servidores finales deben responder a mandatos ping de la máquina Load Balancer.

En general, una estrategia de ipchains adecuada para las máquinas Load Balancer es no permitir todo el tráfico, excepto que sea hacia o desde los servidores finales, el Load Balancer de alta disponibilidad de asociados, cualquier destino de alcance o cualquier sistema principal de configuración.

No se recomienda activar tablas ip cuando se ejecuta Load Balancer en el kernel Linux versión 2.4.10.x. La activación en esta versión del kernel Linux puede provocar con el tiempo una disminución del rendimiento.

Para desactivar las tablas ip, enumere los módulos (lsmod) con el fin de comprobar qué módulo utilizan ip_tables e ip_conntrack, luego elimínelas emitiendo rmmod ip_tables y rmmod ip_conntrack. Cuando reinicie la máquina estos módulos se añadirán de nuevo, de modo que tendrá que repetir este paso cada vez que reinicie la máquina.

Para obtener más información, consulte el apartado “Problema: iptables de Linux puede impedir el direccionamiento de paquetes” en la página 325.

Utilización del componente CBR (Content Based Routing)

En este apartado se describe cómo operar y gestionar el componente CBR de Load Balancer.

Nota: El componente CBR (Content Based Routing) está disponible en todas las plataformas excepto donde se ejecuta la JVM de 64 bits. De modo alternativo, puede utilizar el método de reenvío cbr del componente Dispatcher de Load Balancer para proporcionar direccionamiento basado en contenido sin utilizar Caching Proxy. Si desea más información, consulte el apartado “Direccionamiento basado en contenido de Dispatcher (método de reenvío cbr)” en la página 55.

Inicio y detención de CBR

- Escriba **cbrserver** en la línea de mandatos para iniciar CBR.
- Escriba **cbrserver stop** en la línea de mandatos para detener CBR.

CBR y Caching Proxy colaboran utilizando la API del plug-in de Caching Proxy para gestionar peticiones HTTP y HTTPS (SSL). Caching Proxy debe ejecutarse en la misma máquina para que CBR comience a equilibrar la carga de los servidores. Configure CBR y Caching Proxy como se describe en el apartado “Ejemplo de configuración CBR” en la página 118.

Control de CBR

Después de iniciar CBR, puede controlarlo utilizando uno de estos métodos:

- Configure CBR mediante el mandato **cbrcontrol**. La sintaxis completa de este mandato se describe en el Capítulo 27, “Referencia de mandatos para Dispatcher y CBR”, en la página 347. Se enumeran aquí algunos usos de ejemplo.
- Configure CBR utilizando la GUI (interfaz gráfica de usuario). Escriba **lbadm** en la línea de mandatos para abrir la GUI. Consulte el apartado “GUI” en la página 111 para obtener más información sobre cómo configurar CBR utilizando la GUI.

Utilización de archivos de anotaciones cronológicas de CBR

Los archivos de anotaciones cronológicas utilizados por CBR son similares a los que se utilizan en Dispatcher. Para obtener más información, consulte el apartado “Utilización de archivos de anotaciones cronológicas de Load Balancer” en la página 265.

Nota:

En releases anteriores, para CBR podía cambiar la vía de acceso al directorio de archivos de anotaciones cronológicas en el archivo de configuración de Caching Proxy. Ahora puede cambiar la vía de acceso al directorio donde se almacena el archivo de anotaciones cronológicas en el archivo cbrserver. Consulte el apartado “Cambio de las vías de acceso del archivo de anotaciones cronológicas” en la página 267.

Utilización del componente Site Selector

Inicio y detención de Site Selector

- Escriba **sssserver** en la línea de mandatos para iniciar Site Selector.
- Escriba **sssserver stop** en la línea de mandatos para detener Site Selector.

Control de Site Selector

Después de iniciar Site Selector, puede controlarlo utilizando uno de estos métodos:

- Configure Site Selector mediante el mandato **sscontrol**. La sintaxis completa de este mandato se describe en el Capítulo 28, “Referencia de mandatos para Site Selector”, en la página 403. Se enumeran aquí algunos usos de ejemplo.
- Configure Site Selector utilizando la GUI (interfaz gráfica de usuario). Escriba **lbadmin** en la línea de mandatos para abrir la GUI. Consulte el apartado “GUI” en la página 132 para obtener más información sobre cómo configurar Site Selector utilizando la GUI.

Utilización de archivos de anotaciones cronológicas de Site Selector

Los archivos de anotaciones cronológicas utilizados por Site Selector son similares a los que se utilizan en Dispatcher. Para obtener una mayor descripción, consulte el apartado “Utilización de archivos de anotaciones cronológicas de Load Balancer” en la página 265.

Utilización del componente Cisco CSS Controller

Inicio y detención de Cisco CSS Controller

1. Escriba **ccoserver** en la línea de mandatos para iniciar Cisco CSS Controller.
2. Escriba **ccoserver stop** en la línea de mandatos para detener Cisco CSS Controller.

Control de Cisco CSS Controller

Después de iniciar Cisco CSS Controller, puede controlarlo utilizando uno de estos métodos:

- Configure Cisco CSS Controller mediante el mandato **ccocontrol**. La sintaxis completa de este mandato se describe en el Capítulo 29, “Referencia de mandatos para Cisco CSS Controller”, en la página 431. Se enumeran aquí algunos usos de ejemplo.
- Configure Cisco CSS Controller utilizando la GUI (interfaz gráfica de usuario). Escriba **ladmin** en la línea de mandatos para abrir la GUI. Consulte el apartado “GUI” en la página 151 para obtener más información sobre cómo configurar Cisco CSS Controller utilizando la GUI.

Utilización de archivos de anotaciones cronológicas de Cisco CSS Controller

Los archivos de anotaciones cronológicas utilizados por Cisco CSS Controller son similares a los que se utilizan en Dispatcher. Para obtener una mayor descripción, consulte el apartado “Utilización de archivos de anotaciones cronológicas de Load Balancer” en la página 265.

Utilización del componente Nortel Alteon Controller

Inicio y detención de Nortel Alteon Controller

1. Escriba **nalserver** en la línea de mandatos para iniciar Nortel Alteon Controller.
2. Escriba **nalserver stop** en la línea de mandatos para detener Nortel Alteon Controller.

Control de Nortel Alteon Controller

Después de iniciar Nortel Alteon Controller, puede controlarlo utilizando uno de estos métodos:

- Configure Nortel Alteon Controller mediante el mandato **nalcontrol**. La sintaxis completa de este mandato se describe en el Capítulo 30, “Referencia de mandatos para Nortel Alteon Controller”, en la página 449. Se enumeran aquí algunos usos de ejemplo.
- Configure Nortel Alteon Controller utilizando la GUI (interfaz gráfica de usuario). Escriba **ladmin** en la línea de mandatos para abrir la GUI. Consulte el apartado “GUI” en la página 173 para obtener más información sobre cómo configurar Nortel Alteon Controller utilizando la GUI.

Utilización de archivos de anotaciones cronológicas de Nortel Alteon Controller

Los archivos de anotaciones cronológicas utilizados por Nortel Alteon Controller son similares a los que se utilizan en Dispatcher. Para obtener una mayor descripción, consulte el apartado “Utilización de archivos de anotaciones cronológicas de Load Balancer” en la página 265.

Utilización del componente Metric Server

Inicio y detención de Metric Server

Metric Server proporciona información de carga del servidor a Load Balancer. Metric Server reside en cada uno de los servidores de los que se está equilibrando la carga.

Sistema Linux y UNIX:

- En cada máquina servidor donde reside Metric Server, escriba **metricserver start** en la línea de mandatos para iniciar Metric Server.
- En cada máquina servidor donde reside Metric Server, escriba **metricserver stop** en la línea de mandatos para detener Metric Server.

Sistemas Windows:

Pulse Inicio > Configuración (para Windows 2000) > Panel de control > Herramientas administrativas > Servicios. Pulse con el botón derecho del ratón en IBM Metric Server y seleccione Iniciar. Para detener el servicio, efectúe los mismos pasos y seleccione Detener.

Utilización de archivos de anotaciones cronológicas de Metric Server

Cambie el nivel de anotaciones en el script de inicio de Metric Server. Puede especificar un intervalo de nivel de anotaciones de 0 a 5, similar al intervalo de nivel de anotaciones de los archivos de anotaciones cronológicas de Load Balancer. Esto generará un archivo de anotaciones cronológicas agente en el directorio **...ms/logs**.

Capítulo 25. Resolución de problemas

Este capítulo ayuda a detectar y solucionar problemas asociados a Load Balancer.

- Antes de llamar al servicio de IBM, consulte el apartado “Recopilación de información para la resolución de problemas”.
- Busque el síntoma que le ha aparecido en el apartado “Tablas de resolución de problemas” en la página 285.

Recopilación de información para la resolución de problemas

Utilice la información de este apartado para recopilar los datos que requiere el servicio de IBM. La información se divide en los temas siguientes.

- “Información general (siempre es necesaria)”
- “Problemas de alta disponibilidad (HA)” en la página 282
- “Problemas del asesor” en la página 283
- “Problemas de CBR (Content Based Routing)” en la página 284
- “No se puede acceder al clúster” en la página 284
- “Todo lo demás no funciona” en la página 284
- “Actualizaciones” en la página 285
- “Enlaces de utilidad” en la página 285

Información general (siempre es necesaria)

Sólo para el componente Dispatcher, hay una herramienta de determinación de problemas que recopila automáticamente datos específicos del sistema operativo y archivos de configuración específicos del componente. Para ejecutar esta herramienta, escriba **lbpd** en el directorio adecuado:

Para Sistemas Linux y UNIX: /opt/ibm/edge/lb/servers/bin/

En sistemas Windows C:\Archivos de programa\IBM\edge\lb\servers\bin

La herramienta de determinación de problemas empaqueta los datos en archivos como se detalla a continuación:

Para Sistemas Linux y UNIX: /opt/ibm/edge/lb/**lbpmr.tar.Z**

En sistemas Windows: C:\Archivos de programa\IBM\edge\lb**lbpmr.zip**

Nota: Debe tener un programa de utilidad de compresión zip de línea de mandatos para sistemas Windows.

Antes de llamar al servicio de IBM, tenga a mano la información siguiente.

- Sólo para Dispatcher, el archivo **lbpmr** generado por la herramienta de determinación de problemas descrita antes.
- En entornos de alta disponibilidad, los archivos de configuración de las dos máquinas de Load Balancer. En todos los sistemas operativos, utilice el script que utiliza para cargar la configuración o emita este mandato:
`dscontrol file save primary.cfg`
Este mandato sitúa el archivo de configuración en el directorio **.../ibm/edge/lb/servers/configuration/componentel**.
- El sistema operativo que utiliza y la versión de ese sistema operativo.

- La versión de Load Balancer.
 - Si Load Balancer está en ejecución, emita estos mandatos:
 - Para el componente Dispatcher: `dscontrol executor report`
 - Para CBR: `cbrcontrol executor status`
 - Para Site Selector, compruebe el principio del archivo `server.log`, ubicado en `.../ibm/edge/lb/servers/logs/ss/`.
 - Para Cisco CSS Controller y Nortel Alteon Controller: `xxxcontrol controller report`
 - Emita estos mandatos para asegurarse de que está instalado Load Balancer y para obtener el nivel actual de Load Balancer:
 - En sistemas AIX: `lspp -l | grep ibmlb`
 - En sistemas HP-UX: `swlist | grep ibmlb`
 - En sistemas Linux: `rpm -qa | grep ibmlb`
 - En sistemas Solaris: `pkginfo | grep ibm`

En sistemas Windows, para asegurarse de que está instalado Load Balancer: seleccione Inicio > Configuración > Panel de control > Agregar o quitar programas.
- Emita este mandato para obtener el nivel actual de Java:


```
java -fullversion
```
- ¿Utiliza Token Ring o Ethernet?
- Emita uno de estos mandatos para obtener estadísticas de protocolo e información de conexión TCP/IP:
 - En sistemas AIX, HP-UX, Linux y Solaris: `netstat -ni`
 - En sistemas Windows: `ipconfig /all`

Esto se requiere de todos los servidores y de Load Balancer.
- Emita uno de estos mandatos para obtener información de la tabla de ruta:
 - En sistemas AIX, HP-UX, Linux y Solaris: `netstat -nr`
 - En sistemas Windows: `route print`

Esto se requiere de todos los servidores y de Load Balancer.

Problemas de alta disponibilidad (HA)

Recopile la siguiente información necesaria de problemas en entornos de HA.

- Establezca `hamon.log` en el nivel de anotaciones 5: `dscontrol set loglevel 5`.
- Establezca `reach.log` en el nivel de anotaciones 5: `dscontrol manager reach set loglevel 5`.
- Obtenga los scripts, ubicados como se detalla a continuación:

En sistemas AIX, HP-UX, Linux y Solaris: `/opt/ibm/edge/lb/servers/bin`

Sistemas Windows: `C:\Archivos de programa\ibm\edge\lb\servers\bin`

Los nombres de script son:

```
goActive
goStandby
goIdle (si está presente)
goInOp (si está presente)
```

Incluya también los archivos de configuración. Consulte el apartado “Información general (siempre es necesaria)” en la página 281.

Problemas del asesor

Recopile esta información necesaria para problemas del asesor; por ejemplo, cuando los asesores por error marcan los servidores como inactivos.

- Establezca el archivo de anotaciones cronológicas del asesor en el nivel de anotaciones 5:

```
dscontrol advisor loglevel http 80 5
```

o bien

```
dscontrol advisor loglevel nombreAsesor puerto nivelAnotaciones
```

o bien

```
dscontrol advisor loglevel nombreAsesor clúster:puerto nivelAnotaciones
```

o bien

```
nalcontrol metriccollector set IDconsultor:IDservicio:nombreMétrica  
loglevel valor
```

Se creará un archivo de anotaciones cronológicas llamado

ADV_*nombresAsesor*.log; por ejemplo ADV_http.log. Este archivo de anotaciones cronológicas se ubica como se detalla a continuación:

Plataformas AIX, HP-UX, Linux y Solaris: /opt/ibm/edge/lb/servers/logs/*componente*

Plataformas Windows: C:\Archivos de programa\ibm\edge\lb\servers\logs*componente*

Donde *componente* es:

dispatcher = Dispatcher

cbr = CBR (Content Based Routing)

cco = Cisco CSS Controller

nal = Nortel Alteon Controller

ss = Site Selector

Nota: Cuando escribe asesores personalizados, resulta de utilidad utilizar ADVLOG(*nivelAnotaciones,mensaje*) para verificar que el asesor funciona correctamente.

La llamada a ADVLOG imprime sentencias al archivo de anotaciones cronológicas de asesores cuando el nivel es inferior que el nivel de anotaciones asociado a los asesores. Un nivel de anotaciones de 0 provocará que siempre se grabe la sentencia. No puede utilizar ADVLOG desde el constructor. El archivo de anotaciones cronológicas no se crea hasta inmediatamente después de que el constructor haya terminado porque el nombre de archivo de anotaciones cronológicas depende de la información que está establecida en el constructor.

Hay otro modo de depurar el asesor personalizado que evitará esta limitación. Puede utilizar sentencias System.out.println(*mensaje*) para imprimir mensajes a una ventana. Edite el script dserver y cambie javaw por java para que las sentencias de impresión aparezcan en la ventana. La ventana utilizada para iniciar dserver debe mantenerse abierta para que aparezcan las impresiones. Si utiliza plataformas Windows, debe dejar de ejecutar el Dispatcher como un servicio e iniciarlo manualmente desde una ventana para visualizar los mensajes.

Consulte el manual *Guía de programación de Edge Components* para obtener más información sobre ADVLOG.

Problemas de CBR (Content Based Routing)

Recopile la siguiente información necesaria de problemas de CBR (Content Based Routing).

- Emita este mandato para obtener la versión: `cbrcontrol executor status`.
- Obtenga estos archivos:
 - `ibmproxy.conf`, ubicado como se detalla a continuación:
Sistemas Linux y UNIX: `/etc/`
Sistemas Windows: `C:\Archivos de programa\IBM\edge\cp\etc\en_US\`
 - Archivo de configuración de CBR, ubicado como se indica a continuación:
Sistemas Linux y UNIX: `/opt/ibm/edge/lb/servers/configurations/cbr`
Sistemas Windows: `C:\Archivos de programa\IBM\edge\lb\servers\configurations\cbr`
 - Asegúrese de que se crean las entradas correctas en `ibmproxy.conf`. Consulte el apartado “Paso 1. Configurar Caching Proxy para que pueda utilizar CBR” en la página 113.

No se puede acceder al clúster

Si no se puede acceder al clúster, quizá ninguna de las máquinas de Load Balancer haya creado un alias del clúster. Para determinar qué máquina posee el clúster:

1. En la misma subred y *no* en una máquina o servidor de Load Balancer:

```
ping clúster
arp -a
```

Si utiliza los métodos de reenvío `nat` o `cbr` de Dispatcher, ejecute el mandato `ping` de la dirección de retorno también.

2. Repase la salida de `arp` y compare la dirección MAC (dirección hexadecimal de 16-dígitos) con una de las salidas de `netstat -ni` para determinar qué máquina posee físicamente el clúster.
3. Utilice estos mandatos para interpretar la salida de las dos máquinas para comprobar si las dos tienen la dirección del clúster.

En sistemas AIX y HP-UX: `netstat -ni`

En sistemas Linux y Solaris: `ifconfig -a`

En sistemas Windows: `ipconfig /all`

Si no obtiene una respuesta del mandato `ping` y no utiliza ULB, puede que ninguna máquina haya creado el alias de la dirección IP del clúster para su interfaz; por ejemplo, `en0`, `tr0`, etc.

Nota: En sistemas Linux que se ejecutan en una instalación Load Balancer para IPv4 y IPv6, si no obtiene una respuesta del mandato `ping`, únicamente indica que un servidor de programa de fondo no está disponible; no obstante, la entrada `arp` se debe actualizar. Como alternativa, si está disponible se puede utilizar `arping`.

Todo lo demás no funciona

Si no puede solucionar problemas de direccionamiento y todo lo demás no funciona, emita el mandato siguiente para ejecutar un rastreo en el tráfico de red:

- En sistemas AIX, desde la máquina de Load Balancer:
`iptrace -a -s direcciónIPclienteConError -d direcciónIPclúster -b iptrace.trc`

Ejecute el rastreo, vuelva a crear el problema y elimine con el mandato kill el proceso.

- En sistemas HP-UX:

```
tcpdump -i lan0 host clúster y host cliente
```

Quizá tenga que bajarse tcpdump de uno de los sitios de archivadores del software HP-UX GNU.

- En sistemas Linux:

```
tcpdump -i eth0 host clúster y host cliente
```

Ejecute el rastreo, vuelva a crear el problema y elimine con el mandato kill el proceso.

- En Solaris:

```
snoop -v direcciónIPcliente direcciónIPdestino > snooptrace.out
```

- En sistemas Windows, se necesita un capturador. Utilice las mismas entradas que para un filtro.

También puede aumentar distintos niveles de anotaciones (por ejemplo, el archivo de anotaciones cronológicas del gestor o del asesor, etc.) e investigar su salida.

Actualizaciones

Para identificar un problema que ya se ha corregido en un fix pack de release de servicio o en un parche, compruebe las actualizaciones. Para obtener una lista de defectos de Edge Components corregidos, consulte la página de soporte del sitio Web de WebSphere Application Server: <http://www.ibm.com/software/webservers/appserv/was/support/>. Desde la página de soporte, siga el enlace al sitio de descarga del servicio de corrección.

Código Java

Se instalará la versión correcta de Java como parte de la instalación de Load Balancer.

Enlaces de utilidad

Consulte el apartado “Información de consulta” en la página xvii para obtener enlaces a las páginas Web de soporte y de biblioteca. La página Web de soporte contiene un enlace a la información de autoayuda a modo de Notas técnicas.

Tablas de resolución de problemas

Consulte lo siguiente para obtener:

- Información de resolución de problemas de Dispatcher — Tabla 14 en la página 286
- Información de resolución de problemas de CBR — Tabla 15 en la página 292
- Información de resolución de problemas de Site Selector — Tabla 16 en la página 294
- Información de resolución de problemas de Cisco CSS Controller — Tabla 17 en la página 295
- Información de resolución de problemas de Nortel Alteon Controller — Tabla 18 en la página 297
- Información de resolución de problemas de Metric Server — Tabla 19 en la página 298

Tabla 14. Tabla de resolución de problemas de Dispatcher

Síntoma	Causa posible	Vaya a...
Dispatcher no se ejecuta correctamente	Números de puerto en conflicto	"Comprobación de los números de puerto de Dispatcher" en la página 299
Se ha configurado un servidor con ubicación compartida y no responderá a peticiones de equilibrio de carga	Dirección incorrecta o en conflicto con otra	"Problema: no responderán Dispatcher y el servidor" en la página 303
Conexiones de máquinas cliente no atendidas o que han superado el tiempo de espera	<ul style="list-style-type: none"> • Configuración de direccionamiento incorrecta • NIC no ha creado un alias para la dirección del clúster • El servidor no tiene un dispositivo de bucle de retorno con alias para la dirección del clúster • Ruta adicional no suprimida • No se ha definido un puerto para cada clúster 	"Problema: no se equilibran las peticiones de Dispatcher" en la página 303
Máquinas cliente no atendidas o que han superado el tiempo de espera	No funciona la alta disponibilidad	"Problema: la función de alta disponibilidad de Dispatcher no funciona" en la página 304
No se han podido añadir pulsos (plataformas Windows)	La dirección de origen no se ha configurado en un adaptador	"Problema: no se han podido añadir pulsos (plataforma Windows)" en la página 304
El servidor no atiende las peticiones (plataforma Windows)	Se ha creado una ruta adicional en la tabla de direccionamiento	"Problema: rutas adicionales (Windows 2000)" en la página 304
Los asesores no funcionan correctamente con el área amplia	Los asesores no se ejecutan en máquinas remotas	"Problema: los asesores no funcionan correctamente" en la página 304
Dispatcher, Microsoft IIS y SSL no funcionan o no continuarán	No se han podido enviar datos cifrados entre protocolos	"Problema: Dispatcher, Microsoft IIS y SSL no funcionan (plataforma Windows)" en la página 305
Conexión con la máquina remota rechazada	Todavía se utiliza la versión anterior de las claves	"Problema: conexión de Dispatcher con una máquina remota" en la página 305

Tabla 14. Tabla de resolución de problemas de Dispatcher (continuación)

Síntoma	Causa posible	Vaya a...
El mandato dscontrol o lbadmin ha dado un error e indica el mensaje 'El servidor no responde' o 'No es posible acceder al servidor RMI'	<ol style="list-style-type: none"> 1. Los mandatos dan un error debido a una pila con SOCKS. O porque no se inicia dsserver 2. No se han establecido correctamente los puertos RMI 3. El archivo de sistema principal tiene un sistema principal local incorrecto 	"Problema: el mandato dscontrol o lbadmin da un error" en la página 305
Se produce el mensaje de error "No se puede encontrar el archivo..." cuando se ejecuta Netscape como el navegador por omisión para consultar la ayuda en línea (plataforma Windows)	Valor incorrecto para la asociación de archivo HTML	"Problema: aparece el mensaje de error "No se puede encontrar el archivo..." al intentar consultar la ayuda en línea (plataforma Windows)" en la página 306
La interfaz gráfica de usuario no se inicia correctamente	Espacio de paginación insuficiente	"Problema: la GUI (interfaz gráfica de usuario) no se inicia correctamente" en la página 306
Error al ejecutar Dispatcher con Caching Proxy instalado	Dependencia de archivo de Caching Proxy	"Problema: error al ejecutar Dispatcher con Caching Proxy instalado" en la página 306
La interfaz gráfica de usuario no se muestra correctamente.	La resolución es incorrecta.	"Problema: la GUI (interfaz gráfica de usuario) no se muestra correctamente" en la página 306
Los paneles de ayuda a veces desaparecen detrás de otras ventanas	Limitación de Java	"Problema: en la plataforma Windows, las ventanas de ayuda a veces desaparecen detrás de otras ventanas abiertas" en la página 307
Load Balancer no puede procesar y reenviar una trama	Se necesita una dirección MAC única para cada NIC	"Problema: Load Balancer no puede procesar y reenviar una trama" en la página 307
Aparece una pantalla azul	Tarjeta de red no instalada ni configurada	"Problema: se muestra una pantalla azul cuando se inicia el ejecutor de Load Balancer" en la página 307
La vía de acceso al descubrimiento impide el tráfico de retorno	Se ha creado un alias del clúster en el bucle de retorno	"Problema: la vía de acceso al descubrimiento impide el tráfico de retorno con Load Balancer" en la página 307
No funciona la alta disponibilidad de la modalidad de área amplia de Load Balancer.	El Dispatcher remoto debe definirse como un servidor de un clúster en el Dispatcher local	"Problema: no funciona la alta disponibilidad de la modalidad de área amplia de Load Balancer" en la página 308

Tabla 14. Tabla de resolución de problemas de Dispatcher (continuación)

Síntoma	Causa posible	Vaya a...
Se cierra la comunicación de la GUI (o tiene un comportamiento inesperado) cuando se intenta cargar un archivo de configuración de gran tamaño.	Java no tiene acceso a suficiente memoria para gestionar un cambio de tan gran tamaño en la GUI	“Problema: se cierra la comunicación de la GUI (o tiene un comportamiento inesperado) cuando se intenta cargar un archivo de configuración de gran tamaño” en la página 309
Las direcciones IP no se resuelven correctamente en la conexión remota	Cuando se utiliza un cliente remoto en una implementación de SOCKS segura, los nombres de dominio o de sistema principal plenamente cualificados quizá no se resuelvan con la dirección IP correcta	“Problema: las direcciones IP no se resuelven correctamente en la conexión remota” en la página 310
La interfaz de Load Balancer coreana muestra fonts solapados o no deseados en sistemas AIX y Linux	Se deben cambiar los fonts por omisión	“Problema: la interfaz de Load Balancer coreana muestra fonts solapados o no deseados en sistemas AIX y Linux” en la página 310
En sistemas Windows, después de crear un alias del adaptador MS Loopback, cuando emita determinados mandatos como hostname, el sistema operativo responderá incorrectamente con la dirección del alias	En la lista de conexiones de red, no se enumera el alias recién añadido antes de la dirección local	“Problema: en sistemas Windows, se devuelve una dirección del alias en lugar de la dirección local cuando se emiten mandatos como hostname” en la página 310
Comportamiento de la GUI inesperado cuando se utiliza la plataforma Windows con la tarjeta de vídeo Matrox AGP	Se produce un problema cuando se utilizan tarjetas de vídeo Matrox AGP al ejecutar la GUI de Load Balancer	“Problema: en la plataforma Windows, se produce un comportamiento de la GUI inesperado al utilizar tarjetas de vídeo Matrox AGP” en la página 311
Se produce un comportamiento inesperado, por ejemplo, se cierra la comunicación del sistema, cuando se ejecuta “rmmod ibmlb” en sistemas Linux	Se produce un problema cuando se elimina manualmente el módulo kernel de Load Balancer (ibmlb).	“Problema: comportamiento inesperado al ejecutar “rmmod ibmlb” (sistemas Linux)” en la página 311
Tiempo de respuesta lento cuando se ejecutan mandatos en la máquina de Dispatcher	El tiempo de respuesta lento puede deberse a una sobrecarga de la máquina por un alto volumen de tráfico del cliente	“Problema: tiempo de respuesta lento cuando se ejecutan mandatos en la máquina de Dispatcher” en la página 311
Para el método de reenvío mac de Dispatcher, el asesor SSL o HTTPS no registra las cargas del servidor	Se produce el problema porque la aplicación servidor SSL no se ha configurado con la dirección IP del clúster	“Problema: el asesor SSL o HTTPS no registra cargas del servidor (cuando se utiliza el reenvío mac)” en la página 312

Tabla 14. Tabla de resolución de problemas de Dispatcher (continuación)

Síntoma	Causa posible	Vaya a...
Se produce una desconexión del sistema principal cuando se utiliza la administración Web remota mediante Netscape	Se producirá una desconexión del sistema principal cuando se cambie el tamaño de la ventana del navegador	“Problema: se produce una desconexión del sistema principal si se cambia el tamaño de la ventana del navegador Netscape cuando se utiliza la administración Web” en la página 312
Está habilitada la agrupación de sockets y el servidor Web se enlaza a 0.0.0.0	Configure el servidor IIS de Microsoft para que sea específico del enlace	“Problema: está habilitada la agrupación de sockets y el servidor Web se enlaza a 0.0.0.0” en la página 312
En la plataforma Windows, aparecen en el indicador de mandatos caracteres nacionales Latin-1 dañados	Cambie las propiedades de font de la ventana de indicador de mandatos	“Problema: en sistemas Windows, aparecen caracteres nacionales Latin-1 dañados en la ventana de indicador de mandatos” en la página 313
En la plataforma HP-UX, aparece este mensaje: java.lang.OutOfMemoryError unable to create new native thread (java.lang.OutOfMemoryError no se ha podido crear una nueva hebra nativa)	Algunas instalaciones de HP-UX por omisión permiten 64 hebras por proceso. Esto es insuficiente.	“Problema: en HP-UX, se produce un error de falta de memoria/hebra de Java” en la página 313
En la plataforma Windows, los asesores y los destinos de alcance marcan como inactivos todos los servidores	No está inhabilitada Task Offload (Descarga de tareas) o quizá tenga que habilitarse ICMP.	“Problema: en los sistemas Windows, los asesores y los destinos de alcance marcan como inactivos todos los servidores” en la página 313
En la plataforma Windows, se produce un problema al resolver la dirección IP con nombre de sistema principal cuando se configura más de una dirección con un adaptador	La dirección IP que desea como nombre de sistema principal debe aparecer primero en el registro.	“Problema: en la plataforma Windows, se resuelve la dirección IP con el nombre de sistema principal cuando se ha configurado más de una dirección con el adaptador” en la página 314
En la plataforma Windows, los asesores no funcionan en una configuración de alta disponibilidad después de una caída de la red	Cuando el sistema detecta una caída de la red, borra la antememoria ARP (Address Resolution Protocol)	“Problema: en sistemas Windows, después de una caída de la red, los asesores no funcionan en una configuración de alta disponibilidad” en la página 315
En sistemas Linux, el mandato “IP address add” y varios alias de bucle de retorno del clúster son incompatibles	Cuando cree alias para más de una dirección en el dispositivo de bucle de retorno, debería utilizar el mandato ifconfig , no ip address add	“Problema: en sistemas Linux, no utilice el mandato “IP address add” cuando cree un alias de varios clústeres en el dispositivo de bucle de retorno” en la página 316

Tabla 14. Tabla de resolución de problemas de Dispatcher (continuación)

Síntoma	Causa posible	Vaya a...
Aparece el mensaje de error: "dirección del direccionador no especificada o no válida para el método del puerto" al intentar añadir un servidor	Repase la lista de comprobación de información para determinar el problema que se ha producido al añadir un servidor	"Problema: mensaje de error "dirección del direccionador no especificada o no válida para el método del puerto"" en la página 316
En sistemas Solaris, los procesos de Load Balancer finalizan cuando sale de la ventana de la sesión de terminal desde la que se han iniciado	Utilice el mandato nohup para impedir que los procesos que ha iniciado reciban una señal de cierre de comunicación cuando sale de la sesión de terminal.	"Problema: en sistemas Solaris, los procesos de Load Balancer finalizan cuando sale de la ventana de terminal desde la que se han iniciado" en la página 317
Se produce una ralentización cuando se cargan configuraciones de Load Balancer	El retardo puede deberse a llamadas al Sistema de nombres de dominio (DNS) que se realizan para resolver y verificar la dirección de servidor.	"Problema: Se ha producido un retardo al cargar una configuración de Load Balancer" en la página 317
En sistemas Windows, aparece este mensaje de error: Hay un conflicto de dirección IP con otro sistema en la red	Si se configura la alta disponibilidad, podrían configurarse direcciones del clúster en las dos máquinas por un breve período lo que produce que aparezca este mensaje de error.	"Problema: en sistemas Windows, aparece un mensaje de error de conflicto de dirección IP" en la página 317
Las dos máquinas, primaria y de reserva, están activas en una configuración de alta disponibilidad	Este problema podría producirse cuando no se ejecutan los scripts go en alguna de las máquinas primaria o de reserva.	"Problema: las dos máquinas, primaria y de reserva, están activas en una configuración de alta disponibilidad" en la página 318
No se pueden realizar las peticiones del cliente cuando Dispatcher intenta devolver respuestas de páginas de gran tamaño	Las peticiones del cliente que producen unas respuestas de páginas de gran tamaño superan el tiempo de espera si la unidad de transmisión máxima (MTU) no se establece correctamente en la máquina de Dispatcher cuando se utiliza el reenvío nat o cbr.	"Problema: no se pueden realizar las peticiones del cliente cuando el sistema intenta devolver respuestas de páginas de gran tamaño" en la página 318
En sistemas Windows, se produce el error "el servidor no responde" cuando se emite un mandato dscontrol o lbadmin	Cuando existe más de una dirección IP en un sistema Windows y el archivo de sistema principal no especifica la dirección que se va a asociar al nombre de sistema principal.	"Problema: en sistemas Windows, se produce el error "el servidor no responde" cuando se emite dscontrol o lbadmin" en la página 318

Tabla 14. Tabla de resolución de problemas de Dispatcher (continuación)

Síntoma	Causa posible	Vaya a...
Es posible que las máquinas de Dispatcher de alta disponibilidad no se puedan sincronizar en Linux para S/390 en dispositivos qeth	Cuando utiliza la característica de alta disponibilidad en Linux para S/390 con el controlador de red qeth, puede que los Dispatcher activo y en espera no se sincronicen.	“Problema: es posible que las máquinas de Dispatcher de alta disponibilidad no se puedan sincronizar en sistemas Linux para S/390 en controladores qeth” en la página 319
Sugerencias para configurar la característica de alta configuración para Load Balancer	Las sugerencias pueden ayudarle a reducir los problemas de alta disponibilidad como por ejemplo: <ul style="list-style-type: none"> • Conexiones desactivadas después de la toma de control • No se pueden sincronizar máquinas asociadas • Peticiones dirigidas erróneamente a la máquina asociada de reserva 	“Problema: sugerencias para configurar la alta disponibilidad” en la página 319
Limitaciones de configuración de reenvío MAC de Dispatcher con las plataformas zSeries y S/390	En Linux, existen limitaciones cuando se utilizan servidores zSeries o S/390 que disponen de tarjetas OSA (Open System Adapter). Se proporcionan soluciones alternativas posibles.	“Problema: en Linux, existen limitaciones de configuración de Dispatcher cuando se utilizan servidores zSeries o S/390 que disponen de tarjetas OSA (Open System Adapter” en la página 321
En algunas versiones de Red Hat Linux, se produce una pérdida de memoria al ejecutar Load Balancer configurado con el gestor y los asesores.	Las versiones de la MVM de SDK Java de IBM y la biblioteca de hebras POSIX nativa (NPTL) que se entregan con algunas distribuciones Linux, como Red Hat Enterprise Linux 3.0, pueden hacer que se produzca la pérdida de memoria.	“Problema: en algunas versiones de Linux, se produce una pérdida de memoria al ejecutar Dispatcher configurado con el gestor y los asesores” en la página 323
En SUSE Linux Enterprise Server 9, el informe de Dispatcher indica que se envían paquetes (aumenta el número de paquetes), aunque en realidad los paquetes nunca llegan al servidor de programa de fondo	Se carga el módulo NAT de iptables. En esta versión de iptables hay un posible error, aunque sin confirmar, que provoca un comportamiento extraño al interactuar con Dispatcher.	“Problema: en SUSE Linux Enterprise Server 9, Dispatcher reenvía paquetes, pero éstos no llegan al servidor de programa de fondo” en la página 323

Tabla 14. Tabla de resolución de problemas de Dispatcher (continuación)

Síntoma	Causa posible	Vaya a...
En sistemas Windows, al utilizar la característica de alta disponibilidad de Dispatcher, pueden aparecer problemas durante la toma de control	Si se ejecuta el script go* que configura la dirección IP de clúster de la máquina activa antes de ejecutar el script go* para desconfigurar la dirección IP de clúster de la máquina en espera, pueden surgir problemas.	“Problema: en sistemas Windows, el mensaje de conflicto entre direcciones IP aparece durante la toma de control de alta disponibilidad” en la página 324
En sistemas Linux, iptables puede impedir el direccionamiento de paquetes	iptables en Linux pueden dificultar el equilibrio de carga y debe estar inhabilitado en la máquina de Load Balancer.	“Problema: iptables de Linux puede impedir el direccionamiento de paquetes” en la página 325
En sistemas Solaris, al intentar configurar un servidor IPv6 en la máquina Dispatcher, aparece un mensaje indicando que "no se puede añadir servidor"	Esto se puede producir por la forma en que el sistema operativo Solaris maneja la petición de ping para una dirección IPv6.	“Problema: no se puede añadir un servidor IPv6 a la configuración de Load Balancer en sistemas Solaris” en la página 325
Cuando se instalan arreglos de servicio o se instala de forma nativa mediante las herramientas de paquetes del sistema, aparece un mensaje de aviso del conjunto de archivos Java.	La instalación de producto consta de varios paquetes que no es necesario instalar en la misma máquina y, por lo tanto, cada uno de estos paquetes instala un conjunto de archivos Java. Cuando se instalan en la misma máquina, aparece un mensaje de aviso indicando que el conjunto de archivos Java también es propiedad de otro conjunto de archivos.	“Aparece un mensaje de aviso Java al instalar arreglos de servicio” en la página 325
Actualización del conjunto de archivos Java que se proporciona con las instalaciones de Load Balancer	Si se detecta un problema con el conjunto de archivos Java, debe notificarlo al servicio de IBM para así poder recibir una actualización para el conjunto de archivos Java que se proporcionó con la instalación de Load Balancer.	“Actualización del conjunto de archivos Java con la instalación de Load Balancer” en la página 326

Tabla 15. Tabla de resolución de problemas de CBR

Síntoma	Causa posible	Vaya a...
CBR no se ejecuta correctamente	Números de puerto en conflicto	“Comprobación de los números de puerto de CBR” en la página 300

Tabla 15. Tabla de resolución de problemas de CBR (continuación)

El mandato cbrcontrol o lbadmin ha dado un error e indica el mensaje 'El servidor no responde' o 'No es posible acceder al servidor RMI'	Los mandatos dan un error debido a una pila con SOCKS. O porque no se inicia cbrserver	"Problema: el mandato cbrcontrol o lbadmin da un error" en la página 326
No se equilibra la carga de las peticiones	Se ha iniciado Caching Proxy antes de que se iniciara el ejecutor	"Problema: no se equilibra la carga de las peticiones" en la página 327
En Solaris, el mandato cbrcontrol executor start produce el mensaje de error 'Error: el ejecutor no se ha iniciado'.	El mandato da un error porque quizá sea necesario modificar los valores por omisión de IPC del sistema o el enlace a la biblioteca es incorrecto.	"Problema: en sistemas Solaris, el mandato cbrcontrol executor start da un error" en la página 327
No funciona la norma de URL	Error sintáctico o de configuración	"Problema: error sintáctico o de configuración" en la página 327
Comportamiento de la GUI inesperado cuando se utiliza los sistemas Windows con la tarjeta de vídeo Matrox AGP	Se produce un problema cuando se utilizan tarjetas de vídeo Matrox AGP al ejecutar la GUI de Load Balancer	"Problema: en la plataforma Windows, se produce un comportamiento de la GUI inesperado al utilizar tarjetas de vídeo Matrox AGP" en la página 327
Se cierra la comunicación de la GUI (o tiene un comportamiento inesperado) cuando se intenta cargar un archivo de configuración de gran tamaño.	Java no tiene acceso a suficiente memoria para gestionar un cambio de tan gran tamaño en la GUI	"Problema: se cierra la comunicación de la GUI (o tiene un comportamiento inesperado) cuando se intenta cargar un archivo de configuración de gran tamaño" en la página 309
Se produce una desconexión del sistema principal cuando se utiliza la administración Web remota mediante Netscape	Se producirá una desconexión del sistema principal cuando se cambie el tamaño de la ventana del navegador	"Problema: se produce una desconexión del sistema principal si se cambia el tamaño de la ventana del navegador Netscape cuando se utiliza la administración Web" en la página 328
En la plataforma Windows, aparecen en el indicador de mandatos caracteres nacionales Latin-1 dañados	Cambie las propiedades de font de la ventana de indicador de mandatos	"Problema: en la plataforma Windows, aparecen caracteres nacionales Latin-1 dañados en la ventana de indicador de mandatos" en la página 328
En la plataforma HP-UX, aparece este mensaje: java.lang.OutOfMemoryError unable to create new native thread (java.lang.OutOfMemoryError no se ha podido crear una nueva hebra nativa)	Algunas instalaciones de HP-UX por omisión permiten 64 hebras por proceso. Esto es insuficiente.	"Problema: en HP-UX, se produce un error de falta de memoria/hebra de Java" en la página 328
En la plataforma Windows, los asesores y los destinos de alcance marcan como inactivos todos los servidores	No está inhabilitada Task Offload (Descarga de tareas) o quizá tenga que habilitarse icmp.	"Problema: en los sistemas Windows, los asesores y los destinos de alcance marcan como inactivos todos los servidores" en la página 328

Tabla 15. Tabla de resolución de problemas de CBR (continuación)

En la plataforma Windows, se produce un problema al resolver la dirección IP con nombre de sistema principal cuando se configura más de una dirección con un adaptador	La dirección IP que desea como nombre de sistema principal debe aparecer primero en el registro.	“Problema: en sistemas Windows, se resuelve la dirección IP con el nombre de sistema principal cuando se ha configurado más de una dirección con el adaptador” en la página 329
En sistemas Solaris, los procesos de Load Balancer finalizan cuando sale de la ventana de la sesión de terminal desde la que se han iniciado	Utilice el mandato nohup para impedir que los procesos que ha iniciado reciban una señal de cierre de comunicación cuando sale de la sesión de terminal.	“Problema: en sistemas Solaris, los procesos de Load Balancer finalizan cuando sale de la ventana de terminal desde la que se han iniciado” en la página 317

Tabla 16. Tabla de resolución de problemas de Site Selector

Síntoma	Causa posible	Vaya a...
Site Selector no se ejecuta correctamente	Número de puerto en conflicto	“Comprobación de los números de puerto de Site Selector” en la página 301
Site Selector no utiliza el algoritmo de turno rotativo para peticiones entrantes del cliente Solaris	Los sistemas Solaris ejecutan un “daemon de antememoria del servicio de nombres”	“Problema: Site Selector no utiliza el algoritmo de turno rotativo en el tráfico de clientes Solaris” en la página 329
El mandato sscontrol o lbadmín ha dado un error e indica el mensaje ‘El servidor no responde’ o ‘No es posible acceder al servidor RMI’	Los mandatos dan un error debido a una pila con SOCKS. O porque no se inicia ssserver	“Problema: el mandato sscontrol o lbadmín da un error” en la página 329
No se ha podido iniciar ssserver en la plataforma Windows	Los sistemas Windows no requieren que el nombre de sistema principal esté en el DNS.	“Problema: no se ha podido iniciar ssserver en la plataforma Windows” en la página 330
La máquina con rutas duplicadas no equilibra la carga correctamente — parece que la resolución de nombres da un error	Máquina de Site Selector con varios adaptadores conectados a la misma subred	“Problema: Site Selector con rutas duplicadas no equilibra la carga correctamente” en la página 330
Comportamiento de la GUI inesperado cuando se utiliza la plataforma Windows con la tarjeta de vídeo Matrox AGP	Se produce un problema cuando se utilizan tarjetas de vídeo Matrox AGP al ejecutar la GUI de Load Balancer	“Problema: en la plataforma Windows, se produce un comportamiento de la GUI inesperado al utilizar tarjetas de vídeo Matrox AGP” en la página 330
Se cierra la comunicación de la GUI (o tiene un comportamiento inesperado) cuando se intenta cargar un archivo de configuración de gran tamaño.	Java no tiene acceso a suficiente memoria para gestionar un cambio de tan gran tamaño en la GUI	“Problema: se cierra la comunicación de la GUI (o tiene un comportamiento inesperado) cuando se intenta cargar un archivo de configuración de gran tamaño” en la página 309

Tabla 16. Tabla de resolución de problemas de Site Selector (continuación)

Síntoma	Causa posible	Vaya a...
Se produce una desconexión del sistema principal cuando se utiliza la administración Web remota mediante Netscape	Se producirá una desconexión del sistema principal cuando se cambie el tamaño de la ventana del navegador	“Problema: se produce una desconexión del sistema principal si se cambia el tamaño de la ventana del navegador Netscape cuando se utiliza la administración Web” en la página 331
En la plataforma Windows, aparecen en el indicador de mandatos caracteres nacionales Latin-1 dañados	Cambie las propiedades de font de la ventana de indicador de mandatos	“Problema: en la plataforma Windows, aparecen caracteres nacionales Latin-1 dañados en la ventana de indicador de mandatos” en la página 331
En la plataforma HP-UX, aparece este mensaje: java.lang.OutOfMemoryError unable to create new native thread (java.lang.OutOfMemoryError no se ha podido crear una nueva hebra nativa)	Algunas instalaciones de HP-UX por omisión permiten 64 hebras por proceso. Esto es insuficiente.	“Problema: en HP-UX, se produce un error de falta de memoria/hebra de Java” en la página 331
En la plataforma Windows, los asesores y los destinos de alcance marcan como inactivos todos los servidores	No está inhabilitada Task Offload (Descarga de tareas) o quizá tenga que habilitarse icmp.	“Problema: en los sistemas Windows, los asesores y los destinos de alcance marcan como inactivos todos los servidores” en la página 331
En sistemas Solaris, los procesos de Load Balancer finalizan cuando sale de la ventana de la sesión de terminal desde la que se han iniciado	Utilice el mandato nohup para impedir que los procesos que ha iniciado reciban una señal de cierre de comunicación cuando sale de la sesión de terminal.	“Problema: en sistemas Solaris, los procesos de Load Balancer finalizan cuando sale de la ventana de terminal desde la que se han iniciado” en la página 317

Tabla 17. Tabla de resolución de problemas de Controlador para Conmutadores Cisco CSS

Síntoma	Causa posible	Vaya a...
No se iniciará ccoserver	Números de puerto en conflicto	“Comprobación de los números de puerto de Cisco CSS Controller” en la página 301
El mandato ccocontrol o lbadmin ha dado un error e indica el mensaje ‘El servidor no responde’ o ‘No es posible acceder al servidor RMI’	Los mandatos dan un error debido a una pila con SOCKS. O porque no se inicia ccoserver	“Problema: el mandato ccocontrol o lbadmin da un error” en la página 332
Error de recepción: Cannot create registry on port 13099 (No se ha podido crear el registro en el puerto 13099)	Licencia del producto caducada	“Problema: no se ha podido crear el registro en el puerto 13099” en la página 332

Tabla 17. Tabla de resolución de problemas de Controlador para Conmutadores Cisco CSS (continuación)

Síntoma	Causa posible	Vaya a...
Comportamiento de la GUI inesperado cuando se utiliza la plataforma Windows con la tarjeta de vídeo Matrox AGP	Se produce un problema cuando se utilizan tarjetas de vídeo Matrox AGP al ejecutar la GUI de Load Balancer	“Problema: en la plataforma Windows, se produce un comportamiento de la GUI inesperado al utilizar tarjetas de vídeo Matrox AGP” en la página 333
Se ha recibido un error de conexión al añadir un consultor	Los valores de configuración son incorrectos en el conmutador o el controlador	“Problema: se ha recibido un error de conexión al añadir un consultor” en la página 333
No se actualizan los pesos en el conmutador	La comunicación entre el controlador o el conmutador no está disponible o se ha interrumpido	“Problema: no se actualizan los pesos en el conmutador” en la página 333
El mandato refresh no ha actualizado la configuración del consultor	La comunicación entre el controlador y el conmutador no está disponible o se ha interrumpido	“Problema: el mandato refresh no ha actualizado la configuración del consultor” en la página 333
Se cierra la comunicación de la GUI (o tiene un comportamiento inesperado) cuando se intenta cargar un archivo de configuración de gran tamaño.	Java no tiene acceso a suficiente memoria para gestionar un cambio de tan gran tamaño en la GUI	“Problema: se cierra la comunicación de la GUI (o tiene un comportamiento inesperado) cuando se intenta cargar un archivo de configuración de gran tamaño” en la página 309
Se produce una desconexión del sistema principal cuando se utiliza la administración Web remota mediante Netscape	Se producirá una desconexión del sistema principal cuando se cambie el tamaño de la ventana del navegador	“Problema: se produce una desconexión del sistema principal si se cambia el tamaño de la ventana del navegador Netscape cuando se utiliza la administración Web” en la página 333
En la plataforma Windows, aparecen en el indicador de mandatos caracteres nacionales Latin-1 dañados	Cambie las propiedades de font de la ventana de indicador de mandatos	“Problema: en la plataforma Windows, aparecen caracteres nacionales Latin-1 dañados en la ventana de indicador de mandatos” en la página 334
En la plataforma HP-UX, aparece este mensaje: java.lang.OutOfMemoryError unable to create new native thread (java.lang.OutOfMemoryError no se ha podido crear una nueva hebra nativa)	Algunas instalaciones de HP-UX por omisión permiten 64 hebras por proceso. Esto es insuficiente.	“Problema: en HP-UX, se produce un error de falta de memoria/hebra de Java” en la página 334
En sistemas Solaris, los procesos de Load Balancer finalizan cuando sale de la ventana de la sesión de terminal desde la que se han iniciado	Utilice el mandato nohup para impedir que los procesos que ha iniciado reciban una señal de cierre de comunicación cuando sale de la sesión de terminal.	“Problema: en sistemas Solaris, los procesos de Load Balancer finalizan cuando sale de la ventana de terminal desde la que se han iniciado” en la página 317

Tabla 18. Tabla de resolución de problemas de Nortel Alteon Controller

Síntoma	Causa posible	Vaya a...
No se iniciará nalserver	Números de puerto en conflicto	"Comprobación de los números de puerto de Nortel Alteon Controller" en la página 302
El mandato nalcontrol o lbadmin ha dado un error e indica el mensaje 'El servidor no responde' o 'No es posible acceder al servidor RMI'	Los mandatos dan un error debido a una pila con SOCKS. O porque no se inicia nalserver	"Problema: el mandato nalcontrol o lbadmin da un error" en la página 334
Error de recepción: Cannot create registry on port 14099 (No se ha podido crear el registro en el puerto 14099)	Licencia del producto caducada	"Problema: no se ha podido crear el registro en el puerto 14099" en la página 335
Comportamiento de la GUI inesperado cuando se utiliza la plataforma Windows con la tarjeta de vídeo Matrox AGP	Se produce un problema cuando se utilizan tarjetas de vídeo Matrox AGP al ejecutar la GUI de Load Balancer	"Problema: en la plataforma Windows, se produce un comportamiento de la GUI inesperado al utilizar tarjetas de vídeo Matrox AGP" en la página 335
Se cierra la comunicación de la GUI (o tiene un comportamiento inesperado) cuando se intenta cargar un archivo de configuración de gran tamaño.	Java no tiene acceso a suficiente memoria para gestionar un cambio de tan gran tamaño en la GUI	"Problema: se cierra la comunicación de la GUI (o tiene un comportamiento inesperado) cuando se intenta cargar un archivo de configuración de gran tamaño" en la página 309
Se produce una desconexión del sistema principal cuando se utiliza la administración Web remota mediante Netscape	Se producirá una desconexión del sistema principal cuando se cambie el tamaño de la ventana del navegador	"Problema: se produce una desconexión del sistema principal si se cambia el tamaño de la ventana del navegador Netscape cuando se utiliza la administración Web" en la página 335
Se ha recibido un error de conexión al añadir un consultor	Los valores de configuración son incorrectos en el conmutador o el controlador	"Problema: se ha recibido un error de conexión al añadir un consultor" en la página 336
No se actualizan los pesos en el conmutador	La comunicación entre el controlador o el conmutador no está disponible o se ha interrumpido	"Problema: no se actualizan los pesos en el conmutador" en la página 336
El mandato refresh no ha actualizado la configuración del consultor	La comunicación entre el controlador y el conmutador no está disponible o se ha interrumpido	"Problema: el mandato refresh no ha actualizado la configuración del consultor" en la página 336
En la plataforma Windows, aparecen en el indicador de mandatos caracteres nacionales Latin-1 dañados	Cambie las propiedades de font de la ventana de indicador de mandatos	"Problema: en sistemas Windows, aparecen caracteres nacionales Latin-1 dañados en la ventana de indicador de mandatos" en la página 336

Tabla 18. Tabla de resolución de problemas de Nortel Alteon Controller (continuación)

Síntoma	Causa posible	Vaya a...
En la plataforma HP-UX, aparece este mensaje: java.lang.OutOfMemoryError unable to create new native thread (java.lang.OutOfMemoryError no se ha podido crear una nueva hebra nativa)	Algunas instalaciones de HP-UX por omisión permiten 64 hebras por proceso. Esto es insuficiente.	"Problema: en HP-UX, se produce un error de falta de memoria/hebra de Java" en la página 337
En sistemas Solaris, los procesos de Load Balancer finalizan cuando sale de la ventana de la sesión de terminal desde la que se han iniciado	Utilice el mandato nohup para impedir que los procesos que ha iniciado reciban una señal de cierre de comunicación cuando sale de la sesión de terminal.	"Problema: en sistemas Solaris, los procesos de Load Balancer finalizan cuando sale de la ventana de terminal desde la que se han iniciado" en la página 317

Tabla 19. Tabla de resolución de problemas de Metric Server

Síntoma	Causa posible	Vaya a...
Metric Server IOException en la plataforma Windows al ejecutar los archivos de métrica del usuario .bat o .cmd	Se requiere el nombre de métrica completo	"Problema: Metric Server IOException en la plataforma Windows al ejecutar archivos de métrica del usuario .bat o .cmd" en la página 337
Metric Server no informa de la información de carga a la máquina de Load Balancer	Entre las causas posibles se incluyen: <ul style="list-style-type: none"> No hay archivos de claves en la máquina de Metric Server El nombre de sistema principal de la máquina de Metric Server no se ha registrado con el servidor de nombres local El archivo /etc/hosts ha resuelto el nombre de sistema principal local con la dirección de bucle de retorno 127.0.0.1 	"Problema: Metric Server no informa de las cargas en la máquina de Load Balancer" en la página 337
El archivo de anotaciones cronológicas de Metric Server informa de que "Es necesaria la firma para acceder al agente" cuando se transfieren archivos de claves al servidor	El archivo de claves no ha superado la autorización debido a que está dañado.	"Problema: el archivo de anotaciones cronológicas de Metric Server informa de que "Es necesaria la firma para acceder al agente"" en la página 337
En sistemas AIX, cuando se ejecuta Metric Server bajo gran presión en un sistema multiprocesador (AIX 4.3.3 o AIX 5.1), podría dañar la salida del mandato ps -vg	APAR IY33804 corrige este problema de AIX conocido	"Problema: en sistemas AIX, cuando se ejecuta Metric Server bajo mucha presión, la salida del mandato ps -vg podría dañarse" en la página 338

Tabla 19. Tabla de resolución de problemas de Metric Server (continuación)

Síntoma	Causa posible	Vaya a...
Configuración de Metric Server en una configuración de dos niveles con el equilibrio de carga de Site Selector entre Dispatchers de alta disponibilidad	No se ha configurado Metric Server (que reside en el segundo nivel) para que esté a la escucha en una nueva dirección IP.	“Problema: configuración de Metric Server en una configuración de dos niveles con el equilibrio de carga de Site Selector entre Dispatchers de alta disponibilidad” en la página 338
Los scripts (metricserver, cpuload, memload) que se ejecutan en máquinas Solaris de varias CPU producen mensajes de la consola no deseados	Este comportamiento se debe al uso del mandato de sistema VMSTAT para recopilar estadísticas de la CPU y de memoria del kernel.	“Problema: los scripts, en ejecución en máquinas Solaris de varias CPU, producen mensajes de consola no deseados” en la página 339
En sistemas Solaris, los procesos de Load Balancer finalizan cuando sale de la ventana de la sesión de terminal desde la que se han iniciado	Utilice el mandato nohup para impedir que los procesos que ha iniciado reciban una señal de cierre de comunicación cuando sale de la sesión de terminal.	“Problema: en sistemas Solaris, los procesos de Load Balancer finalizan cuando sale de la ventana de terminal desde la que se han iniciado” en la página 317
En sistemas Linux, cuando se ejecuta Load Balancer para IPv6, no se pueden recuperar valores de Metric Server	Cuando se ejecuta en plataformas Linux, existe una incompatibilidad de selección de dirección de origen IPv6. Como consecuencia, Metric Monitor intenta comunicarse con Metric Server a través de la dirección IP de origen errónea.	“Problema: en Load Balancer para IPv6, no se pueden recuperar los valores de Metric Server en sistemas Linux” en la página 340
El valor de métrica devuelve -1 después de iniciar Metric Server	Este problema puede deberse a que los archivos de claves pierden su integridad durante la transferencia de los mismos al cliente.	“Problema: Después de iniciar Metric Server, el valor de métrica devuelve -1” en la página 340

Comprobación de los números de puerto de Dispatcher

Si experimenta problemas al ejecutar Dispatcher, quizá una de las aplicaciones esté utilizando un número de puerto que Dispatcher normalmente utiliza. Tenga en cuenta que el servidor de Dispatcher utiliza estos números de puerto:

- 10099 para recibir mandatos de dscontrol
- 10004 para enviar consultas de métrica a Metric Server
- 10199 para el puerto del servidor RMI

Si otra aplicación está utilizando uno de los números de puerto de Dispatcher, puede cambiar los números de puerto de Dispatcher o el número de puerto de la aplicación.

Para cambiar los números de puerto de Dispatcher realice lo siguiente:

- Para cambiar el puerto utilizado para recibir mandatos
 - Modifique la variable `LB_RMIPORT` al principio del archivo `dsserver` con el puerto donde desea que Dispatcher reciba los mandatos.
- Para cambiar el puerto utilizado para recibir informes de métrica de Metric Server
 - Modifique la variable `RMI_PORT` en el archivo `metricserver` con el puerto que desea utilizar para que se comuniquen Dispatcher con Metric Server.
 - Proporcione el argumento `metric_port` cuando se inicia el gestor. Consulte la descripción de la sintaxis de mandato **dscontrol manager start** en el apartado “dscontrol manager — controlar el gestor” en la página 373

Para cambiar el número de puerto RMI de la aplicación realice lo siguiente:

- Para cambiar el puerto utilizado por la aplicación
 - Modifique la variable `LB_RMISERVERPORT` del archivo `dsserver` con el puerto que desea que utilice la aplicación. (El valor por omisión del puerto RMI utilizado por la aplicación es 10199).

Nota: Para la plataforma Windows, los archivos `dsserver` y `metricserver` se encuentran en el directorio `C:\winnt\system32`. Para otras plataformas, estos archivos se encuentran en el directorio `/usr/bin/`.

Comprobación de los números de puerto de CBR

Si experimenta problemas al ejecutar CBR, quizá una de las aplicaciones esté utilizando un número de puerto que CBR normalmente utiliza. Tenga en cuenta que CBR utiliza este número de puerto:

- 11099 para recibir mandatos de `cbrcontrol`
- 10004 para enviar consultas de métrica a Metric Server
- 11199 para el puerto del servidor RMI

Nota: El componente CBR (Content Based Routing) está disponible en todas las plataformas excepto donde se ejecuta la JVM de 64 bits. De modo alternativo, puede utilizar el método de reenvío `cbr` del componente Dispatcher de Load Balancer para proporcionar direccionamiento basado en contenido sin utilizar Caching Proxy. Si desea más información, consulte el apartado “Direccionamiento basado en contenido de Dispatcher (método de reenvío `cbr`)” en la página 55.

Si otra aplicación está utilizando uno de los números de puerto de CBR, puede cambiar los números de puerto de CBR o el número de puerto de la aplicación.

Para cambiar los números de puerto de CBR realice lo siguiente:

- Para cambiar el puerto utilizado para recibir mandatos
 - Modifique la variable `LB_RMIPORT` al principio del archivo `cbrserver` con el puerto donde desea que CBR reciba los mandatos.
- Para cambiar el puerto utilizado para recibir informes de métrica de Metric Server
 - Modifique la variable `RMI_PORT` en el archivo `metricserver` con el puerto que desea utilizar para que se comuniquen CBR con Metric Server.
 - Proporcione el argumento `metric_port` cuando se inicia el gestor. Consulte la descripción de la sintaxis de mandato **manager start** en el apartado “dscontrol manager — controlar el gestor” en la página 373

Para cambiar el número de puerto RMI de la aplicación realice lo siguiente:

- Para cambiar el puerto utilizado por la aplicación
 - Modifique la variable LB_RMISERVERPORT al principio del archivo cbrserver con el puerto que desea que la aplicación utilice. (El valor por omisión del puerto RMI utilizado por la aplicación es 11199).

Nota: Para la plataforma Windows, los archivos cbrserver y metricserver se encuentran en el directorio C:\winnt\system32. Para otras plataformas, estos archivos se encuentran en el directorio /usr/bin/.

Comprobación de los números de puerto de Site Selector

Si experimenta problemas al ejecutar el componente Site Selector, quizá una de las aplicaciones esté utilizando un número de puerto que Site Selector normalmente utiliza. Tenga en cuenta que Site Selector utiliza estos números de puerto:

- 12099 para recibir mandatos de sscontrol
- 10004 para enviar consultas de métrica a Metric Server
- 12199 para el puerto del servidor RMI

Si otra aplicación está utilizando uno de los números de puerto de Site Selector, puede cambiar los números de puerto de Site Selector o el número de puerto de la aplicación.

Para cambiar los números de puerto de Site Selector realice lo siguiente:

- Para cambiar el puerto utilizado para recibir mandatos:
 - Modifique la variable LB_RMIPORT al principio del archivo ssserver con el puerto donde desea que Site Selector reciba los mandatos.
- Para cambiar el puerto utilizado para recibir informes de métrica de Metric Server
 - Modifique la variable RMI_PORT en el archivo metricserver con el puerto que desea utilizar para que se comunique Site Selector con Metric Server.
 - Proporcione el argumento metric_port cuando se inicia el gestor. Consulte la descripción de la sintaxis de mandato **manager start** en el apartado “sscontrol manager — controlar el gestor” en la página 413

Para cambiar el número de puerto RMI de la aplicación realice lo siguiente:

- Para cambiar el puerto utilizado por la aplicación
 - Modifique la variable LB_RMISERVERPORT al principio del archivo ssserver con el puerto que desea que la aplicación utilice. (El valor por omisión del puerto RMI utilizado por la aplicación es 12199).

Nota: Para la plataforma Windows, los archivos ssserver y metricserver se encuentran en el directorio C:\winnt\system32. Para otras plataformas, estos archivos se encuentran en el directorio /usr/bin/.

Comprobación de los números de puerto de Cisco CSS Controller

Si experimenta problemas al ejecutar el componente Cisco CSS Controller quizá otra aplicación esté utilizando uno de los números de puerto que ccoserver de Cisco CSS Controller utiliza. Tenga en cuenta que Cisco CSS Controller utiliza estos números de puerto:

- 13099 para recibir mandatos de ccocontrol

10004 para enviar consultas de métrica a Metric Server
13199 para el puerto del servidor RMI

Si otra aplicación está utilizando uno de los números de puerto de Cisco CSS Controller, puede cambiar los números de puerto para Cisco CSS Controller o el número de puerto de la aplicación.

Para cambiar los números de puerto de Cisco CSS Controller realice lo siguiente:

- Para cambiar el puerto utilizado para recibir mandatos de ccocontrol, modifique la variable CCO_RMIPORT en el archivo ccoserver. Cambie 13099 por el puerto con el que desea que Cisco CSS Controller reciba mandatos ccocontrol.
- Para cambiar el puerto utilizado para recibir informes de métrica de Metric Server:
 1. Modifique la variable RMI_PORT en el archivo metricserver. Cambie 10004 con el puerto con el que desea que Cisco CSS Controller se comuniquen con Metric Server.
 2. Proporcione el argumento metric_port cuando inicie el consultor.

Para cambiar el número de puerto RMI de la aplicación realice lo siguiente:

- Para cambiar el puerto utilizado por la aplicación
 - Modifique la variable CCO_RMISERVERPORT al principio del archivo ccoserver con el puerto que desea que la aplicación utilice. (El valor por omisión del puerto RMI utilizado por la aplicación es 13199).

Nota: Para la plataforma Windows, los archivos ccoserver y metricserver se encuentran en el directorio C:\winnt\system32. Para otras plataformas, estos archivos se encuentran en el directorio /usr/bin.

Comprobación de los números de puerto de Nortel Alteon Controller

Si experimenta problemas al ejecutar el componente Nortel Alteon Controller quizá otra aplicación esté utilizando uno de los números de puerto que nalserver de Nortel Alteon Controller utiliza. Tenga en cuenta que Nortel Alteon Controller utiliza estos números de puerto:

14099 para recibir mandatos de nalcontrol
10004 para enviar consultas de métrica a Metric Server
14199 para el puerto del servidor RMI

Si otra aplicación está utilizando uno de los números de puerto de Nortel Alteon Controller, puede cambiar los números de puerto para Nortel Alteon Controller o los números de puerto de la aplicación.

Para cambiar los números de puerto de Nortel Alteon Controller realice lo siguiente:

- Para cambiar el puerto utilizado para recibir mandatos de nalcontrol, modifique la variable NAL_RMIPORT en el archivo nalserver. Cambie 14099 con el puerto con el que desea que Nortel Alteon Controller reciba mandatos nalcontrol.
- Para cambiar el puerto utilizado para recibir informes de métrica de Metric Server:
 1. Modifique la variable RMI_PORT en el archivo metricserver. Cambie 10004 con el puerto con el que desea que Nortel Alteon Controller se comuniquen con Metric Server.

2. Proporcione el argumento `metric_port` cuando inicie el consultor.

Para cambiar el número de puerto RMI de la aplicación realice lo siguiente:

- Para cambiar el puerto utilizado por la aplicación
 - Modifique la variable `NAL_RMISERVERPORT` al principio del archivo `nalserver` con el puerto que desea que la aplicación utilice. (El valor por omisión del puerto RMI utilizado por la aplicación es 14199).

Nota: Para la plataforma Windows, los archivos `nalserver` y `metricserver` se encuentran en el directorio `C:\winnt\system32`. Para otras plataformas, estos archivos se encuentran en el directorio `/usr/bin`.

Resolución de problemas comunes—Dispatcher

Problema: no se ejecutará Dispatcher

Este problema puede producirse si otra aplicación utiliza uno de los puertos utilizados por el `nalserver` de Dispatcher. Para obtener más información, consulte el apartado “Comprobación de los números de puerto de Dispatcher” en la página 299.

Problema: no responderán Dispatcher y el servidor

Este problema se produce cuando se utiliza otra dirección que no es la dirección especificada. Cuando utiliza una ubicación compartida para el Dispatcher y el servidor, asegúrese de que la dirección del servidor utilizada en la configuración es la dirección NFA o que se configura como ubicación compartida. Además, compruebe si el archivo de sistema principal tiene la dirección correcta.

Problema: no se equilibran las peticiones de Dispatcher

Este problema tiene síntomas, por ejemplo, de conexiones de máquinas cliente no atendidas o de tiempo de espera de conexiones superado. Compruebe lo siguiente para diagnosticar este problema:

1. ¿Ha configurado la dirección de no reenvío, los clústeres, los puertos y los servidores para el direccionamiento? Compruebe el archivo de configuración.
2. ¿Se ha creado un alias de la tarjeta de interfaz de red con la dirección del clúster? Para Sistemas Linux y UNIX, utilice `netstat -ni` para comprobarlo.
3. ¿Tiene el dispositivo de bucle de retorno de cada servidor establecido el alias en la dirección del clúster? Para Sistemas Linux y UNIX, utilice `netstat -ni` para comprobarlo.
4. ¿Se ha suprimido la ruta adicional? Para Sistemas Linux y UNIX, utilice `netstat -nr` para comprobarlo.
5. Utilice el mandato **`dscontrol cluster status`** para comprobar la información para cada clúster que ha definido. Asegúrese de que tiene definido un puerto para cada clúster.
6. Utilice el mandato **`dscontrol server report ::`** para asegurarse de que ninguno de los servidores esté inactivo ni tenga establecido su peso en cero.

Para Windows y otras plataformas, consulte también el apartado “Configuración de máquinas de servidor para el equilibrio de carga” en la página 72.

Problema: la función de alta disponibilidad de Dispatcher no funciona

Este problema aparece cuando se configura un entorno de alta disponibilidad de Dispatcher y las conexiones de las máquinas cliente no se atienden o superan el tiempo de espera. Compruebe lo siguiente para corregir o diagnosticar el problema:

- Asegúrese de que ha creado los scripts goActive, goStandby y goInOp y colóquelos en el directorio bin donde se ha instalado Dispatcher. Para obtener más información sobre estos scripts, consulte el apartado “Utilización scripts” en la página 209
- Para sistemas AIX, HP-UX, Linux y Solaris, asegúrese de que los scripts goActive, goStandby y goInOp tienen establecido execute permission.
- Para sistemas Windows, asegúrese de configurar la dirección de no reenvío utilizando el mandato **executor configure**.

Los pasos siguientes son un modo eficaz de probar que los scripts de alta disponibilidad funcionan correctamente:

1. Recopile un informe emitiendo los mandatos netstat -an y ifconfig -a en la máquina
2. Ejecute el script goActive
3. Ejecute el script goStandby
4. Una vez más, recopile un informe emitiendo los mandatos netstat -an y ifconfig -a

Los dos informes serán idénticos si se han configurado correctamente los scripts.

Problema: no se han podido añadir pulsos (plataforma Windows)

Este error de la plataforma Windows se produce si no se configura la dirección de origen en un adaptador. Compruebe lo siguiente para corregir o diagnosticar el problema.

- Para asegurarse de configurar la dirección de no reenvío utilice la interfaz Token-ring o Ethernet y emita cualquiera de estos mandatos:
`dscontrol executor configure <dirección IP>`

Problema: rutas adicionales (Windows 2000)

Después de configurar las máquinas servidor, puede encontrarse con que ha creado sin querer una o más rutas adicionales. Si no se eliminan, estas rutas adicionales impedirán el funcionamiento de Dispatcher. Para comprobarlo y suprimirlas, consulte el apartado “Configuración de máquinas de servidor para el equilibrio de carga” en la página 72.

Problema: los asesores no funcionan correctamente

Si utiliza un soporte de área amplia y parece que los asesores no funcionan correctamente, asegúrese de que se inician en los dos Dispatcher, local y remoto.

Se emite un mandato ping de ICMP a los servidores antes de la petición del asesor. Si existe un cortafuegos entre Load Balancer y los servidores, asegúrese de que se admiten los mandatos ping en el cortafuegos. Si esta configuración posee un riesgo de seguridad para la red, modifique la sentencia java en dsserver para desactivar todos los mandatos ping a los servidores añadiendo la propiedad java:

```
LB_ADV_NO_PING="true"
java -DLB_ADV_NO_PING="true"
```

Consulte el apartado “Utilización de asesores remotos con el soporte de área amplia de Dispatcher” en la página 230.

Problema: Dispatcher, Microsoft IIS y SSL no funcionan (plataforma Windows)

Cuando utiliza Dispatcher, Microsoft IIS y SSL, si no funcionan juntos, quizá haya un problema con la habilitación de la seguridad SSL. Para obtener más información sobre cómo generar un par de claves, adquirir un certificado, instalar un certificado con un par de claves y configurar un directorio para solicitar SSL, consulte la documentación de *Microsoft Information and Peer Web Services*.

Problema: conexión de Dispatcher con una máquina remota

Dispatcher utiliza claves para permitirle conectar con una máquina remota y configurarla. Las claves especifican un puerto RMI para la conexión. Es posible cambiar el puerto RMI por motivos de seguridad o conflictos. Cuando cambia los puertos RMI, el nombre de archivo de la clave es distinto. Si tiene más de una clave en el directorio de claves para la misma máquina remota y las claves especifican puertos RMI distintos, la línea de mandatos sólo intentará la primera que encuentre. Si es incorrecta, se rechazará la conexión. No se realizará la conexión a no ser que suprima la clave incorrecta.

Problema: el mandato dscontrol o lbadmin da un error

1. El mandato dscontrol devuelve: **Error: el servidor no responde**. O bien, el mandato lbadmin devuelve: **Error: no es posible acceder al servidor RMI**. Estos errores pueden producirse si su máquina tiene una pila con SOCKS. Para corregir este problema, edite el archivo socks.cnf para incluir las líneas siguientes:

```
EXCLUDE-MODULE java
EXCLUDE-MODULE javaw
```

2. Las consolas de administración de las interfaces (línea de mandatos, interfaz gráfica de usuario y asistentes) de Load Balancer se comunican con dsserver utilizando RMI (Remote Method Invocation). La comunicación por omisión utiliza tres puertos; cada puerto se establece en el script de inicio de dsserver:

- 10099 para recibir mandatos de dscontrol
- 10004 para enviar consultas de métrica a Metric Server
- 10199 para el puerto del servidor RMI

Esto puede producir problemas si una de las consolas de administración se ejecuta en la misma máquina que un cortafuegos o a través de un cortafuegos. Por ejemplo, cuando Load Balancer se ejecuta en la misma máquina que un cortafuegos y emite mandatos dscontrol, podrían aparecer errores como **Error: el servidor no responde**.

Para impedir este problema, edite el archivo de scripts dsserver para establecer el puerto utilizado por RMI para el cortafuegos (u otra aplicación). Cambie la línea: LB_RMISERVERPORT=10199 por LB_RMISERVERPORT=*suPuerto*. Donde *suPuerto* es otro puerto.

Cuando haya terminado, reinicie dsserver y abra el tráfico para los puertos: 10099, 10004, 10199 y 10100 o para el puerto seleccionado para la dirección del sistema principal desde donde se ejecutará la consola de administración.

3. También se pueden producir estos errores si aún no ha iniciado **dsserver**.

4. Si hay varios adaptadores en la máquina, debe designar el adaptador que dssserver va a utilizar añadiendo lo siguiente al script
`dssserver:java.rmi.server.hostname=<nombre_sistema_principal o dirección_IP>`

Por ejemplo: `java -Djava.rmi.server.hostname="10.1.1.1"`

Problema: aparece el mensaje de error “No se puede encontrar el archivo...” al intentar consultar la ayuda en línea (plataforma Windows)

Para plataformas Windows, cuando utiliza Netscape como el navegador por omisión, puede producirse este mensaje de error: “No se puede encontrar el archivo ‘<nombrearchivo>.html’ (o uno de sus componentes). Asegúrese de que la vía de acceso y el nombre de archivo sean correctos y de que están disponibles todas las bibliotecas necesarias”.

El problema se debe a un valor incorrecto de la asociación de archivo HTML. Esta es la solución:

1. Pulse **Mi PC**, a continuación **Herramientas**, seleccione **Opciones de carpeta** y pulse la pestaña **Tipos de archivo**
2. Seleccione “Documento de hipertexto de Netscape”
3. Pulse el botón **Opciones avanzadas**, seleccione **open**, pulse el botón **Editar**
4. Especifique *NSShell* en el campo **Aplicación:** (no en el campo Aplicación utilizada para realizar la acción:) y pulse **Aceptar**

Problema: la GUI (interfaz gráfica de usuario) no se inicia correctamente

La GUI (interfaz gráfica de usuario), que es lbadmin, requiere una cantidad de espacio de paginación suficiente para funcionar correctamente. Si no hay disponible suficiente espacio para paginación, quizá la GUI no se inicie completamente. Si ocurriera esto, compruebe el espacio de paginación y aumentelo si es necesario.

Problema: error al ejecutar Dispatcher con Caching Proxy instalado

Si desinstala Load Balancer para volver a instalar otra versión y obtiene un error al intentar iniciar el componente Dispatcher, compruebe si está instalado Caching Proxy. Caching Proxy tiene una dependencia en uno de los archivos de Dispatcher; este archivo se desinstalará sólo cuando se desinstale Caching Proxy.

Para evitar este problema:

1. Desinstale Caching Proxy.
2. Desinstale Load Balancer.
3. Vuelva a instalar Load Balancer y Caching Proxy.

Problema: la GUI (interfaz gráfica de usuario) no se muestra correctamente

Si experimenta problemas con la apariencia de la GUI de Load Balancer, compruebe el valor de la resolución del escritorio del sistema operativo. La GUI se visualiza mejor con una resolución de 1024x768 píxeles.

Problema: en la plataforma Windows, las ventanas de ayuda a veces desaparecen detrás de otras ventanas abiertas

En la plataforma Windows, cuando abre por primera vez las ventanas de ayuda, a veces desaparecen en el fondo detrás de ventanas existentes. Si esto sucediera, pulse en la ventana para traerla de nuevo al frente.

Problema: Load Balancer no puede procesar y reenviar una trama

En Solaris cada adaptador de red tiene la misma dirección MAC por omisión. Esto funciona correctamente si cada adaptador se encuentra en una subred IP distinta; no obstante, en un entorno conmutado, cuando varias NIC con la misma dirección MAC y la misma dirección de subred IP se comunican con el mismo conmutador, el conmutador envía todo el tráfico enlazado para la dirección MAC única (y las dos IP) al mismo cable. Sólo el adaptador que incluyó por última vez una trama en el cable detecta los paquetes IP enlazados para los dos adaptadores. Solaris podría descartar paquetes para una dirección IP válida que llegaran en la interfaz "incorrecta".

Si las interfaces de red no están diseñadas para Load Balancer como se configura en `ibmlb.conf` y si la tarjeta NIC que no se define en `ibmlb.conf` recibe una trama, Load Balancer no tiene la posibilidad de procesar y reenviar la trama.

Para evitar este problema, debe alterar temporalmente el valor por omisión y establecer una dirección MAC única para cada interfaz. Utilice este mandato:

```
ifconfig interfaz ether dirMac
```

Por ejemplo:

```
ifconfig eri0 ether 01:02:03:04:05:06
```

Problema: se muestra una pantalla azul cuando se inicia el ejecutor de Load Balancer

En la plataforma Windows, debe tener instalada y configurada una tarjeta de red antes de iniciar el ejecutor.

Problema: la vía de acceso al descubrimiento impide el tráfico de retorno con Load Balancer

El sistema operativo AIX contiene un parámetro de red llamado descubrimiento de MTU de la vía de acceso. Durante la transacción con un cliente, si el sistema operativo determina que debe utilizar una unidad de transmisión máxima (MTU) más pequeña para los paquetes, el descubrimiento de MTU de la vía de acceso hace que AIX cree una ruta para recordar ese dato. La nueva ruta es para esa dirección IP del cliente específica y graba la MTU necesaria para llegar a ella.

Cuando se crea la ruta, podría aparecer un problema en los servidores provocado por el clúster del que se crea un alias en el bucle de retorno. Si la dirección de pasarela para la ruta está dentro de la subred del clúster/máscara de red, los sistemas AIX crean la ruta en el bucle de retorno. Esto sucede porque esa era la última interfaz con alias con esa subred.

Por ejemplo, si el clúster es 9.37.54.69 y se utiliza una máscara de red 255.255.255.0 y la pasarela prevista es 9.37.54.1, los sistemas AIX utilizarán el bucle de retorno para la ruta. Esto provoca que las respuestas del servidor nunca abandonen la

máquina y que el cliente supere el tiempo de espera. El cliente suele detectar una respuesta del clúster, luego se crea la ruta y el cliente ya no recibe nada más.

Hay dos soluciones para este problema.

1. Inhabilite el descubrimiento de MTU de la vía de acceso de modo que el sistema AIX no añada dinámicamente las rutas. Utilice estos mandatos.
no -a enumera los valores de red de AIX
no -o option=value
Establece los parámetros TCP en sistemas AIX
2. Cree un alias de la dirección IP del clúster en el bucle de retorno con una máscara de red 255.255.255.255. Esto significa que la subred con alias es sólo la dirección IP del clúster. Cuando los sistemas AIX crean las rutas dinámicas, la dirección IP de pasarela de destino no coincide con esa subred, lo que produce una ruta que utiliza la interfaz de red correcta. Luego suprima la nueva ruta lo0 que se había creado durante el paso de creación de alias. Para ello, encuentre la ruta en el bucle de retorno con un destino de red de la dirección IP del clúster y suprima esa ruta. Esto debe realizarse cada vez que se crea un alias del clúster.

Notas:

1. El descubrimiento de MTU de la vía de acceso se inhabilita por omisión en AIX 4.3.2 e inferiores; no obstante, en AIX 4.3.3 y superiores se habilita por omisión.
2. Los mandatos siguientes desactivan el descubrimiento de MTU de la vía de acceso y deben ejecutarse cada vez que se arranca el sistema. Añada estos mandatos al archivo /etc/rc.net.
 - -o udp_pmtu_discover=0
 - -o tcp_pmtu_discover=0

Problema: no funciona la alta disponibilidad de la modalidad de área amplia de Load Balancer

Cuando configura un Load Balancer de área amplia, debe definir el Dispatcher remoto como un servidor de un clúster en el Dispatcher local. Normalmente, puede utilizar la dirección de no reenvío (NFA) del Dispatcher remoto como la dirección de destino del servidor remoto. Si hace esto y configura la alta disponibilidad en el Dispatcher remoto, dará un error. Esto sucede porque el Dispatcher local siempre señala a la máquina primaria en el lado remoto cuando utiliza su dirección NFA para acceder a ésta.

Para solucionar este problema:

1. Defina un clúster adicional en el Dispatcher remoto. No es necesario definir puertos o servidores para este clúster.
2. Añada esta dirección del clúster a los scripts goActive y goStandby.
3. En el Dispatcher local, defina esta dirección del clúster como un servidor, en lugar de la dirección NFA del Dispatcher primario remoto.

Cuando aparece el Dispatcher primario remoto, creará un alias de esta dirección en su adaptador, que le permite aceptar tráfico. Si se produce una anomalía, la dirección se desplaza a la máquina de reserva y ésta sigue aceptando el tráfico de esa dirección.

Problema: se cierra la comunicación de la GUI (o tiene un comportamiento inesperado) cuando se intenta cargar un archivo de configuración de gran tamaño

Cuando se utiliza lbadmin o la administración Web (lbwebaccess) para cargar un archivo de configuración de gran tamaño (unos 200 o más mandatos **add**), podría cerrarse la comunicación de la GUI o mostrar un comportamiento inesperado, como una respuesta sumamente lenta a los cambios de pantalla.

Esto se produce porque Java no tiene acceso a suficiente memoria para gestionar una configuración de tan gran tamaño.

Hay una opción en el entorno de ejecución que se puede especificar para aumentar la agrupación de asignaciones de memoria en Java.

La opción es `-Xmxn` donde *n* es el tamaño máximo, en bytes, para la agrupación de asignaciones de memoria. *n* debe ser múltiplo de 1024 y ser mayor que 2 MB. El valor *n* debe ir seguido de *k* o *K* para indicar *kbytes* o de *m* o *M* para indicar *megabytes*. Por ejemplo, `-Xmx128M` y `-Xmx81920k` son dos valores válidos. El valor por omisión son 64 M. Solaris 8 tiene un valor máximo de 4000 M.

Por ejemplo, para añadir esta opción, edite el archivo de scripts lbadmin, modificando "javaw" con "javaw -Xmxn" como se detalla a continuación. (Para sistemas AIX, modifique "java" con "java -Xmxn"):

- **Sistemas AIX**

```
javaw -Xmx256m -cp $LB_CLASSPATH $LB_INSTALL_PATH $LB_CLIENT_KEYS  
com.ibm.internet.nd.framework.FWK_Main 1>/dev/null 2>&1 &
```

- **Sistemas HP-UX**

```
java -Xmx256m -cp $LB_CLASSPATH $LB_INSTALL_PATH $LB_CLIENT_KEYS  
com.ibm.internet.nd.framework.FWK_Main 1>/dev/null 2>&1 &
```

- **Sistemas Linux**

```
javaw -Xmx256m -cp $LB_CLASSPATH $LB_INSTALL_PATH $LB_CLIENT_KEYS  
com.ibm.internet.nd.framework.FWK_Main 1>/dev/null 2>&1 &
```

- **Sistemas Solaris**

```
java -Xmx256m -cp $LB_CLASSPATH $LB_INSTALL_PATH $LB_CLIENT_KEYS  
com.ibm.internet.nd.framework.FWK_Main 1>/dev/null 2>&1 &
```

- **Sistemas Windows**

```
START javaw -Xmx256m -cp %LB_CLASSPATH% %LB_INSTALL_PATH%  
%LB_CLIENT_KEYS% com.ibm.internet.nd.framework.FWK_Main
```

No hay ningún valor recomendado para *n*, pero debería ser mayor que la opción por omisión. Un buen punto de partida sería el doble del valor por omisión.

Problema: lbadmin realiza una desconexión del servidor después de actualizar la configuración

Si la administración de Load Balancer (lbadmin) realiza la desconexión del servidor después de actualizar la configuración, compruebe la versión de dsserver en el servidor que intenta configurar y asegúrese de que es la misma que la versión de lbadmin o dscontrol.

Problema: las direcciones IP no se resuelven correctamente en la conexión remota

Cuando se utiliza un cliente remoto en una implementación de SOCKS segura, quizá los nombres de dominio o de sistema principal plenamente cualificados no se resuelvan con la dirección IP correcta en notación de dirección IP. La implementación de SOCKS podría añadir datos específicos, relacionados con SOCKS a la resolución de DNS.

Si una dirección IP no se resuelve correctamente en la conexión remota, especifique la dirección IP en el formato de notación de dirección IP.

Problema: la interfaz de Load Balancer coreana muestra fonts solapados o no deseados en sistemas AIX y Linux

Para corregir el solapamiento de fonts o fonts no deseados en la interfaz coreana de Load Balancer:

En sistemas AIX

1. Detenga todos los procesos Java en el sistema AIX.
2. Abra el archivo font.properties.ko en un editor. Este archivo se ubica en *inicio/jre/lib* donde *inicio* es el directorio de inicio Java.
3. Busque esta serie:

```
-Monotype-TimesNewRomanWT-medium-r-normal  
--*-%d-75-75-*--ksc5601.1987-0
```

4. Sustituya todas las instancias de la serie con:

```
-Monotype-SansMonoWT-medium-r-normal  
--*-%d-75-75-*--ksc5601.1987-0
```

5. Guarde el archivo.

En sistemas Linux

1. Detenga todos los procesos Java en el sistema.
2. Abra el archivo font.properties.ko en un editor. Este archivo se ubica en *inicio/jre/lib* donde *inicio* es el directorio de inicio Java.
3. Busque esta serie (sin espacios):

```
-monotype-  
timesnewromanwt-medium-r-normal--*-%d-75-75-p-*--microsoft-symbol
```

4. Sustituya todas las instancias de la serie con:

```
-monotype-sansmonowt-medium-r-normal--*-%d-75-75-p-*--microsoft-symbol
```

5. Guarde el archivo.

Problema: en sistemas Windows, se devuelve una dirección del alias en lugar de la dirección local cuando se emiten mandatos como hostname

En sistemas Windows, después de crear un alias del adaptador MS Loopback, cuando emita determinados mandatos como hostname, el sistema operativo responderá incorrectamente con la dirección del alias en lugar de la dirección local. Para corregir este problema, en la lista de conexiones de red, el alias recién añadido debe enumerarse bajo la dirección local. Esto asegurará que se accede a la dirección local antes que al alias de bucle de retorno.

Para comprobar la lista de conexiones de red:

1. Pulse **Inicio > Configuración > Conexiones de red y de acceso telefónico**

2. En la opción de menú **Opciones avanzadas**, seleccione **Configuración avanzada...**
3. Asegúrese de que se enumera en primer lugar **Conexión de área local** en el recuadro **Conexiones**
4. Si es necesario, utilice los botones de ordenación a la derecha para desplazar hacia arriba o abajo las entradas en la lista

Problema: en la plataforma Windows, se produce un comportamiento de la GUI inesperado al utilizar tarjetas de vídeo Matrox AGP

En la plataforma Windows cuando utiliza una tarjeta Matrox AGP, puede aparecer un comportamiento inesperado en la GUI de Load Balancer. Cuando pulsa el ratón, podría dañarse un bloque de espacio ligeramente mayor que el puntero del ratón provocando una posible inversión del resaltado o un desplazamiento de imágenes fuera del lugar de la pantalla. Las tarjetas Matrox anteriores no han mostrado este comportamiento. No hay un fix pack conocido cuando se utilizan tarjetas Matrox AGP.

Problema: comportamiento inesperado al ejecutar "rmmod ibmlb" (sistemas Linux)

En sistemas Linux, si dsserver todavía está en ejecución durante la eliminación manual del módulo kernel de Load Balancer, puede producirse un comportamiento inesperado, como un javacore o que se cierre la comunicación del sistema. Cuando elimina manualmente el módulo kernel de Load Balancer, primero debe detener dsserver.

Si no funciona "dsserver stop", detenga el proceso java con SRV_KNDConfigServer. Para detener el proceso encuentre su identificador de proceso utilizando el mandato `ps -ef | grep SRV_KNDConfigServer` y finalice el proceso utilizando el mandato `kill id_proceso`.

Puede ejecutar de modo seguro el mandato "rmmod ibmlb" para eliminar el módulo Load Balancer del kernel.

Problema: tiempo de respuesta lento cuando se ejecutan mandatos en la máquina de Dispatcher

Si ejecuta el componente Dispatcher para el equilibrio de carga, es posible sobrecargar el sistema con tráfico del cliente. El módulo kernel de Load Balancer tiene la máxima prioridad y, si gestiona constantemente paquetes del cliente, el resto del sistema podría quedarse sin respuesta. La ejecución de mandatos en el espacio de usuario puede llevar mucho tiempo completarse o puede que nunca se complete.

Si esto sucede, debería comenzar a reestructurar su configuración para impedir la sobrecarga de la máquina de Load Balancer con tráfico. Entre las alternativas se incluye distribuir la carga entre varias máquinas de Load Balancer o sustituir la máquina con un sistema más consistente y más rápido.

Cuando intente determinar si el tiempo de respuesta lento en la máquina se debe a un alto volumen de tráfico del cliente, considere si esto se produce durante los momentos de tráfico máximo del cliente. Los sistemas mal configurados que provocan bucles de direccionamiento también pueden provocar los mismos

síntomas. Pero antes de cambiar la configuración de Load Balancer, determine si los síntomas pueden deberse a un gran volumen de carga del cliente.

Problema: el asesor SSL o HTTPS no registra cargas del servidor (cuando se utiliza el reenvío mac)

Cuando se utiliza el método de reenvío mac, Load Balancer enviará paquetes a los servidores utilizando la dirección del clúster de la que se ha creado un alias en el bucle de retorno. Algunas aplicaciones servidor (como SSL) requieren que la información de configuración (como los certificados) sea según la dirección IP. La dirección IP debe ser la dirección del clúster que se configura en el bucle de retorno para que corresponda al contenido de los paquetes de entrada. Si no se utiliza la dirección IP del clúster cuando se configura la aplicación servidor, no se reenviará correctamente la petición del cliente al servidor.

Problema: se produce una desconexión del sistema principal si se cambia el tamaño de la ventana del navegador Netscape cuando se utiliza la administración Web

Si utiliza la administración Web remota para configurar Load Balancer, no cambie el tamaño (Minimizar, Maximizar, Restaurar minimizando, etc.) de la ventana del navegador Netscape en la que aparece la GUI de Load Balancer. Dado que Netscape vuelve a cargar una página cada vez que se cambia el tamaño de la ventana del navegador, esto provocará una desconexión del sistema principal. Tendrá que volver a conectar con el sistema principal cada vez que cambie el tamaño de la ventana. Si realiza administración Web remota en la plataforma Windows, utilice Internet Explorer.

Problema: está habilitada la agrupación de sockets y el servidor Web se enlaza a 0.0.0.0

Cuando ejecuta el servidor IIS de Microsoft versión 5.0 en servidores finales Windows, debe configurar el servidor IIS de Microsoft para que sea específico del enlace. De lo contrario, se inhabilitará la agrupación de sockets por omisión y el servidor Web se enlazarán a 0.0.0.0 y realizará la escucha de todo el tráfico, en lugar de enlazar a las direcciones IP virtuales configuradas como varias identidades para el sitio. Si se queda inactiva una aplicación en el sistema principal local cuando está habilitada la agrupación de sockets, los asesores del servidor ND de AIX o Windows detectarán esto; no obstante, si se queda inactiva una aplicación en un sistema principal virtual cuando el sistema principal local está activo, los asesores no detectarán la anomalía y Microsoft IIS seguirá respondiendo a todo el tráfico, incluida la aplicación inactiva.

Para determinar si está habilitada la agrupación de sockets y si el servidor Web se enlaza a 0.0.0.0, emita este mandato:

```
netstat -an
```

Las instrucciones sobre cómo configurar el servidor IIS de Microsoft para que sea específico de enlace (inhabilite la agrupación de sockets), se encuentran en el sitio Web de servicios de soporte del producto Microsoft. También puede visitar una de estas URL para obtener esta información:

IIS5: Hardware Load Balance Does Not Detect a Stopped Web Site (Q300509)

<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q300509>

How to Disable Socket Pooling (Q238131)

<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q238131>

Problema: en sistemas Windows, aparecen caracteres nacionales Latin-1 dañados en la ventana de indicador de mandatos

En las ventanas de indicador de mandatos del sistema operativo Windows, quizá algunos caracteres nacionales de la familia Latin-1 aparezcan dañados. Por ejemplo, la letra "a" con una tilde podría mostrarse como el símbolo pi. Para corregir esto, debe cambiar las propiedades de font de la ventana de línea de mandatos. Para cambiar el font, realice lo siguiente:

1. Pulse en el icono en la esquina superior izquierda de la ventana de indicador de mandatos
2. Seleccione Propiedades, luego pulse la pestaña Fuente
3. El font por omisión es Fuentes de mapa de bits; cambie este valor por Lucida Console y pulse Aceptar

Problema: en HP-UX, se produce un error de falta de memoria/hebra de Java

Algunas instalaciones de HP-UX 11i están preconfiguradas para sólo permitir 64 hebras por proceso. No obstante, algunas configuraciones de Load Balancer requieren una cantidad mayor. En los sistemas HP-UX, establezca las hebras por proceso como mínimo en 256. Para aumentar este valor, utilice el programa de utilidad "sam" para establecer el parámetro de kernel `max_thread_proc`. Si se espera un uso masivo, puede ser necesario aumentar `max_thread_proc` por encima de 256.

Para aumentar `max_thread_proc`, haga lo siguiente:

1. En la línea de mandatos, escriba: `sam`
2. Seleccione **Kernel Configuration** (Configuración del kernel) > **Configurable Parameters** (Parámetros configurables)
3. Desde la barra de desplazamiento, seleccione `max_thread_proc`
4. Pulse la barra espaciadora para resaltar `max_thread_proc`
5. Pulse la tecla tabuladora una vez y, después, pulse la tecla de flecha a la derecha hasta que seleccione **Actions**
6. Pulse Intro para mostrar el menú **Actions** (Acciones), luego pulse **M** para seleccionar Modify Configurable Parameter (Modificar parámetro configurable). Si no aparece esta opción, resalte `max_thread_proc`
7. Pulse la tecla tabuladora hasta que seleccione el campo **Formula/Value** (Formato/valor)
8. Entre un valor de 256 o superior.
9. Pulse **OK** (Aceptar)
10. Pulse la tecla tabuladora una vez y, después, seleccione **Actions**
11. Pulse **K** para Process New Kernel (Procesar nuevo kernel)
12. Seleccione **Yes** (Sí)
13. Rearranque el sistema

Problema: en los sistemas Windows, los asesores y los destinos de alcance marcan como inactivos todos los servidores

Cuando configura el adaptador en una máquina de Load Balancer, debe asegurarse de que los dos valores siguientes son correctos para que el asesor funcione:

- Inhabilite Task Offloading, que se suele utilizar más usualmente en tarjetas de adaptador 3Com.
 - Para inhabilitar Task offloading: vaya a Inicio > Configuración > Panel de control > Conexiones de red y de acceso telefónico, luego seleccione el adaptador.
 - En la ventana emergente, pulse Propiedades.
 - Pulse Configurar y seleccione la pestaña Opciones avanzadas.
 - En el panel de propiedades, seleccione la propiedad Task Offload, luego seleccione inhabilitar en el campo Valor.
- Habilite el Protocolo 1 (ICMP) para protocolos IP si habilita el filtrado TCP/IP. Si no se habilita ICMP, no se superará la prueba de ping con el servidor final. Para comprobar si ICMP está habilitado:
 - Vaya a Inicio > Configuración > Panel de control > Conexiones de red y de acceso telefónico y seleccione el adaptador.
 - En la ventana emergente, pulse Propiedades.
 - En el panel de componentes, seleccione Protocolo Internet (TCP/IP) y pulse Propiedades.
 - Pulse Opciones avanzadas y seleccione la pestaña Opciones.
 - Seleccione Filtrado TCP/IP en el panel Opciones y pulse Propiedades.
 - Si ha seleccionado **Permitir filtrado TCP/IP** y **Permitir sólo** para Protocolos IP, debe añadir el Protocolo IP 1. Esto debe añadirse además de los puertos TCP y UDP que permite.

Problema: en la plataforma Windows, se resuelve la dirección IP con el nombre de sistema principal cuando se ha configurado más de una dirección con el adaptador

En la plataforma Windows, cuando configura un adaptador con más de una dirección IP, configure la dirección IP que desea afiliar al nombre de sistema principal primero del registro.

Puesto que Load Balancer depende de `InetAddress.getLocalHost()` en muchas instancias (por ejemplo, `lbkeys create`), varias direcciones IP que tienen un alias con un sólo adaptador podrían provocar problemas. Para impedir este problema, enumere la dirección IP con la que desea que se resuelva la dirección IP primero en el registro. Por ejemplo:

1. Inicie Regedit
2. Modifique estos nombres de valor como se detalla a continuación:
 - `HKEY_LOCAL_MACHINE -> SYSTEM -> ControlSet001 -> Services -> SuDirecciónInterfaz} -> Parameters -> Tcpi -> IPAddress`
 - Sitúe la dirección IP con la que desea que el nombre de sistema principal se resuelva primero.
 - `HKEY_LOCAL_MACHINE -> SYSTEM -> ControlSet001 -> Services -> Tcpi -> Parameters -> Interfaces -> SuDirecciónInterfaz -> IPAddress`
 - Sitúe la dirección IP con la que desea que el nombre de sistema principal se resuelva primero.
 - `HKEY_LOCAL_MACHINE -> SYSTEM -> ControlSet002 -> Services -> SuDirecciónInterfaz -> Parameters -> Tcpi -> IPAddress`
 - Sitúe la dirección IP con la que desea que el nombre de sistema principal se resuelva primero.

- HKEY_LOCAL_MACHINE -> SYSTEM -> ControlSet002 -> Services -> Tcpip -> Parameters -> Interfaces -> *SuDirecciónInterfaz* -> IPAddress
 - Sitúe la dirección IP con la que desea que el nombre de sistema principal se resuelva primero.
 - HKEY_LOCAL_MACHINE -> SYSTEM -> CurrentControlSet -> Services-> *SuDirecciónInterfaz* -> Parameters -> Tcpip- > IPAddress
 - Sitúe la dirección IP con la que desea que el nombre de sistema principal se resuelva primero.
 - HKEY_LOCAL_MACHINE -> SYSTEM -> CurrentControlSet -> Services-> Tcpip -> Parameters -> Interfaces -> *SuDirecciónInterfaz* -> IPAddress
 - Sitúe la dirección IP con la que desea que el nombre de sistema principal se resuelva primero.
3. Rearranque el equipo
 4. Compruebe que el nombre de sistema principal se resuelve con la dirección IP correcta. Por ejemplo, ejecute ping *SuNombreSistemaPrpal*.

Problema: en sistemas Windows, después de una caída de la red, los asesores no funcionan en una configuración de alta disponibilidad

Por omisión, cuando el sistema operativo Windows detecta una caída de la red, borra su antememoria ARP (Address Resolution Protocol), incluidas todas las entradas estáticas. Cuando la red está disponible, la antememoria ARP se vuelve a rellenar con peticiones ARP enviadas en la red.

Con una configuración de alta disponibilidad, cuando una pérdida de conectividad de red influye en uno o los dos servidores, éstos se hacen con el control de las operaciones primarias. Cuando se envía la petición ARP para rellenar la antememoria ARP, los dos servidores responden, lo que provoca que la antememoria ARP marque la entrada como no válida. Por lo tanto, los asesores no pueden crear un socket para los servidores finales.

Si se impide que el sistema operativo Windows borre la antememoria ARP cuando hay una pérdida de conectividad se soluciona este problema. Microsoft ha publicado un artículo que describe cómo llevar a cabo esta tarea. Este artículo está en el sitio Web de Microsoft, ubicado en la en la base de información de Microsoft, artículo número 239924: <http://support.microsoft.com/default.aspx?scid=kb;en-us;239924>.

A continuación figura un resumen de los pasos, que se describen en el artículo de Microsoft, para impedir que el sistema borre la antememoria ARP:

1. Utilice el Editor del Registro (regedit o regedit32) para abrir el registro.
2. Consulte la clave siguiente del registro:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters
3. Añada este valor del registro: Nombre de valor: DisableDHCPMediaSense Tipo de valor: REG_DWORD.
4. Después de que se añade la clave, edite el valor y establézcalo en 1.
5. Rearranque la máquina para que el cambio entre en vigor.

Nota: Esto influye en la antememoria ARP independientemente del valor de DHCP.

Problema: en sistemas Linux, no utilice el mandato "IP address add" cuando cree un alias de varios clústeres en el dispositivo de bucle de retorno

Se deben tener determinadas consideraciones cuando se utilizan servidores Linux kernel 2.4.x y el método de reenvío MAC de Dispatcher. Si el servidor tiene una dirección del clúster configurada en el dispositivo de bucle de retorno utilizando el mandato `ip address add`, sólo se puede crear un alias de clúster de dirección.

Cuando cree un alias de varios clústeres con el dispositivo de bucle de retorno utilice el mandato `ifconfig`, por ejemplo:

```
ifconfig lo:núm direcciónClúster netmask 255.255.255.255 up
```

Además, hay incompatibilidades entre los métodos `ifconfig` e `ip` de configurar interfaces. El procedimiento recomendado sugiere que un sitio seleccione un método y utilice ese método de forma exclusiva.

Problema: mensaje de error "dirección del direccionador no especificada o no válida para el método del puerto"

Cuando añada servidores a la configuración de Dispatcher, puede producirse este mensaje de error: "Error: dirección del direccionador no especificada o no válida para el método del puerto".

Utilice la lista de comprobación para determinar el problema:

- Asegúrese de que ha aplicado el último nivel de mantenimiento.
- Asegúrese de que utiliza una distribución IBM de Java (excepto en plataformas Solaris).
- Asegúrese de que no está configurado su sistema para utilizar DHCP en sistemas Windows.
- Si el método de reenvío es `mac` (valor por omisión) deben estar en la misma subred el servidor, el clúster y al menos una tarjeta NIC admitida. Por ejemplo, no puede definir un clúster de 10.1.1.1 y un servidor de 130.2.3.4 porque no están en la misma subred.

Nota: Si el método de reenvío es `nat` o `cbr`, los servidores no tienen que estar en la misma subred que el clúster.

- Si todos están en la misma subred y ha creado un alias del clúster, asegúrese de que crea un alias del clúster en una tarjeta NIC que direcciona a esta subred. Por ejemplo si se define `en0` para 13.2.3.4 y `en1` para 9.1.2.3 y la definición de clúster es 9.5.7.3, debe configurar el clúster en `en1`. La interfaz por omisión es `en0`.
- En plataformas Linux, para asegurarse de que ha cargado el kernel correcto busque en el directorio `/usr/lpp/ibm/internet/nd/logs/dispatcher` el archivo `loadoutput.log`. Compruebe si en este archivo se informa de errores.

El valor por omisión del parámetro de direccionador es 0, que indica que el servidor es local. Si establece la dirección del direccionador del servidor en un valor que no es 0, esto indica que es un servidor remoto, en una subred distinta. Si desea más información sobre el parámetro del direccionador en el mandato `server add`, consulte el apartado "dscontrol server — configurar servidores" en la página 392.

Si el servidor que añade se ubica en una subred distinta, el parámetro de direccionador debería ser la dirección del direccionador que se va a utilizar en la subred local para comunicarse con el servidor remoto.

Problema: en sistemas Solaris, los procesos de Load Balancer finalizan cuando sale de la ventana de terminal desde la que se han iniciado

En sistemas Solaris, después de iniciar scripts de Load Balancer (como `dsserver` o `lbadmin`) desde una ventana de terminal, si sale de esa ventana, también sale el proceso de Load Balancer.

Para solucionar este problema, inicie los scripts de Load Balancer con el mandato **nohup**. Por ejemplo: **nohup dsserver**. Este mandato impide que los procesos iniciados desde la sesión de terminal reciban una señal de cierre de comunicación del sistema del terminal cuando sale, que permite a los procesos continuar incluso después de que haya finalizado la sesión de terminal. Utilice el mandato **nohup** delante de cualquier script de Load Balancer que desee seguir procesando cuando haya terminado la sesión de terminal.

Problema: Se ha producido un retardo al cargar una configuración de Load Balancer

La configuración de Load Balancer puede tardar mucho en cargarse debido a las llamadas al Sistema de nombres de dominio (DNS) que se realizan para resolver y verificar la dirección de servidor.

Si el DNS de la máquina de Load Balancer se configura incorrectamente o si el DNS en general lleva mucho tiempo, disminuirá la velocidad de la carga de la configuración debido a los procesos Java que envían peticiones de DNS en la red.

Una solución para esto es añadir las direcciones del servidor y los nombres de sistema principal al archivo `/etc/hosts` local.

Problema: en sistemas Windows, aparece un mensaje de error de conflicto de dirección IP

Si se configura la alta disponibilidad, podrían configurarse direcciones del clúster en las dos máquinas por un breve período y provocar este mensaje de error: Hay un conflicto de dirección IP con otro sistema en la red. En este caso, puede ignorar el mensaje con seguridad. Es posible que una dirección del clúster se configure brevemente en las dos máquinas de alta disponibilidad a la vez, especialmente durante el inicio de cualquiera de las máquinas o cuando se ha iniciado la toma del control.

Compruebe los scripts `go*` para asegurarse de que configuran y desconfiguran correctamente direcciones del clúster. Si ha invocado un archivo de configuración y tiene scripts `go*` instalados, asegúrese de que no tiene ninguna sentencia de mandato `"executor configure"` para las direcciones del clúster en el archivo de configuración, porque esto entrará en conflicto con los mandatos `configure` y `unconfigure` de los scripts `go*`.

Si desea más información sobre scripts `go*` cuando configura la característica de alta disponibilidad, consulte el apartado "Utilización scripts" en la página 209.

Problema: las dos máquinas, primaria y de reserva, están activas en una configuración de alta disponibilidad

Este problema podría producirse cuando no se ejecutan los scripts go en alguna de las máquinas primaria o de reserva. Los scripts go no pueden ejecutarse si no se ha iniciado dsserver en las dos máquinas. Compruebe las dos máquinas y asegúrese de que dsserver está en ejecución.

Problema: no se pueden realizar las peticiones del cliente cuando el sistema intenta devolver respuestas de páginas de gran tamaño

Las peticiones del cliente que producen unas respuestas de páginas de gran tamaño superan el tiempo de espera si la unidad de transmisión máxima (MTU) no se establece correctamente en la máquina de Dispatcher. Para los métodos de reenvío cbr y nat del componente Dispatcher, esto puede suceder porque Dispatcher toma por omisión el valor de la MTU, en lugar de negociar el valor.

La MTU se establece en cada sistema operativo basándose en el tipo de soporte de comunicaciones (por ejemplo, Ethernet o Token-Ring). Los direccionadores del segmento local podrían tener establecida una MTU de menor tamaño si se conectan con un tipo de soporte de comunicaciones distinto. En condiciones de tráfico normal de TCP, se produce una negociación de la MTU durante la configuración de la conexión y se utiliza la MTU de menor tamaño para enviar datos entre máquinas.

Dispatcher no admite la negociación de la MTU para el método de reenvío cbr o nat de Dispatcher porque interviene activamente como un punto final para conexiones TCP. Para el reenvío cbr y nat, Dispatcher toma por omisión el valor de MTU de 1500. Este valor es el tamaño de la MTU típico para Ethernet estándar, de manera que la mayoría de los clientes no tienen que ajustar este valor.

Cuando se utiliza el método de reenvío cbr o nat de Dispatcher, si tiene un direccionador al segmento local que tiene una MTU de menor tamaño, debe establecer la MTU en la máquina de Dispatcher para que coincida con la MTU de menor tamaño.

Para resolver este problema, utilice el mandato siguiente para establecer el valor del tamaño de segmento máximo (mss): `dscontrol executor set mss nuevo_valor`

Por ejemplo:

```
dscontrol executor set mss 1400
```

El valor por omisión de mss es 1460.

El valor de mss no se aplica para el método de reenvío mac de Dispatcher ni para ningún otro componente no Dispatcher de Load Balancer.

Problema: en sistemas Windows, se produce el error "el servidor no responde" cuando se emite dscontrol o lbadmin

Cuando existe más de una dirección IP en un sistema Windows y el archivo `hosts` no especifica la dirección que se va a asociar al nombre de sistema principal, el sistema operativo selecciona la dirección de menor tamaño para asociarla al nombre de sistema principal.

Para resolver este problema, actualice el archivo `c:\Windows\system32\drivers\etc\hosts` con el nombre de sistema principal de su máquina y la dirección IP que desee asociar al nombre de sistema principal.

IMPORTANTE: la dirección IP no puede ser una dirección del clúster.

Problema: es posible que las máquinas de Dispatcher de alta disponibilidad no se puedan sincronizar en sistemas Linux para S/390 en controladores qeth

Cuando utiliza la característica de alta disponibilidad en máquinas Linux para S/390 con el controlador de red qeth, puede que los Dispatcher activo y en espera no se sincronicen. Este problema podría limitarse a Linux Kernel 2.6.

Si aparece este problema, utilice este método alternativo:

Defina un dispositivo de red de canal a canal (CTC) entre las imágenes de Dispatcher activa y en espera y añada pulsos entre las dos direcciones IP de punto final de CTC.

Problema: sugerencias para configurar la alta disponibilidad

Con la función de alta disponibilidad de Load Balancer, una máquina asociada puede tomar el control del equilibrio de carga si la máquina asociada primaria sufre una anomalía o se apaga. Para mantener conexiones entre las máquinas asociadas de alta disponibilidad, se pasan entre ellas registros de conexión. Cuando la máquina asociada en espera toma el control de la función de equilibrio de carga, la dirección IP de clúster se suprime de la máquina en espera y se añade a la nueva máquina primaria. Esta operación de toma de control puede verse afectada por muchos factores de tiempo y configuración.

Las sugerencias que se detallan en este apartado puede ayudarle a reducir la cantidad de problemas derivados de los problemas de configuración de alta disponibilidad, como por ejemplo:

- Conexiones desactivadas después de la toma de control
- No se pueden sincronizar máquinas asociadas
- Peticiones dirigidas erróneamente a la máquina asociada de reserva

Las siguientes sugerencias le ayudarán a configurar correctamente la característica de alta disponibilidad de las máquinas de Load Balancer.

- La posición de los mandatos de alta disponibilidad en los archivos de script es muy importante y puede influir en los resultados.

Ejemplos de mandatos de alta disponibilidad son:

```
dscontrol highavailability heartbeat add ...  
dscontrol highavailability backup add ...  
dscontrol highavailability reach add ...
```

En la mayoría de los casos, debe colocar las definiciones de alta disponibilidad al final del archivo. Las sentencias de clúster, puerto y servidor se deben colocar antes de las sentencias de alta disponibilidad. Esto se debe a que al sincronizar la alta disponibilidad, busca las definiciones de clúster, puerto y servidor cuando se recibe un registro de conexión.

Si el clúster, puerto y servidor no existen, se elimina el registro de conexión. Si se produce una toma de control y el registro de conexión no se ha duplicado en la máquina asociada, la conexión falla.

La excepción a esta norma es cuando se utilizan servidores con ubicación compartida que configurados con el método de reenvío MAC. En este caso, las sentencias de alta disponibilidad deben indicarse antes de las sentencias de servidor con ubicación compartida. Si las sentencias de alta disponibilidad no se indican antes de las sentencias de servidor con ubicación compartida, Load Balancer recibe una petición para el servidor con ubicación compartida, pero parece la misma que una petición entrante para el clúster y se equilibra la carga. Esto lleva a una repetición en bucle de los paquetes de la red y a un tráfico excesivo. Cuando las sentencias de alta disponibilidad se colocan antes del servidor con ubicación compartida, Load Balancer sabe que no debe reenviar tráfico entrante a menos que esté en estado ACTIVO.

- En los sistemas operativos z/OS o OS/390, el hipervisor controla la interfaz y conecta la interfaz real con los sistemas operativos invitados. El hipervisor sólo permite que un sistema invitado se registre a la vez para una dirección IP y hay una ventana de actualización. Esto significa que cuando se elimina el IP de clúster de la máquina de reserva, es posible que se tenga que añadir un retardo antes de añadir el IP de clúster a la máquina primaria; de lo contrario, fallará y no se procesarán las conexiones entrantes.

Para corregir este comportamiento, añada un retardo de inactividad en el script goActive. El intervalo de tiempo de inactividad necesario depende del despliegue. Se recomienda iniciar con un tiempo de demora de inactividad de 10.

- Los sistemas asociados de alta disponibilidad deben poder detectarse mediante el mandato ping y deben estar en la misma subred.

Por omisión, las máquinas intentan comunicarse entre sí cada medio segundo y detectarán una anomalía después de cuatro intentos fallidos. Si hay mucha actividad en la máquina, esto puede producir casos de sustitución por anomalía cuando el sistema en realidad sigue funcionando correctamente. Puede aumentar el número de veces hasta que se produce la anomalía emitiendo:

```
dscontrol executor set hatimeout <valor>
```

- Cuando se sincronizan las máquinas asociadas, todos los registros de conexión se envían de la máquina activa a la máquina de reserva. La sincronización debe realizarse dentro del límite por omisión de 50 segundos.

Para llevarlo a cabo, las conexiones antiguas no deben permanecer en la memoria durante un periodo de tiempo largo. En concreto, han habido problemas con los puertos LDAP y grandes periodos staletimeout (más de un día). Si se establece un periodo staletimeout grande las conexiones antiguas permanecerán en memoria, lo que provocará que se pasen más registros de conexión durante la sincronización así como más uso de memoria en las dos máquinas.

Si la sincronización sufre una anomalía con un periodo staletimeout razonable, puede aumentar el tiempo de espera de sincronización emitiendo el mandato:

```
e xm 33 5 new_timeout
```

Este mandato no se almacena en el archivo de configuración cuando se guarda, por lo que se debe añadir manualmente al archivo de configuración si desea que este valor permanezca entre conclusiones.

El valor de tiempo de espera se almacena la mitad de segundos; por lo tanto, el valor por omisión de nuevo_valor_por_omisión es 100 (50 segundos).

- Cuando una máquina asociada toma el control de la carga de trabajo, emite una respuesta ARP injustificada para notificar a las máquinas de la misma subred la nueva dirección de hardware asociada a la dirección IP de clúster. Debe

asegurarse de que los direccionadores reconozcan los ARP injustificados y actualicen su antememoria o las peticiones se enviarán a la máquina asociada inactiva.

Nota: Para obtener información sobre la configuración de la característica de alta disponibilidad, consulte “Alta disponibilidad” en la página 204.

Problema: en Linux, existen limitaciones de configuración de Dispatcher cuando se utilizan servidores zSeries o S/390 que disponen de tarjetas OSA (Open System Adapter)

En general, cuando se utiliza el método de reenvío MAC, los servidores de la configuración de Load Balancer deben estar todos en el mismo segmento de red misma, independientemente de la plataforma. Los dispositivos de red activos como el direccionador, los puentes y los cortafuegos dificultan el funcionamiento de Load Balancer. Esto se debe a las funciones de Load Balancer, como un direccionador especializado, que sólo modifican las cabeceras de capa de enlace para su salto siguiente y final. Cualquier topología de red en la que el salto siguiente no sea el último salto no es válida para Load Balancer.

Nota: Los túneles, como los dispositivos de canal a canal (CTC) o el vehículo de comunicación entre usuarios (IUCV) suelen recibir soporte. Sin embargo, Load Balancer debe reenviar a través del túnel directamente al destino final, no puede ser un túnel de red a red.

Se trata de una limitación para los servidores zSeries y S/390 que comparten la tarjeta OSA, porque este adaptador opera de forma distinta a la mayoría de las tarjetas de red. La tarjeta OSA dispone de una implementación de capa de enlace propia, que no tiene nada que ver con Internet, que se muestra a los sistemas principales Linux y z/OS por detrás. En efecto, las tarjetas OSA se comunican como si fueran sistemas de Ethernet a Ethernet (no como sistemas principales OSA) y los sistemas principales que la utilizan responderán como si fueran Ethernet.

La tarjeta OSA también lleva a cabo algunas funciones que se relacionan directamente con la capa IP. Un ejemplo de la función que realiza es responder a peticiones ARP (Address Resolution Protocol). Otra función es que la tarjeta OSA compartida direcciona los paquetes IP en base a la dirección IP de destino, en lugar de una dirección Ethernet como un conmutador de capa 2. En efecto, la tarjeta OSA es en sí un segmento de red con puente.

Load Balancer ejecutándose en un sistema principal S/390 Linux o zSeries Linux puede efectuar reenvíos a sistemas principales en el mismo OSA o a sistemas principales en Ethernet. Todos los sistemas principales que comparten OSA están en efecto en el mismo segmento.

Load Balancer puede *reenviar fuera* de una tarjeta OSA compartida debido a la naturaleza del puente de OSA. El puente reconoce el puerto OSA propietario de la dirección IP de clúster. El puente reconoce la dirección MAC de los sistemas principales conectados directamente con el segmento Ethernet. Por lo tanto, Load Balancer puede utilizar el reenvío MAC a través de un puente OSA.

Sin embargo, Load Balancer no puede realizar reenvíos a una tarjeta OSA compartida. Esto incluye Load Balancer en un sistema S/390 Linux cuando el servidor de activar está en una tarjeta OSA distinta de la de Load Balancer. La tarjeta OSA correspondiente al servidor de servidor anuncia la dirección MAC de

OSA para la dirección IP del servidor, pero cuando llega un paquete con la dirección de destino Ethernet de la tarjeta OSA del servidor y la dirección IP del clúster, la tarjeta OSA del servidor no sabe cuál de los sistemas principales, si hay alguno, debe recibir dicho paquete. Los mismos principios que permiten que el reenvío MAC de OSA a Ethernet funcione fuera de una tarjeta OSA compartida no se aplican al intentar el reenvío a una tarjeta OSA compartida.

Método alternativo:

En configuraciones de Load Balancer que utilizan servidores zSeries o S/390 que tienen tarjetas OSA; hay dos enfoques que puede utilizar para resolver temporalmente el problema descrito.

1. Utilizando características de plataforma

: si los servidores de la configuración de Load Balancer están en el mismo tipo de plataforma zSeries o S/390, puede definir conexiones de punto a punto (CTC o IUCV) entre Load Balancer y cada servidor. Configurar los puntos finales con direcciones IP privadas. La conexión de punto a punto sólo se utiliza para el tráfico de Load Balancer a servidor. A continuación, añada los servidores con la dirección IP del punto final de servidor del túnel. Con esta configuración, el tráfico de clúster atraviesa la tarjeta OSA de Load Balancer y se reenvía a través de la conexión punto a punto donde el servidor responde mediante su propia ruta por omisión. La respuesta utiliza la tarjeta OSA del servidor para enviarse, que puede o no ser la misma tarjeta.

2. Utilizando la característica GRE de Load Balancer

Nota: Nota: la característica GRE no está disponible en el entorno de protocolo dual de Load Balancer para IPv4 y IPv6.

Si los servidores de la configuración de Load Balancer no están en el mismo tipo de plataforma zSeries o S/390, o si no es posible definir una conexión de punto a punto entre Load Balancer y cada servidor, se recomienda utilizar la característica GRE (encapsulamiento genérico de direccionamiento) de Load Balancer, que es un protocolo que permite a Load Balancer realizar reenvíos a través de direccionadores.

Al utilizar GRE, Load Balancer recibe el paquete de IP cliente a clúster encapsulado y lo envía al servidor. En el servidor, el paquete IP de cliente a clúster original se excapsula y el servidor responde directamente al cliente. La ventaja de utilizar GRE es que Load Balancer sólo detecta el tráfico de cliente a servidor, no detecta el tráfico de servidor a cliente. La desventaja es que reduce el tamaño de segmento máximo (MSS) de la conexión TCP debido a la carga adicional de encapsulación.

Para configurar Load Balancer para realizar reenvíos con encapsulación GRE, añada los servidores utilizando el siguiente mandato:

```
dscontrol server add cluster_addr:port:backend_server router
backend_server
```

donde router backend_server es válido si Load Balancer y el servidor de programa de fondo están en la misma subred IP. De lo contrario, especifique como direccionador la dirección IP válida del salto siguiente.

Para configurar sistemas Linux para realizar la excapsulación GRE nativa, para cada servidor de programa de fondo, emita los siguientes mandatos:

```
modprobe ip_gre
ip tunnel add gre1b0 mode gre ikey 3735928559
ip link set gre1b0 up
ip addr add cluster_addr dev gre1b0
```


Nota: No defina la dirección de clúster en el bucle de retorno de los servidores de programa de fondo. Cuando se utilizan servidores de programa de fondo z/OS, se deben utilizar mandatos específicos de z/O2 para configurar los servidores para realizar la excapsulación GRE.

Problema: en algunas versiones de Linux, se produce una pérdida de memoria al ejecutar Dispatcher configurado con el gestor y los asesores

Al ejecutar Load Balancer configurado con las características de gestor y asesor, se pueden producir grandes pérdidas de memoria en algunas versiones de Red Hat Linux. La pérdida de memoria Java aumenta si configura un valor pequeño de intervalo de tiempo para el asesor.

Las versiones de la MVM de SDK Java de IBM y la biblioteca de hebras POSIX nativa (NPTL) que se entregan con algunas distribuciones Linux, como Red Hat Enterprise Linux 3.0, pueden hacer que se produzca la pérdida de memoria. La biblioteca de hebras mejorada que se proporciona con algunas distribuciones de sistemas Linux como Red Hat Enterprise Linux 3.0 da soporte a NPTL.

Consulte <http://www.ibm.com/developerworks/java/jdk/linux/tested.html> para obtener la última información sobre sistemas Linux y el SDK Java de IBM que se entrega con estos sistemas.

Como herramienta de determinación de problemas, utilice el mandato `vmstat` o `ps` para detectar pérdidas de memoria.

Para corregir la pérdida de memoria, emita el siguiente mandato antes de ejecutar la máquina Load Balancer para así inhabilitar la biblioteca NPTL:

```
export LD_ASSUME_KERNEL=2.4.10
```

Problema: en SUSE Linux Enterprise Server 9, Dispatcher reenvía paquetes, pero éstos no llegan al servidor de programa de fondo

En Suse Linux Enterprise Server 9, cuando se utiliza el método de reenvío MAC, el informe de Dispatcher puede indicar que se ha reenviado el paquete (la cuenta de paquetes aumenta); sin embargo, el paquete nunca llega al servidor de programa de fondo.

Cuando aparece este problema, puede observar una de las dos cosas:

- En el máquina Dispatcher, se visualiza un mensaje parecido al siguiente:
`ip_finish_output2: No hay antememoria de cabecera ni vecina`
- En el cliente, se visualiza un mensaje parecido al siguiente:
`ICMP No se puede alcanzar la fragmentación: es necesaria la fragmentación`

Este problema puede deberse al módulo NAT de tablas `ip` que se carga. En SLES 9, existe un posible error, aunque sin confirmar, en esta versión de iptables que provoca un comportamiento extraño al interactuar con Dispatcher.

Solución:

Descargue el módulo NAT de iptables y el módulo de seguimiento de conexiones.

Por ejemplo:

```
# lsmod | grep ip
  iptable_filter          3072  0
  iptable_nat            22060  0
  ip_conntrack           32560  1 iptable_nat
  ip_tables              17280  2
  iptable_filter,iptable_nat
  ipv6                  236800  19
  # rmmod iptable_nat
  # rmmod ip_conntrack
```

Elimine los módulos en el orden de su uso. De manera específica, puede eliminar un módulo sólo si la cuenta de referencia (la última columna de la salida `lsmod`) es cero. Si ha configurado alguna norma en iptables, debe eliminarla. Por ejemplo: `iptables -t nat -F`.

El módulo `iptable_nat` utiliza `ip_conntrack`, por lo que primero se debe eliminar el módulo `iptable_nat` y, a continuación, el módulo `ip_conntrack`.

Nota: Con sólo tratar de listar las normas configuradas en una tabla se carga el módulo correspondiente; por ejemplo, `iptables -t nat -L`. Asegúrese de que no ejecutar este mandato después de eliminar los módulos.

Problema: en sistemas Windows, el mensaje de conflicto entre direcciones IP aparece durante la toma de control de alta disponibilidad

En sistemas Windows, si ejecuta la característica de alta disponibilidad de Load Balancer, los scripts `go*` se utilizan para configurar la dirección IP de clúster en el sistema activo de Load Balancer y para desconfigurar la dirección IP de clúster del sistema de reserva cuando se produce una toma de control. Si se ejecuta el script `go*` que configura la dirección IP de clúster de la máquina activa antes de ejecutar el script `go*` para desconfigurar la dirección IP de clúster de la máquina en espera, pueden surgir problemas. Es posible que aparezca una ventana emergente que le indique que el sistema ha detectado un conflicto entre direcciones IP. Si ejecuta el mandato `ipconfig /all`, también puede ver que aparece una dirección IP 0.0.0.0 de la máquina.

Solución:

Emita el mandato siguiente para desconfigurar manualmente la dirección IP de clúster de la máquina primaria:

```
dscontrol executor unconfigure clusterIP
```

Esto elimina la dirección 0.0.0.0 de la pila IP de Windows.

Una vez que la máquina asociada de alta disponibilidad libera la dirección IP de clúster, emita el siguiente mandato para volver a añadir manualmente la dirección IP de clúster:

```
dscontrol executor configure clusterIP
```

Después de emitir este mandato, busque de nuevo la dirección IP de clúster en la pila IP de Windows emitiendo el siguiente mandato:

```
ipconfig /all
```

Problema: iptables de Linux puede impedir el direccionamiento de paquetes

iptables en Linux puede dificultar el equilibrio de carga y debe estar inhabilitado en la máquina de Dispatcher.

Emita el siguiente mandato para determinar si iptables se ha cargado:

```
lsmod | grep ip_tables
```

La salida del mandato anterior puede ser parecida a la siguiente:

```
ip_tables          22400    3 iptable_mangle,iptable_nat,iptable_filter
```

Emita el siguiente mandato para cada iptable que aparece en la salida para visualizar las normas de las tablas:

```
iptables -t <nombre_abreviado> -L
```

Por ejemplo:

```
iptables -t mangle -L
iptables -t nat -L
iptables -t filter -L
```

Si iptable_nat se ha cargado, se debe descargar. Puesto que iptable_nat tiene una dependencia en iptable_conntrack, también se debe eliminar iptable_conntrack.

Emita el siguiente mandato para descargar estas dos tablas ip:

```
rmmod iptable_nat iptable_conntrack
```

Problema: no se puede añadir un servidor IPv6 a la configuración de Load Balancer en sistemas Solaris

En sistemas Solaris, al intentar configurar un servidor IPv6 en una instalación de Load Balancer para IPv4 y IPv6, aparece el mensaje no se puede añadir servidor. Esto se puede producir por la forma en que el sistema operativo Solaris maneja la petición de ping para una dirección IPv6.

En sistemas Solaris, al añadir un servidor a la configuración, Load Balancer intenta comunicarse con un mandato ping con el servidor para obtener la dirección MAC del servidor. La máquina Solaris puede elegir una dirección de clúster configurada como la dirección de origen de la petición ping, en lugar de utilizar la dirección NFA de la máquina. Si la dirección de clúster se ha configurado en el bucle de retorno del servidor, la respuesta al mandato ping no se recibe en la máquina de Load Balancer; por lo tanto, no añade el servidor a la configuración.

La solución es configurar otra dirección IPv6 en la máquina de Load Balancer antes o después de configurar la dirección de clúster IPv6. Esta dirección debe ser una dirección que no tenga un alias en el bucle de retorno del servidor de programa de fondo que se trata de añadir a la configuración de Load Balancer. A continuación, añada el servidor a la configuración de Load Balancer.

Aparece un mensaje de aviso Java al instalar arreglos de servicio

Load Balancer proporciona un conjunto de archivos Java junto con la instalación del producto. La instalación de producto consta de varios paquetes que no es necesario instalar en la misma máquina. Un ejemplo de ello es el paquete de Metric Server, el paquete de administración y el paquete base. Todos estos paquetes de código requieren un conjunto de archivos Java para funcionar, aunque

cada uno de los tres paquetes puede instalarse en una máquina distinta. Como tal, cada uno de estos paquetes instala un conjunto de archivos Java. Cuando se instalan en la misma máquina, cada uno de estos conjuntos de archivos será propietario del conjunto de archivos Java. Al instalar el segundo y tercer conjunto de datos Java, recibirá mensajes de aviso indicando que el conjunto de archivos Java también es propiedad de otro conjunto de archivos.

Al instalar código utilizando los métodos de instalación nativos (por ejemplo, installp en AIX), debe ignorar los mensajes de aviso que comunican que el conjunto de archivos Java es propiedad de otro conjunto de archivos.

Actualización del conjunto de archivos Java con la instalación de Load Balancer

Durante el proceso de instalación de Load Balancer, también se instala un conjunto de archivos Java. Load Balancer será la única aplicación que utilice la versión Java que se instala con el producto. No debe actualizar esta versión del conjunto de archivos Java sin ayuda especializada. Si hay un problema que requiera una actualización del conjunto de archivos Java, debe notificarlo al servicio de IBM para actualizar al nivel de arreglo oficial el conjunto de archivos Java que se envía con Load Balancer.

Resolución de problemas comunes—CBR

Problema: no se ejecutará CBR

Este problema puede producirse si otra aplicación utiliza uno de los puertos que CBR utiliza. Para obtener más información, consulte el apartado “Comprobación de los números de puerto de CBR” en la página 300.

Problema: el mandato cbrcontrol o lbadmin da un error

1. El mandato cbrcontrol devuelve: **Error: el servidor no responde**. O bien, el mandato lbadmin devuelve: **Error: no es posible acceder al servidor RMI**. Estos errores pueden producirse si su máquina tiene una pila con SOCKS. Para corregir este problema, edite el archivo socks.cnf para incluir las líneas siguientes:

```
EXCLUDE-MODULE java
EXCLUDE-MODULE javaw
```

2. Las consolas de administración de las interfaces (línea de mandatos, interfaz gráfica de usuario y asistentes) de Load Balancer se comunican con cbrserver utilizando RMI (Remote Method Invocation). La comunicación por omisión utiliza tres puertos; cada puerto se establece en el script de inicio de cbrserver:
 - 11099 para recibir mandatos de cbrcontrol
 - 10004 para enviar consultas de métrica a Metric Server
 - 11199 para el puerto del servidor RMI

Esto puede producir problemas si una de las consolas de administración se ejecuta en la misma máquina que un cortafuegos o a través de un cortafuegos. Por ejemplo, cuando Load Balancer se ejecuta en la misma máquina que un cortafuegos y emite mandatos cbrcontrol, podrían aparecer errores como **Error: el servidor no responde**.

Para impedir este problema, edite el archivo de scripts cbrserver para establecer el puerto utilizado por RMI para el cortafuegos (u otra aplicación). Cambie la línea: `LB_RMISERVERPORT=11199` por `LB_RMISERVERPORT=suPuerto`. Donde *suPuerto* es otro puerto.

Cuando haya terminado, reinicie `cbrserver` y abra el tráfico para los puertos: 11099, 10004, 11199 y 11100 o para el puerto seleccionado para la dirección del sistema principal desde donde se ejecutará la consola de administración.

3. También se pueden producir estos errores si aún no ha iniciado `cbrserver`.

Problema: no se equilibra la carga de las peticiones

Se ha iniciado Caching Proxy y CBR, pero no se equilibra la carga de las peticiones. Este error puede aparecer si inicia Caching Proxy antes de iniciar el ejecutor. Si esto sucede, el archivo de anotaciones cronológicas `stderr` para Caching Proxy contendrá este mensaje de error: "ndServerInit: Could not attach to executor" (ndServerInit: no se ha podido conectar con el ejecutor). Para evitar que suceda este problema, inicie el ejecutor antes de iniciar Caching Proxy.

Problema: en sistemas Solaris, el mandato `cbrcontrol executor start` da un error

En sistemas Solaris, el mandato `cbrcontrol executor start` devuelve: "Error: el ejecutor no se ha iniciado". Aparece este error si no configura la IPC (Comunicación entre procesos) para el sistema de modo que el tamaño máximo de un segmento de memoria compartida y los ID de semáforo sean mayores que el valor por omisión del sistema operativo. Para aumentar el tamaño del segmento compartido y de los ID de semáforo, debe editar el archivo `/etc/system`. Si desea más información sobre cómo configurar este archivo, consulte la página 113.

Problema: error sintáctico o de configuración

Si la norma de URL no funciona, esto puede deberse a un error sintáctico o de configuración. Para corregir este problema compruebe lo siguiente:

- Verifique que la norma se ha configurado correctamente. Consulte el Apéndice B, "Sintaxis de la norma de contenido (patrón)", en la página 475, si desea más detalles.
- Emita un mandato `cbrcontrol rule report` para esta norma y compruebe la columna de 'Número de veces aplicada' para ver si ha aumentado de acuerdo al número de peticiones realizadas. Si ha aumentado correctamente, vuelva a comprobar la configuración del servidor.
- Si no se aplica esta norma, añada una norma 'siempre cierta'. Emita un mandato `cbrcontrol rule report` sobre la norma 'siempre cierta' para verificar que se aplica.

Problema: en la plataforma Windows, se produce un comportamiento de la GUI inesperado al utilizar tarjetas de vídeo Matrox AGP

En la plataforma Windows cuando utiliza una tarjeta Matrox AGP, puede aparecer un comportamiento inesperado en la GUI de Load Balancer. Cuando pulsa el ratón, podría dañarse un bloque de espacio ligeramente mayor que el puntero del ratón provocando una posible inversión del resaltado o un desplazamiento de imágenes fuera del lugar de la pantalla. Las tarjetas Matrox anteriores no han mostrado este comportamiento. No hay un fix pack conocido cuando se utilizan tarjetas Matrox AGP.

Problema: se produce una desconexión del sistema principal si se cambia el tamaño de la ventana del navegador Netscape cuando se utiliza la administración Web

Si utiliza la administración Web remota para configurar Load Balancer, no cambie el tamaño (Minimizar, Maximizar, Restaurar minimizando, etc.) de la ventana del navegador Netscape en la que aparece la GUI de Load Balancer. Dado que Netscape vuelve a cargar una página cada vez que se cambia el tamaño de la ventana del navegador, esto provocará una desconexión del sistema principal. Tendrá que volver a conectar con el sistema principal cada vez que cambie el tamaño de la ventana. Si realiza administración Web remota en la plataforma Windows, utilice Internet Explorer.

Problema: en la plataforma Windows, aparecen caracteres nacionales Latin-1 dañados en la ventana de indicador de mandatos

En ventanas de indicador de mandatos del sistema operativo Windows, quizá algunos caracteres nacionales de la familia Latin-1 aparezcan dañados. Por ejemplo, la letra "a" con una tilde podría mostrarse como el símbolo pi. Para corregir esto, debe cambiar las propiedades de font de la ventana de línea de mandatos. Para cambiar el font, realice lo siguiente:

1. Pulse en el icono en la esquina superior izquierda de la ventana de indicador de mandatos
2. Seleccione Propiedades, luego pulse la pestaña Fuente
3. El font por omisión es Fuentes de mapa de bits; cambie este valor por Lucida Console y pulse Aceptar

Problema: en HP-UX, se produce un error de falta de memoria/hebra de Java

Algunas instalaciones de HP-UX 11i están preconfiguradas para sólo permitir 64 hebras por proceso. No obstante, algunas configuraciones de Load Balancer requieren una cantidad mayor. En los sistemas HP-UX, establezca las hebras por proceso como mínimo en 256. Para aumentar este valor, utilice el programa de utilidad "sam" para establecer el parámetro de kernel `max_thread_proc`. Si se espera un uso masivo, puede ser necesario aumentar `max_thread_proc` por encima de 256.

Para aumentar `max_thread_proc`, consulte los pasos de la página 313.

Problema: en los sistemas Windows, los asesores y los destinos de alcance marcan como inactivos todos los servidores

Cuando configura el adaptador en una máquina de Load Balancer, debe asegurarse de que los dos valores siguientes son correctos para que el asesor funcione:

- Inhabilite Task Offloading, que se suele utilizar más usualmente en tarjetas de adaptador 3Com.
- Habilite el Protocolo 1 (ICMP) para protocolos IP si habilita el filtrado TCP/IP. Si no se habilita ICMP, no se superará la prueba de ping con el servidor final.

Si desea instrucciones sobre cómo configurar este valor, consulte la página 313.

Problema: en sistemas Windows, se resuelve la dirección IP con el nombre de sistema principal cuando se ha configurado más de una dirección con el adaptador

En la plataforma Windows, cuando configura un adaptador con más de una dirección IP, configure la dirección IP que desea afiliar al nombre de sistema principal primero del registro.

Puesto que Load Balancer depende de `InetAddress.getLocalHost()` en muchas instancias (por ejemplo, `lbkeys create`), varias direcciones IP que tienen un alias con un sólo adaptador podrían provocar problemas. Para impedir este problema, enumere la dirección IP con la que desea que se resuelva la dirección IP primero en el registro.

Consulte la página 314 si desea obtener los pasos para configurar el nombre de sistema principal primero en el registro.

Resolución de problemas comunes—Site Selector

Problema: no se ejecutará Site Selector

Este problema puede producirse si otra aplicación utiliza uno de los puertos que Site Selector utiliza. Para obtener más información, consulte el apartado “Comprobación de los números de puerto de Site Selector” en la página 301.

Problema: Site Selector no utiliza el algoritmo de turno rotativo en el tráfico de clientes Solaris

Síntoma: el componente Site Selector no utiliza el algoritmo de turno rotativo para peticiones entrantes de clientes Solaris.

Causa posible: los sistemas Solaris ejecutan un “daemon de antememoria del servicio de nombres. Si este daemon está en ejecución, se contestará la petición subsiguiente del solucionador de esta antememoria en lugar de consultar Site Selector.

Solución: desactive el daemon del servicio de nombres en la máquina de Solaris.

Problema: el mandato `sscontrol` o `lbadmind` da un error

1. El mandato `sscontrol` devuelve: **Error: el servidor no responde**. O bien, el mandato `lbadmind` devuelve: **Error: no es posible acceder al servidor RMI**. Estos errores pueden producirse si su máquina tiene una pila con SOCKS. Para corregir este problema, edite el archivo `socks.cnf` para incluir las líneas siguientes:

```
EXCLUDE-MODULE java
EXCLUDE-MODULE javaw
```
2. Las consolas de administración de las interfaces (línea de mandatos, interfaz gráfica de usuario y asistentes) de Load Balancer se comunican con `ssserver` utilizando RMI (Remote Method Invocation). La comunicación por omisión utiliza tres puertos; cada puerto se establece en el script de inicio de `ssserver`:
 - 12099 para recibir mandatos de `sscontrol`
 - 10004 para enviar consultas de métrica a Metric Server
 - 12199 para el puerto del servidor RMI
 - 53 para enviar y recibir tráfico de DNS

Esto puede producir problemas si una de las consolas de administración se ejecuta en la misma máquina que un cortafuegos o a través de un cortafuegos. Por ejemplo, cuando Load Balancer se ejecuta en la misma máquina que un cortafuegos y emite mandatos `sscontrol`, podrían aparecer errores como **Error: el servidor no responde**.

Para impedir este problema, edite el archivo de scripts `ssserver` para establecer el puerto utilizado por RMI para el cortafuegos (u otra aplicación). Cambie la línea: `LB_RMISERVERPORT=10199` por `LB_RMISERVERPORT=suPuerto`. Donde *suPuerto* es otro puerto.

Cuando haya terminado, reinicie `ssserver` y abra el tráfico para los puertos: 12099, 10004, 12199 y 12100 o para el puerto seleccionado para la dirección del sistema principal desde donde se ejecutará la consola de administración.

3. También se pueden producir estos errores si aún no ha iniciado `ssserver`.

Problema: no se ha podido iniciar ssserver en la plataforma Windows

Site Selector debe ser capaz de participar en un DNS. Todas las máquinas que intervienen en la configuración también deberían participar de este sistema. Los sistemas Windows no siempre requieren que el nombre de sistema principal configurado esté en el DNS. Site Selector requiere que su nombre de sistema principal se defina en el DNS para que se inicie correctamente.

Verifique que este sistema principal se ha definido en el DNS. Edite el archivo `ssserver.cmd` y elimine la "w" de "javaw". Esto debe proporcionar más información sobre errores.

Problema: Site Selector con rutas duplicadas no equilibra la carga correctamente

El servidor de nombres de Site Selector no se enlaza a ninguna dirección en la máquina. Responderá a peticiones destinadas para cualquier dirección IP válida en la máquina. Site Selector confía en el sistema operativo para direccionar la respuesta de nuevo al cliente. Si la máquina de Site Selector tiene varios adaptadores y cualquier número de ellos está conectado a la misma subred, es posible que el O/S enviará la respuesta al cliente desde una dirección distinta de donde la ha recibido. Algunas aplicaciones cliente no aceptarán una respuesta recibida de una dirección que no sea de donde se ha enviado. Como consecuencia, parecerá que la resolución de nombres da un error.

Problema: en la plataforma Windows, se produce un comportamiento de la GUI inesperado al utilizar tarjetas de vídeo Matrox AGP

En la plataforma Windows cuando utiliza una tarjeta Matrox AGP, puede aparecer un comportamiento inesperado en la GUI de Load Balancer. Cuando pulsa el ratón, podría dañarse un bloque de espacio ligeramente mayor que el puntero del ratón provocando una posible inversión del resaltado o un desplazamiento de imágenes fuera del lugar de la pantalla. Las tarjetas Matrox anteriores no han mostrado este comportamiento. No hay un fix pack conocido cuando se utilizan tarjetas Matrox AGP.

Problema: se produce una desconexión del sistema principal si se cambia el tamaño de la ventana del navegador Netscape cuando se utiliza la administración Web

Si utiliza la administración Web remota para configurar Load Balancer, no cambie el tamaño (Minimizar, Maximizar, Restaurar minimizando, etc.) de la ventana del navegador Netscape en la que aparece la GUI de Load Balancer. Dado que Netscape vuelve a cargar una página cada vez que se cambia el tamaño de la ventana del navegador, esto provocará una desconexión del sistema principal. Tendrá que volver a conectar con el sistema principal cada vez que cambie el tamaño de la ventana. Si realiza administración Web remota en la plataforma Windows, utilice Internet Explorer.

Problema: en la plataforma Windows, aparecen caracteres nacionales Latin-1 dañados en la ventana de indicador de mandatos

En ventanas de indicador de mandatos del sistema operativo Windows, quizá algunos caracteres nacionales de la familia Latin-1 aparezcan dañados. Por ejemplo, la letra "a" con una tilde podría mostrarse como el símbolo pi. Para corregir esto, debe cambiar las propiedades de font de la ventana de línea de mandatos. Para cambiar el font, realice lo siguiente:

1. Pulse en el icono en la esquina superior izquierda de la ventana de indicador de mandatos
2. Seleccione Propiedades, luego pulse la pestaña Fuente
3. El font por omisión es Fuentes de mapa de bits; cambie este valor por Lucida Console y pulse Aceptar

Problema: en HP-UX, se produce un error de falta de memoria/hebra de Java

Algunas instalaciones de HP-UX 11i están preconfiguradas para sólo permitir 64 hebras por proceso. No obstante, algunas configuraciones de Load Balancer requieren una cantidad mayor. En los sistemas HP-UX, establezca las hebras por proceso como mínimo en 256. Para aumentar este valor, utilice el programa de utilidad "sam" para establecer el parámetro de kernel max_thread_proc. Si se espera un uso masivo, puede ser necesario aumentar max_thread_proc por encima de 256.

Para aumentar max_thread_proc, consulte los pasos de la página 313.

Problema: en los sistemas Windows, los asesores y los destinos de alcance marcan como inactivos todos los servidores

Cuando configura el adaptador en una máquina de Load Balancer, debe asegurarse de que los dos valores siguientes son correctos para que el asesor funcione:

- Inhabilite Task Offloading, que se suele utilizar más usualmente en tarjetas de adaptador 3Com.
- Habilite el Protocolo 1 (ICMP) para protocolos IP si habilita el filtrado TCP/IP. Si no se habilita ICMP, no se superará la prueba de ping con el servidor final.

Si desea instrucciones sobre cómo configurar este valor, consulte la página 313.

Resolución de problemas comunes—Cisco CSS Controller

Problema: no se iniciará ccoserver

Este problema puede producirse si otra aplicación utiliza uno de los puertos utilizados por el ccoserver de Cisco CSS Controller. Para obtener más información, consulte el apartado “Comprobación de los números de puerto de Cisco CSS Controller” en la página 301.

Problema: el mandato ccocontrol o lbadmin da un error

1. El mandato ccocontrol devuelve: **Error: el servidor no responde**. O bien, el mandato lbadmin devuelve: **Error: no es posible acceder al servidor RMI**. Estos errores pueden producirse si su máquina tiene una pila con SOCKS. Para corregir este problema, edite el archivo socks.cnf para incluir las líneas siguientes:

```
EXCLUDE-MODULE java
EXCLUDE-MODULE javaw
```

2. Las consolas de administración de las interfaces (línea de mandatos e interfaz gráfica de usuario) de Load Balancer se comunican con ccoserver utilizando RMI (Remote Method Invocation). La comunicación por omisión utiliza tres puertos; cada puerto se establece en el script de inicio de ccoserver:

- 13099 para recibir mandatos de ccocontrol
- 10004 para enviar consultas de métrica a Metric Server
- 13199 para el puerto del servidor RMI

Esto puede producir problemas si una de las consolas de administración se ejecuta en la misma máquina que un cortafuegos o a través de un cortafuegos. Por ejemplo, cuando Load Balancer se ejecuta en la misma máquina que un cortafuegos y emite mandatos ccocontrol, podrían aparecer errores como **Error: el servidor no responde**.

Para impedir este problema, edite el archivo de scripts ccoserver para establecer el puerto utilizado por RMI para el cortafuegos (u otra aplicación). Cambie la línea: `CCO_RMISERVERPORT=14199` por `CCO_RMISERVERPORT=suPuerto`. Donde *suPuerto* es otro puerto.

Cuando haya terminado, reinicie ccoserver y abra el tráfico para los puertos: 13099, 10004, 13199 y 13100 o para el puerto seleccionado para la dirección del sistema principal desde donde se ejecutará la consola de administración.

3. También se pueden producir estos errores si aún no ha iniciado **ccoserver**.

Problema: no se ha podido crear el registro en el puerto 13099

Este problema puede aparecer si falta una licencia del producto válida. Cuando intenta iniciar ccoserver, recibe este mensaje:

La licencia ha caducado. Póngase en contacto con el representante local de IBM o un distribuidor autorizado de IBM.

Para corregir este problema:

1. Si ya ha intentado iniciar ccoserver, escriba **ccoserver stop**.
2. Copie la licencia válida al directorio `...ibm/edge/lb/servers/conf`.
3. Escriba **ccoserver** para iniciar el servidor.

Problema: en la plataforma Windows, se produce un comportamiento de la GUI inesperado al utilizar tarjetas de vídeo Matrox AGP

En la plataforma Windows cuando utiliza una tarjeta Matrox AGP, puede aparecer un comportamiento inesperado en la GUI de Load Balancer. Cuando pulsa el ratón, podría dañarse un bloque de espacio ligeramente mayor que el puntero del ratón provocando una posible inversión del resaltado o un desplazamiento de imágenes fuera del lugar de la pantalla. Las tarjetas Matrox anteriores no han mostrado este comportamiento. No hay un fix pack conocido cuando se utilizan tarjetas Matrox AGP.

Problema: se ha recibido un error de conexión al añadir un consultor

Cuando añade un consultor, podría experimentar un error de conexión debido a valores de configuración incorrectos. Para corregir este problema:

- Asegúrese de que la dirección o la comunidad especificada coincide exactamente con los valores configurados en el conmutador.
- Asegúrese de que esté disponible la conectividad entre el controlador y el conmutador.
- Asegúrese de que la comunidad tenga permiso de lectura-grabación en el conmutador. El controlador intentará habilitar la variable `ApSvcLoadEnable` (SNMP) cuando pruebe la conexión para verificar el acceso de grabación.

Problema: no se actualizan los pesos en el conmutador

Para corregir este problema:

- Si utiliza las medidas de conexiones activas o de velocidad de conexión, emita `ccontrol service SWID:0CID:serviceIO report`. Verifique que los valores de métrica cambian de acuerdo al tráfico de procesamiento en el conmutador.
- Aumente el nivel de anotaciones cronológicas del archivo de anotaciones cronológicas del consultor y busque las apariciones de tiempo de espera SNMP. Si se producen tiempos de espera superados, entre las posibles soluciones se incluye:
 - Disminuya la carga en el conmutador.
 - Disminuya el retardo de red entre el conmutador y el controlador.
- Detenga y reinicie el consultor.

Problema: el mandato refresh no ha actualizado la configuración del consultor

Aumente el nivel de anotaciones cronológicas del consultor y vuelva a intentar el mandato. Si vuelve a dar un error, busque en el archivo de anotaciones cronológicas si se ha excedido el tiempo de espera SNMP u otros errores de comunicación SNMP.

Problema: se produce una desconexión del sistema principal si se cambia el tamaño de la ventana del navegador Netscape cuando se utiliza la administración Web

Si utiliza la administración Web remota para configurar Load Balancer, no cambie el tamaño (Minimizar, Maximizar, Restaurar minimizando, etc.) de la ventana del navegador Netscape en la que aparece la GUI de Load Balancer. Dado que

Netscape vuelve a cargar una página cada vez que se cambia el tamaño de la ventana del navegador, esto provocará una desconexión del sistema principal. Tendrá que volver a conectar con el sistema principal cada vez que cambie el tamaño de la ventana. Si realiza administración Web remota en la plataforma Windows, utilice Internet Explorer.

Problema: en la plataforma Windows, aparecen caracteres nacionales Latin-1 dañados en la ventana de indicador de mandatos

En ventanas de indicador de mandatos del sistema operativo Windows, quizá algunos caracteres nacionales de la familia Latin-1 aparezcan dañados. Por ejemplo, la letra "a" con una tilde podría mostrarse como el símbolo pi. Para corregir esto, debe cambiar las propiedades de font de la ventana de línea de mandatos. Para cambiar el font, realice lo siguiente:

1. Pulse en el icono en la esquina superior izquierda de la ventana de indicador de mandatos
2. Seleccione Propiedades, luego pulse la pestaña Fuente
3. El font por omisión es Fuentes de mapa de bits; cambie este valor por Lucida Console y pulse Aceptar

Problema: en HP-UX, se produce un error de falta de memoria/hebra de Java

Algunas instalaciones de HP-UX 11i están preconfiguradas para sólo permitir 64 hebras por proceso. No obstante, algunas configuraciones de Load Balancer requieren una cantidad mayor. En los sistemas HP-UX, establezca las hebras por proceso como mínimo en 256. Para aumentar este valor, utilice el programa de utilidad "sam" para establecer el parámetro de kernel max_thread_proc. Si se espera un uso masivo, puede ser necesario aumentar max_thread_proc por encima de 256.

Para aumentar max_thread_proc, consulte los pasos de la página 313.

Resolución de problemas comunes—Nortel Alteon Controller

Problema: no se iniciará nalserver

Este problema puede producirse si otra aplicación utiliza uno de los puertos utilizados por el nalserver de Nortel Alteon Controller. Para obtener más información, consulte el apartado "Comprobación de los números de puerto de Nortel Alteon Controller" en la página 302.

Problema: el mandato nalcontrol o lbadmin da un error

1. El mandato nalcontrol devuelve: **Error: el servidor no responde**. O bien, el mandato lbadmin devuelve: **Error: no es posible acceder al servidor RMI**. Estos errores pueden producirse si su máquina tiene una pila con SOCKS. Para corregir este problema, edite el archivo socks.cnf para incluir las líneas siguientes:

```
EXCLUDE-MODULE java
EXCLUDE-MODULE javaw
```
2. Las consolas de administración de las interfaces (línea de mandatos e interfaz gráfica de usuario) de Load Balancer se comunican con nalserver utilizando

RMI (Remote Method Invocation). La comunicación por omisión utiliza tres puertos; cada puerto se establece en el script de inicio de nalserver:

- 14099 para recibir mandatos de nalcontrol
- 10004 para enviar consultas de métrica a Metric Server
- 14199 para el puerto del servidor RMI

Esto puede producir problemas si una de las consolas de administración se ejecuta en la misma máquina que un cortafuegos o a través de un cortafuegos. Por ejemplo, cuando Load Balancer se ejecuta en la misma máquina que un cortafuegos y emite mandatos nalcontrol, podrían aparecer errores como **Error: el servidor no responde**.

Para impedir este problema, edite el archivo de scripts nalserver para establecer el puerto utilizado por RMI para el cortafuegos (u otra aplicación). Cambie la línea: `NAL_RMISERVERPORT=14199` por `NAL_RMISERVERPORT=suPuerto`. Donde *suPuerto* es otro puerto.

Cuando haya terminado, reinicie nalserver y abra el tráfico para los puertos: 14099, 10004, 14199 y 14100 o para el puerto seleccionado para la dirección del sistema principal desde donde se ejecutará la consola de administración.

3. También se pueden producir estos errores si aún no ha iniciado **nalserver**.

Problema: no se ha podido crear el registro en el puerto 14099

Este problema puede aparecer si falta una licencia del producto válida. Cuando intenta iniciar nalserver, recibe este mensaje:

La licencia ha caducado. Póngase en contacto con el representante local de IBM o un distribuidor autorizado de IBM.

Para corregir este problema:

1. Si ya ha intentado iniciar nalserver, escriba **nalserver stop**.
2. Copie la licencia válida al directorio `...ibm/edge/lb/servers/conf`.
3. Escriba **nalserver** para iniciar el servidor.

Problema: en la plataforma Windows, se produce un comportamiento de la GUI inesperado al utilizar tarjetas de vídeo Matrox AGP

En la plataforma Windows cuando utiliza una tarjeta Matrox AGP, puede aparecer un comportamiento inesperado en la GUI de Load Balancer. Cuando pulsa el ratón, podría dañarse un bloque de espacio ligeramente mayor que el puntero del ratón provocando una posible inversión del resaltado o un desplazamiento de imágenes fuera del lugar de la pantalla. Las tarjetas Matrox anteriores no han mostrado este comportamiento. No hay un fix pack conocido cuando se utilizan tarjetas Matrox AGP.

Problema: se produce una desconexión del sistema principal si se cambia el tamaño de la ventana del navegador Netscape cuando se utiliza la administración Web

Si utiliza la administración Web remota para configurar Load Balancer, no cambie el tamaño (Minimizar, Maximizar, Restaurar minimizando, etc.) de la ventana del navegador Netscape en la que aparece la GUI de Load Balancer. Dado que Netscape vuelve a cargar una página cada vez que se cambia el tamaño de la ventana del navegador, esto provocará una desconexión del sistema principal.

Tendrá que volver a conectar con el sistema principal cada vez que cambie el tamaño de la ventana. Si realiza administración Web remota en la plataforma Windows, utilice Internet Explorer.

Problema: se ha recibido un error de conexión al añadir un consultor

Cuando añade un consultor, podría experimentar un error de conexión debido a valores de configuración incorrectos. Para corregir este problema:

- Asegúrese de que la dirección o la comunidad especificada coincide exactamente con los valores configurados en el conmutador.
- Asegúrese de que esté disponible la conectividad entre el controlador y el conmutador.
- Asegúrese de que la comunidad tenga permiso de lectura-grabación en el conmutador. El controlador intentará habilitar la variable `ApSvcLoadEnable` (SNMP) cuando pruebe la conexión para verificar el acceso de grabación.

Problema: no se actualizan los pesos en el conmutador

Para corregir este problema:

- Si utiliza las medidas de conexiones activas o de velocidad de conexión, emita `cccontrol service SWID:OCID:serviceIO report`. Verifique que los valores de métrica cambian de acuerdo al tráfico de procesamiento en el conmutador.
- Aumente el nivel de anotaciones cronológicas del archivo de anotaciones cronológicas del consultor y busque las apariciones de tiempo de espera SNMP. Si se producen tiempos de espera superados, entre las posibles soluciones se incluye:
 - Disminuya la carga en el conmutador.
 - Disminuya el retardo de red entre el conmutador y el controlador.
- Detenga y reinicie el consultor.

Problema: el mandato refresh no ha actualizado la configuración del consultor

Aumente el nivel de anotaciones cronológicas del consultor y vuelva a intentar el mandato. Si vuelve a dar un error, busque en el archivo de anotaciones cronológicas si se ha excedido el tiempo de espera SNMP u otros errores de comunicación SNMP.

Problema: en sistemas Windows, aparecen caracteres nacionales Latin-1 dañados en la ventana de indicador de mandatos

En ventanas de indicador de mandatos de la plataforma de sistema operativo Windows, quizá algunos caracteres nacionales de la familia Latin-1 aparezcan dañados. Por ejemplo, la letra "a" con una tilde podría mostrarse como el símbolo pi. Para corregir esto, debe cambiar las propiedades de font de la ventana de línea de mandatos. Para cambiar el font, realice lo siguiente:

1. Pulse en el icono en la esquina superior izquierda de la ventana de indicador de mandatos
2. Seleccione Propiedades, luego pulse la pestaña Fuente
3. El font por omisión es Fuentes de mapa de bits; cambie este valor por Lucida Console y pulse Aceptar

Problema: en HP-UX, se produce un error de falta de memoria/hebra de Java

Algunas instalaciones de HP-UX 11i están preconfiguradas para sólo permitir 64 hebras por proceso. No obstante, algunas configuraciones de Load Balancer requieren una cantidad mayor. En los sistemas HP-UX, establezca las hebras por proceso como mínimo en 256. Para aumentar este valor, utilice el programa de utilidad "sam" para establecer el parámetro de kernel `max_thread_proc`. Si se espera un uso masivo, puede ser necesario aumentar `max_thread_proc` por encima de 256.

Para aumentar `max_thread_proc`, consulte los pasos de la página 313.

Resolución de problemas comunes—Metric Server

Problema: Metric Server IOException en la plataforma Windows al ejecutar archivos de métrica del usuario .bat o .cmd

Debe utilizar el nombre de métrica completo para métricas grabadas por el usuario en Metric Servers que se ejecutan en la plataforma Windows. Por ejemplo, debe especificar **usermetric.bat** en lugar de **usermetric**. El nombre **usermetric** es válido en la línea de mandatos, pero no funcionará cuando se ejecute desde dentro del entorno de ejecución. Si no utiliza el nombre de métrica completo, recibirá una IOException de Metric Server. Establezca la variable `LOG_LEVEL` en un valor de 3 en el archivo de mandatos `metricserver`, luego compruebe la salida de anotaciones cronológicas. En este ejemplo, aparece la excepción como:

```
... java.io.IOException: CreateProcess: usermetric error=2
```

Problema: Metric Server no informa de las cargas en la máquina de Load Balancer

Puede haber varios motivos por los que Metric Server no informa de la información de carga a Load Balancer. Para determinar la causa, realice estas comprobaciones:

- Asegúrese de que los archivos de claves se han transferido a Metric Server.
- Verifique que el nombre de sistema principal de la máquina de Metric Server está registrado con el servidor de nombres local.

También puede resolver este problema especificando el nombre de sistema principal en la propiedad Java `java.rmi.server.hostname` en el script `metricserver`.

- Reinicie el equipo con un nivel de anotaciones cronológicas mayor y busque los errores.
- En la máquina de Load Balancer, aumente el nivel de anotaciones cronológicas del archivo de anotaciones cronológicas de supervisor de métrica utilizando el mandato **dscontrol manager metric set**. Busque errores en el archivo `MetricMonitor.log`.

Problema: el archivo de anotaciones cronológicas de Metric Server informa de que "Es necesaria la firma para acceder al agente"

El archivo de anotaciones cronológicas de Metric Server informa de este mensaje de error después de que se han transferido archivos al servidor.

Este error se anota cuando el archivo de claves no supera la autorización con la clave emparejada debido a que se ha dañado la pareja. Para corregir este problema intente lo siguiente:

- Transfiera de nuevo por FTP el archivo de claves utilizando el método de transferencia binaria.
- Cree una nueva clave y redistribúyala.

Problema: en sistemas AIX, cuando se ejecuta Metric Server bajo mucha presión, la salida del mandato ps -vg podría dañarse

Cuando ejecuta Metric Server bajo una gran presión en una plataforma AIX multiprocesador (4.3.3, de 32 bits 5.1 o de 64 bits 5.1), la salida del mandato ps -vg podría dañarse. Por ejemplo:

```
55742 - A 88:19 42 18014398509449680 6396 32768 22 36 2.8 1.0 java -Xms
```

El campo SIZE y/o RSS del mandato ps podría mostrar una cantidad excesiva de memoria utilizada.

Este es un problema del kernel AIX conocido. Apar IY33804 corregirá este problema. Obtenga el fix pack del soporte de AIX en <http://techsupport.services.ibm.com/server/fixes> o póngase en contacto con el representante de soporte de AIX local.

Problema: configuración de Metric Server en una configuración de dos niveles con el equilibrio de carga de Site Selector entre Dispatchers de alta disponibilidad

En una configuración de Load Balancer de dos niveles, si se está equilibrando la carga de Site Selector (primer nivel) entre un par de asociados de alta disponibilidad de Dispatcher (segundo nivel), hay pasos que debe completar para configurar el componente Metric Server. Debe configurar Metric Server para que esté a la escucha en una nueva dirección IP que es específicamente para uso de Metric Server. En las dos máquinas de Dispatcher de alta disponibilidad, Metric Server está activo sólo en el Dispatcher activo.

Para configurar correctamente esta configuración, complete estos pasos:

- Configure Metric Server para que esté a la escucha en la nueva dirección IP local. No debe dejarse para responder en la dirección NFA local. Si desea información de configuración, consulte el apartado “Metric Server” en la página 196.
- Dado que Site Selector sólo debe comunicarse con el Dispatcher activo, debe iniciar y detener Metric Server en los scripts go de alta disponibilidad. Para iniciar o detener Metric Server correctamente, cree un alias de la nueva dirección IP específica de Metric Server en la máquina. Modifique los scripts go para desplazar la dirección IP de Metric Server (similar a desplazar las direcciones del clúster) de modo que el script goActive desplace la dirección IP de Metric Server del bucle de retorno a un adaptador físico y el script goStandby no se invierta. Después de desplazar la dirección IP, el script goActive debe ejecutar el mandato **metricserver start** para iniciar Metric Server. El script goStandby debe ejecutar **metricserver stop** para impedir que Metric Server se comunique con Site Selector estando en modalidad de reposo.
- En la plataforma Windows, consulte el apartado “Utilización scripts” en la página 209 para desplazar la dirección IP específica de Metric Server.

- Los cambios del script goStandby incluyen instrucciones específicas de operación como se detalla a continuación:
 - **Sistemas HP-UX, Linux y Solaris:** en la sección dentro del script goStandby donde la dirección del clúster se desplaza al bucle de retorno, inserte mandatos para desplazar la dirección IP específica de Metric Server al bucle de retorno. A continuación, inserte el mandato **metricserver stop** para que Metric Server deje de responder a Site Selector.
 - **Sistemas AIX:** en la sección dentro del script goStandby donde la dirección del clúster se desplaza al bucle de retorno, inserte mandatos para desplazar la dirección IP específica de Metric Server al bucle de retorno. A continuación, añada una ruta de modo que pueda comunicarse con el alias de bucle de retorno. Ejecute el mandato **route add IPmetricserver 127.0.0.1**. Luego inserte el mandato **metricserver stop** para impedir que Metric Server siga respondiendo a Site Selector. Después de que se detiene Metric Server, el paso final es eliminar la ruta de bucle de retorno. Para impedir cualquier confusión futura, inserte **route delete IPmetricserver**.

Por ejemplo:

```
ifconfig en0 delete 9.27.23.61
ifconfig lo0 alias 9.27.23.61 netmask 255.255.255.0
route add 9.27.23.61 127.0.0.1
metricserver stop
# Está inactivo durante un número máximo de 60 segundos o hasta que se
# detiene metricserver
let loopcount=0
while [[ "$loopcount" -lt "60" && 'ps -ef | grep AgentStop|
      grep -c -v gr ep' -eq "1"]]
do
  sleep 1
  let loopcount=$loopcount+1
done
route delete 9.27.23.61
```

- **Sistemas Windows:** primero tenga instalado el adaptador de bucle de retorno de Metric Server (que se llama Conexión de área local 2 en el ejemplo siguiente) en la máquina con una dirección IP. Añádale un tipo de dirección de red privada que no se haya utilizado, como 10.1.1.1. Después de configurar el bucle de retorno, realice cambios en los scripts go. El script goStandby incluirá el mandato netsh para desplazar la dirección IP de Metric Server al adaptador de bucle de retorno de Metric Server. Luego ejecute el mandato **metricserver stop**.

Por ejemplo:

```
call netsh interface ip delete address "Conexión de área local" addr=9.27.23.61
call netsh interface ip add address "Conexión de área local 2" addr=9.27.23.61
mask = 255.255.255.0
sleep 3
metricserver stop
```

Problema: los scripts, en ejecución en máquinas Solaris de varias CPU, producen mensajes de consola no deseados

Cuando se ejecutan los scripts metricserver, cpuload y memload en máquinas Solaris de varias CPU pueden producir mensajes de consola no deseados. Este comportamiento se debe al uso del mandato de sistema VMSTAT para recopilar estadísticas de la CPU y de memoria del kernel. Algunos mensajes que VMSTAT devuelve indican que el estado del kernel ha cambiado. Los scripts no pueden gestionar estos mensajes, lo que provoca mensajes de consola innecesarios procedentes del shell.

Ejemplos de estos mensajes de consola son:

```
/opt/ibm/edge/lb/ms/script/memload[29]: TOTAL=: syntax error
/opt/ibm/edge/lb/ms/script/memload[31]: LOAD=4*100/0: divide by zero
/opt/ibm/edge/lb/ms/script/memload[29]: TOTAL=659664+: more tokens expected
```

Estos mensajes se pueden ignorar.

Problema: en Load Balancer para IPv6, no se pueden recuperar los valores de Metric Server en sistemas Linux

Cuando se ejecuta en plataformas Linux, existe una incompatibilidad de selección de dirección de origen IPv6. Como consecuencia, Metric Monitor intenta comunicarse con Metric Server a través de la dirección IP de origen errónea.

En sistemas Linux, la selección de dirección de origen IPv6 para una ruta concreta toma el valor por omisión de la última dirección configurada que coincide con el fragmento de red de la ruta.

Si un clúster IPv6 es la última interfaz configurada y dicha interfaz coincide con el fragmento de red de una ruta en la tabla de direccionamiento, esa interfaz se utiliza como la dirección IP de origen por omisión para dicha ruta. Si entre Load Balancer y Metric Server se está utilizando esa ruta, no se establecerán las comunicaciones entre los dos nodos.

La comunicación no se establece porque el nodo de Load Balancer intenta comunicarse con Metric Server utilizando la dirección del clúster como dirección IP de origen. Cuando el clúster se configura en el activar del nodo de Metric Server, la respuesta procedente de Metric Server se dirige al bucle de retorno y no se establece comunicación.

Solución:

Para determinar qué dirección está utilizando el nodo de Linux para una determinada ruta y qué interfaz se utiliza para las comunicaciones RMI entre Metric Monitor y Metric Server, emita el siguiente mandato:

```
ip -6 route get ruta_ipv6
```

Por ejemplo, cuando se emite este mandato:

```
ip -6 route get fec0::/64
```

Se devuelve lo siguiente:

```
fec0:: via fec0:: dev eth0 src fec0::4 metric 0 cache mtu 1500 advmss 1383
```

Si `fec0::4` es una dirección de clúster, se debe añadir otra interfaz al dispositivo para impedir que el clúster se utilice como origen por omisión o se puede eliminar una interfaz de no clúster anterior y volverse a añadir.

Por ejemplo:

```
ip -6 addr add fec0::5/64 dev eth0
```

Problema: Después de iniciar Metric Server, el valor de métrica devuelve -1

Este problema puede deberse a la pérdida de integridad de los archivos de claves durante la transferencia al cliente.

Si utiliza FTP para transferir los archivos de claves desde la máquina de Load Balancer al servidor de programa de fondo, asegúrese de que está utilizando la modalidad binaria cuando utiliza los mandatos `put` o `get` para transferir archivos de claves al o desde el servidor FTP.

Parte 9. Referencia de mandatos

Esta parte proporciona información de referencia de mandatos para todos los componentes de Load Balancer. Contiene los capítulos siguientes:

- Capítulo 26, “Cómo leer un diagrama de sintaxis”, en la página 345
- Capítulo 27, “Referencia de mandatos para Dispatcher y CBR”, en la página 347
- Capítulo 28, “Referencia de mandatos para Site Selector”, en la página 403
- Capítulo 29, “Referencia de mandatos para Cisco CSS Controller”, en la página 431
- Capítulo 30, “Referencia de mandatos para Nortel Alteon Controller”, en la página 449

Capítulo 26. Cómo leer un diagrama de sintaxis

El diagrama de sintaxis muestra cómo especificar un mandato para que el sistema operativo puede interpretar correctamente lo que se escribe. Lea el diagrama de sintaxis de izquierda a derecha y de arriba a abajo, siguiendo la línea horizontal (la ruta principal).

Símbolos y puntuación

En los diagramas de sintaxis se utilizan los símbolos siguientes:

Símbolo

Descripción

- ▶▶ Marca el principio de la sintaxis de mandato.
- ◀◀ Marca el final de la sintaxis de mandato.

Debe incluir todos los símbolos de puntuación, como dos puntos, comillas y signos menos que se muestran en el diagrama de sintaxis.

Parámetros

En los diagramas de sintaxis se utilizan los siguientes tipos de parámetros.

Parámetro

Descripción

Necesario

Los parámetros necesarios se muestran en la ruta principal.

Opcional

Los parámetros opcionales se muestran debajo de la ruta principal.

Los parámetros se clasifican como palabras clave o variables. Las palabras clave se muestran en letras minúsculas y se pueden especificar en minúscula. Por ejemplo, un nombre de mandato es una palabra clave. Las variables van en cursiva y representan nombres o valores que se suministran.

Ejemplos de sintaxis

En el ejemplo siguiente, el mandato `user` es una palabra clave. La variable necesaria es `id_usuario` y la variable opcional es `contraseña`. Sustituya las variables por sus propios valores.

▶▶—`user`—*id_usuario*—*contraseña*————▶◀

Palabras clave necesarias: las palabras clave y variables necesarias aparecen en la línea de ruta principal.

▶▶—`palabra_clave_necesaria`————▶◀

Debe incluir el código de las palabras clave y los valores necesarios.

Seleccione un elemento necesario de la pila: si hay más de una palabra clave o variable mutuamente exclusivas entre las que elegir, se apilarán verticalmente por orden alfanumérico.



Valores opcionales: las palabras clave y variables opcionales aparecen debajo de la línea de ruta principal.



Puede determinar no incluir en el código palabras clave y variables opcionales.

Seleccione una palabra clave opcional de una pila: si hay más de una palabra clave o variable opcional mutuamente exclusivas entre las que elegir, se apilarán verticalmente por orden alfanumérico debajo de la línea de ruta principal.



Variables: una palabra toda en cursiva es una *variable*. Donde aparece una variable en la sintaxis, debe sustituirla por uno de sus nombres o valores permitidos, como se define en el texto.



Caracteres no alfanuméricos: si un diagrama muestra un carácter que no es alfanumérico (como dos puntos, comillas o signos menos), debe codificar el carácter como parte de la sintaxis. En este ejemplo, debe codificar *clúster:puerto*.



Capítulo 27. Referencia de mandatos para Dispatcher y CBR

En este capítulo se describe cómo utilizar los mandatos **dscontrol** de Dispatcher. También es una referencia de mandatos de CBR.

En las versiones anteriores, cuando el producto se denominaba Network Dispatcher, el nombre del mandato de control de Dispatcher era **ndcontrol**. El nombre del mandato de control de Dispatcher ahora es **dscontrol**. Asegúrese de actualizar todos los archivos de script anteriores de modo que utilicen **dscontrol** (no **ndcontrol**) para configurar Dispatcher.

CBR utiliza un subconjunto de los mandatos de Dispatcher que se enumeran en esta referencia de mandatos. Al utilizar estos diagramas de sintaxis para **CBR**, sustituya **cbrcontrol** por **dscontrol**. Para obtener información, consulte el apartado “Diferencias de configuración entre CBR y Dispatcher” en la página 348.

IMPORTANTE: si utiliza la instalación Load Balancer para IPv4 y IPv6 de este producto, sólo estará disponible el componente Dispatcher. El sistema Dispatcher para este tipo de instalación utiliza un subconjunto de los mandatos **dscontrol** que se enumeran en esta referencia de mandatos. Cuando utilice estos diagramas de sintaxis, sustituya el símbolo de arroba (@) por dos puntos (:) como el delimitador dentro del mandato **dscontrol**. Para obtener más información, consulte los apartados “Diferencias de sintaxis de mandato” en la página 92 y “Mandatos **dscontrol** admitidos” en la página 92 para la instalación de Load Balancer para IPv4 y IPv6.

La lista siguiente contiene los mandatos que se describen en este capítulo:

- “**dscontrol advisor** — controlar el asesor” en la página 349
- “**dscontrol binlog** — controlar el archivo de anotaciones cronológicas binario” en la página 354
- “**dscontrol cluster** — configurar clústeres” en la página 355
- “**dscontrol executor** — control del ejecutor” en la página 359
- “**dscontrol file** — gestionar archivos de configuración” en la página 364
- “**dscontrol help** — mostrar o imprimir ayuda para este mandato” en la página 366
- “**dscontrol highavailability** — controlar alta disponibilidad” en la página 367
- “**dscontrol host** — configurar un máquina remota” en la página 371
- “**dscontrol logstatus** — mostrar valores de anotaciones cronológicas de servidor” en la página 372
- “**dscontrol manager** — controlar el gestor” en la página 373
- “**dscontrol metric** — configurar métrica del sistema” en la página 379
- “**dscontrol port** — configurar puertos” en la página 380
- “**dscontrol rule** — configurar normas” en la página 386
- “**dscontrol server** — configurar servidores” en la página 392
- “**dscontrol set** — configurar anotaciones cronológicas de servidor” en la página 398
- “**dscontrol status** — mostrar si el gestor y los asesores se están ejecutando” en la página 399
- “**dscontrol subagent** — configurar subagente SNMP” en la página 400

Puede escribir una versión minimizada de los parámetros del mandato **dscontrol**. Sólo es necesario especificar las letras exclusivas de los parámetros. Por ejemplo, para obtener ayuda sobre el mandato para guardar archivos, puede escribir **dscontrol he f** en lugar de **dscontrol help file**.

Para iniciar la interfaz de línea de mandatos: emita **dscontrol** para recibir un indicador de mandatos **dscontrol**.

Para finalizar la interfaz de línea de mandatos, emita **exit** o **quit**.

Los valores de los parámetros de mandatos deben especificarse en caracteres del idioma inglés. Las únicas excepciones son los nombres de sistema principal (que se utilizan en los mandatos **cluster**, **server** y **highavailability**) y nombres de archivo (que se utilizan en los mandatos de archivo).

Diferencias de configuración entre CBR y Dispatcher

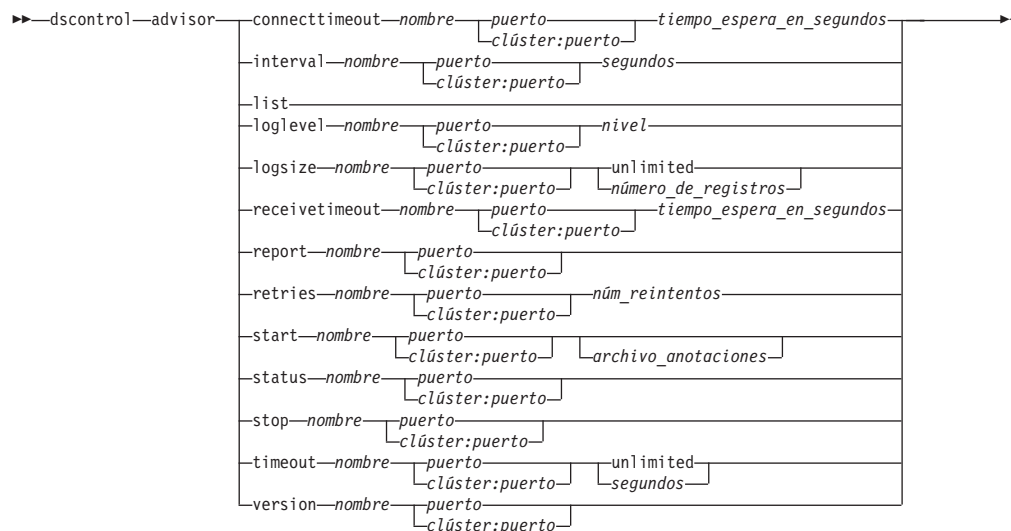
La interfaz de línea de mandatos de CBR es un subconjunto de la interfaz de línea de mandatos de Dispatcher. Para CBR, indique el mandato **cbrcontrol** en lugar de **dscontrol** para configurar el componente.

Nota: El componente CBR (Content Based Routing) está disponible en todas las plataformas excepto donde se ejecuta la JVM de 64 bits. De modo alternativo, puede utilizar el método de reenvío **cbr** del componente Dispatcher de Load Balancer para proporcionar direccionamiento basado en contenido sin utilizar Caching Proxy. Si desea más información, consulte el apartado “Direccionamiento basado en contenido de Dispatcher (método de reenvío **cbr**)” en la página 55.

A continuación se listan algunos de los mandatos que se *omiten* en CBR.

1. **highavailability**
2. **subagent**
3. **executor**
 - **report**
 - **set nfa <valor>**
 - **set fintimeout <valor>**
 - **set hatimeout <valor>**
 - **set hasynctimeout <valor>**
 - **set porttype <valor>**
4. **cluster**
 - **report {c}**
 - **set {c} porttype**
5. **port**
 - **add {c:p} porttype**
 - **add {c:p} protocol**
 - **set {c:p} porttype**
6. **rule add {c:p:r} type port**
7. **server**
 - **add {c:p:s} router**
 - **set {c:p:s} router**

dscontrol advisor — controlar el asesor



connecttimeout

Establece cuánto tiempo espera un asesor antes de notificar que se ha producido un error en una conexión a un servidor para un puerto concreto en un servidor (un servicio). Para obtener más información, consulte el apartado “Tiempo de espera de conexión y recepción del asesor para los servidores” en la página 188.

nombre

Nombre del asesor. Los valores posibles incluyen **connect**, **db2**, **dns**, **ftp**, **http**, **https**, **cachingproxy**, **imap**, **ldap**, **nntp**, **ping**, **pop3**, **self**, **sip**, **smtp**, **ssl**, **ssl2http**, **telnet** y **wlm**.

Consulte el apartado “Lista de asesores” en la página 188 para obtener información sobre los asesores que proporciona Load Balancer.

Los nombres de asesores personalizados están en formato xxxx, donde ADV_xxxx es el nombre de la clase que implementa el asesor personalizado. Consulte el apartado “Crear asesores personalizados (personalizables)” en la página 192 para obtener más información.

puerto

Número del puerto que el asesor está supervisando.

clúster:puerto

El valor de clúster es opcional en los mandatos del asesor, pero el valor de puerto sí es necesario. Si no se especifica el valor de clúster, el asesor empezará a ejecutarse en el puerto correspondiente a todos los clústeres. Si especifica un clúster, el asesor empezará a ejecutarse en el puerto, pero sólo para el clúster especificado. Consulte el apartado “Inicio y detención de un asesor” en la página 186 para obtener más información.

El clúster es la dirección en formato de dirección IP o un nombre simbólico. El puerto es el número del puerto que el asesor está supervisando.

tiempo_espera_en_segundos

Entero positivo que representa el tiempo de espera en segundos durante el que el asesor espera antes de notificar que se ha producido una anomalía en una conexión a un servidor. El valor por omisión es 3 veces el valor especificado para el intervalo del asesor.

interval

Establece con qué frecuencia el asesor consultará si hay información en los servidores.

segundos

Entero positivo que representa el número de segundos entre las peticiones a los servidores sobre su estado actual. El valor por omisión es 7.

list

Muestra una lista de los asesores que actualmente proporcionan información al gestor.

loglevel

Establece el nivel de registro cronológico para las anotaciones cronológicas del asesor.

nivel

El número del nivel (0 a 5). El valor por omisión es 1. Cuanto más alto sea el número, más información se anotará en las anotaciones cronológicas del asesor. A continuación se muestran los valores posibles: 0 equivale a Ninguno, 1 a Mínimo, 2 a Básico, 3 a Moderado, 4 a Avanzado, 5 a Detallado.

logsize

Establece el tamaño máximo de las anotaciones cronológicas del asesor. Cuando se establece un tamaño máximo para el archivo de anotaciones cronológicas, el texto del archivo vuelve al principio; es decir, cuando el archivo alcanza el tamaño especificado, las entradas subsiguientes se anotarán al principio del archivo y se grabarán encima de las entradas de anotaciones cronológicas anteriores. El tamaño de las anotaciones cronológicas no puede establecerse más pequeño que el tamaño actual de las anotaciones cronológicas. Las entradas de anotaciones cronológicas incluyen la indicación de la hora para poder saber el orden en el que se anotaron. Cuando más alto se establezca el nivel de anotaciones cronológicas, más cuidado deberá tener al elegir el tamaño de las anotaciones cronológicas porque, cuando el registro cronológico está establecido en los niveles más altos, puede quedarse sin espacio rápidamente.

número_de_registros

El tamaño máximo en bytes para el archivo de anotaciones cronológicas del asesor. Puede especificar un número positivo mayor que cero o la palabra **unlimited**. Es posible que el archivo de anotaciones cronológicas no alcance el tamaño máximo exacto antes de empezar a sobrescribir porque el tamaño de las entradas del archivo varían. El valor por omisión es 1 MB.

receivetimeout

Establece cuánto tiempo espera un asesor antes de notificar que se ha producido un error en una recepción en un puerto concreto o un servidor (un servicio). Para obtener más información, consulte el apartado “Tiempo de espera de conexión y recepción del asesor para los servidores” en la página 188.

tiempo_espera_en_segundos

Entero positivo que representa el tiempo de espera en segundos durante el que el asesor espera antes de notificar que se ha producido una anomalía en una recepción en un servidor. El valor por omisión es 3 veces el valor especificado para el intervalo del asesor.

report

Muestra un informe sobre el estado del asesor.

retry

El parámetro retry establece el número de reintentos que un asesor puede realizar antes de marcar un servidor como inactivo.

núm_reintentos

Número entero mayor que o igual a cero. Este valor no debe ser mayor que 3. Si la palabra clave retries no está configurada, el número de reintentos tendrá el valor por omisión de cero.

start

Inicia el asesor. Estos son asesores de cada protocolo. Los puertos por omisión son los siguientes:

Nombre del asesor	Protocolo	Puerto
cachingproxy	HTTP (mediante Caching Proxy)	80
connect	ICMP	12345
db2	private	50000
dns	DNS	53
ftp	FTP	21
http	HTTP	80
https	SSL	443
imap	IMAP	143
ldap	LDAP	389
nntp	NNTP	119
ping	PING	0
pop3	POP3	110
self	private	12345
sip	SIP	5060
smtp	SMTP	25
ssl	SSL	443
ssl2http	SSL	443
telnet	Telnet	23
WLM	private	10.007

Nota: El asesor FTP sólo debe asesorar sobre el puerto de control FTP (21). No iniciar un asesor FTP en el puerto de datos FTP (20).

archivo_annotaciones

Nombre de archivo en el que se anotan los datos de gestión. Cada registro del archivo de anotaciones cronológicas tiene la indicación de la hora.

El archivo por omisión es *puerto_nombre_asesor.log*, por ejemplo, **http_80.log**. Para cambiar el directorio en el que se guardan los archivos de anotaciones cronológicas, consulte el apartado “Cambio de las vías de acceso del archivo de anotaciones cronológicas” en la página 267. Los archivos de anotaciones cronológicas por omisión para los asesores específicos del clúster (o sitio) se crean con la dirección del clúster, por ejemplo, **http_127.40.50.1_80.log**.

status

Muestra el estado actual de todos los valores de un asesor que se pueden establecer globalmente y sus valores por omisión.

stop

Detiene el asesor.

timeout

Establece el número de segundos durante los que el gestor considerará válida la información del asesor. Si el gestor cree que la información del asesor es anterior a este intervalo de tiempo de espera, el gestor no la utilizará para determinar los pesos para los servidores en el puerto que el asesor está supervisando. Una excepción a este tiempo de espera es cuando el asesor ha notificado al gestor que un servidor específico está inactivo. El gestor utilizará dicha información sobre el servidor incluso después de que el servidor exceda el tiempo de espera.

segundos

Número positivo que representa el número de segundos o la palabra **unlimited**. El valor por omisión es unlimited.

version

Muestra la versión actual del asesor.

Ejemplos

- Iniciar el asesor http en el puerto 80 para el clúster 127.40.50.1:
`dscontrol advisor start http 127.40.50.1:80`
- Iniciar el asesor http en el puerto 88 para todos los clústeres:
`dscontrol advisor start http 88`
- Detener el asesor http en el puerto 80 para el clúster 127.40.50.1:
`dscontrol advisor stop http 127.40.50.1:80`
- Establecer el tiempo (30 segundos) que un asesor HTTP para el puerto 80 espera antes de notificar que se ha producido una anomalía en una conexión a un servidor:
`dscontrol advisor connecttimeout http 80 30`
- Establecer el tiempo (20 segundos) que un asesor HTTP para el puerto 80 en el clúster 127.40.50.1 esperará antes de notificar que se ha producido una anomalía en una conexión a un servidor:
`dscontrol advisor connecttimeout http 127.40.50.1:80 20`
- Establecer el intervalo para el asesor FTP (para el puerto 21) en 6 segundos:
`dscontrol advisor interval ftp 21 6`
- Mostrar la lista de asesores que actualmente proporcionan información al gestor:
`dscontrol advisor list`

Este mandato genera una salida parecida a la siguiente:

ASESOR	CLÚSTER:PUERTO	TPO ESPERA
http	127.40.50.1:80	unlimited
ftp	21	unlimited

- Cambiar el nivel de anotaciones cronológicas de las anotaciones cronológicas del asesor y establecerlo en 0 para mejorar el rendimiento:
`dscontrol advisor loglevel http 80 0`
- Cambiar el tamaño de las anotaciones cronológicas del asesor FTP para el puerto 21 y establecerlo en 5000 bytes:
`dscontrol advisor logsize ftp 21 5000`

- Establecer el tiempo (60 segundos) que un asesor HTTP (para el puerto 80) espera antes de notificar que se ha producido una anomalía en una recepción de un servidor:

```
dscontrol advisor receivetimeout http 80 60
```

- Mostrar un informe en el estado del asesor ftp (para el puerto 21):

```
dscontrol advisor report ftp 21
```

Este mandato genera una salida parecida a la siguiente:

Informe del asesor:

Nombre del asesor Ftp

Número de puerto 21

Dirección del clúster 9.67.131.18

Dirección del servidor ... 9.67.129.230

Carga 8

Dirección del clúster 9.67.131.18

Dirección del servidor ... 9.67.131.215

Carga -1

- Mostrar el estado actual de los valores asociados al asesor http para el puerto 80:

```
dscontrol advisor status http 80
```

Este mandato genera una salida parecida a la siguiente:

Estado del asesor:

Intervalo (segundos) 7

Tiempo de espera (segundos) ... Unlimited

Tiempo espera conexión (seg) .. 21

Tiempo espera recepción (seg).. 21

Nombre anotaciones asesor Http_80.log

Nivel anotación cronológica ... 1

Tam. máx. arch. anot. (bytes) . Unlimited

Número de reintentos 0

- Establecer el valor de tiempo de espera para la información del asesor ftp en el puerto 21 en 5 segundos:

```
dscontrol advisor timeout ftp 21 5
```

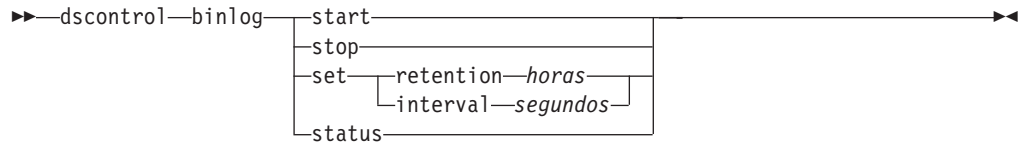
- Mostrar el número de versión actual del asesor SSL para el puerto 443:

```
dscontrol advisor version ssl 443
```

Este mandato genera una salida parecida a la siguiente:

Versión: 04.00.00.00 - 07/12/2001-10:09:56-EDT

dscontrol binlog — controlar el archivo de anotaciones cronológicas binario



start

Inicia las anotaciones cronológicas en binario.

stop

Detiene las anotaciones cronológicas en binario.

set

Establece campos para el registro cronológico en binario. Si desea más información sobre cómo establecer los campos para el registro cronológico en binario, consulte el apartado “Utilización del registro cronológico binario para analizar estadísticas de servidor” en la página 241.

retention

Número de horas que se conservan los archivos de anotaciones cronológicas en binario. El valor por omisión de retention es 24.

horas

Número de horas.

interval

Número de segundos entre las entradas de anotaciones cronológicas. El valor por omisión de interval es 60.

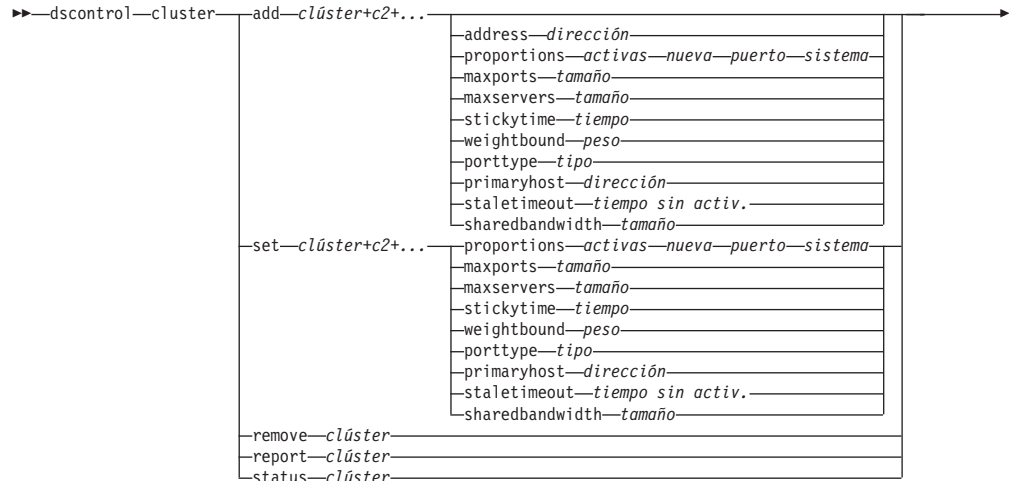
segundos

Número de segundos.

status

Muestra la retención y los intervalos de las anotaciones cronológicas en binario.

dscontrol cluster — configurar clústeres



add

Añade este clúster. Debe definir como mínimo un clúster.

clúster

Nombre o dirección del clúster con el que conectan los clientes. El valor del clúster es un nombre simbólico o está en un formato de dirección IP. Se puede utilizar un valor de clúster de 0.0.0.0 para especificar un clúster comodín. Consulte el apartado “Utilizar un clúster comodín para combinar configuraciones de servidores” en la página 237 para obtener más información.

Con la excepción del mandato dscontrol cluster add, puede utilizar dos puntos (:) como carácter comodín. Por ejemplo, al emitir el siguiente mandato, dscontrol cluster set : weightbound 80, se establecerá una ponderación de 80 en todos los clústeres.

Nota: Los clústeres adicionales se separan mediante un signo más (+).

address

La dirección IP exclusiva de la máquina TCP en formato de nombre de sistema principal o en formato de dirección IP. Si el valor del clúster no puede resolverse, debe proporcionar esta dirección IP de la máquina física.

Nota: address sólo se aplica al componente Dispatcher.

dirección

Valor de la dirección del clúster.

proportions

A nivel de clúster, establezca la proporción de importancia para las conexiones activas (*activas*), las nuevas conexiones (*nuevas*), la información de todos los asesores (*puerto*) y la información de un programa de supervisión del sistema como Metric Server (*sistema*) que utilizará el gestor para establecer los pesos del servidor. Cada uno de estos valores, que se describen a continuación, se expresan como porcentaje del total y, por lo tanto, siempre suman 100. Si desea más información, consulte el apartado “Proporción de la importancia otorgada a la información de estado” en la página 180.

activas

Número de 0 a 100 que representa la proporción del peso que se dará a las conexiones activas. El valor por omisión es 50.

nueva

Número de 0 a 100 que representa la proporción del peso que se dará a las conexiones nuevas. El valor por omisión es 50.

puerto

Número de 0 a 100 que representa la proporción del peso que se dará a la información de asesores. El valor por omisión es 0.

Nota: Al iniciar un asesor y la proporción del puerto es 0, Load Balancer establece automáticamente este valor en 1 para que el gestor utilice la información del asesor como entrada para calcular el peso del servidor.

sistema

Número de 0 a 100 que representa la proporción del peso que se dará a la información de la métrica del sistema, como la de Metric Server. El valor por omisión es 0.

maxports

Número máximo de puertos. El valor por omisión de maxports es 8.

tamaño

Número de puertos permitido.

maxservers

Número máximo por omisión de servidores por puertos. Este valor puede alterarse para puertos individuales mediante **port maxservers**. El valor por omisión de maxservers es 32.

tamaño

Número de servidores permitido en un puerto.

stickytime

El tiempo de permanencia en memoria por omisión para los puertos que se van a crear. Este valor puede alterarse para puertos individuales mediante **port stickytime**. El valor por omisión de stickytime es 0.

Nota: En el caso del método de reenvío CBR de Dispatcher, si establece el tiempo de permanencia en memoria en un valor distinto de cero, el tiempo de permanencia en memoria del puerto está habilitado si el puerto es SSL (no HTTP). Si el tiempo de permanencia en memoria para los puertos que van a crearse es un valor distinto de cero y el nuevo puerto añadido es SSL, la afinidad de ID de SSL está habilitada para el puerto. Para inhabilitar la afinidad de ID SSL en el puerto, será necesario establecer de forma explícita el tiempo de permanencia en memoria en 0.

tiempo

El valor del tiempo de permanencia en memoria en segundos.

weightbound

Ponderación de puerto por omisión. Este valor puede alterarse para puertos individuales mediante **port weightbound**. El valor por omisión de weightbound es 20.

peso

El valor de weightbound.

porttype

El tipo de puerto por omisión. Este valor puede alterarse para puertos individuales mediante **port porttype**.

tipo

Los valores posibles son **tcp**, **udp** y **both**.

primaryhost

Dirección NFA de esta máquina Dispatcher o la dirección NFA de la máquina Dispatcher de reserva. En una configuración de alta disponibilidad mutua , un clúster se asocia con la máquina primaria o de reserva.

Si cambia el valor de primaryhost de un clúster una vez que se han iniciado las máquinas primaria y de reserva y están ejecutando alta disponibilidad mutua, también debe forzar al nuevo sistema principal primario que tome control. Asimismo, es necesario actualizar los scripts y desconfigurar y configurar manualmente el clúster correctamente. Consulte el apartado “Alta disponibilidad mutua” en la página 61 para obtener más información.

dirección

Valor de dirección de primaryhost. El valor por omisión es la dirección NFA de esta máquina.

staletimeout

Número de segundos durante los que se puede estar sin actividad en una conexión antes de que ésta se elimine. El valor por omisión para FTP es 900; el valor por omisión para Telnet es 32.000.000. El valor por omisión para todos los demás protocolos es 300. Este valor puede alterarse para puertos individuales mediante **port staletimeout**. Consulte el apartado “Utilización del valor de tiempo de espera sin actividad” en la página 268 para obtener más información.

tiempo sin actividad

El valor del tiempo sin actividad.

sharedbandwidth

La cantidad máxima de ancho de banda (en kilobytes por segundo) que puede compartirse en el nivel del clúster. Para más información sobre el ancho de banda compartido, consulte los apartados “Utilización de normas basadas en ancho de banda reservado y ancho de banda compartido” en la página 216 y “Norma de ancho de banda compartido” en la página 216.

Nota: sharedbandwidth se aplica al componente Dispatcher.

tamaño

El tamaño de **sharedbandwidth** es un valor entero. El valor por omisión es cero. Si el valor es cero, la anchura de banda no puede compartirse a nivel de clúster.

set

Establece las propiedades del clúster.

remove

Elimina este clúster.

report

Muestra los campos internos del clúster.

Nota: report se aplica al componente Dispatcher.

status

Muestra el estado actual de un clúster específico.

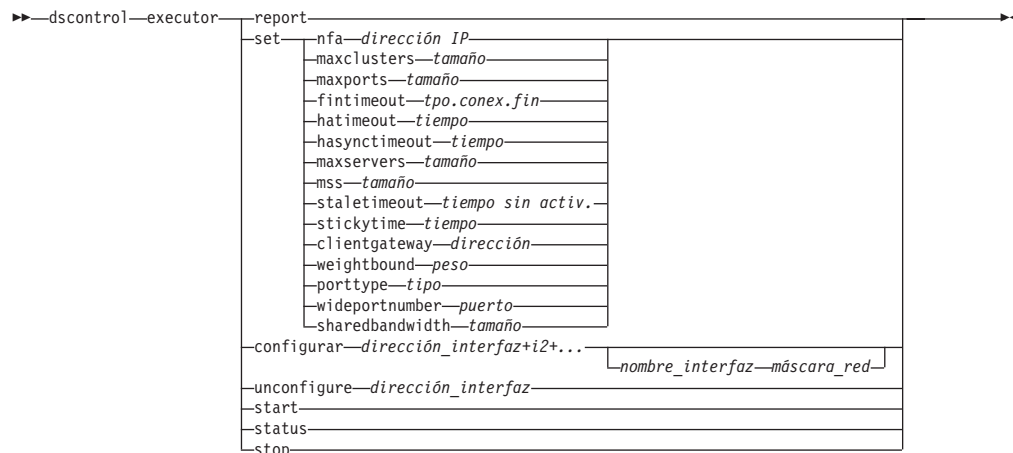
Ejemplos

- Añadir la dirección de clúster 130.40.52.153:
`dscontrol cluster add 130.40.52.153`
- Eliminar la dirección de clúster 130.40.52.153:
`dscontrol cluster remove 130.40.52.153`
- Establecer la importancia relativa indicada en la entrada (activa, nueva, puerto, sistema) que ha recibido el gestor para los servidores que residen en el clúster 9.6.54.12:
`dscontrol cluster set 9.6.54.12 proportions 60 35 5 0`
- Añadir un clúster comodín:
`dscontrol cluster add 0.0.0.0`
- Para una configuración de alta disponibilidad mutua, establecer la dirección de clúster 9.6.54.12 con la NFA de la máquina de reserva (9.65.70.19) que el sistema principal primario:
`dscontrol cluster set 9.6.54.12 primaryhost 9.65.70.19`
- Mostrar el estado de la dirección del clúster 9.67.131.167:
`dscontrol cluster status 9.67.131.167`

Este mandato genera una salida parecida a la siguiente:

```
Estado del clúster:
-----
Clúster ..... 9.67.131.167
Dirección ..... 9.67.131.167
Número de puertos de destino ..... 3
Tiempo permanencia mem. por omisión ..... 0
Tiempo de espera por omisión ..... 30
Ponderación por omisión para puerto ..... 20
Máximo número de puertos ..... 8
Protocolo de puerto por omisión ..... tcp/udp
Número máximo de servidores por omisión . 32
Proporción asignada a conexiones activas. 0.5
Proporción asignada a conexiones nuevas . 0.5
Proporción asignada especif. para puerto. 0
Proporción asignada a métrica sistema ... 0
Ancho de banda compartido (KBytes) ..... 0
Dirección sistema principal primario .... 9.67.131.167
```

dscontrol executor — control del ejecutor



report

Muestra un informe de instantánea de estadísticas. Por ejemplo: total de paquetes recibidos, paquetes descartados, paquetes reenviados con errores, etc.

Nota: report se aplica al componente Dispatcher.

set

Establece los campos del ejecutor.

nfa

Establecer la dirección de no reenvío. La máquina Dispatcher no enviará ninguno de los paquetes reenviados a esta dirección.

Nota: NFA se aplica al componente Dispatcher.

dirección IP

La dirección Internet Protocol como nombre simbólico o en formato decimal separado por puntos.

maxclusters

Número máximo de clústeres que pueden configurarse. El valor por omisión de maxclusters es 100.

tamaño

Número máximo de clústeres que pueden configurarse.

maxports

El valor por omisión de maxports para clústeres que puede crearse. Puede alterarse mediante el mandato **cluster set** o **cluster add**. El valor por omisión de maxports es 8.

tamaño

El tamaño de puertos.

fintimeout

El número de segundos que debe mantenerse una conexión en memoria después de poner la conexión en el estado FIN. El valor por omisión de fintimeout es 60.

tpo.conex.fin

El valor de tiempo de espera para estado FIN.

Nota: `fintimeout` se aplica al componente Dispatcher.

hatimeout

Número de segundos que el ejecutor utiliza para indicar el tiempo de espera de los pulsos de alta disponibilidad. El valor por omisión es 2.

Nota: `hatimeoute` se aplica al componente Dispatcher.

tiempo

El valor de tiempo de espera para alta disponibilidad.

hasynctimeout

Número de segundos que el ejecutor utiliza para indicar el tiempo de espera de la duplicación de registros de conexión entre las máquinas primaria y de reserva. El valor por omisión es 50.

El temporizador se utiliza para asegurarse de que las máquinas primaria y de reserva intentan sincronizarse. Sin embargo, si existen demasiadas conexiones y la máquina activa sigue gestionando una carga significativa del tráfico entrante, es posible que la sincronización no se haya completado antes de que caduque el temporizador. Como consecuencia, Load Balancer intentará volver a sincronizarse constantemente y las dos máquinas nunca se sincronizan. Si se da esta situación, establezca `hasynctimeout` en un valor más alto que el valor por omisión para dar a las dos máquinas suficiente tiempo para intercambiar información sobre las conexiones existentes. Para establecer este temporizador, el mandato `hasynctimeout` se debe emitir después del mandato `dscontrol executor start` pero antes de emitir los mandatos de alta disponibilidad (`dscontrol highavailability`).

Nota: El valor `hasynctimeout` se aplica al componente Dispatcher.

tiempo

El valor de tiempo de espera de sincronización para alta disponibilidad.

maxservers

Número máximo por omisión de servidores por puerto. Puede alterarse mediante el mandato **cluster** o **port**. El valor por omisión de `maxservers` es 32.

mss

Número máximo de bytes del segmento de datos de la conexión TCP/UDP. La suma del número de bytes del segmento de datos y la cabecera debe ser menor que el número de bytes de la MTU (unidad máxima de transmisión). El valor por omisión de `mss` es 1460.

Nota: El tamaño máximo del segmento sólo se aplica al método de reenvío `nat` o `cbr` del componente Dispatcher.

tamaño

Número de servidores.

staletimeout

Número de segundos durante los que se puede estar sin actividad en una conexión antes de que ésta se elimine. El valor por omisión para FTP es 900; el valor por omisión para Telnet es 32.000.000. El valor por omisión para todos los demás puertos 300. Puede alterarse mediante el mandato **cluster** o **port**. Consulte el apartado “Utilización del valor de tiempo de espera sin actividad” en la página 268 para obtener más información.

tiempo sin actividad

El valor del tiempo sin actividad.

stickytime

El valor de tiempo de permanencia en memoria del puerto por omisión para todos los clústeres futuros. Puede alterarse mediante el mandato **cluster** o **port**. El valor por omisión de stickytime es 0.

tiempo

El valor del tiempo de permanencia en memoria en segundos.

clientgateway

Clientgateway es una dirección IP que se utiliza para NAT/NAPT o Direccionamiento basado en contenido de Dispatcher. Es la dirección del direccionador a través del que se reenvía el tráfico en la dirección de retorno desde Load Balancer a los clientes. Clientgateway debe establecerse en un valor distinto de cero antes de añadir un puerto con el método de reenvío NAT/NAPT o Direccionamiento basado en contenido de Dispatcher. Consulte los apartados “NAT/NAPT de Dispatcher (método de reenvío nat)” en la página 53 y “Direccionamiento basado en contenido de Dispatcher (método de reenvío cbr)” en la página 55 para obtener más información.

Nota: clientgateway sólo se aplica al componente Dispatcher.

dirección

La dirección de clientgateway como nombre simbólico o en formato decimal separado por puntos. El valor por omisión es 0.0.0.0.

weightbound

El valor de ponderación del puerto determinado para todos los puertos futuros. Puede alterarse mediante el mandato **cluster** o **port**. El valor por omisión de weightbound es 20.

peso

El valor de ponderación.

porttype

El valor de tipo de puerto del puerto por omisión para todos los puertos futuros. Puede alterarse mediante el mandato **cluster** o **port**.

Nota: porttype se aplica al componente Dispatcher.

tipo

Los valores posibles son **tcp**, **udp** y **both**.

wideportnumber

Puerto TCP no utilizado en cada máquina Dispatcher. El valor de *wideportnumber* debe ser el mismo para todas las máquinas de Dispatcher. El valor por omisión de wideportnumber es 0, lo que indica que no se está utilizando el soporte de área amplia.

Nota: wideportnumber se aplica al componente Dispatcher.

puerto

El valor de **wideportnumber**.

sharedbandwidth

La cantidad máxima de ancho de banda (en kilobytes por segundo) que puede compartirse en el nivel del ejecutor. Para más información sobre el ancho de banda compartido, consulte los apartados “Utilización de normas basadas en ancho de banda reservado y ancho de banda compartido” en la página 216 y “Norma de ancho de banda compartido” en la página 216.

Nota: sharedbandwidth se aplica al componente Dispatcher.

tamaño

El tamaño de **sharedbandwidth** es un valor entero. El valor por omisión es cero. Si el valor es cero, la anchura de banda no puede compartirse a nivel de ejecutor.

configure

Configura una dirección (por ejemplo, una dirección de clúster, dirección de retorno o una dirección de pulso de alta disponibilidad) para la tarjeta de interfaz de red de la máquina Dispatcher. También se conoce como configuración de un alias en la máquina Dispatcher.

Nota: configure se aplica al componente Dispatcher.

dirección_interfaz

La dirección es un nombre simbólico o aparecer en formato de dirección IP.

Nota: Las direcciones de interfaces adicionales se separan mediante un signo más (+).

nombre_interfaz máscara_red

Esta opción sólo es necesaria si la dirección no coincide con ninguna subred de las direcciones existentes. *nombre_interfaz* puede ser un valor como: en0, eth1, eri0. La *máscara_red* es la máscara de 32 bits utilizada para identificar los bits de la dirección de subred en la parte que muestra el sistema principal en una dirección IP.

unconfigure

Suprime la dirección de alias de la tarjeta de interfaz de red.

Nota: unconfigure se aplica al componente Dispatcher.

start

Inicia el ejecutor.

status

Muestra el estado actual de los valores en el ejecutar que puede establecerse y sus valores por omisión.

stop

Detiene el ejecutor.

Nota: stop se aplica a Dispatcher y a CBR.

Ejemplos

- Mostrar los contadores internos para Dispatcher:

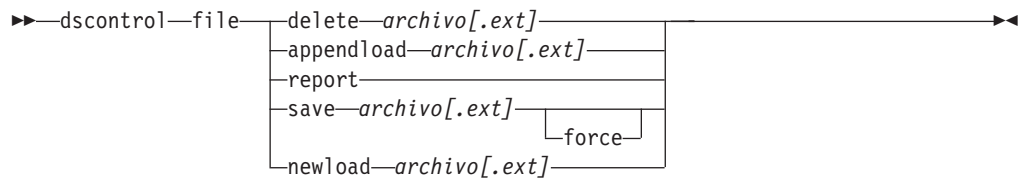
```
dscontrol executor status
```

Estado del ejecutor:

```
-----  
Dirección de no reenvío ..... 9.67.131.151  
Dirección de pasarela del cliente ... 0.0.0.0  
Tiempo de espera para estado FIN .... 60  
Número puerto de red de área amplia . 0  
Ancho de banda compartido (Kbytes) .. 0  
Núm. máx. omisión puertos por clúster 8  
Número máximo de clústeres ..... 100  
Núm. máx. omisión servid. por puerto. 32  
Tiempo de espera por omisión ..... 300  
Tiempo permanencia memoria omisión .. 0  
Ponderación por omisión ..... 20  
Tipo de puerto por omisión ..... tcp/udp
```


- Establecer la dirección de no reenvío 130.40.52.167:
`dscontrol executor set nfa 130.40.52.167`
- Establecer el número máximo de clústeres:
`dscontrol executor set maxclusters 4096`
- Iniciar el ejecutor:
`dscontrol executor start`
- Detener el ejecutor:
`dscontrol executor stop`

dscontrol file — gestionar archivos de configuración



delete

Suprime el archivo.

archivo[.ext]

Archivo de configuración que consta de mandatos dscontrol.

La extensión de archivo (*.ext*) puede ser cualquiera y puede omitirse.

appendload

Para actualizar la configuración actual, el mandato `appendload` ejecuta los mandatos ejecutables para el archivo de script.

report

Informa sobre el archivo o archivos disponibles.

save

Guarda la configuración actual de Load Balancer en el archivo.

Nota: Los archivos se guardan y se cargan de los siguientes directorios, donde *componente* es Dispatcher o CBR:

- Sistemas Linux y UNIX: `/opt/ibm/edge/lb/servers/configurations/componente`
- Plataforma Windows: `C:\Archivos de programa\ibm\edge\lb\servers\configurations\componente`

force

Para guardar el archivo en un archivo existente con el mismo nombre, utilice **force** para suprimir el archivo existente antes de guardar el nuevo archivo. Si no utiliza la opción `force`, no se sobrescribirá el archivo existente.

newload

Carga y ejecuta un nuevo archivo de configuración en Load Balancer. El nuevo archivo de configuración sustituye a la configuración actual.

Ejemplos

- Suprimir un archivo:

```
dscontrol file delete file3
```

Se ha suprimido el archivo (file3).

- Cargar un nuevo archivo de configuración para que sustituya a la configuración actual:

```
dscontrol file newload file1.sv
```

El archivo (file1.sv) se ha cargado en Dispatcher.

- Adjuntar un archivo de configuración a una configuración actual y cargar:

```
dscontrol file appendload file2.sv
```

El archivo (file2.sv) se ha añadido a la configuración actual y se ha cargado.

- Ver un informe de los archivos (es decir, estos archivos que ha guardado anteriormente):

```
dscontrol file report
```

```
INFORME SOBRE EL ARCHIVO:
```

```
file1.save
```

```
file2.sv
```

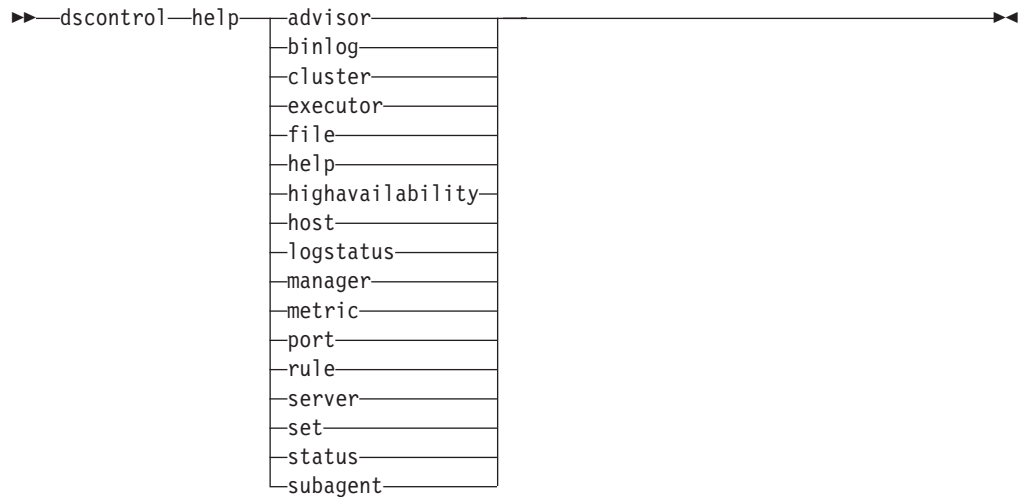
```
file3
```

- Guardar la configuración en un archivo denominado file3:

```
dscontrol file save file3
```

La configuración se ha guardado en el archivo (file3).

dscontrol help — mostrar o imprimir ayuda para este mandato



Ejemplos

- Obtener ayuda sobre el mandato dscontrol:
`dscontrol help`

Este mandato genera una salida parecida a la siguiente:

ARGUMENTOS DEL MANDATO DE AYUDA:

Uso: help <opción de ayuda>

Ejemplo: help cluster

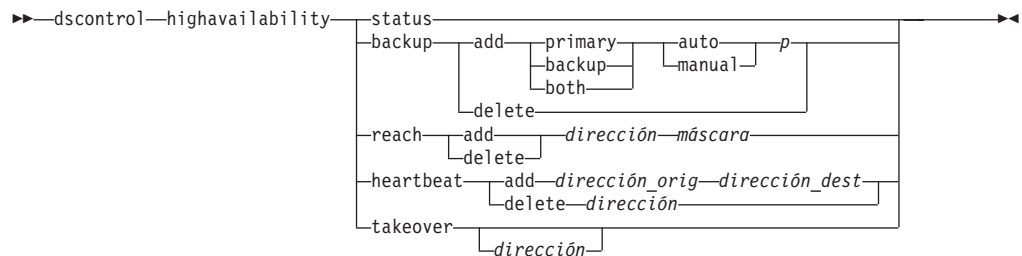
help	- imprime el texto completo de la ayuda
advisor	- ayuda para el mandato advisor
cluster	- ayuda para el mandato cluster
executor	- ayuda para el mandato executor
file	- ayuda para el mandato file
host	- ayuda para el mandato host
binlog	- ayuda para el mandato binary log
manager	- ayuda para el mandato manager
metric	- ayuda para el mandato metric
port	- ayuda para el mandato port
rule	- ayuda para el mandato rule
server	- ayuda para el mandato server
set	- ayuda para el mandato set
status	- ayuda para el mandato status
logstatus	- ayuda para el mandato logstatus del servidor
subagent	- ayuda para el mandato subagent
highavailability	- ayuda para el mandato highavailability

Observe que los parámetros dentro de <> son variables.

- Algunas veces la ayuda mostrará opciones para las variables utilizando | para separar las opciones:
`fintimeout <dirección de clúster>|all <hora>`
-Cambiar tiempo de espera FIN
(Usar 'all' para cambiar todos los clústeres)

dscontrol highavailability — controlar alta disponibilidad

Nota: El diagrama de sintaxis de alta disponibilidad de dscontrol sólo se aplica al componente Dispatcher.



status

Devuelve un informe de alta disponibilidad. Las máquinas se identifican con una de tres condiciones o estados:

Active Una máquina determinada (una máquina primaria, de reserva o ambas) está direccionando los paquetes.

Standby

Una máquina determinada (una máquina primaria, de reserva o ambas) no está direccionando paquetes; está supervisando el estado de una máquina Dispatcher **activa**.

Idle Una máquina determinada está direccionando paquetes y no intenta establecer contacto con su sistema Dispatcher asociado.

Además, la palabra clave **status** devuelve información sobre diversos subestados:

Synchronized

Una máquina determinada ha establecido contacto con otro sistema Dispatcher.

Other substates

Esta máquina intenta establecer contacto con su sistema Dispatcher asociado, pero todavía no ha dado resultado.

backup

Especifique la información para la máquina primaria o de reserva.

add

Define y ejecuta las funciones de alta disponibilidad para esta máquina.

primary

Identifica la máquina Dispatcher que tiene un rol *primario*.

backup

Identifica la máquina Dispatcher que tiene un rol de *reserva*.

both

Identifica la máquina Dispatcher que tiene *ambos* roles, *primario* y de *reserva*. Se trata de una característica de alta disponibilidad mutua en donde los roles *primario* y de *reserva* están asociados para cada conjunto de clústeres. Consulte el apartado “Alta disponibilidad mutua” en la página 61 para obtener más información.

auto

Especifica una estrategia de recuperación *automática*, en la que la máquina primaria reanudará el direccionamiento de paquetes tan pronto como vuelva a estar en funcionamiento.

manual

Especifica la estrategia de recuperación *manual*, en la que la máquina primaria no reanuda el direccionamiento de paquetes hasta que el administrador emite un mandato **takeover**.

p[uerto]

Puerto TCP sin utilizar en ambas máquinas que utilizará Dispatcher para sus mensajes de pulso. El *puerto* debe ser el mismo para las máquinas primaria y de reserva.

delete

Saca esta máquina de la configuración de alta disponibilidad, por lo que ya no se podrá utilizar como máquina primaria o de reserva.

reach

Añade o suprime la dirección de destino para los sistemas Dispatcher primario y de reserva, el asesor de alcance emite mandatos *ping* a los sistemas Dispatcher primario y de reserva para determinar la accesibilidad de sus destinos.

Nota: Al configurar el destino de alcance, también debe iniciar el asesor de alcance. El asesor de alcance lo inicia automáticamente la función de gestor.

add

Añade una dirección de destino para el asesor de alcance.

delete

Elimina una dirección de destino del asesor de alcance.

dirección

Dirección IP (en formato de dirección IP o nombre simbólico) del nodo de destino.

máscara

Una máscara de subred.

heartbeat

Define una sesión de comunicación entre las máquinas Dispatcher primaria y de reserva.

add

Informa al sistema Dispatcher de origen de la dirección de su socio (dirección de destino).

dirección_orig

Dirección de origen. La dirección (IP o simbólica) de esta máquina Dispatcher.

dirección_dest

Dirección de destino. La dirección (IP o simbólica) de la otra máquina Dispatcher.

Nota: La *dirección_orig* y la *dirección_dest* deben ser las NFA de las máquinas para como mínimo un par de pulsos.

delete

Elimina el par de dirección de la información de pulso. Puede especificar la dirección de destino o de origen del par de pulso.

dirección

La dirección (IP o simbólica) del destino o del origen.

takeover

Configuración de alta disponibilidad simple (el rol de las máquinas Dispatcher puede ser primario, *primary* o de reserva, *backup*):

- La opción takeover indica al sistema Dispatcher en espera que pase a estar activo y empiece a direccionar paquetes. Esto forzará a que el sistema Dispatcher activo actualmente pase al estado en espera. El mandato takeover debe emitirse en una máquina en espera y sólo funciona cuando la estrategia es **manual**. El subestado debe ser *synchronized*.

Configuración de alta disponibilidad mutua (el rol de cada máquina Dispatcher es ambos, *both*):

- La máquina Dispatcher con la característica de alta disponibilidad mutua contiene dos clústeres que coinciden con sus asociados. Uno de los clústeres se considera el clúster primario (el clúster de copia de seguridad del asociado) y el otro es el clúster de reserva (el clúster primario del asociado). Takeover indica a la máquina Dispatcher que empiece el direccionamiento de paquetes hacia los clúster(es) de la otra máquina. El mandato takeover sólo puede emitirse cuando los clústeres de la máquina Dispatcher están en estado *standby* y es subestado es *synchronized*. Esto forzará que los clústeres activos actualmente del asociado pasen al estado en espera. El mandato takeover sólo funciona cuando la estrategia es **manual**. Consulte el apartado “Alta disponibilidad mutua” en la página 61 para obtener más información.

Notas:

1. Tenga en cuenta que los *roles* de las máquinas (*primary*, *backup*, *both*) no cambian. Sólo cambian su *status* relativo (*active* o *standby*).
2. existen tres posibles *scripts* de takeover: *goActive*, *goStandby* y *goInOp*. Consulte el apartado “Utilización scripts” en la página 209.

dirección

El valor de la dirección de takeover es opcional. Sólo debe utilizarse cuando el rol de la máquina es *both*, es decir primario y de reserva (configuración de alta disponibilidad mutua). La dirección especificada es la NFA de la máquina Dispatcher que normalmente direcciona el tráfico de este clúster. Cuando se produce un proceso de toma de control en ambos clústeres, especifique la propia dirección NFA del sistema Dispatcher.

Ejemplos

- Comprobar el estado de alta disponibilidad de una máquina:

```
dscontrol highavailability status
```

Salida:

Estado de alta disponibilidad:

```
Rol .....primario
Estrategia de recuperación .. manual
Estado ..... Activo
Subestado ..... Sincronizado
Sis. principal primario ..... 9.67.131.151
Puerto ..... 12345
Destino preferente ..... 9.67.134.223
```

Estado de pulso:

Recuento 1

Origen/destino 9.67.131.151/9.67.134.223

Estado de accesibilidad:

Recuento 1

Dirección 9.67.131.1 accesible

- Añadir la información de copia de seguridad a la máquina primaria con la estrategia de recuperación automática y el puerto 80:
dscontrol highavailability backup add primary auto 80
- Añadir una dirección a la que Dispatcher debe poder acceder:
dscontrol highavailability reach add 9.67.125.18
- Añadir información de pulso para las máquinas primaria y de reserva.
Primary - highavailability heartbeat add 9.67.111.3 9.67.186.8
Backup - highavailability heartbeat add 9.67.186.8 9.67.111.3
- Indicar a Dispatcher en espera que pase a estar activo, forzando que la máquina activa pase a estar en espera:
dscontrol highavailability takeover

dscontrol host — configurar un máquina remota

►►—dscontrol—host:—*sistppal_remoto*—◄◄

sistppal_remoto

Nombre de la máquina Load Balancer remota que se configura. Cuando escriba este mandato, asegúrese de que no hay ningún espacio entre **host:** y *sistppal_remoto*, por ejemplo:

dscontrol host:*sistppal_remoto*

Después de emitir el mandato en el indicador de mandatos, escriba cualquier mandato dscontrol válido que desee emitir en la máquina Load Balancer remota.

dscontrol logstatus — mostrar valores de anotaciones cronológicas de servidor

►—dscontrol—logstatus—◄◄

logstatus

Muestra los valores de las anotaciones cronológicas del servidor (nombre de archivo de anotaciones cronológicas, nivel de registro cronológico y tamaño de las anotaciones cronológicas).

Ejemplos

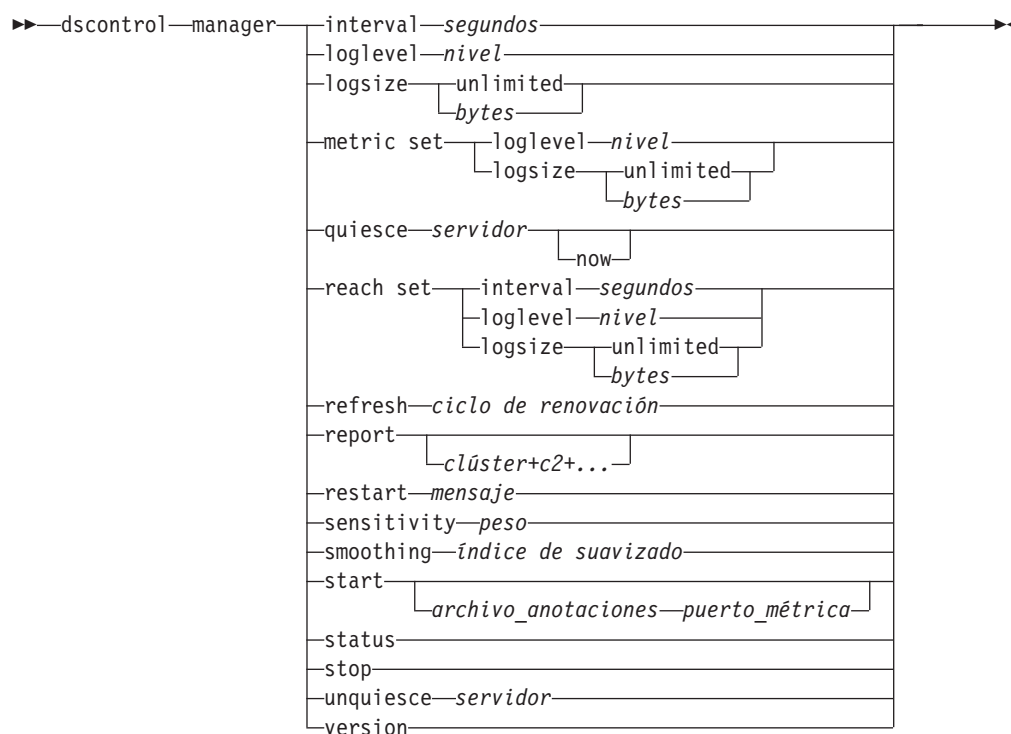
Mostrar el estado de las anotaciones cronológicas:

```
dscontrol logstatus
```

Este mandato genera una salida parecida a la siguiente:

```
Estado de anotaciones de Dispatcher
-----
Archivo de anotaciones ..... C:\ARCHIV~1\IBM\edge\lb\servers\logs\dispatcher
\server.log
Nivel anotación cronológica. 1
Tam. máx. archivo anotac. .. 1048576
```

dscontrol manager — controlar el gestor



interval

Establece la frecuencia con que el gestor actualizará los pesos de los servidores para el ejecutor, actualizando los criterios que el ejecutor utiliza para direccionar peticiones de clientes.

segundos

Número positivo que representa la frecuencia en segundos con la que el gestor actualizará los pesos para el ejecutor. El valor por omisión es 2.

loglevel

Establece el nivel de registro cronológico para las anotaciones cronológicas del gestor.

nivel

El número del nivel (0 a 5). Cuanto más alto sea el número, más información se anotará en las anotaciones cronológicas del gestor. El valor por omisión es 1. A continuación se muestran los valores posibles: 0 equivale a Ninguno, 1 a Mínimo, 2 a Básico, 3 a Moderado, 4 a Avanzado, 5 a Detallado.

logsize

Establece el tamaño máximo de las anotaciones cronológicas del gestor. Cuando se establece un tamaño máximo para el archivo de anotaciones cronológicas, el texto del archivo vuelve al principio; es decir, cuando el archivo alcanza el tamaño especificado, las entradas subsiguientes se anotarán al principio del archivo y se grabarán encima de las entradas de anotaciones cronológicas anteriores. El tamaño de las anotaciones cronológicas no puede establecerse más pequeño que el tamaño actual de las anotaciones cronológicas. Las entradas de las anotaciones cronológicas incluyen la indicación de la hora para poder saber el orden en el que se anotaron. Cuando más alto se establezca el nivel de anotaciones cronológicas, más cuidado deberá tener al

elegir el tamaño de las anotaciones cronológicas porque, cuando el registro cronológico está establecido en los niveles más altos, puede quedarse sin espacio rápidamente.

bytes

El tamaño máximo en bytes para el archivo de anotaciones cronológicas de gestor. Puede especificar un número positivo mayor que cero o la palabra **unlimited**. Es posible que el archivo de anotaciones cronológicas no alcance el tamaño máximo exacto antes de empezar a sobrescribir porque el tamaño de las entradas del archivo varían. El valor por omisión es 1 MB.

metric set

Establece **loglevel** y **logsize** para las anotaciones cronológicas del supervisor de métrica. **loglevel** es el nivel de registro cronológico del supervisor de métrica (0 - Ninguno, 1 - Mínimo, 2 - Básico, 3 - Moderado, 4 - Avanzado o 5 - Detallado). El valor por omisión de **loglevel** es 1. El **logsize** es el número máximo de bytes que deben anotarse en el archivo de anotaciones cronológicas del supervisor de métrica. Puede especificar un número positivo mayor que cero o **unlimited**. El valor por omisión es 1 MB.

quiesce

No especifique más conexiones para enviar a un servidor, a excepción de las nuevas conexiones subsiguientes del cliente al servidor desactivado temporalmente, si la conexión se designa como de permanencia en memoria y el tiempo de permanencia en memoria no ha caducado. El gestor establece el peso para dicho servidor en 0 en cada puerto para el que está definido. Utilice este mandato si desea realizar un mantenimiento rápido en un servidor y, a continuación, desactivarlo temporalmente. Si suprime un servidor desactivado temporalmente de la configuración y después lo vuelve a añadir, no retendrá el estado que tenía antes de desactivarse temporalmente. Para obtener más información, consulte el apartado “Desactivar temporalmente el manejo de conexiones de servidor” en la página 224.

servidor

Dirección IP del servidor en forma de nombre simbólico o en formato decimal separado por puntos.

O, si ha utilizado la partición del servidor, utilice el nombre exclusivo del servidor lógico. Consulte el apartado “Creación de particiones del servidor: servidores lógicos configurados con un servidor físico (dirección IP)” en la página 58 para obtener más información.

now

Utilice la opción **quiesce “now”** sólo si ha fijado el tiempo de permanencia en memoria y desea que las nuevas conexiones se envíen a otro servidor (distinto del servidor desactivado temporalmente) antes de que caduque el tiempo de permanencia en memoria. Para obtener más información, consulte el apartado “Desactivar temporalmente el manejo de conexiones de servidor” en la página 224.

reach set

Establece el intervalo, el nivel de anotaciones cronológicas y el tamaño de las anotaciones cronológicas para el asesor de alcance.

refresh

Establece el número de intervalos antes de solicitar al ejecutor que renueve la información sobre conexiones nuevas y activas.

ciclo de renovación

Número positivo que representa el número de intervalos. El valor por omisión es 2.

report

Muestra un informe de instantánea de estadísticas.

clúster

La dirección del clúster que desea que se muestre en el informe. La dirección puede ser un nombre simbólico o aparecer en formato de dirección IP. El valor por omisión es una pantalla de informe de gestor para todos los clústeres.

Nota: Los clústeres adicionales se separan mediante un signo más (+).

restart

Reinicia todos los servidores (que no están inactivos) para pesos normalizados (1/2 del peso máximo).

mensaje

Mensaje que desea escribir en el archivo de anotaciones cronológicas del gestor.

sensitivity

Establece la sensibilidad mínima en la que se actualizan los pesos. Este valor define cuando el gestor debe cambiar su ponderación para el servidor basándose en información externa.

peso

Número comprendido entre 1 y 100 que debe utilizarse como porcentaje de peso. El valor por omisión 5 crea una sensibilidad mínima del 5%.

smoothing

Establece un índice que suavice las variaciones en el peso al realizar el equilibrio de carga. Un índice de suavizado más alto hará que los pesos de servidores cambien menos radicalmente cuando cambian las condiciones de la red. Un índice más bajo hará que los pesos de servidores cambien de forma más radical.

índice

Número de coma flotante positivo. El valor por omisión es 1,5.

start

Inicia el gestor.

archivo_anotaciones

Nombre de archivo en el que se anotan los datos del gestor. Cada registro del archivo de anotaciones cronológicas tiene la indicación de la hora.

El archivo por omisión se instala en el directorio **logs**. Consulte el Apéndice C, "Archivos de configuración de ejemplo", en la página 479. Para cambiar el directorio en el que se guardan los archivos de anotaciones cronológicas, consulte el apartado "Cambio de las vías de acceso del archivo de anotaciones cronológicas" en la página 267.

puerto_métrica

Puerto que Metric Server utilizará para notificar cargas del sistema. Si especifica un puerto de métrica, debe especificar un nombre de archivo de anotaciones cronológicas. El puerto de métrica por omisión es 10004.

status

Muestra el estado actual de todos los valores del gestor que pueden establecerse globalmente y sus valores por omisión.

stop

Detiene el gestor.

unquiesce

Especifica que el gestor puede empezar a otorgar un peso superior a 0 a un servidor que anteriormente se había desactivado temporalmente, en cada puerto en el que está definido.

servidor

Dirección IP del servidor en forma de nombre simbólico o en formato decimal separado por puntos.

version

Muestra la versión actual del gestor.

Ejemplos

- Establecer el intervalo de actualización del gestor en cada 5 segundos:
`dscontrol manager interval 5`
- Establecer el nivel de registro cronológico en 0 para obtener un mejor rendimiento:
`dscontrol manager loglevel 0`
- Establecer el tamaño de las anotaciones cronológicas del gestor en 1.000.000 bytes:
`dscontrol manager logsize 1000000`
- Especificar que no se envíen más conexiones al servidor 130.40.52.153:
`dscontrol manager quiesce 130.40.52.153`
- Establecer el número de intervalos de actualización antes de que los pasos se renueven en 3:
`dscontrol manager refresh 3`
- Obtener una instantánea de estadísticas del gestor:
`dscontrol manager report`

Este mandato genera una salida parecida a la siguiente:

SERVIDOR		DIRECCIÓN IP		ESTADO	
mach14.dmz.com		10.6.21.14		ACTIVO	
mach15.dmz.com		10.6.21.15		ACTIVO	

LEYENDA INFORMES GESTOR	
ACTV	Conexiones activas
NEWC	Conexiones nuevas
SYS	Métrica del sistema
NOW	Peso actual
NEW	Nuevo peso
WT	Peso
CONN	Conexiones

www.dmz.com	PESO		ACTV	NUEVAC	PUERTO	SIS
10.6.21.100	NOW NUE		49%	50%	1%	0%
PUERTO: 21						

mach14.dmz.com	10	10	0	0	-1	0
mach15.dmz.com	10	10	0	0	-1	0

www.dmz.com	PESO		ACTV	NUEVAC	PUERTO	SIS
10.6.21.100	NOW NUE		49%	50%	1%	0%
PUERTO: 80						

mach14.dmz.com	10	10	0	0	23	0
mach15.dmz.com	9	9	0	0	30	0

ASESOR	CLÚSTER:PUERTO	TPO ESPERA
--------	----------------	------------

http	80	unlimited
ftp	21	unlimited

- Reiniciar todos los servidores para pesos normalizados y escribe un mensaje en el archivo de anotaciones cronológicas del gestor:
dscontrol manager restart Reiniciando el gestor para actualizar código

Este mandato genera una salida parecida a la siguiente:

320-14:04:54 Reiniciando el gestor para actualizar código

- Establecer la sensibilidad de cambios de peso en 10:
dscontrol manager sensitivity 10
- Establecer el índice de suavidad 2.0:
dscontrol manager smoothing 2.0
- Iniciar el gestor y especificar el archivo de anotaciones cronológicas denominado ndmgr.log (no se pueden establecer vías de acceso)
dscontrol manager start ndmgr.log
- Mostrar el estado actual de los valores asociados al gestor:
dscontrol manager status

Este mandato genera una salida parecida al siguiente ejemplo:

Estado del gestor:

=====

```
Puerto de métrica ..... 10004
Archivo anotaciones del gestor ..... manager.log
Nivel anotaciones del gestor ..... 1
Tamaño máximo anotaciones de gestor (bytes) .. unlimited
Nivel de sensibilidad ..... 0,05
Índice de suavizado ..... 1,5
Intervalo de actualización (segundos) ..... 2
Ciclo de renovación de pesos ..... 2
Nivel de anotaciones asesor de alcance ..... 1
Tamaño máximo anot. asesor alcance (bytes) ... unlimited
Intervalo intentos acceso a destino (seg.) ... 7
Nombre archivo anotaciones supervisor métrica. MetricMonitor.log
Nivel anotac. cronológicas supervisor métrica 1
Tam. máx. arch. anotac. cronológicas supervisor métrica 1048576
```

- Detener el gestor:
`dscontrol manager stop`
- Especificar que no se envíen más conexiones nuevas al servidor 130.40.52.153.
(Nota: desactive temporalmente el servidor “ahora” sólo si ha establecido el tiempo de permanencia en memoria y desea enviar nuevas conexiones a otro servidor antes de que caduque el tiempo de permanencia en memoria). :
`dscontrol manager quiesce 130.40.52.153 now`
- Especificar que no se envíen más conexiones nuevas al servidor 130.40.52.153.
(Nota: si ha establecido el tiempo de permanencia en memoria, las conexiones nuevas subsiguientes del cliente se envían a este servidor hasta que caduque el tiempo de permanencia en memoria). :
`dscontrol manager quiesce 130.40.52.153`
- Especificar que el gestor puede empezar a otorgar un peso superior a 0 a un servidor en la dirección 130.40.52.153 que anteriormente se había desactivado temporalmente:
`dscontrol manager unquiesce 130.40.52.153`
- Mostrar el número de versión actual del gestor:
`dscontrol manager version`

dscontrol metric — configurar métrica del sistema

```
➤—dscontrol—metric—add—clúster+c2+...+cN:métrica+métrica1+...+métricaN—
—remove—clúster+c2+...+cN:métrica+métrica1+...+métricaN—
—proportions—clúster+c2+...+cN proporción1 prop2 prop3...propN—
—status—clúster+c2+...+cN:métrica+métrica1+...+métricaN—➤
```

add

Añadir la métrica específica.

clúster

Dirección a la que se conectan los clientes. La dirección puede ser el nombre de sistema principal de la máquina o el formato de notación de dirección IP. Los clústeres adicionales se separan mediante un signo más (+).

métrica

El nombre del sistema métrico. Debe ser el nombre de un archivo script o ejecutable en el directorio de scripts de Metric Server.

remove

Elimina la métrica especificada.

proportions

Establece las proporciones para toda la métrica asociada a este objeto.

status

Muestra los valores actuales de esta métrica.

Ejemplos

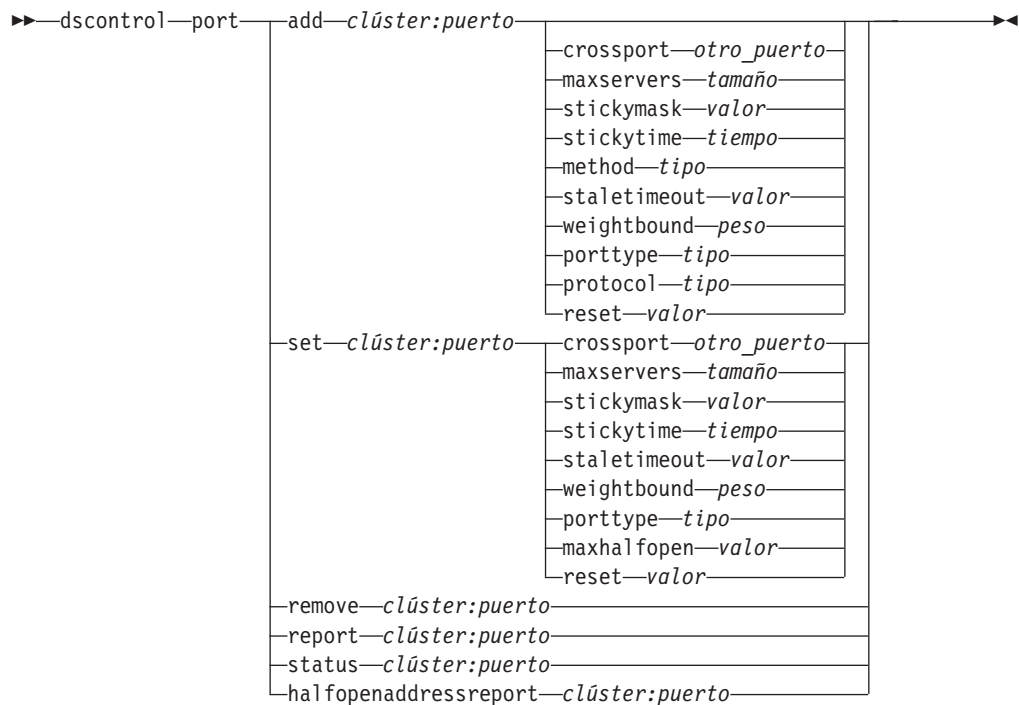
- Para añadir una métrica de sistema:
`dscontrol metric add sitio1:métrica1`
- Para establecer proporciones para el nombre de sitio con dos métricas de sistema:
`dscontrol metric proportions sitio1 0 100`
- Mostrar el estado actual de valores asociados a la métrica especificada:
`dscontrol metric status sitio1:métrica1`

Este mandato genera una salida parecida a la siguiente:

Estado de métrica:

```
Clúster ..... 10.10.10.20
Nombre de métrica ..... metric1
Proporción de métrica ..... 50
  Servidor ..... plm3
  Datos métrica ..... -1
```

dscontrol port — configurar puertos



add

Añade un puerto a un clúster. Debe añadir un puerto a un clúster para poder añadir servidores a dicho puerto. Si no hay puertos para un clúster, todas las peticiones de cliente se procesan localmente. Con este mandato puede añadir más de un puerto a la vez.

clúster

La dirección del clúster, en forma de nombre simbólico o en un formato de dirección IP. Puede utilizar dos puntos (:) como carácter comodín. Por ejemplo, al emitir el mandato `dscontrol port add :80` se añadirá el puerto 80 a todos los clústeres.

Nota: Los clústeres adicionales se separan mediante un signo más (+).

puerto

El número del puerto. El valor de número de puerto 0 (cero) puede utilizarse para especificar un puerto comodín.

Nota: Los puertos adicionales se separan mediante un signo más (+).

crossport

Crossport permite expandir la característica de permanencia en memoria/afinidad por varios puertos para que las peticiones de cliente recibidas en distintos puertos se puedan seguir enviando al mismo servidor para las peticiones subsiguientes. En el valor `crossport`, especifique el número `otro_puerto` para el que desea compartir la característica de afinidad entre puertos. Para utilizar esta característica, los puertos deben:

- compartir la misma dirección de clúster
- compartir los mismos servidores
- tener el mismo valor de permanencia en memoria (no cero)

- tener el mismo valor de máscara de permanencia en memoria

Para eliminar la característica crossport, establezca el valor de crossport de nuevo en el número de su propio puerto. Para obtener más información sobre la característica de afinidad entre puertos, consulte el apartado “Afinidad entre puertos” en la página 222.

Nota: crossport sólo se aplica a los métodos de reenvío NAT/NATP y MAC del componente Dispatcher.

otro_puerto

El valor de crossport. El valor por omisión es el número de su propio *puerto*.

maxservers

Número máximo de servidores. El valor por omisión de maxservers es 32.

tamaño

El valor de maxservers.

stickymask

La característica de máscara de dirección de afinidad agrupa las peticiones de cliente entrantes en base a direcciones de subred comunes. La primera vez que una petición de cliente establece una conexión con el puerto, todas las peticiones subsiguientes procedentes de clientes con la misma dirección de subred (representada por la parte de la dirección IP que está enmascarada) se dirigen al mismo servidor. Para poder habilitar stickymask, port stickytime debe tener un valor distinto de cero. Consulte el apartado “Máscara de dirección de afinidad (stickymask)” en la página 223 para obtener más información.

Nota: La palabra clave stickymask sólo se aplica al componente Dispatcher.

valor

El valor stickymask es el número de bits de orden superior de la dirección IP de 32 bits que desea ocultar. Los valores posibles son: 8, 16, 24 y 32. El valor por omisión es 32, que inhabilita la característica de máscara de dirección de afinidad.

stickytime

El período de permanencia en memoria es el intervalo entre el cierre de una conexión y la apertura de una conexión nueva, durante el cual un cliente se volverá a enviar al mismo servidor utilizado durante la primera conexión. Una vez transcurrido el tiempo de permanencia en memoria, puede enviarse el cliente a un servidor distinto del primero.

para el componente Dispatcher:

- Para el método de reenvío CBR de Dispatcher
 - Sólo puede establecer stickytime (en un valor distinto de cero) en un puerto SSL (no HTTP) porque al definir stickytime se habilita la afinidad de ID de SSL.
 - Si establece port stickytime, el tipo de afinidad en la norma debe ser none (valor por omisión). La afinidad basada en normas (cookie pasivo, URI) no puede coexistir cuando stickytime se establece en el puerto.
- Para los métodos de reenvío NAT y MAC de Dispatcher
 - Si establece port stickytime (en un valor distinto de cero), no puede establecer un tipo de afinidad en la norma. La afinidad basada en normas no puede coexistir cuando stickytime se establece en el puerto.

- Si se define un valor `port stickytime` se habilitará la afinidad de dirección IP.

Para el componente CBR: si establece `port stickytime` en un valor distinto de cero, el tipo de afinidad en la norma debe ser `none` (valor por omisión). La afinidad basada en normas (cookie pasivo, URI, cookie activo) no puede coexistir cuando `stickytime` se establece en el puerto.

tiempo

El tiempo de permanencia en memoria en número de segundos. Cero significa que el puerto no es de permanencia en memoria.

method

Método de reenvío. Los métodos de reenvío posibles son: reenvío MAC, reenvío NAT o reenvío CBR (Content Based Routing). *No* debería añadir un método de reenvío NAT o CBR, a menos que primero especifique una dirección IP distinta de cero en el parámetro `clientgateway` del mandato `dscontrol` ejecutor. Consulte los apartados “NAT/NAPT de Dispatcher (método de reenvío nat)” en la página 53 y “Direccionamiento basado en contenido de Dispatcher (método de reenvío cbr)” en la página 55 para obtener más información.

Notas:

1. `method` sólo se aplica al componente Dispatcher.
2. Si un servidor de programa de fondo está en la misma subred que la dirección de retorno, y está utilizando el método de reenvío CBR o el método de reenvío NAT, debe definir la dirección del direccionador de modo que sea la dirección del servidor de programa de fondo.
3. Si añade un método de reenvío MAC, es necesario que especifique el parámetro “protocol” como HTTP o SSL.

tipo

Tipo del método de reenvío. Los valores posibles son: `mac`, `nat` o `cbr`. El valor por omisión es el reenvío MAC.

staletimeout

Número de segundos durante los que se puede estar sin actividad en una conexión antes de que ésta se elimine. Para el componente Dispatcher, el valor por omisión es 900 para el puerto 21 (FTP) y 32.000.000 para el puerto 23 (Telnet). Para los demás puertos Dispatcher y todos los puertos CBR, el valor por omisión es 300. `Staletimeout` también puede establecerse en el nivel del ejecutor o del clúster. Consulte el apartado “Utilización del valor de tiempo de espera sin actividad” en la página 268 para obtener más información.

valor

El valor de **`staletimeout`** en número de segundos.

weightbound

Establece el peso máximo de servidores para este puerto. Esto afecta a la diferencia permitida entre el número de peticiones que el ejecutor puede otorgar a cada servidor. El valor por omisión es 20.

peso

Número de 1 a 100 que representa la máquina ponderación.

porttype

El tipo de puerto.

Nota: `porttype` sólo se aplica a Dispatcher.

tipo

Los valores posibles son **tcp**, **udp** y **both**. El valor por omisión es (tcp/udp).

protocolo

El tipo de protocolo. Para el componente Dispatcher, es un parámetro necesario cuando se especifica un método "cbr" en el puerto. Si selecciona un protocolo de puerto, escriba **SSL**, también debe especificar un tiempo permanencia en memoria no cero para habilitar la afinidad de ID SSL. Si selecciona el protocolo **HTTP**, puede establecer la afinidad de servidor mediante las normas "content". Consulte el apartado "Direccionamiento basado en contenido de Dispatcher (método de reenvío cbr)" en la página 55 para obtener más información.

Nota: protocol sólo se aplica al método de reenvío CBR de Dispatcher.

tipo

Los valores posibles son **HTTP** o **SSL**.

maxhalfopen

Umbral para el número máximo de conexiones medio abiertas. Utilice este parámetro para detectar posibles ataques para rechazo de servicio (DoS) que resultan en un gran número de conexiones TCP medio abiertas en servidores.

Un valor positivo indica que se realiza una comprobación para determinar si las conexiones medio abiertas actuales exceden el umbral. Si el valor actual excede el umbral, se realiza una llamada a un script de alerta. Consulte el apartado "Detección de ataques para rechazo de servicio (DoS)" en la página 239 para obtener más información.

Nota: maxhalfopen sólo se aplica a Dispatcher.

valor

El valor de maxhalfopen. El valor por omisión es cero (no se realizará ninguna comprobación).

reset

Reset permite especificar si Load Balancer enviará restauraciones TCP a servidores inactivos en el puerto. Una restauración TCP hace que la conexión se cierre inmediatamente. Consulte el apartado "Envío de una restauración TCP a un servidor inactivo (sólo componente Dispatcher)" en la página 182 para obtener más información.

Nota: reset sólo se aplica al componente Dispatcher. Para poder utilizar la palabra clave reset se debe establecer la opción `clientgateway` del mandato `dscontrol` `executor` en una dirección de direccionador.

valor

Los valores posibles para una restauración son yes y no. El valor por omisión es no (no se llevan a cabo restauraciones TCP en servidores inactivos). Cuando reset tiene el valor yes, las restauraciones TCP se envían a servidores inactivos.

set

Establece los campos de un puerto.

remove

Suprime este puerto.

report

Informa sobre este puerto.

status

Muestra el estado de servidores en este puerto. Si desea ver el estado en todos los puertos, no especifique un *puerto* con este mandato. Recuerde indicar los dos puntos.

númSegundos

La cantidad de tiempo en segundos que debe transcurrir antes de restaurar conexiones medio abiertas.

halfopenaddressreport

Genera entradas en las anotaciones cronológicas (halfOpen.log) para todas las direcciones de cliente (hasta aproximadamente 8000 pares de direcciones) que han accedido a servidores que tienen conexiones medio abiertas. Además, los datos estadísticos se envían a la línea de mandatos, como por ejemplo: el número total, el número más grande y el promedio de conexiones medio abiertas, así como el tiempo medio en las conexiones medio abiertas (en segundos). Consulte el apartado “Detección de ataques para rechazo de servicio (DoS)” en la página 239 para obtener más información.

Ejemplos

- Añadir el puerto 80 y 23 a la dirección de clúster 130.40.52.153:
`dscontrol port add 130.40.52.153:80+23`
- Añadir un puerto comodín a la dirección de clúster 130.40.52.153:
`dscontrol port set 130.40.52.153:0`
- Establecer el peso máximo 10 en el puerto 80 en la dirección de clúster 130.40.52.153:
`dscontrol port set 130.40.52.153:80 weightbound 10`
- Establecer el valor de tiempo de permanencia en memoria en 60 segundos para el puerto 80 y el puerto 23 en la dirección de clúster 130.40.52.153:
`dscontrol port set 130.40.52.153:80+23 stickytime 60`
- Establecer la afinidad entre puertos del puerto 80 y el puerto 23 en la dirección del clúster 130.40.52.153:
`dscontrol port set 130.40.52.153:80 crossport 23`
- Eliminar el puerto 23 de la dirección de clúster 130.40.52.153:
`dscontrol port remove 130.40.52.153:23`
- Obtener el estado del puerto 80 en la dirección de clúster 9.67.131.153:
`dscontrol port status 9.67.131.153:80`

Este mandato genera una salida parecida a la siguiente:

Estado del puerto:

```
Número de puerto ..... 80
Clúster ..... 9.67.131.153
Tiempo de espera sin actividad . 300
Ponderación ..... 20
Número máximo de servidores .... 32
Tiempo de permanencia en memoria 0
Tipo de puerto ..... tcp/udp
Afinidad entre puertos ..... 80
Bits máscara permanen. memoria . 32
Máx conexiones medio abiertas .. 0
Enviar restauraciones TCP ..... no
```

- Obtener el informe del puerto 80 en la dirección de clúster 9.62.130.157:
`dscontrol port report 9.62.130.157:80`

Este mandato genera una salida parecida a la siguiente:

Informe del puerto:

Dirección de clúster 9.62.130.157
Número de puerto 80
Número de servidores 5
Peso máximo del servidor 10
Total de conexiones activas 55
Conexiones por segundo 12
KBytes por segundo 298
Número de medio abiertas 0
Restaur. TCP enviadas 0
Método de reenvío Reenvío basado en dirección MAC

- Obtener el informe de direcciones medio abiertas para el puerto 80 en la dirección de clúster 9.67.127.121:

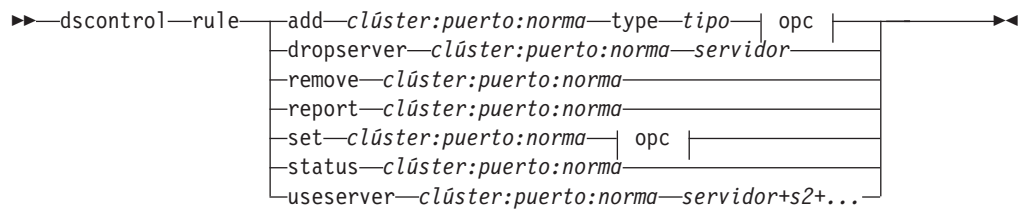
dscontrol port halfopenaddressreport 9.67.127.121:80

Este mandato genera una salida parecida a la siguiente:

El informe de conexiones parciales se ha creado con éxito

Informe direcciones medio abiertas para clúster:puerto = 9.67.127.121:80
Total registrado de direcciones con conexiones medio abiertas ... 0
Número total registrado de conexiones medio abiertas 0
Número mayor registrado de conexiones medio abiertas 0
Número medio registrado de conexiones medio abiertas 0
Tiempo medio registrado (segs) de conexiones medio abiertas 0
Total registrado de conexiones medio abiertas 0

dscontrol rule — configurar normas



opc:

beginrange	bajo	endrange	alto
priority	nivel		
pattern	patrón		
tos	valor		
stickytime	tiempo		
affinity	tipo_afinidad		
cookie name	valor		
evaluate	nivel		
sharelevel	nivel		

add

Añade esta norma a un puerto.

clúster

La dirección del clúster, en forma de nombre simbólico o en un formato de dirección IP. Puede utilizar dos puntos (:) como carácter comodín. Por instancia, el siguiente mandato, `dscontrol rule add :80:NormaA type tipo`, añadirá NormaA al puerto 80 para todos los clústeres.

Nota: Los clústeres adicionales se separan mediante un signo más (+).

puerto

El número del puerto. Puede utilizar dos puntos (:) como carácter comodín. Por instancia, el siguiente mandato, `dscontrol rule add clusterA::NormaA type tipo`, añadirá NormaA a todos los puertos para ClusterA.

Nota: Los puertos adicionales se separan mediante un signo más (+).

norma

Nombre que se selecciona para la norma. Este nombre puede contener cualquier carácter alfanumérico, subrayado, guión o punto. Puede tener de 1 a 20 caracteres y no puede contener blancos.

Nota: Las normas adicionales se separan mediante un signo más (+).

type

Tipo de norma.

tipo

Las opciones de *tipo* son:

ip La norma se basa en la dirección IP de cliente.

time La norma se basa en la hora del día.

connection

La norma se basa en el número de conexiones por segundo para el puerto. Esta norma sólo se aplicará si el gestor está en ejecución.

active La norma se basa en el número total de conexiones activas para el puerto. Esta norma sólo se aplicará si el gestor está en ejecución.

port La norma se basa en el puerto de cliente.

Nota: port se aplica al componente Dispatcher.

service

Esta norma se basa en el campo de byte de tipo de servicio (TOS) en la cabecera IP.

Nota: service sólo se aplica al componente Dispatcher.

reservedbandwidth

Esta norma se basa en el ancho de banda (kilobytes por segundo) que proporciona un conjunto de servidores. Para obtener más información, consulte los apartados “Utilización de normas basadas en ancho de banda reservado y ancho de banda compartido” en la página 216 y “Norma de ancho de banda reservado” en la página 216.

Nota: reservedbandwidth sólo se aplica al componente Dispatcher.

sharedbandwidth

Esta norma se basa en la cantidad de ancho de banda (kilobytes por segundo) que se comparte en el nivel del ejecutor o del clúster. Para obtener más información, consulte los apartados “Utilización de normas basadas en ancho de banda reservado y ancho de banda compartido” en la página 216 y “Norma de ancho de banda compartido” en la página 216.

Nota: sharedbandwidth sólo se aplica al componente Dispatcher.

true Esta norma es siempre cierta. Piense en ella como si fuera una sentencia else en lógica de programación.

content

Esta norma describe una expresión regular que se comparará con los URL solicitados por el cliente. Es válida para Dispatcher y CBR.

beginrange

El valor más pequeño del rango utilizado para determinar si una norma es cierta.

bajo

Depende del tipo de norma. El tipo de valor y su valor por omisión se listan según el tipo de norma:

ip La dirección del cliente, en forma de nombre simbólico o en un formato de dirección IP. El valor por omisión es 0.0.0.0.

hora Número entero. El valor por omisión es 0, que representa medianoche.

conexión

Número entero. El valor por omisión es 0.

activa Número entero. El valor por omisión es 0.

puerto Número entero. El valor por omisión es 0.

ancho de banda reservado

Número entero (kilobytes por segundo). El valor por omisión es 0.

endrange

El valor más alto del rango utilizado para determinar si la norma es cierta.

alto

Depende del tipo de norma. El tipo de valor y su valor por omisión se listan según el tipo de norma:

- ip* La dirección del cliente, en forma de nombre simbólico o en un formato de dirección IP. El valor por omisión es 255.255.255.254.
- hora* Número entero. El valor por omisión es 24, que representa medianoche.

Nota: Al definir beginrange y endrange de los intervalos de tiempo, tenga en cuenta que cada valor debe ser un entero que represente sólo la porción de la hora del tiempo; no se especifican las fracciones de una hora. Por esta razón, para especificar una sola hora, por ejemplo la hora entre las 3:00 y las 4:00, debería especificar 3 en beginrange y también 3 en endrange. Esto indicará todos los minutos, empezando en 3:00 y terminando en 3:59. Si especifica 3 en beginrange y 4 en endrange, abarcará un periodo de dos horas, de las 3:00 hasta las 4:59.

conexiones

Número entero. El valor por omisión es 2 elevado a la 32 menos 1.

activa Número entero. El valor por omisión es 2 elevado a la 32 menos 1.

puerto Número entero. El valor por omisión es 65535.

ancho de banda reservado

Número entero (kilobytes por segundo). El valor por omisión es 2 elevado a la 32 menos 1.

priority

El orden en el que se revisan las normas.

nivel

Número entero. Si no especifica la prioridad de la primera norma que añade, por omisión Dispatcher la establecerá en 1. Cuando posteriormente se añade otra norma, por omisión su prioridad se calcula sumando 10 a la prioridad más baja actual de cualquier norma existente. Por ejemplo, suponga que tiene una norma existente con una prioridad 30. Añada una nueva norma con la prioridad 25 (recuerde que esta prioridad es *más alta* que 30). A continuación, añada una tercera norma sin establecer la prioridad. La prioridad de la tercera norma se calculará como 40 (30 + 10).

pattern

Especifica el patrón que se debe utilizar para una norma de tipo contenido.

patrón

El patrón que se utilizará. Para obtener más información sobre los valores válidos, consulte el Apéndice B, "Sintaxis de la norma de contenido (patrón)", en la página 475.

tos

Especifica el valor de "tipo de servicio" (TOS) utilizado para la norma de tipo **servicio** type rule.

Nota: TOS sólo se aplica al componente Dispatcher.

valor

Serie de ocho caracteres que va a utilizarse para el valor TOS, donde los caracteres válidos son: 0 (cero binario), 1 (uno binario) y x (no importa). Por ejemplo: 0xx1010x. Para obtener más información, consulte el apartado “Utilización de normas basadas en el tipo de servicio (TOS)” en la página 214.

stickytime

Especifica el tiempo de permanencia en memoria que debe utilizarse para una norma. Si se establece el parámetro affinity en “activecookie” en el mandato rule, stickytime debe establecerse en un valor distinto de cero para habilitar este tipo de afinidad. La opción stickytime de la norma no se aplica a los tipos de normas de afinidad “passivecookie” ni “uri”.

Consulte el apartado “Afinidad de cookies activos” en la página 225 para obtener más información.

Nota: rule stickytime sólo se aplica al componente CBR.

tiempo

Intervalo en segundos.

affinity

Especifica el tipo de afinidad que debe utilizarse para una norma: cookie activo, cookie pasivo, URI o ninguno.

El tipo de afinidad “activecookie” habilita el equilibrio de carga del tráfico Web con afinidad para el mismo servidor basándose en los cookies generados por Load Balancer.

El tipo de afinidad “passivecookie” habilita el equilibrio de carga del tráfico Web con afinidad para el mismo servidor basándose en los cookies que se identifican a sí mismos generados por los servidores. Debe utilizar el parámetro cookiename junto con la afinidad de cookie pasivo.

El tipo de afinidad “URI” habilita el equilibrio de carga en el tráfico Web para los servidores Caching Proxy de forma que aumente de manera eficaz el tamaño de la antememoria.

Consulte los apartados “Afinidad de cookies activos” en la página 225, “Afinidad de cookies pasivos” en la página 227 y “Afinidad de URI” en la página 228 para obtener más información.

Nota: affinity se aplica a normas configuradas con el método de reenvío CBR del componente Dispatcher.

tipo_afinidad

Los valores posibles para el tipo de afinidad son: none (valor por omisión), activecookie, passivecookie o uri.

cookiename

Nombre arbitrario establecido por el administrador que actúa como identificador para Load Balancer. Es el nombre que Load Balancer debe buscar en la petición de cabecera HTTP del cliente. El nombre de cookie, junto con el valor de cookie, actúa como identificador para Load Balancer y permite que Load Balancer envíe peticiones subsiguientes a un sitio Web a la misma máquina servidor. El nombre de cookie sólo se puede aplicar con la afinidad “cookie pasivo”.

Consulte el apartado “Afinidad de cookies pasivos” en la página 227 para obtener más información.

Nota: cookiename se aplica a las normas configuradas con el método de reenvío CBR del componente Dispatcher y al componente CBR.

valor

El valor del nombre de cookie.

evaluate

Esta opción sólo está disponible en el componente Dispatcher. Especifica si se debe evaluar la condición de la norma en todos los servidores incluidos en el puerto o en todos los servidores incluidos en la norma. Esta opción sólo es válida para las normas que toman sus decisiones en función de las características de los servidores, como por ejemplo: las normas connection, active y reservedbandwidth. Para obtener más información, consulte el apartado “Opción de evaluación del servidor para normas” en la página 220.

En la norma de tipo conexión, también puede especificar una opción de evaluación: upserversonrule. Si especifica upserversonrule, puede asegurarse de que no se cargará en exceso los servidores restantes incluidos en la norma, si algunos de los servidores incluidos en el conjunto están inactivos.

nivel

Los valores posibles son port, rule o upserversonrule. El valor por omisión es port. upserversonrule sólo está disponible para la norma de tipo conexión.

sharelevel

Este parámetro sólo se aplica a la norma de ancho de banda compartido. Especifica si debe compartirse el ancho de banda en el nivel del clúster o en el nivel de ejecutor. Si se comparte el ancho de banda en el nivel de clúster se permite que un puerto (o varios puertos) compartan una cantidad máxima de ancho de banda por varios puertos dentro del mismo clúster. Si se comparte el ancho de banda a nivel del ejecutor se permite que un clúster (o varios clústeres) incluidos en la configuración completa de Dispatcher compartan una cantidad máxima de ancho de banda. Para más información, consulte el apartado “Norma de ancho de banda compartido” en la página 216.

nivel

Los valores posibles son executor o cluster.

dropserver

Elimina un servidor del conjunto de normas.

servidor

Dirección IP de la máquina servidor TCP como nombre simbólico o en formato de dirección IP.

O, si ha utilizado la partición del servidor, utilice el nombre exclusivo del servidor lógico. Consulte el apartado “Creación de particiones del servidor: servidores lógicos configurados con un servidor físico (dirección IP)” en la página 58 para obtener más información.

Nota: Los servidores adicionales se separan mediante un signo más (+).

remove

Elimina una o más normas, separadas entre sí por signos más.

report

Muestra los valores internos de una o más normas.

set

Establece los valores para esta norma.

status

Muestra los valores de una o más normas que pueden establecerse.

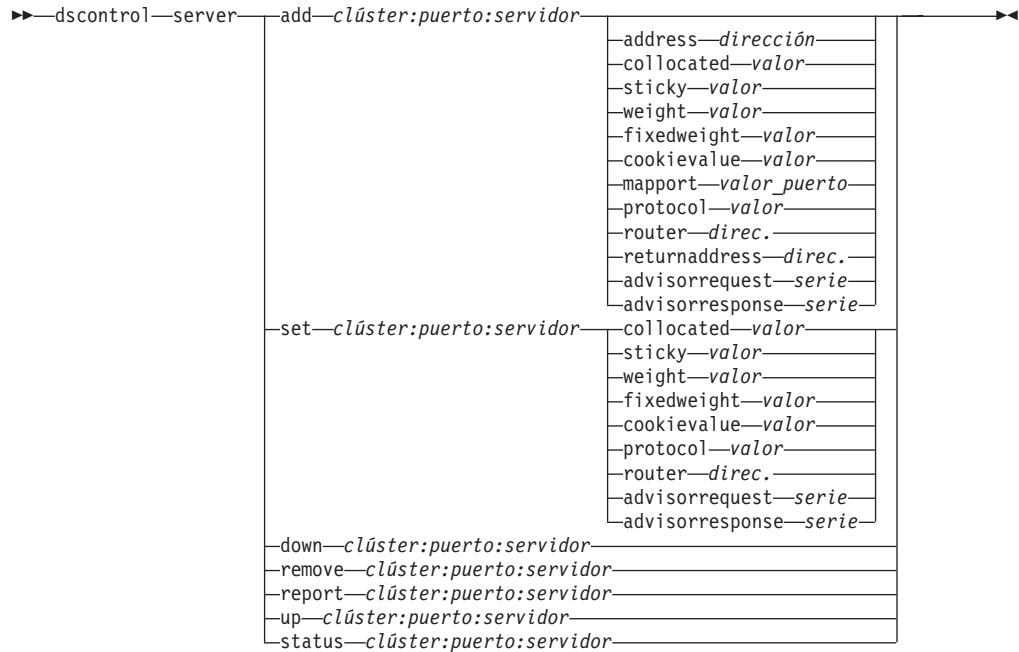
useserver

Inserta servidores en un conjunto de normas.

Ejemplos

- Para añadir una norma que será siempre cierta, no especifique el inicio del rango ni el fin del rango:
`dscontrol rule add 9.37.67.100:80:trule type true priority 100`
- Crear una norma que prohíba el acceso a un rango de direcciones IP, en este caso las que empiecen por "9:"
`dscontrol rule add 9.37.131.153:80:ni type ip b 9.0.0.0 e 9.255.255.255`
- Crear una norma que especificará el uso de un servidor específico desde las 11:00 hasta las 15:00.
`dscontrol rule add cluster1:80:timerule type time beginrange 11 endrange 14`
`dscontrol rule useserver cluster1:80:timerule server05`
- Crear una norma basada en el contenido del campo de byte TOS en la cabecera de IP:
`dscontrol rule add 9.67.131.153:80:tosrule type service tos 0xx1001x`
- Crear una norma basada en el ancho de banda reservado que asignará un conjunto de servidores (evaluados dentro de la norma) para que entreguen datos hasta una velocidad de 100 kilobytes por segundo:
`dscontrol rule add 9.67.131.153:80:rbwrule type reservedbandwidth`
`beginrange 0 endrange 100 evaluate rule`
- Crear una norma basada en el ancho de banda compartido que incorporará ancho de banda no utilizado en el nivel de clúster. (Nota: primero debe especificar, mediante el mandato `dscontrol cluster`, la cantidad máxima de ancho de banda (kilobytes por segundo) que puede compartirse en el nivel de clúster):
`dscontrol cluster set 9.67.131.153 sharedbandwidth 200`
`dscontrol rule add 9.67.131.153:80:shbwrule type sharedbandwidth`
`sharelevel cluster`

dscontrol server — configurar servidores



add

Añade este servidor.

clúster

La dirección del clúster, en forma de nombre simbólico o en un formato de dirección IP. Puede utilizar dos puntos (:) como carácter comodín. Por ejemplo, al emitir el siguiente mandato, `dscontrol server add :80:ServidorA`, se añadirá ServidorA al puerto 80 en todos los clústeres.

Nota: Los clústeres adicionales se separan mediante un signo más (+).

puerto

El número del puerto. Puede utilizar dos puntos (:) como carácter comodín. Por ejemplo, el siguiente mandato, `dscontrol server add ::ServidorA`, añadirá ServidorA a todos los servidores de todos los puertos.

Nota: Los puertos adicionales se separan mediante un signo más (+).

servidor

El **servidor** es la dirección IP exclusiva de la máquina servidor TCP como nombre simbólico o en formato de dirección IP.

O, si utiliza un nombre exclusivo que no se resuelva en una dirección IP, debe proporcionar el parámetro **address** del servidor en el mandato **dscontrol server add**. Consulte el apartado “Creación de particiones del servidor: servidores lógicos configurados con un servidor físico (dirección IP)” en la página 58 para obtener más información.

Nota: Los servidores adicionales se separan mediante un signo más (+).

address

La dirección IP exclusiva de la máquina servidor TCP en formato de nombre de sistema principal o en formato de dirección IP. Si el servidor no puede resolverse, debe proporcionar la dirección de la máquina servidor física.

Consulte el apartado “Creación de particiones del servidor: servidores lógicos configurados con un servidor físico (dirección IP)” en la página 58 para obtener más información.

dirección

Valor de la dirección del servidor.

collocated

La ubicación compartida permite especificar si Dispatcher está instalado en una de las máquinas de servidor sobre las que realiza el equilibrio de carga.

Nota: El parámetro `collocated` es válido cuando se utilizan los métodos de reenvío MAC, NAT o CBR de Dispatcher. Site Selector y CBR pueden compartir ubicación en todas las plataformas, pero no requieren esta palabra clave. Para obtener más información, consulte el apartado “Utilización de servidores con ubicación compartida” en la página 203.

valor

Valor de `collocated`: yes o no. El valor por omisión es no.

sticky

Permite a un servidor alterar el valor de permanencia en memoria en este puerto. Con el valor por omisión “yes”, el servidor retiene la afinidad normal, como se ha definido en el puerto. Con el valor “no,” el cliente *no* volverá a dicho servidor la próxima vez que emita una petición en dicho puerto, independientemente del valor de tiempo de permanencia en memoria de dicho puerto. Es útil en determinadas situaciones cuando se utilizan normas. Para obtener más información, consulte el apartado “Alteración temporal de la afinidad entre puertos” en la página 219.

valor

Valor de `sticky`: yes o no. El valor por omisión es yes.

weight

Número comprendido entre 1 y 100 (aunque sin exceder el valor de ponderación del puerto especificado) que representa el peso de este servidor. Si se establece el peso en cero, se impedirá que se envíen nuevas peticiones al servidor, aunque no se terminarán ninguna de las conexiones actualmente activas con dicho servidor. El valor por omisión es la mitad del máximo valor de ponderación del puerto especificado. Si el gestor se está ejecutando, este valor se sobrescribirá.

valor

Valor del peso del servidor.

fixedweight

La opción `fixedweight` permite especificar si desea que el gestor modifique el peso del servidor. Si establece el valor de `fixedweight` en yes, cuando el gestor lo ejecuta no podrá modificar el peso del servidor. Para obtener más información, consulte el apartado “Pesos fijos del gestor” en la página 182.

valor

Valor de `fixedweight`: yes o no. El valor por omisión es no.

cookievalue

`Cookievalue` es un valor arbitrario que representa el servidor en el par de nombre de cookie y valor de cookie. El nombre de cookie, junto con el nombre de cookie, actúa como identificador que permite a Load Balancer enviar peticiones de cliente subsiguientes al mismo servidor. Consulte el apartado “Afinidad de cookies pasivos” en la página 227 para obtener más información.

Nota: cookievalue es válido para Dispatcher (utilizando el método de reenvío CBR) y CBR.

valor

Valor es cualquier valor arbitrario. El valor por omisión es sin valor de cookie.

mapport

Correlaciona el número de puerto de destino de la petición del cliente (que es para Dispatcher) con el número de puerto del servidor que Dispatcher utiliza para equilibrar la carga de la petición del cliente. Permite a Load Balancer recibir una petición del cliente en un puerto y transmitirla a un puerto distinto de la máquina servidor. Con mapport puede realizar el equilibrio de carga de peticiones de un cliente para un servidor que puede tener en ejecución varios daemons de servidor.

Nota: mapport se aplica a Dispatcher (utilizando los métodos de reenvío NAT o CBR) y a CBR. Para Dispatcher, consulte los apartados “NAT/NAPT de Dispatcher (método de reenvío nat)” en la página 53 y “Direccionamiento basado en contenido de Dispatcher (método de reenvío cbr)” en la página 55. Para CBR, consulte el apartado “Equilibrio de carga de cliente a proxy en SSL y de proxy a servidor en HTTP” en la página 108.

protocolo

Los valores válidos para el protocolo son HTTP y HTTPS. El valor por omisión es HTTP.

Nota: El protocolo sólo se aplica al componente CBR.

valor_puerto

Valor del número de puerto de correlación. El valor por omisión es el número de destino de la petición del cliente.

router

Si está configurando una red de área amplia, la dirección del direccionador para el servidor remoto. El valor por omisión es 0, lo que indica un servidor local. Tenga en cuenta que una vez que la dirección de direccionador de un servidor se establece en un valor distinto de cero (lo que indica un servidor remoto), no puede restablecerse en 0 para que el servidor vuelva a ser local. En su lugar, el servidor debe eliminarse y, a continuación, añadirse de nuevo sin especificar una dirección de router. De forma parecida, un servidor definido como local (dirección de router = 0) no puede convertirse en remoto cambiando la dirección del direccionador. El servidor debe eliminarse y añadirse de nuevo. Consulte el apartado “Configurar soporte de Dispatcher de área amplia” en la página 229 para obtener más información.

Nota: router sólo se aplica a Dispatcher. Si utiliza los métodos de reenvío CBR o NAT, al añadir un servidor a la configuración deberá especificar la dirección del direccionador.

direc

Valor de la dirección del direccionador.

returnaddress

Una dirección IP o nombre de sistema principal exclusivo. Es una dirección configurada en la máquina Dispatcher que Dispatcher utiliza como dirección de origen cuando equilibra la carga de la petición del cliente para el servidor. Esto garantiza que el servidor devuelve el paquete a la máquina Dispatcher para procesar el contenido de la petición en lugar de enviar el paquete

directamente al cliente. (A continuación, Dispatcher reenviará el paquete IP al cliente). Cuando se añade el servidor, se debe especificar el valor de dirección de retorno. La dirección de retorno no se puede modificar a menos que se elimine el servidor y se añada de nuevo. La dirección de retorno no puede ser la misma que la dirección de clúster, servidor o NFA.

Nota: `returnaddress` sólo se aplica a Dispatcher. Si utiliza los métodos de reenvío CBR o NAT, al añadir un servidor a la configuración deberá especificar `returnaddress`.

direc

Valor de la dirección de retorno.

advisorrequest

El asesor HTTP o HTTPS utiliza la serie de petición de asesor para examinar el estado de los servidores. Sólo es válido para los servidores que reciben asesoramiento del asesor HTTP o HTTPS. Para habilitar este valor debe iniciar el asesor HTTP o HTTPS. Consulte el apartado “Configuración del asesor HTTP o HTTPS utilizando la opción de petición y respuesta (URL)” en la página 190 para obtener más información.

Nota: `advisorrequest` se aplica a los componentes Dispatcher y CBR.

serie

Valor de la serie utilizada por el asesor HTTP o HTTPS. El valor por omisión es `HEAD / HTTP/1.0`.

Nota: Si la serie incluye un espacio en blanco:

- Al emitir el mandato desde el indicador del shell **dscontrol**>>, debe especificar la serie entre comillas. Por ejemplo: **server set clúster:puerto:servidor advisorrequest "head / http/1.0"**
- Al emitir el mandato **dscontrol** desde el indicador del sistema operativo, debe preceder el texto con `"\"` y terminarlo con `\"`. Por ejemplo: **dscontrol server set clúster:puerto:servidor advisorrequest "\"head / http/1.0\""**

advisorresponse

Serie de respuesta del asesor en la que el asesor HTTP o HTTPS busca la respuesta HTTP. Sólo será válido para los servidores que reciben asesoramiento del asesor HTTP o HTTPS. Para habilitar este valor debe iniciar el asesor HTTP o HTTPS. Consulte el apartado “Configuración del asesor HTTP o HTTPS utilizando la opción de petición y respuesta (URL)” en la página 190 para obtener más información.

Nota: `advisorresponse` se aplica a los componentes Dispatcher y CBR.

serie

Valor de la serie utilizada por el asesor HTTP o HTTPS. El valor por omisión es nulo.

Nota: Si la serie incluye un espacio en blanco:

- Al emitir el mandato desde el indicador del shell **dscontrol**>>, debe especificar la serie entre comillas.
- Al emitir el mandato **dscontrol** desde el indicador del sistema operativo, debe preceder el texto con `"\"` y terminarlo con `\"`.

down

Marca este servidor como inactivo. Este mandato interrumpe todas las

conexiones activas con dicho servidor e impide que se establezcan otras conexiones con dicho servidor ni que se envíen paquetes al mismo.

Cuando se utiliza un mandato server down para poner un servidor fuera de línea, si el valor de tiempo de permanencia en memoria (stickytime) no es cero para dicho servidor, ese servidor seguirá atendiendo los clientes existentes hasta que caduque el tiempo de permanencia en memoria. El servidor pasará a estar inactivo una vez que caduque el valor de tiempo de permanencia en memoria (stickytime).

remove

Elimina este servidor.

report

Informa sobre este servidor. El informe contiene la siguiente información de cada servidor: número actual de conexiones por segundo (CPS), kilobytes transferidos en un segundo intervalo (KBPS), el número total de conexiones(Total), número de conexiones que están en estado activo (Active), número de conexiones que están en el estado FIN (FIN) y el número de conexiones completadas (Comp).

set

Establece los valores para este servidor.

status

Muestra el estado de los servidores.

up Marca este servidor como activo. Dispatcher enviará nuevas conexiones a dicho servidor.

Ejemplos

- Añadir el servidor con la dirección 27.65.89.42 al puerto 80 con una dirección de clúster 130.40.52.153:
`dscontrol server add 130.40.52.153:80:27.65.89.42`
- Establecer el servidor 27.65.89.42 como no de permanencia en memoria (característica de alteración temporal de afinidad entre puertos):
`dscontrol server set 130.40.52.153:80:27.65.89.42 sticky no`
- Marcar el servidor en 27.65.89.42 como inactivo:
`dscontrol server down 130.40.52.153:80:27.65.89.42`
- Eliminar el servidor en 27.65.89.42 en todos los puertos de todos los clústeres:
`dscontrol server remove ::27.65.89.42`
- Establecer el servidor en 27.65.89.42 como de ubicación compartida (el servidor reside en la misma máquina que el Load Balancer):
`dscontrol server set 130.40.52.153:80:27.65.89.42 collocated yes`
- Establecer el peso en 10 para el servidor 27.65.89.42 en el puerto 80 en la dirección de clúster 130.40.52.153:
`dscontrol server set 130.40.52.153:80:27.65.89.42 weight 10`
- Marcar el servidor en 27.65.89.42 como activo:
`dscontrol server up 130.40.52.153:80:27.65.89.42`
- Añadir un servidor remoto:
`dscontrol server add 130.40.52.153:80:130.60.70.1 router 130.140.150.0`
- Permitir que el asesor HTTP examine una petición de URL de HTTP HEAD / HTTP/1.0 para el servidor 27.65.89.42 en el puerto 80 HTTP:
`dscontrol server set 130.40.52.153:80:27.65.89.42
advisorrequest "\"HEAD / HTTP/1.0\""`

- Mostrar el estado para el servidor 9.67.143.154 en el puerto 80:
dscontrol server status 9.67.131.167:80:9.67.143.154

Este mandato genera una salida parecida a la siguiente:

Estado de servidor:

```
-----
Servidor ..... 9.67.143.154
Número de puerto ..... 80
Clúster ..... 9.67.131.167
Dirección del clúster ..... 9.67.131.167
Inmovilizado ..... N
Servidor activo ..... Y
Peso ..... 10
Peso fijo ..... N
Permanencia memoria de norma ... Y
Servidor remoto ..... N
Dirección direccionador de red . 0.0.0.0
Ubicación compartida ..... N
Petición del asesor ..... HEAD / HTTP/1.0
Respuesta del asesor .....
Valor del cookie ..... n/d
ID de clon ..... n/d
```

dscontrol set — configurar anotaciones cronológicas de servidor



loglevel

El nivel en el que el dsserver anota sus actividades.

nivel

El valor por omisión de **loglevel** es 0. El rango es de 0 a 5. A continuación se muestran los valores posibles: 0 equivale a Ninguno, 1 a Mínimo, 2 a Básico, 3 a Moderado, 4 a Avanzado, 5 a Detallado.

logsize

El número máximo de bytes que se deben anotar en el archivo de anotaciones cronológicas.

tamaño

El valor por omisión de `logsize` es 1 MB.

dscontrol status — mostrar si el gestor y los asesores se están ejecutando

►►—dscontrol—status—◀◀

Ejemplos

- Para ver lo que está en ejecución:

```
dscontrol status
```

Este mandato genera una salida parecida a la siguiente:

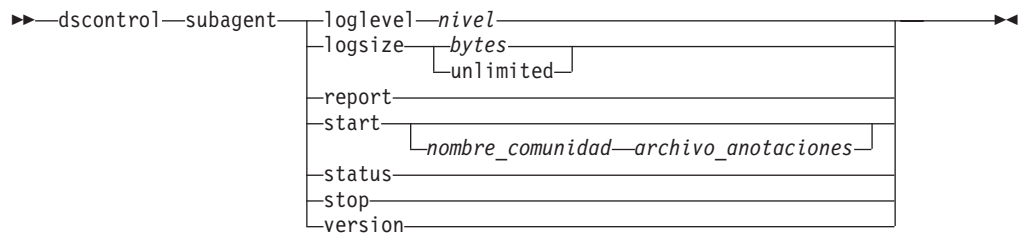
Se ha iniciado el ejecutor.

Se ha iniciado el gestor.

ASESOR	CLÚSTER:PUERTO	TPO ESPERA
reach	0	unlimited
http	80	unlimited
ftp	21	unlimited

dscontrol subagent — configurar subagente SNMP

Nota: Los diagramas de sintaxis del mandato dscontrol subagent hacen referencia al componente Dispatcher.



loglevel

Nivel en el que el subagente anota sus actividades en un archivo.

nivel

El número del nivel (0 a 5). Cuanto más alto sea el número, más información se anotará en las anotaciones cronológicas del gestor. El valor por omisión es 1. A continuación se muestran los valores posibles: 0 equivale a Ninguno, 1 a Mínimo, 2 a Básico, 3 a Moderado, 4 a Avanzado, 5 a Detallado.

logsize

Establece el tamaño máximo de bytes que se deben anotar en las anotaciones cronológicas del subagente. El valor por omisión es 1 MB. Cuando se establece un tamaño máximo para el archivo de anotaciones cronológicas, el texto del archivo vuelve al principio; es decir, cuando el archivo alcanza el tamaño especificado, las entradas subsiguientes se anotarán al principio del archivo y se grabarán encima de las entradas de anotaciones cronológicas anteriores. El tamaño de las anotaciones cronológicas no puede establecerse más pequeño que el tamaño actual de las anotaciones cronológicas. Las entradas de las anotaciones cronológicas incluyen la indicación de la hora para poder saber el orden en el que se anotaron. Cuando más alto se establezca el nivel de anotaciones cronológicas, más cuidado deberá tener al elegir el tamaño de las anotaciones cronológicas porque, cuando el registro cronológico está establecido en los niveles más altos, puede quedarse sin espacio rápidamente.

bytes

El tamaño máximo en bytes para el archivo de anotaciones cronológicas de subagente. Puede especificar un número positivo mayor que cero o la palabra **unlimited**. Es posible que el archivo de anotaciones cronológicas no alcance el tamaño máximo exacto antes de empezar a sobrescribir porque el tamaño de las entradas del archivo varían. El valor por omisión es unlimited.

report

Muestra un informe de instantánea de estadísticas.

start

Inicia el subagente.

nombre_comunidad

Nombre del valor SNMP del nombre de comunidad que puede utilizar como contraseña de seguridad. El valor por omisión es public.

En la plataforma **Windows**: se utiliza el nombre de comunidad del sistema operativo.

archivo_annotaciones

Nombre de archivo en el que se anotan los datos del subagente SNMP. Cada registro del archivo de anotaciones cronológicas tiene la indicación de la hora. El valor por omisión es `subagent.log`. El archivo por omisión se instala en el directorio **logs**. Consulte el Apéndice C, “Archivos de configuración de ejemplo”, en la página 479. Para cambiar el directorio en el que se guardan los archivos de anotaciones cronológicas, consulte el apartado “Cambio de las vías de acceso del archivo de anotaciones cronológicas” en la página 267.

status

Muestra el estado actual de todos los valores de un subagente SNMP que se pueden establecer globalmente y sus valores por omisión.

version

Muestra la versión actual del subagente.

Ejemplos

- Iniciar el subagente con el nombre de comunidad `bigguy`:
`dscontrol subagent start bigguy bigguy.log`

Capítulo 28. Referencia de mandatos para Site Selector

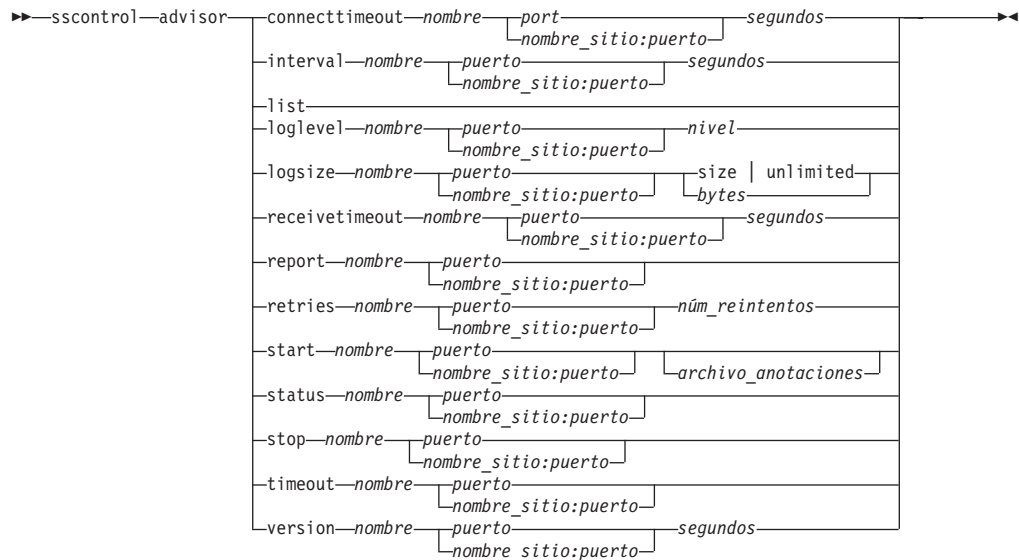
En este capítulo se describe cómo utilizar los siguientes mandatos **sscontrol** de Site Selector:

- “**sscontrol advisor** — controlar el asesor” en la página 404
- “**sscontrol file** — gestionar archivos de configuración” en la página 409
- “**sscontrol help** — mostrar o imprimir ayuda para este mandato” en la página 411
- “**sscontrol logstatus** — mostrar valores de anotaciones cronológicas de servidor” en la página 412
- “**sscontrol manager** — controlar el gestor” en la página 413
- “**sscontrol metric** — configurar métrica del sistema” en la página 418
- “**sscontrol nameserver** — controlar el servidor de nombres” en la página 419
- “**sscontrol rule** — configurar normas” en la página 420
- “**sscontrol server** — configurar servidores” en la página 423
- “**sscontrol set** — configurar anotaciones cronológicas de servidor” en la página 425
- “**sscontrol sitename** — configurar un nombre de sitio” en la página 426
- “**sscontrol status** — mostrar si el gestor y los asesores se están ejecutando” en la página 429

Puede escribir una versión minimizada de los parámetros del mandato **sscontrol**. Sólo es necesario especificar las letras exclusivas de los parámetros. Por ejemplo, para obtener ayuda sobre el mandato para guardar archivos, puede escribir **sscontrol he f** en lugar de **sscontrol help file**.

Nota: Los valores de los parámetros de mandatos deben especificarse en caracteres del idioma inglés. Las únicas excepciones son los nombres de sistema principal (que se utilizan en los mandatos del clúster y servidor) y los nombres de archivo (que se utilizan en los mandatos de archivo).

sscontrol advisor — controlar el asesor



connecttimeout

Establece cuánto tiempo espera un asesor antes de notificar que se ha producido un error en una conexión a un servidor. Para obtener más información, consulte el apartado “Tiempo de espera de conexión y recepción del asesor para los servidores” en la página 188.

nombre

Nombre del asesor. Los valores posibles incluyen **http**, **https**, **ftp**, **sip**, **ssl**, **smtp**, **imap**, **pop3**, **ldap**, **nntp**, **telnet**, **connect**, **ping**, **WLM** y **WTE**. Los nombres de asesores personalizados están en formato **xxxx**, donde **ADV_xxxx** es el nombre de la clase que implementa el asesor personalizado.

puerto

Número del puerto que el asesor está supervisando.

segundos

Entero positivo que representa el tiempo en segundos durante el que el asesor espera antes de notificar que se ha producido una anomalía en una conexión a un servidor. El valor por omisión es 3 veces el valor especificado para el intervalo del asesor.

interval

Establece con qué frecuencia el asesor consulta si hay información en los servidores.

segundos

Entero positivo que representa el número de segundos entre las peticiones a los servidores sobre su estado. El valor por omisión es 7.

list

Muestra una lista de los asesores que actualmente proporcionan información al gestor.

loglevel

Establece el nivel de registro cronológico para las anotaciones cronológicas del asesor.

nivel

El número del nivel (0 a 5). El valor por omisión es 1. Cuanto más alto sea el número, más información se anotará en las anotaciones cronológicas del asesor. Los valores posibles son:

- 0 es Ninguno
- 1 es Mínimo
- 2 es Básico
- 3 es Moderado
- 4 es Avanzado
- 5 es Detallado

logsize

Establece el tamaño máximo de las anotaciones cronológicas del asesor. Cuando se establece un tamaño máximo para el archivo de anotaciones cronológicas, el texto del archivo vuelve al principio; es decir, cuando el archivo alcanza el tamaño especificado, las entradas subsiguientes se grabarán encima de las entradas de anotaciones cronológicas anteriores. El tamaño de las anotaciones cronológicas no puede establecerse más pequeño que el tamaño actual de las anotaciones cronológicas. Las entradas de las anotaciones cronológicas incluyen la indicación de la hora para poder saber el orden en el que se anotaron. Cuando más alto se establezca el nivel de anotaciones cronológicas, más cuidado deberá tener al elegir el tamaño de las anotaciones cronológicas porque, cuando el registro cronológico está establecido en los niveles más altos, puede quedarse sin espacio rápidamente.

tamaño | unlimited

El tamaño máximo en bytes para el archivo de anotaciones cronológicas del asesor. Puede especificar un número positivo mayor que cero o la palabra **unlimited**. Es posible que el archivo de anotaciones cronológicas no alcance el tamaño máximo exacto antes de empezar a sobrescribir porque el tamaño de las entradas del archivo varían. El valor por omisión es 1 MB.

receivetimeout

Establece cuánto tiempo espera un asesor antes de notificar que se ha producido un error en una recepción en un servidor. Para obtener más información, consulte el apartado “Tiempo de espera de conexión y recepción del asesor para los servidores” en la página 188.

segundos

Entero positivo que representa el tiempo en segundos durante el que el asesor espera antes de notificar que se ha producido una anomalía en una recepción en un servidor. El valor por omisión es 3 veces el valor especificado para el intervalo del asesor.

report

Muestra un informe sobre el estado del asesor.

retries

El número de reintentos que un asesor puede realizar antes de marcar un servidor como inactivo.

núm_reintentos

Número entero mayor que o igual a cero. Este valor no debe ser mayor que 3. Si la palabra clave retries no está configurada, el número de reintentos tendrá el valor por omisión de cero.

start

Inicia el asesor. Estos son asesores de cada protocolo. Los puertos por omisión son:

Nombre del asesor	Protocolo	Puerto
Connect	n/d	definido por el usuario
db2	private	50000
ftp	FTP	21
http	HTTP	80
https	SSL	443
imap	IMAP	143
ldap	LDAP	389
nntp	NNTP	119
PING	PING	N/D
pop3	POP3	110
sip	SIP	5060
smtp	SMTP	25
ssl	SSL	443
telnet	Telnet	23

nombre

Nombre del asesor.

nombre_sitio:puerto

El valor de nombre de sitio es opcional en los mandatos del asesor; sin embargo, el valor de puerto sí es necesario. Si no se especifica el valor de nombre de sitio, el asesor empieza a ejecutarse en todos los nombres de sitio disponibles configurados. Si especifica un nombre de sitio, el asesor sólo empieza a ejecutarse en el nombre del sistema que especifique. Los nombres de sitios adicionales se separan mediante un signo más (+).

archivo_annotaciones

Nombre de archivo en el que se anotan los datos de gestión. Cada registro de las anotaciones cronológicas incluye la indicación de la hora.

El archivo por omisión es *puerto_nombre_asesor.log*, por ejemplo, **http_80.log**. Para cambiar el directorio en el que se guardan los archivos de anotaciones cronológicas, consulte el apartado “Cambio de las vías de acceso del archivo de anotaciones cronológicas” en la página 267.

Sólo puede iniciar un asesor para cada nombre de sitio.

status

Muestra el estado actual y los valores por omisión de todos los valores globales de un asesor.

stop

Detiene el asesor.

timeout

Establece el número de segundos durante los que el gestor considerará válida la información del asesor. Si el gestor cree que la información del asesor es anterior a este intervalo de tiempo de espera, el gestor no la utiliza para determinar los pesos para los servidores en el puerto que el asesor está supervisando. Una excepción a este tiempo de espera es cuando el asesor ha

notificado al gestor que un servidor específico está inactivo. El gestor utiliza dicha información sobre el servidor, incluso después de que el información del asesor exceda el tiempo de espera.

segundos

Número positivo que representa el número de segundos o la palabra **unlimited**. El valor por omisión es unlimited.

version

Muestra la versión actual del asesor.

Ejemplos

- Establecer el tiempo (30 segundos) que un asesor HTTP (para el puerto 80) espera antes de notificar que se ha producido una anomalía en una conexión a un servidor:
`sscontrol advisor connecttimeout http 80 30`
- Establecer el intervalo para el asesor FTP (para el puerto 21) en 6 segundos:
`sscontrol advisor interval ftp 21 6`
- Mostrar la lista de asesores que actualmente proporcionan información al gestor:
`sscontrol advisor list`

Este mandato genera una salida parecida a la siguiente:

```
-----  
| ASESOR | NOM_SITIO:PUERTO | TIEMPO ESP. |  
-----  
| http   |          80 | unlimited |  
| ftp    |          21 | unlimited |  
-----
```

- Cambiar el nivel de anotaciones cronológicas de las anotaciones cronológicas del asesor http para el nombre de sitio misitio en 0 para un mejor rendimiento:
`sscontrol advisor loglevel http misitio:80 0`
- Cambiar el tamaño de las anotaciones cronológicas del asesor ftp para el nombre del sitio misitio en 5000 bytes:
`sscontrol advisor logsize ftp misitio:21 5000`
- Establecer el tiempo (60 segundos) que un asesor HTTP (para el puerto 80) espera antes de notificar que se ha producido una anomalía en una recepción de un servidor:
`sscontrol advisor receivetimeout http 80 60`
- Mostrar un informe en el estado del asesor ftp (para el puerto 21):
`sscontrol
advisor report ftp 21`

Este mandato genera una salida parecida a la siguiente:

Informe del asesor:

```
-----  
Nombre del asesor ..... http  
Número de puerto ..... 80  
  
Nombre sitio ..... miSitio  
Dirección del servidor ... 9.67.129.230  
Carga ..... 8
```

- Iniciar el asesor con el archivo ftpadv.log:
`sscontrol advisor start ftp 21 ftpadv.log`
- Mostrar el estado actual de los valores asociados al asesor http:
`sscontrol advisor status http 80`

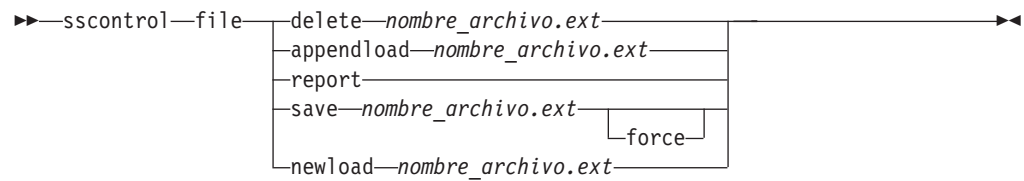
Este mandato genera una salida parecida a la siguiente:

Estado del asesor:

Intervalo (segundos) 7
Tiempo de espera (segundos) ... Unlimited
Tiempo espera conexión (seg) .. 21
Tiempo espera recepción (seg).. 21
Nombre anotaciones asesor Http_80.log
Nivel anotación cronológica ... 1
Tam. máx. arch. anot. (bytes) . Unlimited
Número de reintentos 0

- Detener el asesor http en el puerto 80:
sscontrol advisor stop http 80
- Establecer el valor de tiempo de espera para la información del asesor en 5 segundos:
sscontrol advisor timeout ftp 21 5
- Averiguar el número de versión actual del asesor SSL:
sscontrol advisor version ssl 443

sscontrol file — gestionar archivos de configuración



delete

Suprime el archivo.

archivo.ext

Un archivo de configuración.

La extensión de archivo (*.ext*) puede ser cualquiera y es opcional.

appendload

Adjunta un archivo de configuración a la configuración actual y la carga en Site Selector.

report

Informa sobre el archivo o archivos disponibles.

save

Guarda la configuración actual de Site Selector en el archivo.

Nota: Los archivos se guardan y se cargan de los siguientes directorios:

- Sistemas Linux y UNIX: `/opt/ibm/edge/lb/servers/configurations/ss`
- Sistemas Windows: `C:\Archivos de programa\ibm\edge\lb\servers\configurations\componente`

force

Para guardar el archivo en un archivo existente con el mismo nombre, utilice **force** para suprimir el archivo existente antes de guardar el nuevo archivo. Si no utiliza la opción **force**, no se sobrescribirá el archivo existente.

newload

Cargar un nuevo archivo de configuración en Site Selector. El nuevo archivo de configuración sustituirá a la configuración actual.

Ejemplos

- Suprimir un archivo:

```
sscontrol file delete file3
```

Se ha suprimido el archivo (file3).

- Cargar un nuevo archivo de configuración para que sustituya a la configuración actual:

```
sscontrol file newload file1.sv
```

El archivo (file1.sv) se ha cargado en Dispatcher.

- Adjuntar un archivo de configuración a un configuración actual y cargar:

```
sscontrol file appendload file2.sv
```

El archivo (file2.sv) se ha añadido a la configuración actual y se ha cargado.

- Ver un informe de los archivos (es decir, estos archivos que ha guardado anteriormente):

```
sscontrol file report
```

INFORME SOBRE EL ARCHIVO:

file1.save

file2.sv

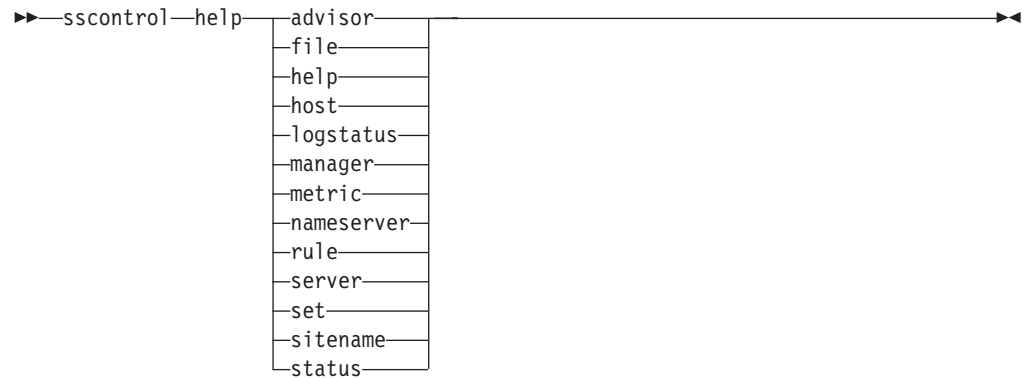
file3

- Guardar la configuración en un archivo denominado file3:

```
sscontrol file save file3
```

La configuración se ha guardado en el archivo (file3).

sscontrol help — mostrar o imprimir ayuda para este mandato



Ejemplos

- Obtener ayuda sobre el mandato sscontrol:

```
sscontrol help
```

Este mandato genera una salida parecida a la siguiente:

ARGUMENTOS DEL MANDATO DE AYUDA:

Uso: help <opción de ayuda>

Ejemplo: help nombre

help	- imprime el texto completo de la ayuda
advisor	- ayuda para el mandato advisor
file	- ayuda para el mandato file
host	- ayuda para el mandato host
manager	- ayuda para el mandato manager
metric	- ayuda para el mandato metric
sitename	- ayuda para el mandato sitename
nameserver	- ayuda para el mandato nameserver
rule	- ayuda para el mandato rule
server	- ayuda para el mandato server
set	- ayuda para el mandato set
status	- ayuda para el mandato status
logstatus	- ayuda para el mandato logstatus

Los parámetros dentro de < > son variables.

- Algunas veces la ayuda muestra opciones para las variables utilizando | para separar las opciones:

```
logsize <número de bytes | unlimited>
```

-Establece el número máximo de bytes anotados en el archivo de anotaciones cronológicas

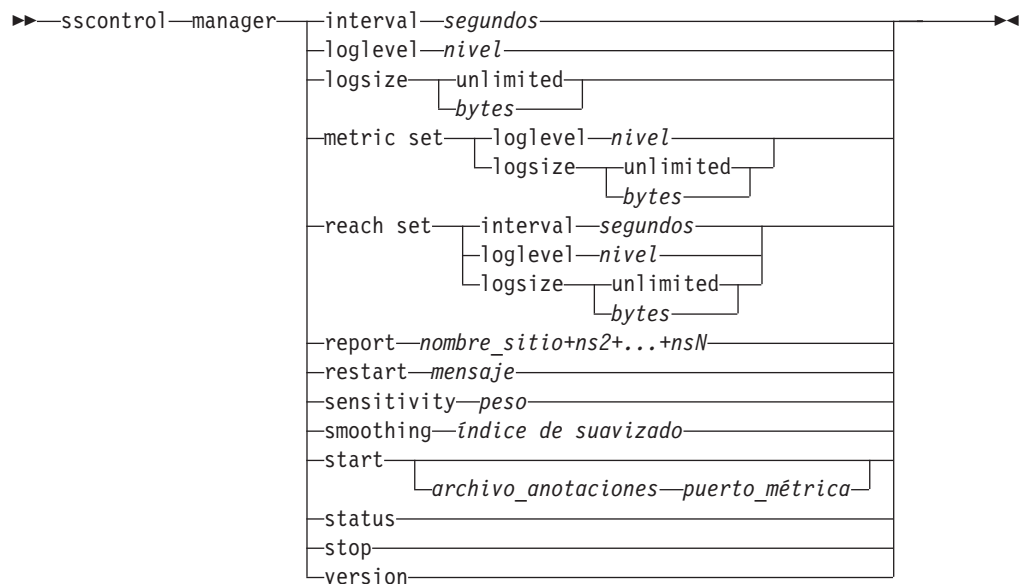
sscontrol logstatus — mostrar valores de anotaciones cronológicas de servidor

►►—sscontrol—logstatus—◄◄

logstatus

Muestra los valores de las anotaciones cronológicas del servidor (nombre de archivo de anotaciones cronológicas, nivel de registro cronológico y tamaño de las anotaciones cronológicas).

sscontrol manager — controlar el gestor



interval

Establece la frecuencia con la que el gestor actualiza los pesos de los servidores.

segundos

Número positivo en segundos que representa la frecuencia con la que el gestor actualiza pesos. El valor por omisión es 2.

loglevel

Establece el nivel de registro cronológico para las anotaciones cronológicas del gestor.

nivel

El número del nivel (0 a 5). Cuanto más alto sea el número, más información se anotará en las anotaciones cronológicas del gestor. El valor por omisión es 1. Los valores posibles son:

- 0 es Ninguno
- 1 es Mínimo
- 2 es Básico
- 3 es Moderado
- 4 es Avanzado
- 5 es Detallado

logsize

Establece el tamaño máximo de las anotaciones cronológicas del gestor. Cuando se establece un tamaño máximo para el archivo de anotaciones cronológicas, el texto del archivo vuelve al principio; es decir, cuando el archivo alcanza el tamaño especificado, las entradas subsiguientes se anotarán al principio del archivo y se grabarán encima de las entradas de anotaciones cronológicas anteriores. El tamaño de las anotaciones cronológicas no puede establecerse más pequeño que el tamaño actual de las anotaciones cronológicas. Las entradas de las anotaciones cronológicas incluyen la indicación de la hora para poder saber el orden en el que se anotaron. Cuando más alto se establezca el nivel de anotaciones cronológicas, más cuidado deberá tener al

elegir el tamaño de las anotaciones cronológicas porque, cuando el registro cronológico está establecido en los niveles más altos, puede quedarse sin espacio rápidamente.

bytes

El tamaño máximo en bytes para el archivo de anotaciones cronológicas de gestor. Puede especificar un número positivo mayor que cero o la palabra **unlimited**. Es posible que el archivo de anotaciones cronológicas no alcance el tamaño máximo exacto antes de empezar a sobrescribir porque el tamaño de las entradas del archivo varían. El valor por omisión es 1 MB.

metric set

Establece **loglevel** y **logsize** para las anotaciones cronológicas del supervisor de métrica. **loglevel** es el nivel de registro cronológico del supervisor de métrica (0 - Ninguno, 1 - Mínimo, 2 - Básico, 3 - Moderado, 4 - Avanzado o 5 - Detallado). El valor por omisión de **loglevel** es 1. El **logsize** es el número máximo de bytes que deben anotarse en el archivo de anotaciones cronológicas del supervisor de métrica. Puede especificar un número positivo mayor que cero o **unlimited**. El valor por omisión de **logsize** es 1.

reach set

Establece el intervalo, el nivel de anotaciones cronológicas y el tamaño de las anotaciones cronológicas para el asesor de alcance.

report

Muestra un informe de instantánea de estadísticas.

nombre_sitio

El nombre de sitio que desea que se muestre en el informe. Esto es un nombre de sistema principal que no es posible resolver que el cliente solicitará. El nombre de sitio debe ser un nombre de dominio completamente cualificado.

Nota: Los nombres de sitios adicionales se separan mediante un signo más (+).

restart

Reinicia todos los servidores (que no están inactivos) para pesos normalizados (1/2 del peso máximo).

mensaje

Mensaje que desea escribir en el archivo de anotaciones cronológicas del gestor.

sensitivity

Establece la sensibilidad mínima en la que se actualizan los pesos. Este valor define cuando el gestor debe cambiar su ponderación para el servidor basándose en información externa.

peso

Número comprendido entre 0 y 100 utilizado como porcentaje de peso. El valor por omisión 5 crea una sensibilidad mínima del 5%.

smoothing

Establece un índice que suavice las variaciones en el peso al realizar el equilibrio de carga. Un índice de suavizado más alto hará que los pesos de servidores cambien menos radicalmente cuando cambian las condiciones de la red. Un índice más bajo hará que los pesos de servidores cambien de forma más radical.

índice

Número de coma flotante positivo. El valor por omisión es 1,5.

start

Inicia el gestor.

archivo_annotaciones

Nombre de archivo en el que se anotan los datos del gestor. Cada registro de las anotaciones cronológicas incluye la indicación de la hora.

El archivo por omisión se instala en el directorio **logs**. Consulte el Apéndice C, “Archivos de configuración de ejemplo”, en la página 479. Para cambiar el directorio en el que se guardan los archivos de anotaciones cronológicas, consulte el apartado “Cambio de las vías de acceso del archivo de anotaciones cronológicas” en la página 267.

puerto_métrica

Puerto que Metric Server utiliza para notificar cargas del sistema. Si especifica un puerto de métrica, debe especificar un nombre de archivo de anotaciones cronológicas. El puerto de métrica por omisión es 10004.

status

Muestra el estado actual y los valores por omisión de todos los valores globales del gestor.

stop

Detiene el gestor.

version

Muestra la versión actual del gestor.

Ejemplos

- Establecer el intervalo de actualización del gestor en cada 5 segundos:
`sscontrol manager interval 5`
- Establecer el nivel de registro cronológico en 0 para obtener un mejor rendimiento:
`sscontrol manager loglevel 0`
- Establecer el tamaño de las anotaciones cronológicas del gestor en 1.000.000 bytes:
`sscontrol manager logsize 1000000`
- Obtener una instantánea de estadísticas del gestor:
`sscontrol manager report`

Este mandato genera una salida parecida a la siguiente:

SERVIDOR	ESTADO
9.67.129.221	ACTIVO
9.67.129.213	ACTIVO
9.67.134.223	ACTIVO

LEYENDA INFORMES GESTOR

CPU	Carga CPU
MEM	Carga memoria
SYS	Métrica sistema
NOW	Peso actual
NEW	Nuevo peso
WT	Peso

miSitio	PESO	CPU 49%	MEM 50%	PUERTO 1%	SYS 0%
	NOW NEW	WT CARGA	WT CARGA	WT CARGA	WT CARGA
9.37.56.180	10 10	-99 -1	-99 -1	-99 -1	0 0
TOTALES:	10 10	-1	-1	-1	0

ASESOR	NOM_SITIO:PUERTO	TIEMPO ESP.
http	80	unlimited

- Reiniciar todos los servidores para pesos normalizados y escribe un mensaje en el archivo de anotaciones cronológicas del gestor:
sscontrol manager restart Reiniciando el gestor para actualizar código

Este mandato genera una salida parecida a la siguiente:

320-14:04:54 Reiniciando el gestor para actualizar código

- Establecer la sensibilidad de cambios de peso en 10:
sscontrol manager sensitivity 10
- Establecer el índice de suavidad 2.0:
sscontrol manager smoothing 2.0
- Iniciar el gestor y especificar el archivo de anotaciones cronológicas denominado ndmgr.log (no se pueden establecer vías de acceso)
sscontrol manager start ndmgr.log
- Mostrar el estado actual de los valores asociados al gestor:
sscontrol manager status

Este mandato genera una salida parecida al siguiente ejemplo:

Estado del gestor:

=====

```
Puerto de métrica ..... 10004
Archivo anotaciones del gestor ..... manager.log
Nivel anotaciones del gestor ..... 1
Tamaño máximo anotaciones de gestor (bytes) .. unlimited
Nivel de sensibilidad ..... 5
Índice de suavizado ..... 1,5
Intervalo de actualización (segundos) ..... 2
Ciclo de renovación de pesos ..... 2
Nivel de anotaciones asesor de alcance ..... 1
Tamaño máximo anot. asesor alcance (bytes) ... unlimited
Intervalo intentos acceso a destino (seg.) ... 7
```

- Detener el gestor:

```
sscontrol manager stop
```

- Mostrar el número de versión actual del gestor:

```
sscontrol manager version
```

sscontrol metric — configurar métrica del sistema

```
►►—sscontrol—metric—┐add—nombre_sitio+sn2+...+nsN:métrica+métrica1+...+métricaN┐
                      └remove—nombre_sitio+sn2+...+nsN:métrica+métrica1+...+métricaN┘
                      └proportions—nombre_sitio+ns2+...+nsN:proporción1 prop2 prop3...propN┘
                      └status—nombre_sitio+ns2+...+nsN métrica+métrica1+...+métricaN┘
```

add

Añadir la métrica específica.

nombre_sitio

El nombre de sitio configurado. Los nombres de sitios adicionales se separan mediante un signo más (+).

métrica

El nombre del sistema métrico. Debe ser el nombre de un archivo script o ejecutable en el directorio de scripts de Metric Server.

remove

Elimina la métrica especificada.

proportions

Proportions determina la importancia de cada métrica en comparación con las demás cuando se combinan en una sola carga del sistema para un servidor.

status

Muestra los valores de servidor actuales para esta métrica.

Ejemplos

- Para añadir una métrica de sistema:
`sscontrol metric add sitio1:métrica1`
- Para establecer proporciones para el nombre de sitio con dos métricas de sistema:
`sscontrol metric proportions sitio1 0 100`
- Mostrar el estado actual de valores asociados a la métrica especificada:
`sscontrol metric status sitio1:métrica1`

Este mandato genera una salida parecida a la siguiente:

Estado de métrica:

```
nombre_sitio ..... sitio1
Nombre de métrica ..... métrica1
Proporción de métrica ..... 50
  Servidor ..... 9.37.56.100
  Datos métrica .. -1
```

sscontrol nameserver — controlar el servidor de nombres



start

Inicia el servidor de nombres.

bindaddress

Inicia el enlace del servidor de nombres con la dirección especificada. El servidor de nombres responde sólo a una petición destinada para esta dirección.

dirección

Dirección (IP o simbólica) configurada en la máquina Site Selector.

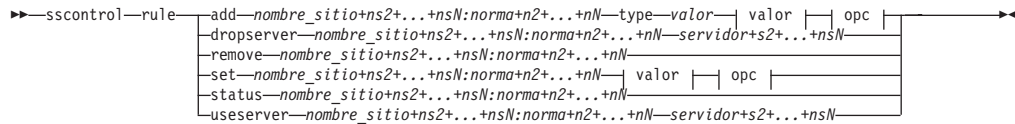
stop

Detiene el servidor de nombres.

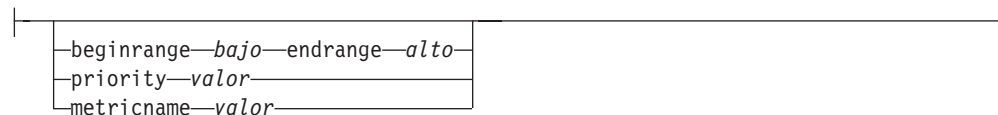
status

Muestra el estado del servidor de nombres.

sscontrol rule — configurar normas



opc:



add

Añade esta norma a un nombre de sitio.

nombre_sitio

Nombre de sistema principal que no es posible resolver que el cliente solicitará. El nombre de sitio debe ser un nombre de dominio completamente cualificado. Los nombres de sitios adicionales se separan mediante un signo más (+).

norma

Nombre que se selecciona para la norma. Este nombre puede contener cualquier carácter alfanumérico, subrayado, guión o punto. Puede tener de 1 a 20 caracteres y no puede contener blancos.

Nota: Las normas adicionales se separan mediante un signo más (+).

type

Tipo de norma.

tipo

Las opciones de *tipo* son:

ip La norma se basa en la dirección IP de cliente.

metricall

La norma se basa en el valor de métrica actual para todos los servidores en el conjunto de servidores.

metricavg

La norma se basa en el promedio de los valores de métrica actual para todos los servidores en el conjunto de servidores.

time La norma se basa en la hora del día.

true Esta norma es siempre cierta. Piense en ella como si fuera una sentencia else en lógica de programación.

beginrange

El valor más pequeño del rango utilizado para determinar si una norma es cierta.

bajo

Depende del tipo de norma. El tipo de valor y su valor por omisión se listan según el tipo de norma:

ip La dirección del cliente, en forma de nombre simbólico o en un formato de dirección IP. El valor por omisión es 0.0.0.0.

tiempo Número entero. El valor por omisión es 0, que representa medianoche.

metricall

Número entero. El valor por omisión es 100.

metricavg

Número entero. El valor por omisión es 100.

endrange

El valor más alto del rango utilizado para determinar si la norma es cierta.

alto

Depende del tipo de norma. El tipo de valor y su valor por omisión se listan según el tipo de norma:

ip La dirección del cliente, en forma de nombre simbólico o en un formato de dirección IP. El valor por omisión es 255.255.255.254.

tiempo Número entero. El valor por omisión es 24, que representa medianoche.

Nota: Al definir *beginrange* y *endrange* de los intervalos de tiempo, tenga en cuenta que cada valor debe ser un entero que represente sólo la porción de la hora del tiempo; no se especifican las fracciones de una hora. Por esta razón, para especificar una sola hora, por ejemplo la hora entre las 3:00 y las 4:00, debería especificar 3 en *beginrange* y también 3 en *endrange*. Esto indicará todos los minutos, empezando en 3:00 y terminando en 3:59. Si especifica 3 en *beginrange* y 4 en *endrange*, abarcará un periodo de dos horas, de las 3:00 hasta las 4:59.

metricall

Número entero. El valor por omisión es 2 elevado a la 32 menos 1.

metricavg

Número entero. El valor por omisión es 2 elevado a la 32 menos 1.

priority

El orden en el que se revisan las normas.

nivel

Número entero. Si no especifica la prioridad de la primera norma que añade, por omisión Site Selector la establece en 1. Cuando posteriormente se añade otra norma, por omisión su prioridad se calcula sumando 10 a la prioridad más baja actual de cualquier norma existente. Por ejemplo, suponga que tiene una norma existente con una prioridad 30. Añada una nueva norma con la prioridad 25 (que es una prioridad *más alta* que 30). A continuación, añada una tercera norma sin establecer la prioridad. La prioridad de la tercera norma se calculará como 40 (30 + 10).

metricname

Nombre de la métrica medida para una norma.

dropserver

Elimina un servidor del conjunto de normas.

servidor

Dirección IP de la máquina servidor TCP como nombre simbólico o en formato de dirección IP.

Nota: Los nombres de sitios adicionales se separan mediante un signo más (+).

remove

Elimina una o más normas, separadas entre sí por signos más.

set

Establece los valores para esta norma.

status

Muestra todos los valores de una o más normas.

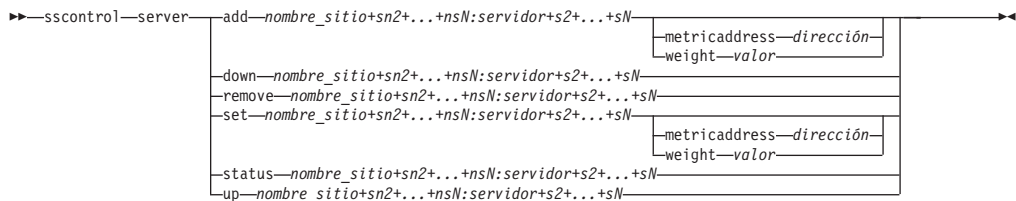
useserver

Inserta el servidor en un conjunto de normas.

Ejemplos

- Para añadir una norma que será siempre cierta, no especifique el inicio del rango ni el fin del rango:
`sscontrol rule add nombresitio:nombrenorma type true priority 100`
- Crear una norma que prohíba el acceso a un rango de direcciones IP, en este caso las que empiecen por "9":
`sscontrol rule add nombresitio:nombrenorma type ip b 9.0.0.0 e 9.255.255.255`
- Crear una norma que especificará el uso de un servidor específico desde las 11:00 hasta las 15:00.
`sscontrol rule add nombresitio:nombrenorma type time beginrange 11 endrange 14`
`sscontrol rule useserver nombresitio:nombrenorma server05`

sscontrol server — configurar servidores



add

Añade este servidor.

nombre_sitio

Nombre de sistema principal que no es posible resolver que el cliente solicitará. El nombre de sitio debe ser un nombre de dominio completamente cualificado. Los nombres de sitios adicionales se separan mediante un signo más (+).

servidor

Dirección IP de la máquina servidor TCP como nombre simbólico o en formato de dirección IP.

Nota: Los servidores adicionales se separan mediante un signo más (+).

metricaddress

Dirección de Metric Server.

dirección

La dirección del servidor, en forma de nombre simbólico o en un formato de dirección IP.

weight

Número comprendido entre 1 y 100 (no exceda el máximo valor de ponderación del puerto del nombre del sitio especificado) que representa el peso de este servidor. Si se establece el peso en cero, se impedirá que se envíen nuevas peticiones al servidor. El valor por omisión es la mitad del máximo valor de ponderación del nombre de sitio especificado. Si el gestor se está ejecutando, este valor se sobrescribirá.

valor

El valor de peso del servidor.

down

Marca este servidor como inactivo. Este mandato impide que se resuelva cualquier otra petición para dicho servidor.

remove

Elimina este servidor.

set

Establece los valores para este servidor.

status

Muestra el estado de los servidores.

up Marca este servidor como activo. Site Selector ahora resolverá nuevas peticiones para dicho servidor.

Ejemplos

- Añadir el servidor con la dirección 27.65.89.42 al nombre de sitio sitio1:
`sscontrol server add sitio1:27.65.89.42`
- Marcar el servidor en 27.65.89.42 como inactivo:
`sscontrol server down sitio1:27.65.89.42`
- Eliminar el servidor en 27.65.89.42 para todos los nombres de sitios:
`sscontrol server remove :27.65.89.42`
- Marcar el servidor en 27.65.89.42 como activo:
`sscontrol server up sitio1:27.65.89.42`

sscontrol set — configurar anotaciones cronológicas de servidor



loglevel

El nivel en el que el ssserver anota sus actividades.

nivel

El valor por omisión de **loglevel** es 0. Los valores posibles son:

- 0 es Ninguno
- 1 es Mínimo
- 2 es Básico
- 3 es Moderado
- 4 es Avanzado
- 5 es Detallado

logsize

El número máximo de bytes que se deben anotar en el archivo de anotaciones cronológicas.

tamaño

El valor por omisión de logsize es 1 MB.

sscontrol sitename — configurar un nombre de sitio



add

Añade un nuevo nombre de sitio.

nombre_sitio

Nombre de sistema principal que no se puede resolver, solicitado por el cliente. Los nombres de sitios adicionales se separan mediante un signo más (+).

cachelife

Cantidad de tiempo que una respuesta de proximidad será válida y se guardará en la antememoria. El valor por omisión es 1800. Consulte el apartado “Utilización de la característica proximidad de red” en la página 128 para obtener más información.

valor

Número positivo que representa el número de segundos que una respuesta de proximidad será válida y se guardará en la antememoria.

networkproximity

Determina la proximidad de red de cada servidor al cliente que realiza la petición. Utilice esta respuesta de proximidad en la decisión de equilibrio de carga. Activa o desactiva la proximidad. Consulte el apartado “Utilización de la característica proximidad de red” en la página 128 para obtener más información.

valor

Los valores son yes o no. El valor por omisión es no, que significa que la proximidad de red está desactivada.

proportions

Establece la proporción de la importancia para la CPU, la memoria, el puerto (información de todos los asesores) y la métrica del sistema del Metric Server que utiliza el gestor para establecer pesos de servidor. Cada uno de estos valores se expresan como porcentaje del total y el total siempre es 100.

cpu El porcentaje de la CPU en uso para cada máquina servidor con equilibrio de carga (entrada del agente de Metric Server).

memoria

El porcentaje de la memoria en uso (entrada del agente de Metric Server) en cada servidor con equilibrio de carga

puerto La entrada de los asesores que escuchan en el puerto.

sistema La entrada desde Metric Server.

proximitypercentage

Establece la importancia de la respuesta de proximidad frente al estado del servidor (peso del gestor). Consulte el apartado “Utilización de la característica proximidad de red” en la página 128 para obtener más información.

valor

El valor por omisión es 50.

stickytime

El intervalo durante el que un cliente recibirá el mismo ID de servidor devuelto anteriormente para la primera petición. El valor por omisión de stickytime es 0, lo que significa que el nombre de sitio no es permanente en memoria.

tiempo

Número positivo distinto de cero que representa el número de segundos durante los que el cliente recibe el mismo ID de servidor devuelto anteriormente para la primera petición.

ttl Establece la duración. Esto indica cuánto tiempo otro servidor de nombres guardará en la antememoria la respuesta resuelta. El valor por omisión es 5.

valor

Número positivo que representa el número de segundos que el servidor de nombres guardará en la antememoria la respuesta resuelta.

waitforallresponses

Establece si se debe esperar a recibir todas las respuestas de proximidad de los servidores antes de responder a la petición de cliente. Consulte el apartado “Utilización de la característica proximidad de red” en la página 128 para obtener más información.

valor

Los valores son yes o no. El valor por omisión es yes.

weightbound

Número que representa el peso máximo que puede establecerse para los servidores en este nombre de sitio. El valor de weightbound establecido para el nombre de sitio puede alterarse temporalmente para servidores individuales mediante **server weight**. El valor por omisión de sitename weightbound es 20.

peso

El valor de weightbound.

set

Establece las propiedades del nombre del sitio.

remove

Elimina este nombre de sitio.

status

Muestra el estado actual de un nombre de sitio específico.

Ejemplos

- Añadir un nombre de sitio:
`sscontrol sitename add 130.40.52.153`
- Activar la proximidad de red:
`sscontrol sitename set miSitio networkproximity yes`
- Establecer la duración de antememoria en 1900000 segundos:
`sscontrol sitename set miSitio cachelife 1900000`

- Establecer el porcentaje de proximidad 45:
sscontrol sitename set miSitio proximitypercentage 45
- Establecer un nombre de sitio de forma que no espere todas las respuestas antes de responder:
sscontrol sitename set miSitio waitforallresponses no
- Establecer la duración en 7 segundos:
sscontrol sitename set miSitio ttl 7
- Establecer la proporciones de la importancia para CpuLoad, MemLoad, Port y System Metric, respectivamente:
sscontrol sitename set miSitio proportions 50 48 1 1
- Eliminar un nombre de sitio:
sscontrol sitename remove 130.40.52.153
- Mostrar el estado para el nombre de sitio miSitio:
sscontrol sitename status miSitio

Este mandato genera una salida parecida a la siguiente:

Estado del nombre del sitio:

```
Nombre de sitio ..... miSitio
Ponderación ..... 20
TTL ..... 5
Tiempo permanencia en memoria ..... 0
Número de servidores ..... 1
Proporción asignada a CpuLoad ..... 49
Proporción asignada a MemLoad ..... 50
Proporción asignada a Port ..... 1
Proporción asignada a métrica sist . 0
Asesor ejecutándose en puerto ..... 80
Utilización de proximidad ..... N
```

sscontrol status — mostrar si el gestor y los asesores se están ejecutando

►►—sscontrol—status—◀◀

Ejemplos

- Para ver lo que está en ejecución, escriba:
`sscontrol status`

Este mandato genera una salida parecida a la siguiente:

Se ha iniciado el servidor de nombres.
Se ha iniciado el gestor.

```
-----  
| ASESOR | NOM_SITIO:PUERTO|TIEMPO ESP.|  
-----  
| http | 80 | unlimited |  
-----
```

Capítulo 29. Referencia de mandatos para Cisco CSS Controller

En este capítulo se describe cómo utilizar los siguientes mandatos **ccocontrol** para Cisco CSS Controller:

- “ccocontrol consultant — configurar y controlar un consultor” en la página 432
- “ccocontrol controller — gestionar el controlador” en la página 435
- “ccocontrol file — gestionar archivos de configuración” en la página 437
- “ccocontrol help — mostrar o imprimir ayuda para este mandato” en la página 438
- “ccocontrol highavailability — controlar alta disponibilidad” en la página 439
- “ccocontrol metriccollector — configurar recopilador de métricas” en la página 442
- “ccocontrol ownercontent — controlar el nombre de propietario y la norma de contenido” en la página 444
- “ccocontrol service — configurar un servicio” en la página 447

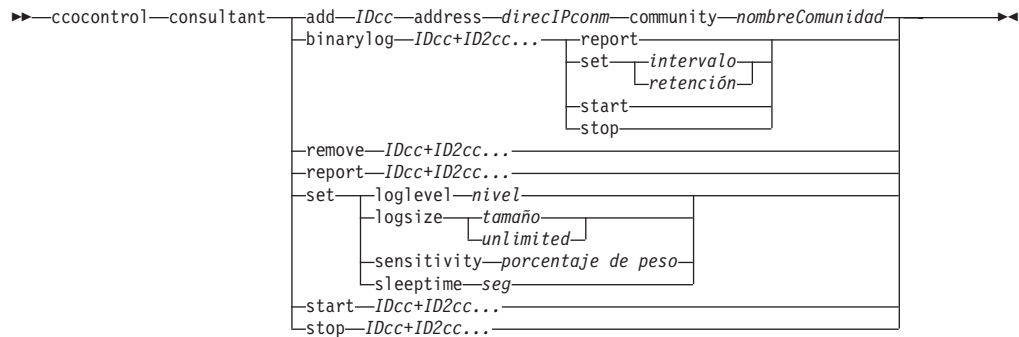
Puede utilizar una versión abreviada de los parámetros del mandato **ccocontrol** escribiendo las letras exclusivas de los parámetros. Por ejemplo, para obtener ayuda sobre el mandato para guardar archivos, puede escribir **ccocontrol he f** en lugar de **ccocontrol help file**.

Para obtener el indicador de mandatos **ccocontrol**, escriba **ccocontrol**.

Para finalizar la interfaz de línea de mandatos, escriba **exit** o **quit**.

Nota: Debe utilizar caracteres del idioma inglés en todos los valores de parámetros de mandatos. Las únicas excepciones son los nombres de sistema principal (que se utilizan en los mandatos del servidor) y los nombres de archivo (que se utilizan en los mandatos de archivo).

cococontrol consultant — configurar y controlar un consultor



add

Añade un consultor de conmutador.

IDcc (**ID_consultor_conmutador**)

Serie definida por el usuario que hace referencia al consultor.

address

Dirección IP de Conmutador Cisco CSS al que el consultor proporciona pesos.

direcIPconm (**direcciónIPconmutador**)

Dirección IP del conmutador.

community

Nombre utilizado en SNMP para obtener y establecer comunicaciones con el Conmutador Cisco CSS.

nombreComunidad

Nombre de comunidad de lectura/escritura del Conmutador Cisco CSS.

binarylog

Controla el registro cronológico en binario para un consultor.

report

Informa sobre las características del registro cronológico.

set

Establece la frecuencia, en segundos, con la que la información se escribe en las anotaciones cronológicas en binario. La característica de registro cronológico permite almacenar la información de servicio en archivos de anotaciones cronológicas en binario para cada servicio definido en la configuración. La información se graba en las anotaciones cronológicas sólo cuando hayan transcurrido los segundos especificados en el intervalo de anotaciones cronológicas después de anotarse el último registro en el archivo de anotaciones cronológicas. El intervalo de registro cronológico en binario por omisión es 60.

intervalo

Establece el número de segundos entre las entradas de las anotaciones cronológicas en binario.

retención

Establece el número de horas que se conservan los archivos de anotaciones cronológicas en binario.

start

Inicia el registro cronológico en binario.

stop

Detiene el registro cronológico en binario.

remove

Elimina un consultor de conmutador.

report

Informa sobre las características de consultores del conmutador.

set

Establece las características de consultores de conmutador.

loglevel

Establece el nivel en el que el consultor de conmutador registra las actividades. El valor por omisión es 1.

nivel

El número del nivel de 0 a 5. El valor por omisión es 1. Los valores posibles son:

- 0 = Ninguno
- 1 = Mínimo
- 2 = Básico
- 3 = Moderado
- 4 = Avanzado
- 5 = Detallado

logsize

Establece el número máximo de bytes anotados en el archivo de anotaciones cronológicas. El valor por omisión es 1048576. Cuando se establece un tamaño máximo para el archivo de anotaciones cronológicas, el texto del archivo vuelve al principio; es decir, cuando el archivo alcanza el tamaño especificado, las entradas subsiguientes se anotarán al principio del archivo y se grabarán encima de las entradas de anotaciones cronológicas anteriores. El tamaño de las anotaciones cronológicas no puede establecerse más pequeño que el tamaño actual de las anotaciones cronológicas. Las entradas de las anotaciones cronológicas incluyen la indicación de la hora para poder saber el orden en el que se anotaron. Cuando más alto se establezca el nivel de anotaciones cronológicas, más cuidado deberá tener al elegir el tamaño de las anotaciones cronológicas porque, cuando el registro cronológico está establecido en los niveles más altos, puede quedarse sin espacio rápidamente.

tamaño

Número máximo de bytes anotados en las anotaciones cronológicas del consultor. Puede especificar un número positivo mayor que cero o la palabra **unlimited**. Es posible que el archivo de anotaciones cronológicas no alcance el tamaño máximo exacto antes de empezar a sobrescribir porque el tamaño de las entradas del archivo varían.

sensitivity

Indica la cantidad de cambio que debe tener lugar entre los pesos anteriores y nuevos para que el peso cambie. Para que el peso cambie, la diferencia entre el peso nuevo y el antiguo debe ser mayor que el porcentaje de sensibilidad. El rango válido es de 0 a 100; el valor por omisión es 5.

porcentaje de peso

Entero que oscila entre 0 y 100, que representa el valor de sensibilidad.

sleeptime

Establece el número de segundos de inactividad entre ciclos de definición de pesos. El valor por omisión es 7.

seg

Entero que representa el tiempo de inactividad en segundos. El rango válido es de 0 a 2.147.460.

start

Inicia la recopilación de métricas y la definición de pesos.

stop

Detiene la recopilación de métricas y la definición de pesos.

Ejemplos

- Añadir un consultor de conmutador con un identificador de conmutador sc1, la dirección IP 9.37.50.17 y el nombre de comunidad comm1:

```
ccocontrol consultant add sc1 address 9.37.50.17 community comm2
```

- Iniciar el registro cronológico binario:

```
ccocontrol consultant binarylog sc1 start
```

- Ver un informe sobre las características del consultor de conmutador sc1:

```
ccocontrol consultant report sc1
```

Este mandato genera una salida parecida a la siguiente:

```
Consultor sc1 conectado al conmutador en 9.37.50.1:cn1
```

```
El consultor se ha iniciado
```

```
Tiempo de inactividad      = 7
```

```
Sensibilidad               = 5
```

```
Nivel anotación cronológica = 5
```

```
Tamaño de anotaciones      = 1,048,576
```

```
Contenido de propietario:
```

```
  contenido de propietario ocl
```

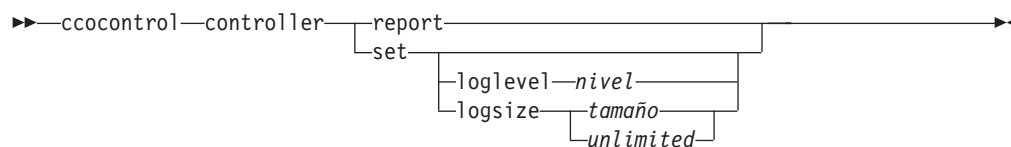
- Establecer el tiempo de inactividad entre los ciclos de definición de pesos para el ID de conmutador sc1 en 10 segundos:

```
ccocontrol consultant set sc1 sleeptime 10
```

- Iniciar la recopilación de métricas y la definición de pesos para el ID de consultor sc1:

```
ccocontrol consultant start sc1
```

cococontrol controller — gestionar el controlador



report

Muestra características del controlador. La información de la versión se muestra como parte de este informe.

set

Establece las características del controlador.

loglevel

Establece el nivel en el que el controlador registra las actividades. El valor por omisión es 1.

nivel

El número del nivel de 0 a 5. El valor por omisión es 1. Los valores posibles son:

- 0 = Ninguno
- 1 = Mínimo
- 2 = Básico
- 3 = Moderado
- 4 = Avanzado
- 5 = Detallado

logsize

Establece el número máximo de bytes anotados en el archivo de anotaciones cronológicas. El valor por omisión es 1048576. Cuando se establece un tamaño máximo para el archivo de anotaciones cronológicas, el texto del archivo vuelve al principio; es decir, cuando el archivo alcanza el tamaño especificado, las entradas subsiguientes se anotarán al principio del archivo y se grabarán encima de las entradas de anotaciones cronológicas anteriores. El tamaño de las anotaciones cronológicas no puede establecerse más pequeño que el tamaño actual de las anotaciones cronológicas. Las entradas de las anotaciones cronológicas incluyen la indicación de la hora para poder saber el orden en el que se anotaron. Cuando más alto se establezca el nivel de anotaciones cronológicas, más cuidado deberá tener al elegir el tamaño de las anotaciones cronológicas porque, cuando el registro cronológico está establecido en los niveles más altos, puede quedarse sin espacio rápidamente.

tamaño | unlimited

Número máximo de bytes anotados en las anotaciones cronológicas del consultor. Puede especificar un número positivo mayor que cero o la palabra **unlimited**. Es posible que el archivo de anotaciones cronológicas no alcance el tamaño máximo exacto antes de empezar a sobrescribir porque el tamaño de las entradas del archivo varían.

Ejemplos

- Mostrar un informe en el controlador:
`cococontrol controller report`

Este mandato genera una salida parecida a la siguiente:

Informe del controlador:

Versión Versión: 05.00.00.00 - 03/21/2002-09:49:57-EST

Nivel de anotaciones . . 1

Tamaño de anotaciones . . 1048576

Archivo de configuración. config1.xml

Consultores:

El consultor consult1 se ha iniciado

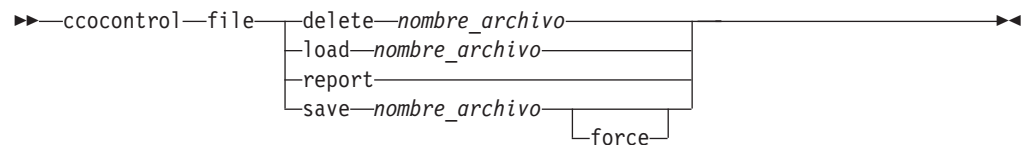
- Establecer el nivel de registro cronológico en cero para obtener un mejor rendimiento:

`ccocontrol set loglevel 0`

- Establecer el tamaño de las anotaciones cronológicas del controlador en 1.000.000 bytes:

`ccocontrol controller set logsize 1000000`

ccocontrol file — gestionar archivos de configuración



delete

Suprime el archivo de configuración especificado.

nombre_archivo

Un archivo de configuración. La extensión de archivo debe ser .xml. Si no se especifica esta extensión, se supondrá.

load

Carga la configuración almacenada en el archivo especificado.

Nota: Cuando se carga un archivo se añadirá a la configuración que se ejecuta la configuración almacenada en dicho archivo. Si desea cargar una *nueva* configuración, debe detener y reiniciar el servidor antes de cargar el archivo.

report

Lista los archivos de configuración.

save

Guarda la configuración actual en el archivo especificado.

Nota: Los archivos se guardan y se cargan de los siguientes directorios:

- Sistemas AIX: **/opt/ibm/edge/lb/servers/configurations/cco**
- Sistemas Linux: **/opt/ibm/edge/lb/servers/configurations/cco**
- Sistemas Solaris: **/opt/ibm/edge/lb/servers/configurations/cco**
- Sistemas Windows:

Directorio de instalación (por omisión): **C:\Archivos de programa\ibm\edge\lb\servers\configurations\cco**

force

Guarda en un archivo existente.

Ejemplos

- Suprimir un archivo denominado file1:
`ccocontrol file delete file1`
- Añadir la configuración del archivo a la configuración actual:
`ccocontrol file load config2`
- Ver un informe de archivos guardados anteriormente:
`ccocontrol file report`

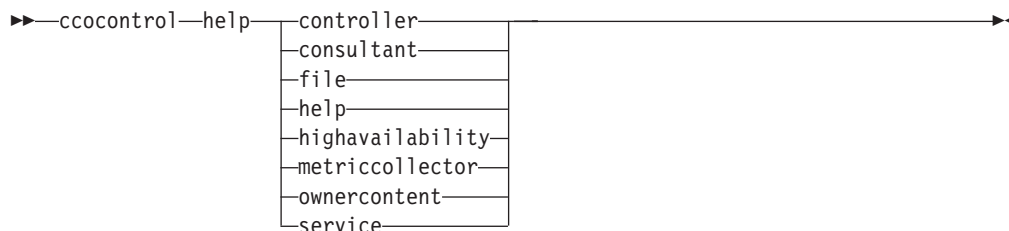
Este mandato genera una salida parecida a la siguiente:

INFORME SOBRE EL ARCHIVO:

```
-----  
file1.xml  
file2.xml  
file3.xml
```

- Guardar el archivo de configuración en un archivo llamado config2.xml:
`ccocontrol file save config2`

cococontrol help — mostrar o imprimir ayuda para este mandato



Ejemplos

- Para obtener ayuda sobre el mandato cococontrol, escriba:

```
cococontrol help
```

Este mandato genera una salida parecida a la siguiente:

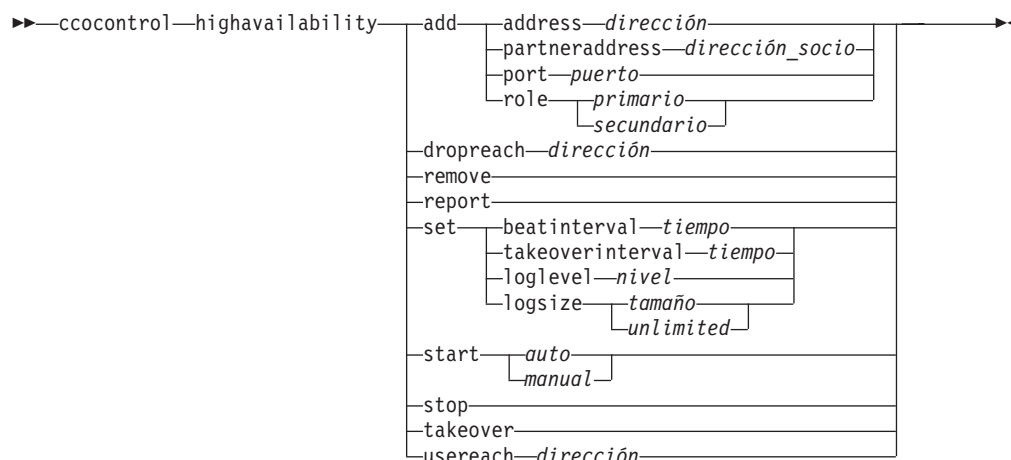
Están disponibles los siguientes mandatos:

controller	- opera en el controlador
consultant	- opera en consultores de conmutador
file	- opera en archivos de configuración
help	- opera en ayuda
highavailability	- opera en alta disponibilidad
metriccollector	- opera en recopiladores de métricas
ownerContent	- opera en contenido de propietario
service	- opera en servicios

- En la sintaxis de ayuda en línea se utilizan los siguientes símbolos:

< >	Los corchetes angulares se especifican alrededor de parámetros o una secuencia de caracteres.
[]	Los corchetes se especifican alrededor de elementos opcionales.
	Una barra vertical separa alternativas rodeadas de corchetes y corchetes angulares.
:	Dos puntos es un separador que se especifica entre nombres; por ejemplo, consultor1:contenido propietario1 .

cococontrol highavailability — controlar alta disponibilidad



add

Configura un nodo de alta disponibilidad, un socio y destinos de alcance.

address

Dirección de la que se reciben los pulsos.

dirección

Dirección IP del nodo de alta disponibilidad.

partneraddress

Dirección a la que se envían los pulsos. Se trata de la dirección IP o el nombre de sistema principal configurado en el nodo asociado. Esta dirección se utiliza para comunicarse con la máquina de alta disponibilidad asociada.

dirección

Dirección IP del asociado.

port

Puerto utilizado para comunicarse con el socio. El valor por omisión es 12345.

puerto

El número del puerto.

role

El rol de alta disponibilidad.

primario | *secundario*

El rol primario o secundario.

dropreach

Elimina este destino de alcance de los criterios de alta disponibilidad.

dirección

Dirección IP del destino de alcance.

remove

Elimina el nodo, el socio y el destino de alcance de la configuración de alta disponibilidad. Antes de utilizar este mandato debe detenerse la alta disponibilidad.

report

Muestra información de alta disponibilidad.

set

Establece las características de alta disponibilidad.

beatinterval

Establece la frecuencia, en milisegundos, con la que se envían pulsos al socio.
El valor por omisión es 500.

tiempo

Entero positivo que representa el intervalo de pulso, en milisegundos.

takeoverinterval

Establece el intervalo de tiempo, en milisegundos, que debe transcurrir (durante el que no se recibe ningún pulso) antes de que se produzca una toma de control. El valor por omisión es 2000.

tiempo

Entero positivo que representa el intervalo de toma de control, en milisegundos.

loglevel

Establece el nivel en el que se registran las actividades. El valor por omisión es 1.

nivel

El número del nivel de 0 a 5. El valor por omisión es 1. Los valores posibles son:

- 0 = Ninguno
- 1 = Mínimo
- 2 = Básico
- 3 = Moderado
- 4 = Avanzado
- 5 = Detallado

logsize

Establece el número máximo de bytes anotados en el archivo de anotaciones cronológicas de alta disponibilidad. El valor por omisión es 1048576. Cuando se establece un tamaño máximo para el archivo de anotaciones cronológicas, el texto del archivo vuelve al principio; es decir, cuando el archivo alcanza el tamaño especificado, las entradas subsiguientes se anotarán al principio del archivo y se grabarán encima de las entradas de anotaciones cronológicas anteriores. El tamaño de las anotaciones cronológicas no puede establecerse más pequeño que el tamaño actual de las anotaciones cronológicas. Las entradas de las anotaciones cronológicas incluyen la indicación de la hora para poder saber el orden en el que se anotaron. Cuando más alto se establezca el nivel de anotaciones cronológicas, más cuidado deberá tener al elegir el tamaño de las anotaciones cronológicas porque, cuando el registro cronológico está establecido en los niveles más altos, puede quedarse sin espacio rápidamente.

tamaño | unlimited

Número máximo de bytes anotados en las anotaciones cronológicas de alta disponibilidad. Puede especificar un número positivo mayor que cero o la palabra **unlimited**. Es posible que el archivo de anotaciones cronológicas no alcance el tamaño máximo exacto antes de empezar a sobrescribir porque el tamaño de las entradas del archivo varían.

start

Inicia el uso de alta disponibilidad. Antes de utilizar este mandato se debe configurar un nodo de alta disponibilidad, un socio y destino de alcance.

auto | manual

Determina si se inicia la alta disponibilidad con una estrategia de recuperación automática o manual.

stop

Deja de utilizar la alta disponibilidad.

takeover

Asume el control desde el nodo de alta disponibilidad activo.

usereach

La dirección del destino de alcance que empezará a utilizar la alta disponibilidad. Añada un destino de alcance al que pueda accederse mediante un mandato ping, para que los socios de alta disponibilidad puedan determinar la accesibilidad de sus destinos.

dirección

Dirección IP del destino de alcance.

Ejemplos

- Añadir un nodo de alta disponibilidad con la dirección IP 9.37.50.17 con un rol primario en el puerto 12345 y la dirección de socio 9.37.50.14:

```
cococontrol highavailability add  
address 9.37.50.17 role primary port 12345 partneraddress 9.37.50.14
```

- Añadir la dirección de destino de alcance 9.37.50.9:

```
cococontrol highavailability usereach 9.37.50.9
```

- Eliminar la dirección de destino de alcance 9.37.50.9:

```
cococontrol highavailability dropreach 9.37.50.9
```

- Iniciar alta disponibilidad con una estrategia de recuperación manual:

```
cococontrol highavailability start manual
```

- Obtener una instantánea de estadísticas de alta disponibilidad:

```
cococontrol highavailability report
```

Este mandato genera una salida parecida a la siguiente:

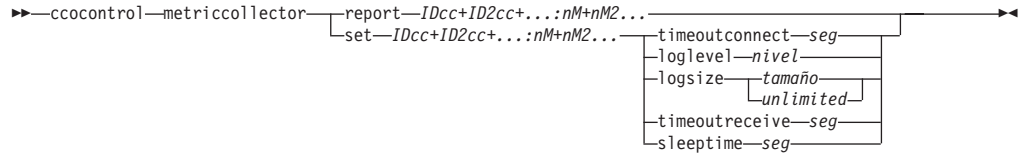
Estado de alta disponibilidad:

```
Nodo . . . . . primario  
Dirección de nodo . . . . 9.37.50.17  
Puerto . . . . . 12345  
Dirección de socio . . . . 9.37.50.14  
Estrategia de recuperación manual  
Intervalo de pulso . . . . 500  
Intervalo de toma control. 2000  
Estado . . . . . desocupado  
Subestado. . . . . no sincronizado
```

Estado de accesibilidad : Nodo/Socio

Destinos de alcance no configurados

cococontrol metriccollector — configurar recopilador de métricas



report

Muestra las características de un recopilador de métricas.

IDcc (ID de consultor de conmutador)

Serie definida por el usuario que hace referencia al consultor.

nM (nombre de métrica)

Nombre que identifica la métrica proporcionada o personalizada.

set

Establece las características de un recopilador de métricas.

timeoutconnect

Establece cuánto tiempo espera el recopilador de métricas antes de notificar que una conexión es anómala.

seg

Entero positivo que representa el tiempo en segundos durante el que el recopilador de métricas espera antes de notificar que se ha producido una anomalía en una conexión a un servicio.

loglevel

Establece el nivel en el que el consultor especificado registra las actividades. El valor por omisión es 1.

nivel

El número del nivel. El valor por omisión es 1. Cuanto más alto sea el número, más información se anotará en las anotaciones cronológicas del consultor. Los valores posibles son:

- 0 = Ninguno
- 1 = Mínimo
- 2 = Básico
- 3 = Moderado
- 4 = Avanzado
- 5 = Detallado

logsize

Establece el número máximo de bytes anotados en el archivo de anotaciones cronológicas. El valor por omisión es 1048576. Cuando se establece un tamaño máximo para el archivo de anotaciones cronológicas, el texto del archivo vuelve al principio; es decir, cuando el archivo alcanza el tamaño especificado, las entradas subsiguientes se anotarán al principio del archivo y se grabarán encima de las entradas de anotaciones cronológicas anteriores. El tamaño de las anotaciones cronológicas no puede establecerse más pequeño que el tamaño actual de las anotaciones cronológicas. Las entradas de las anotaciones cronológicas incluyen la indicación de la hora para poder saber el orden en el que se anotaron. Cuando más alto se establezca el nivel de anotaciones cronológicas, más cuidado deberá tener al elegir el tamaño de las anotaciones

cronológicas porque, cuando el registro cronológico está establecido en los niveles más altos, puede quedarse sin espacio rápidamente.

tamaño | unlimited

Número máximo de bytes anotados en las anotaciones cronológicas del consultor. Puede especificar un número positivo mayor que cero o la palabra **unlimited**. Es posible que el archivo de anotaciones cronológicas no alcance el tamaño máximo exacto antes de empezar a sobrescribir porque el tamaño de las entradas del archivo varían.

timeoutreceive

Establece cuánto tiempo el consultor espera antes de informar de que no se ha podido realizar una recepción del servicio.

seg

Entero positivo que representa la cantidad de tiempo en segundos que el consultor espera antes de informar que no se ha podido realizar una recepción de un servicio.

sleeptime

Establece la cantidad de tiempo en segundos que el recopilador de métricas permanece inactivo entre los ciclos de recolección de métricas.

Entero positivo que representa el número de segundos de tiempo de inactividad.

Ejemplos

- Ver un informe sobre las características de un recopilador de métricas:

```
cococontrol metriccollector report sc1:http
```

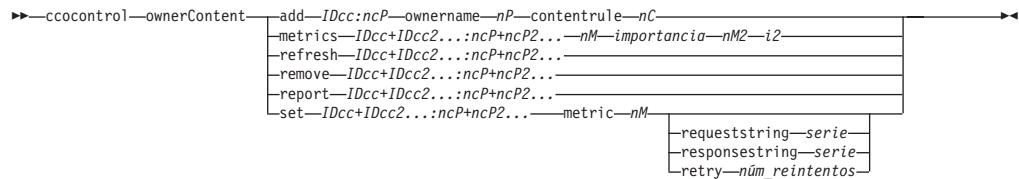
Este mandato genera una salida parecida a la siguiente:

```
MetricCollector sc1:http
collected metric(s).... http
loglevel..... 5
logSize..... 1048576
sleepTimeSeconds..... 7
timeoutConnectSeconds.. 21
timeoutReceiveSeconds.. 21
```

- Establecer un valor de timeoutconnect de 15 segundos y un valor de logsize de unlimited para el consultor de conmutador sc1 y la métrica http:

```
cococontrol metriccollector set sc1:http timeoutconnect 15 logsize unlimited
```

cococontrol ownercontent — controlar el nombre de propietario y la norma de contenido



add

Añade un contenido de propietario al consultor especificado.

IDcc (ID de consultor de conmutador)

Serie definida por el usuario que representa al consultor.

ncP (nombre de contenido de propietario)

Serie definida por el usuario que representa el nombre del propietario y la norma de contenido del conmutador.

ownername

Nombre configurado en el conmutador que identifica la configuración de propietario.

nP (nombre de propietario)

Serie de texto exclusivo sin espacios. El nombre de propietario debe ser el mismo que el especificado en el conmutador Cisco.

contentrule

Nombre configurado en el conmutador que identifica la configuración de normas de contenido del propietario.

Nc (nombre de contenido)

Serie de texto exclusivo sin espacios. El nombre de contenido debe ser el mismo que el especificado en el conmutador Cisco.

metrics

Especifica el conjunto de métricas utilizado en el cálculo de pesos y la importancia de cada métrica. La importancia se expresa como porcentaje del total. La suma de los valores de importancia debe ser 100. La métrica puede ser cualquier combinación de la métrica de datos de conexiones, métrica de asesor de aplicaciones y métrica de Metric Server. Los valores por omisión son las métricas de conexión activa (activeconn) y velocidad de conexión (connrate) con una importancia de 50/50.

nM (nombre de métrica)

Nombre que identifica el recopilador de métricas que recopilará las medidas para determinar el peso del servidor.

A continuación se muestra una lista de nombres de métrica válidos y sus puertos asociados:

Nombre del asesor	Protocolo	Puerto
connect	ICMP	12345
db2	private	50000
dns	DNS	53
ftp	FTP	21

Nombre del asesor	Protocolo	Puerto
http	HTTP	80
https	SSL	443
cachingproxy	HTTP (mediante Caching Proxy)	80
imap	IMAP	143
ldap	LDAP	389
nntp	NNTP	119
ping	PING	0
pop3	POP3	110
sip	SIP	5060
smtp	SMTP	25
ssl	SSL	443
telnet	Telnet	23
WLM	private	10.007
activeconn	n/a	n/a
connrate	n/a	n/a
cpuload	n/a	n/a
memload	n/a	n/a

importancia

Número de 0 a 100 que representa la importancia de esta métrica en el cálculo de pesos de servidores.

refresh

Renueva los servicios configurados con información de Conmutador Cisco CSS.

remove

Elimina un contenido de propietario.

report

Informa de las características de contenido de propietario.

set

Establece las características del contenido de propietario.

metric

Establece las características de una métrica.

Nm

Nombre de la métrica que desee.

requeststring

Establece una serie de petición para la métrica especificada. Representa la petición que ha enviado un recopilador de métricas para recopilar información de métricas.

serie

Serie de petición que ha enviado el recopilador de métricas al servidor.

responsestring

Establece una serie de respuesta para la métrica especificada. La serie de respuesta especificada la utiliza el recopilador de métricas para comparar las respuestas que recibe de servidores y posteriormente determinar la disponibilidad de servidores.

serie

Serie de respuesta con la que el recopilador de métricas compara las respuestas de servidor recibidas.

retry

El parámetro retry establece el número de reintentos que se pueden llevar a cabo antes de marcar un servidor como inactivo.

núm_reintentos

Número entero mayor que o igual a cero. Este valor no debe ser mayor que 3. Si la palabra clave retry no está configurada, el número de reintentos tendrá el valor por omisión de cero.

Ejemplos

- Añadir un ownerContent llamado oc1 (con el nombre de propietario owner1 y el nombre de contenido content1) al ID de consultor de conmutador sc1:

```
cococontrol ownerContent add sc1:oc1 ownername owner1 contentrule content1
```

- Especificar la proporción 50 en la métrica activeconn y http:

```
cococontrol ownerContent metrics sc1:oc1 activeconn 50 http 50
```

- Ver un informe de características de contenido de propietario:

```
cococontrol ownerContent report sc1:oc1
```

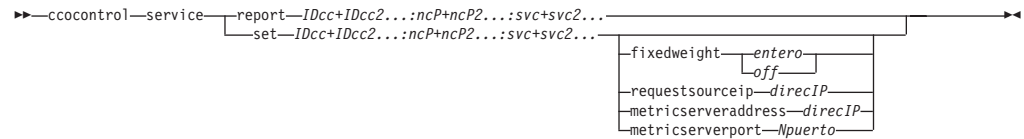
Este mandato genera una salida parecida a la siguiente:

```
ownerContent sc1:oc1
  Weightbound = 10
  Metric activeconn has proportion 25
    ResponseString... n/a
    RequestString.... n/a
  Metric http has proportion 50
    ResponseString... n/a
    RequestString.... n/a
  Metric connrate has proportion 25
    ResponseString... n/a
    RequestString.... n/a
  Contains Service t3
  Contains Service t2
  Contains Service t1
```

- Establecer una serie de petición http:

```
cococontrol ownerContent set sc1:oc1 metric http requeststring getCookie
```

cococontrol service — configurar un servicio



report

Muestra las características de servicios.

IDcc (ID de consultor de conmutador)

Serie definida por el usuario que representa al consultor.

ncP (nombre de contenido de propietario)

Serie definida por el usuario que representa el nombre del propietario y la norma de contenido del conmutador.

svc (servicio)

Serie definida por el usuario en el conmutador que representa al servicio.

set

Establece características de servicios.

fixedweight

Establece un peso fijo para este servicio. El valor por omisión es off.

entero | off

Entero positivo que oscila entre 0 y 10, que representa el peso fijo de este servicio, o la palabra **off** que especifica que no hay peso fijo.

requestsourceip

Establece la dirección desde la que ponerse en contacto con el servicio para obtener las peticiones de aplicación.

dirIP (dirección IP)

Dirección IP desde la que ponerse en contacto con el servicio; puede especificarse como nombre simbólico o en formato de dirección IP.

metricserveraddress

Establece la dirección en la que ponerse en contacto con el servicio para obtener peticiones de Metric Server.

dirIP (dirección IP)

Dirección IP de Metric Server como nombre simbólico o en formato de dirección IP.

metricserverport

Establece el puerto que debe utilizarse para ponerse en contacto con Metric Server.

Npuerto (número de puerto)

Número de puerto utilizado para ponerse en contacto con Metric Server.

Ejemplos

- Mostrar un informe sobre el servicio t1 para el consultor sc1:

```
cococontrol service report sc1:oc1:t1
```

Este mandato genera una salida parecida a la siguiente:

El servicio sc1:oc1:ta tiene un peso de 10

El peso fijo tiene el valor off

IP origen solicitud .. 9.27.24.156

```
Puerto de aplicación . 80
Direc. MetricServer .. 1.0.0.1
Puerto MetricServer .. 10004
  activeconn de métrica tiene el valor -99
  http de métrica tiene el valor -99
  connrate de métrica tiene el valor -99
```

- Establecer una dirección de Metric Server para el servicio t2:
ccocontrol service set sc1:ocl:t2 metricserveraddress 9.37.50.17

Capítulo 30. Referencia de mandatos para Nortel Alteon Controller

En este capítulo se describe cómo utilizar los siguientes mandatos **nalcontrol** para Nortel Alteon Controller:

- “**nalcontrol consultant** — configurar y controlar un consultor” en la página 450
- “**nalcontrol controller** — gestionar el controlador” en la página 453
- “**nalcontrol file** — gestionar archivos de configuración” en la página 455
- “**nalcontrol help** — mostrar o imprimir ayuda para este mandato” en la página 456
- “**nalcontrol highavailability** — controlar alta disponibilidad” en la página 457
- “**nalcontrol metriccollector** — configurar recopilador de métricas” en la página 460
- “**nalcontrol service** — configurar un servicio” en la página 464
- “**nalcontrol server** — configurar un servidor” en la página 462

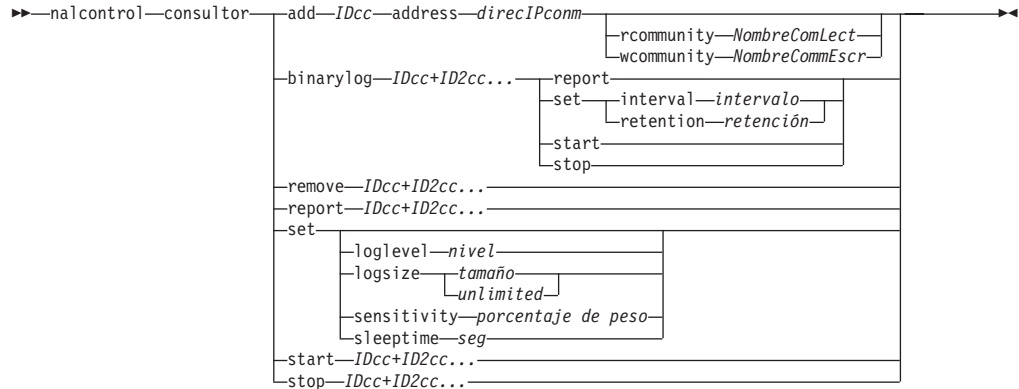
Puede utilizar una versión abreviada de los parámetros del mandato **nalcontrol** escribiendo las letras exclusivas de los parámetros. Por ejemplo, para obtener ayuda sobre el mandato para guardar archivos, puede escribir **nalcontrol he f** en lugar de **nalcontrol help file**.

Para obtener el indicador de mandatos **nalcontrol**, escriba **nalcontrol**.

Para finalizar la interfaz de línea de mandatos, escriba **exit** o **quit**.

Nota: Debe utilizar caracteres del idioma inglés en todos los valores de parámetros de mandatos. Las únicas excepciones son los nombres de sistema principal (que se utilizan en los mandatos del servidor) y los nombres de archivo (que se utilizan en los mandatos de archivo).

nalcontrol consultant — configurar y controlar un consultor



add

Añade un consultor de conmutador.

IDcc

Serie definida por el usuario que hace referencia al consultor.

address

Dirección IP de Conmutador Nortel Alteon Web al que el consultor proporciona pesos.

direcIPconn

Dirección IP del conmutador.

rcommunity

Nombre de comunidad de lectura utilizado en comunicaciones de obtención SNMP con el Conmutador Nortel Alteon Web. El valor por omisión es public.

NombreComLect

Serie que representa el nombre de comunidad de lectura, tal como se ha configurado en el Conmutador Nortel Alteon Web. El valor por omisión es public.

wcommunity

Nombre de comunidad de escritura utilizado en las comunicaciones de establecimiento SNMP.

NombreCommEscr

Serie que representa el nombre de comunidad de escritura, tal como se ha configurado en el Conmutador Nortel Alteon Web. El valor por omisión es private.

binarylog

Controla el registro cronológico en binario para un consultor.

report

Informa sobre las características del registro cronológico.

set

Establece la frecuencia, en segundos, con la que la información se escribe en las anotaciones cronológicas en binario. La característica de registro cronológico permite almacenar la información de servicio en archivos de anotaciones cronológicas en binario para cada servicio definido en la configuración. La información se graba en las anotaciones cronológicas sólo cuando hayan transcurrido los segundos especificados en el intervalo de anotaciones

cronológicas después de anotarse el último registro en el archivo de anotaciones cronológicas. El intervalo de registro cronológico en binario por omisión es 60.

interval

Establece el número de segundos entre las entradas de las anotaciones cronológicas en binario.

retention

Establece el número de horas que se conservan los archivos de anotaciones cronológicas en binario.

start

Inicia el registro cronológico en binario.

stop

Detiene el registro cronológico en binario.

remove

Elimina un consultor de conmutador.

report

Informa sobre las características de consultores del conmutador.

set

Establece las características de consultores de conmutador.

loglevel

Establece el nivel en el que el consultor de conmutador registra las actividades. El valor por omisión es 1.

nivel

El número del nivel de 0 a 5. El valor por omisión es 1. Los valores posibles son:

- 0 = Ninguno
- 1 = Mínimo
- 2 = Básico
- 3 = Moderado
- 4 = Avanzado
- 5 = Detallado

logsize

Establece el número máximo de bytes anotados en el archivo de anotaciones cronológicas. El valor por omisión es 1048576. Cuando se establece un tamaño máximo para el archivo de anotaciones cronológicas, el texto del archivo vuelve al principio; es decir, cuando el archivo alcanza el tamaño especificado, las entradas subsiguientes se anotarán al principio del archivo y se grabarán encima de las entradas de anotaciones cronológicas anteriores. El tamaño de las anotaciones cronológicas no puede establecerse más pequeño que el tamaño actual de las anotaciones cronológicas. Las entradas de las anotaciones cronológicas incluyen la indicación de la hora para poder saber el orden en el que se anotaron. Cuando más alto se establezca el nivel de anotaciones cronológicas, más cuidado deberá tener al elegir el tamaño de las anotaciones cronológicas porque, cuando el registro cronológico está establecido en los niveles más altos, puede quedarse sin espacio rápidamente.

tamaño

Número máximo de bytes anotados en las anotaciones cronológicas del consultor. Puede especificar un número positivo mayor que cero o la palabra

unlimited. Es posible que el archivo de anotaciones cronológicas no alcance el tamaño máximo exacto antes de empezar a sobrescribir porque el tamaño de las entradas del archivo varían.

sensitivity

Indica la cantidad de cambio que debe tener lugar entre los pesos anteriores y nuevos para que el peso cambie. Para que el peso cambie, la diferencia entre el peso nuevo y el antiguo debe ser mayor que el porcentaje de sensibilidad. El rango válido es de 0 a 100; el valor por omisión es 5.

porcentaje de peso

Entero que oscila entre 0 y 100, que representa el valor de sensibilidad.

sleeptime

Establece el número de segundos de inactividad entre ciclos de definición de pesos. El valor por omisión es 7.

segundos

Entero que representa el tiempo de inactividad en segundos. El rango válido es de 0 a 2.147.460.

start

Inicia la recopilación de métricas y la definición de pesos.

stop

Detiene la recopilación de métricas y la definición de pesos.

Ejemplos

- Añadir un consultor de conmutador con un identificador de conmutador sc1, la dirección IP 9.37.50.17:

```
nalcontrol consultant add sc1 address 9.37.50.17
```

- Iniciar el registro cronológico binario:

```
nalcontrol consultant binarylog sc1 start
```

- Ver un informe sobre las características del consultor de conmutador sc1:

```
nalcontrol consultant report sc1
```

Este mandato genera una salida parecida a la siguiente:

```
ID de consultor: sc1 Direc. IP conmutador: 9.37.50.1
Comunidad de lectura: public
Comunidad de lectura: private
El consultor se ha iniciado
    Tiempo de inactividad      = 7
    Sensibilidad               = 5
    Nivel anotación cronológica = 5
    Tamaño de anotaciones      = 1,048,576
    Servicio(s):
        Servicio svc1
```

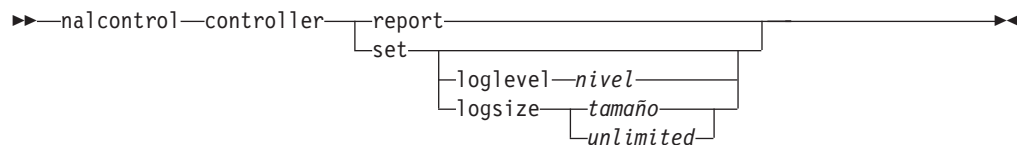
- Establecer el tiempo de inactividad entre los ciclos de definición de pesos para el ID de conmutador sc1 en 10 segundos:

```
nalcontrol consultant set sc1 sleeptime 10
```

- Iniciar la recopilación de métricas y la definición de pesos para el ID de consultor sc1:

```
nalcontrol consultant start sc1
```

nalcontrol controller — gestionar el controlador



report

Muestra características del controlador. La información de la versión se muestra como parte de este informe.

set

Establece las características del controlador.

loglevel

Establece el nivel en el que el controlador registra las actividades. El valor por omisión es 1.

nivel

El número del nivel de 0 a 5. El valor por omisión es 1. Los valores posibles son:

- 0 = Ninguno
- 1 = Mínimo
- 2 = Básico
- 3 = Moderado
- 4 = Avanzado
- 5 = Detallado

logsize

Establece el número máximo de bytes anotados en el archivo de anotaciones cronológicas. El valor por omisión es 1048576. Cuando se establece un tamaño máximo para el archivo de anotaciones cronológicas, el texto del archivo vuelve al principio; es decir, cuando el archivo alcanza el tamaño especificado, las entradas subsiguientes se anotarán al principio del archivo y se grabarán encima de las entradas de anotaciones cronológicas anteriores. El tamaño de las anotaciones cronológicas no puede establecerse más pequeño que el tamaño actual de las anotaciones cronológicas. Las entradas de las anotaciones cronológicas incluyen la indicación de la hora para poder saber el orden en el que se anotaron. Cuando más alto se establezca el nivel de anotaciones cronológicas, más cuidado deberá tener al elegir el tamaño de las anotaciones cronológicas porque, cuando el registro cronológico está establecido en los niveles más altos, puede quedarse sin espacio rápidamente.

tamaño | unlimited

Número máximo de bytes anotados en las anotaciones cronológicas del consultor. Puede especificar un número positivo mayor que cero o la palabra **unlimited**. Es posible que el archivo de anotaciones cronológicas no alcance el tamaño máximo exacto antes de empezar a sobrescribir porque el tamaño de las entradas del archivo varían.

Ejemplos

- Mostrar un informe en el controlador:
`nalcontrol controller report`

Este mandato genera una salida parecida a la siguiente:

Informe del controlador:

Versión Versión: 05.00.00.00 - 03/21/2002-09:49:57-EST

Nivel de anotaciones . . 1

Tamaño de anotaciones . . 1048576

Archivo de configuración. config1.xml

Consultores:

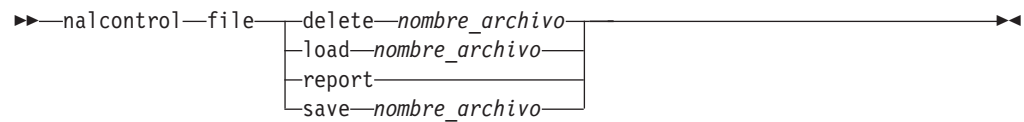
El consultor consult1 se ha iniciado

- Establecer el nivel de registro cronológico en cero para obtener un mejor rendimiento:

nalcontrol set loglevel 0

- Establecer el tamaño de las anotaciones cronológicas del controlador en 1.000.000 bytes:

nalcontrol controller set logsize 1000000



delete

Suprime el archivo de configuración especificado.

nombre_archivo

Un archivo de configuración. La extensión de archivo debe ser .xml. Si no se especifica esta extensión, se supondrá.

load

Carga la configuración almacenada en el archivo especificado.

Nota: Cuando se carga un archivo se añadirá a la configuración que se ejecuta la configuración almacenada en dicho archivo. Si desea cargar una *nueva* configuración, debe detener y reiniciar el servidor antes de cargar el archivo.

report

Lista los archivos de configuración.

save

Guarda la configuración actual en el archivo especificado.

Nota: Los archivos se guardan y se cargan de los siguientes directorios:

- Sistemas AIX: `/opt/ibm/edge/lb/servers/configurations/nal`
- Sistemas Linux: `/opt/ibm/edge/lb/servers/configurations/nal`
- Sistemas Solaris: `/opt/ibm/edge/lb/servers/configurations/nal`
- Sistemas Windows:

Vía de acceso al directorio de instalación común — C:\Archivos de programa\ibm\edge\lb\servers\configurations\nal

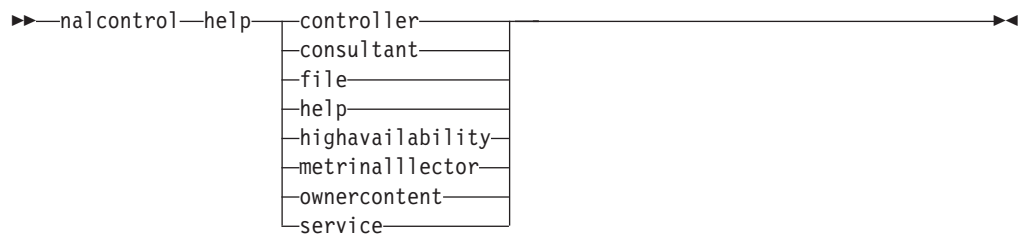
Vía de acceso de directorio de instalación nativo — C:\Archivos de programa\ibm\lb\servers\configurations\nal

Ejemplos

- Suprimir un archivo denominado file1:
`nalcontrol file delete file1`
 - Cargar un nuevo archivo de configuración para que sustituya a la configuración actual:
`nalcontrol file load config2`
 - Ver un informe de archivos guardados anteriormente:
`nalcontrol file report`
- Este mandato genera una salida parecida a la siguiente:
- INFORME SOBRE EL ARCHIVO:

file1.xml
file2.xml
file3.xml
- Guardar el archivo de configuración en un archivo llamado config2:
`nalcontrol file save config2`

nalcontrol help — mostrar o imprimir ayuda para este mandato



Ejemplos

- Para obtener ayuda sobre el mandato nalcontrol, escriba:

`nalcontrol help`

Este mandato genera una salida parecida a la siguiente:

Están disponibles los siguientes mandatos:

controller	- opera en el controlador
consultant	- opera en consultores de conmutador
file	- opera en archivos de configuración
help	- opera en ayuda
highavailability	- opera en alta disponibilidad
metriccollector	- opera en recopiladores de métricas
server	- opera en servidores
service	- opera en servicios

- En la sintaxis de ayuda en línea se utilizan los siguientes símbolos:

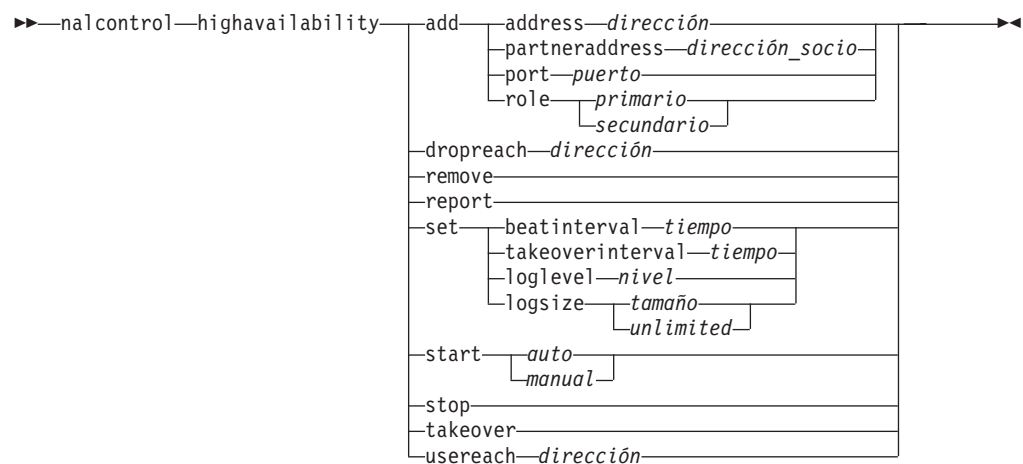
< > Los corchetes angulares se especifican alrededor de parámetros o una secuencia de caracteres.

[] Los corchetes se especifican alrededor de elementos opcionales.

| Una barra vertical separa alternativas rodeadas de corchetes y corchetes angulares.

: Dos puntos es un separador que se especifica entre nombres; por ejemplo, **consultor1:servicio1**.

nalcontrol highavailability — controlar alta disponibilidad



add
Configura un nodo de alta disponibilidad, un socio y destinos de alcance.

address
Dirección de la que se reciben los pulsos.

dirección
Dirección IP del nodo de alta disponibilidad.

partneraddress
Dirección a la que se envían los pulsos. Se trata de la dirección IP o el nombre de sistema principal configurado en el nodo asociado. Esta dirección se utiliza para comunicarse con la máquina de alta disponibilidad asociada.

dirección
Dirección IP del asociado.

port
Puerto utilizado para comunicarse con el socio. El valor por omisión es 12345.

puerto
El número del puerto.

role
El rol de alta disponibilidad.

primario | secundario
El rol primario o secundario.

dropreach
Elimina este destino de alcance de los criterios de alta disponibilidad.

dirección
Dirección IP del destino de alcance.

remove
Elimina el nodo, el socio y el destino de alcance de la configuración de alta disponibilidad. Antes de utilizar este mandato debe detenerse la alta disponibilidad.

report
Muestra información de alta disponibilidad.

set

Establece las características de alta disponibilidad.

beatinterval

Establece la frecuencia, en milisegundos, con la que se envían pulsos al socio.
El valor por omisión es 500.

tiempo

Entero positivo que representa el intervalo de pulso, en milisegundos.

takeoverinterval

Establece el intervalo de tiempo, en milisegundos, que debe transcurrir (durante el que no se recibe ningún pulso) antes de que se produzca una toma de control. El valor por omisión es 2000.

tiempo

Entero positivo que representa el intervalo de toma de control, en milisegundos.

loglevel

Establece el nivel en el que se registran las actividades. El valor por omisión es 1.

nivel

El número del nivel de 0 a 5. El valor por omisión es 1. Los valores posibles son:

- 0 = Ninguno
- 1 = Mínimo
- 2 = Básico
- 3 = Moderado
- 4 = Avanzado
- 5 = Detallado

logsize

Establece el número máximo de bytes anotados en el archivo de anotaciones cronológicas de alta disponibilidad. El valor por omisión es 1048576. Cuando se establece un tamaño máximo para el archivo de anotaciones cronológicas, el texto del archivo vuelve al principio; es decir, cuando el archivo alcanza el tamaño especificado, las entradas subsiguientes se anotarán al principio del archivo y se grabarán encima de las entradas de anotaciones cronológicas anteriores. El tamaño de las anotaciones cronológicas no puede establecerse más pequeño que el tamaño actual de las anotaciones cronológicas. Las entradas de las anotaciones cronológicas incluyen la indicación de la hora para poder saber el orden en el que se anotaron. Cuando más alto se establezca el nivel de anotaciones cronológicas, más cuidado deberá tener al elegir el tamaño de las anotaciones cronológicas porque, cuando el registro cronológico está establecido en los niveles más altos, puede quedarse sin espacio rápidamente.

tamaño | unlimited

Número máximo de bytes anotados en las anotaciones cronológicas de alta disponibilidad. Puede especificar un número positivo mayor que cero o la palabra **unlimited**. Es posible que el archivo de anotaciones cronológicas no alcance el tamaño máximo exacto antes de empezar a sobrescribir porque el tamaño de las entradas del archivo varían.

start

Inicia el uso de alta disponibilidad. Antes de utilizar este mandato se debe configurar un nodo de alta disponibilidad, un socio y destino de alcance.

auto | manual

Determina si se inicia la alta disponibilidad con una estrategia de recuperación automática o manual.

stop

Deja de utilizar la alta disponibilidad.

takeover

Asume el control desde el nodo de alta disponibilidad activo.

usereach

La dirección del destino de alcance que empezará a utilizar la alta disponibilidad. Añada un destino de alcance al que pueda accederse mediante un mandato ping, para que los socios de alta disponibilidad puedan determinar la accesibilidad de sus destinos.

dirección

Dirección IP del destino de alcance.

Ejemplos

- Añadir un nodo de alta disponibilidad con la dirección IP 9.37.50.17 con un rol primario en el puerto 12345 y la dirección de socio 9.37.50.14:

```
nalcontrol highavailability add  
address 9.37.50.17 role primary port 12345 partneraddress 9.37.50.14
```

- Añadir la dirección de destino de alcance 9.37.50.9:

```
nalcontrol highavailability usereach 9.37.50.9
```

- Eliminar la dirección de destino de alcance 9.37.50.9:

```
nalcontrol highavailability dropreach 9.37.50.9
```

- Iniciar alta disponibilidad con una estrategia de recuperación manual:

```
nalcontrol highavailability start manual
```

- Obtener una instantánea de estadísticas de alta disponibilidad:

```
nalcontrol highavailability report
```

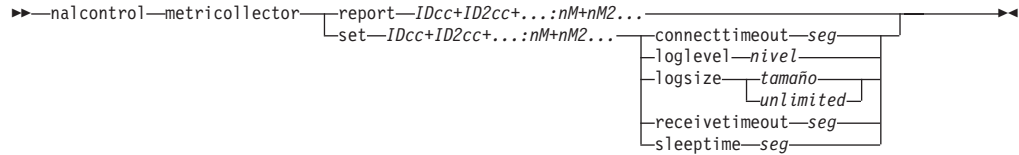
Este mandato genera una salida parecida a la siguiente:

Estado de alta disponibilidad:

```
Nodo . . . . . primario  
Dirección de nodo . . . . 9.37.50.17  
Puerto . . . . . 12345  
Dirección de socio . . . . 9.37.50.14  
Estrategia de recuperación manual  
Intervalo de pulso . . . . 500  
Intervalo de toma control. 2000  
Iniciado . . . . . N  
Estado . . . . . desocupado  
Subestado. . . . . no sincronizado
```

Estado de accesibilidad : Nodo/Socio

nalcontrol metriccollector — configurar recopilador de métricas



report

Muestra las características de un recopilador de métricas.

IDcc (ID de consultor de conmutador)

Serie definida por el usuario que hace referencia al consultor.

nM (nombre de métrica)

Nombre que identifica la métrica proporcionada o personalizada.

set

Establece las características de un recopilador de métricas.

connecttimeout

Establece cuánto tiempo espera el recopilador de métricas antes de notificar que una conexión es anómala.

seg

Entero positivo que representa el tiempo en segundos durante el que el recopilador de métricas espera antes de notificar que se ha producido una anomalía en una conexión a un servicio.

loglevel

Establece el nivel en el que el consultor especificado registra las actividades. El valor por omisión es 1.

nivel

El número del nivel. El valor por omisión es 1. Cuanto más alto sea el número, más información se anotará en las anotaciones cronológicas del consultor. Los valores posibles son:

- 0 = Ninguno
- 1 = Mínimo
- 2 = Básico
- 3 = Moderado
- 4 = Avanzado
- 5 = Detallado

logsize

Establece el número máximo de bytes anotados en el archivo de anotaciones cronológicas. El valor por omisión es 1048576. Cuando se establece un tamaño máximo para el archivo de anotaciones cronológicas, el texto del archivo vuelve al principio; es decir, cuando el archivo alcanza el tamaño especificado, las entradas subsiguientes se anotarán al principio del archivo y se grabarán encima de las entradas de anotaciones cronológicas anteriores. El tamaño de las anotaciones cronológicas no puede establecerse más pequeño que el tamaño actual de las anotaciones cronológicas. Las entradas de las anotaciones cronológicas incluyen la indicación de la hora para poder saber el orden en el que se anotaron. Cuando más alto se establezca el nivel de anotaciones cronológicas, más cuidado deberá tener al elegir el tamaño de las anotaciones

cronológicas porque, cuando el registro cronológico está establecido en los niveles más altos, puede quedarse sin espacio rápidamente.

tamaño | unlimited

Número máximo de bytes anotados en las anotaciones cronológicas del consultor. Puede especificar un número positivo mayor que cero o la palabra **unlimited**. Es posible que el archivo de anotaciones cronológicas no alcance el tamaño máximo exacto antes de empezar a sobrescribir porque el tamaño de las entradas del archivo varían.

receivetimeout

Establece cuánto tiempo el consultor espera antes de informar de que no se ha podido realizar una recepción del servicio.

seg

Entero positivo que representa la cantidad de tiempo en segundos que el consultor espera antes de informar que no se ha podido realizar una recepción de un servicio.

sleeptime

Establece la cantidad de tiempo en segundos que el recopilador de métricas permanece inactivo entre los ciclos de recolección de métricas.

seg

Entero positivo que representa el número de segundos de tiempo de inactividad.

Ejemplos

- Ver un informe sobre las características de un recopilador de métricas:

```
nalcontrol metrinalllector report sc1:http
```

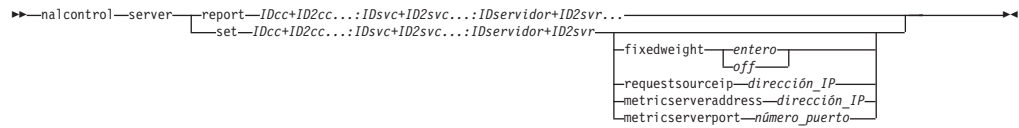
Este mandato genera una salida parecida a la siguiente:

```
Metrinalllector sc1:http
collected metric(s).... http
loglevel..... 5
logSize..... 1048576
sleepTimeSeconds..... 7
timeoutConnectSeconds.. 21
timeoutReceiveSeconds.. 21
```

- Establecer un valor de connecttimeout de 15 segundos y un valor de logsize de unlimited para el consultor de conmutador sc1 y la métrica http:

```
nalcontrol metrinalllector set sc1:http connecttimeout 15 logsize unlimited
```

nalcontrol server — configurar un servidor



report

Muestra las características de servidores.

IDcc

Serie definida por el usuario que representa al consultor.

IDsvc

Serie definida por el usuario que representa el identificador de servicio virtual y el número de puerto virtual del conmutador.

IDServidor

Entero que representa el servidor en el conmutador.

set

Establece características de servidores

fixedweight

Establece un peso fijo para este servidor. El valor por omisión es off. El valor máximo de fixedweight es 48.

entero | *off*

Entero positivo que representa el peso fijo para este servidor o la palabra **off** para especificar que no hay peso fijo.

requestsourceip

Establece la dirección desde la que ponerse en contacto con el servidor para obtener las peticiones de aplicación.

dirección_IP

Dirección IP desde la que ponerse en contacto con el servidor; puede especificarse como nombre simbólico o en formato de dirección IP.

metricserveraddress

Establece la dirección desde la que ponerse en contacto con el servidor para obtener peticiones de Metric Server.

dirección_IP

Dirección IP de Metric Server como nombre simbólico o en formato de dirección IP.

metricserverport

Establece el puerto que debe utilizarse para ponerse en contacto con Metric Server.

número_puerto

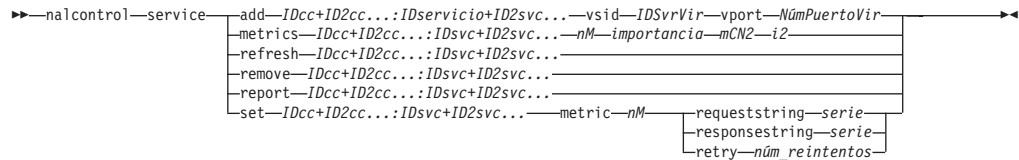
Número de puerto utilizado para ponerse en contacto con Metric Server.

Ejemplos

- Mostrar un informe sobre el servidor 1 para el consultor sc1:
nalcontrol server report sc1:svc1:1
Este mandato genera una salida parecida a la siguiente:

- El servidor scl:svcl:1 tiene un peso de -99
 El peso fijo tiene el valor off
 IP origen solicitud ... 9.27.24.156
 Puerto de aplicación .. 99
 Dirección MetricServer 9.99.99.98
 Puerto de MetricServer 10004
 activeconn de métrica tiene el valor -99
 connrate de métrica tiene el valor -99
- Establecer una dirección de Metric Server para el servicio 2:
 nalcontrol server set scl:svcl:2 metricserveraddress 9.37.50.17

nalcontrol service — configurar un servicio



add

Añade un servicio al consultor especificado.

IDcc (ID_consultor_conmutador)

Serie definida por el usuario que hace referencia al consultor.

IDSvc (ID de servicio)

Serie definida por el usuario que identifica el servicio.

vsid

Palabra clave del identificador de servicio virtual.

IDSvrVir (ID de servidor virtual)

Número del conmutador que representa el servidor virtual.

vport

Palabra clave de puerto virtual.

NúmPuertoVirtual (número de puerto virtual)

Número de puerto del servicio configurado actualmente en el conmutador.

metrics

Especifica el conjunto de métricas utilizado en el cálculo de pesos y la importancia de cada métrica. La importancia se expresa como porcentaje del total. La suma de los valores de importancia debe ser 100. La métrica puede ser cualquier combinación de la métrica de datos de conexiones, métrica de asesor de aplicaciones y métrica de Metric Server. Los valores por omisión son las métricas de conexión activa (activeconn) y velocidad de conexión (connrate) con una importancia de 50/50.

nM (nombre de métrica)

Nombre que identifica el recopilador de métricas que recopilará las medidas para determinar el peso del servidor.

A continuación se muestra una lista de nombres de métrica válidos y sus puertos asociados:

Nombre del asesor	Protocolo	Puerto
connect	ICMP	12345
db2	private	50000
dns	DNS	53
ftp	FTP	21
http	HTTP	80
https	SSL	443
cachingproxy	HTTP (mediante Caching Proxy)	80
imap	IMAP	143
ldap	LDAP	389
nnntp	NNTP	119

Nombre del asesor	Protocolo	Puerto
ping	PING	0
pop3	POP3	110
sip	SIP	5060
smtp	SMTP	25
ssl	SSL	443
telnet	Telnet	23
WLM	private	10.007
activeconn	n/d	n/d
connrate	n/d	n/d
cpuload	n/d	n/d
memload	n/d	n/d

importancia

Número de 0 a 100 que representa la importancia de esta métrica en el cálculo de pesos de servidores.

refresh

Renueva un servicio con información del Conmutador Nortel Alteon Web.

remove

Elimina un servicio.

report

Informa de las características de un servicio.

set

Establece las características de un servicio.

metric

Establece las características de una métrica configurada.

nM (nombre de métrica)

Nombre de la métrica que desee.

requeststring

Establece una serie de petición para la métrica especificada. Representa la petición que ha enviado un recopilador de métricas para recopilar información de métricas.

serie

Serie de petición que ha enviado el recopilador de métricas al servidor.

responsestring

Establece una serie de respuesta para la métrica especificada. La serie de respuesta especificada la utiliza el recopilador de métricas para comparar las respuestas que recibe de servidores y posteriormente determinar la disponibilidad de servidores.

serie

Serie de respuesta con la que el recopilador de métricas compara las respuestas de servidor recibidas.

retry

El parámetro retry establece el número de reintentos que se pueden llevar a cabo antes de marcar un servidor como inactivo.

núm_reintentos

Número entero mayor que o igual a cero. Este valor no debe ser mayor que 3. Si la palabra clave retries no está configurada, el número de reintentos tendrá el valor por omisión de cero.

Ejemplos

- Añadir un servicio llamado svc1 (con el ID de servidor virtual 1 y el puerto virtual 80) al ID de consultor de conmutador sc1:

```
nalcontrol service add sc1:svc1 vsid 1 vport 80
```

- Especificar la proporción 50 en la métrica activeconn y http:

```
nalcontrol service metrics sc1:svc1 activeconn 50 http 50
```

- Ver un informe de características de contenido de propietario:

```
nalcontrol service report sc1:svc1
```

Este mandato genera una salida parecida a la siguiente:

```
Service sc1:svc1
  Weightbound = 48
  Metric activeconn has proportion 50
  Metric connrate has rproportion 50
  Contains Server 4
  Contains Server 3
  Contains Server 2
  Contains Server 1
```

- Establecer una serie de petición http:

```
nalcontrol service set sc1:svc1 metric http requeststring getLastErrorCode
```

Apéndice A. GUI: instrucciones generales

En la interfaz gráfica de usuario de Load Balancer, el lado izquierdo del panel muestra una estructura de árbol con Load Balancer en el nivel superior, y Dispatcher, CBR (Content Based Routing), Site Selector, Cisco CSS Controller y Nortel Alteon Controller como componentes.

Si utiliza la instalación de Load Balancer para IPv4 y IPv6, sólo está disponible el componente Dispatcher. Para obtener más información, consulte el Capítulo 8, “Despliegue de Dispatcher en Load Balancer para IPv4 y IPv6”, en la página 81.

Para obtener ejemplos gráficos de la GUI de Load Balancer que resaltan cada uno de los distintos componentes, consulte lo siguiente:

- Consulte la Figura 41 en la página 468 para Dispatcher
- Consulte la Figura 42 en la página 469 para CBR
- Consulte la Figura 43 en la página 470 para Site Selector
- Consulte la Figura 44 en la página 471 para Cisco CSS Controller
- Consulte la Figura 45 en la página 472 para Nortel Alteon Controller

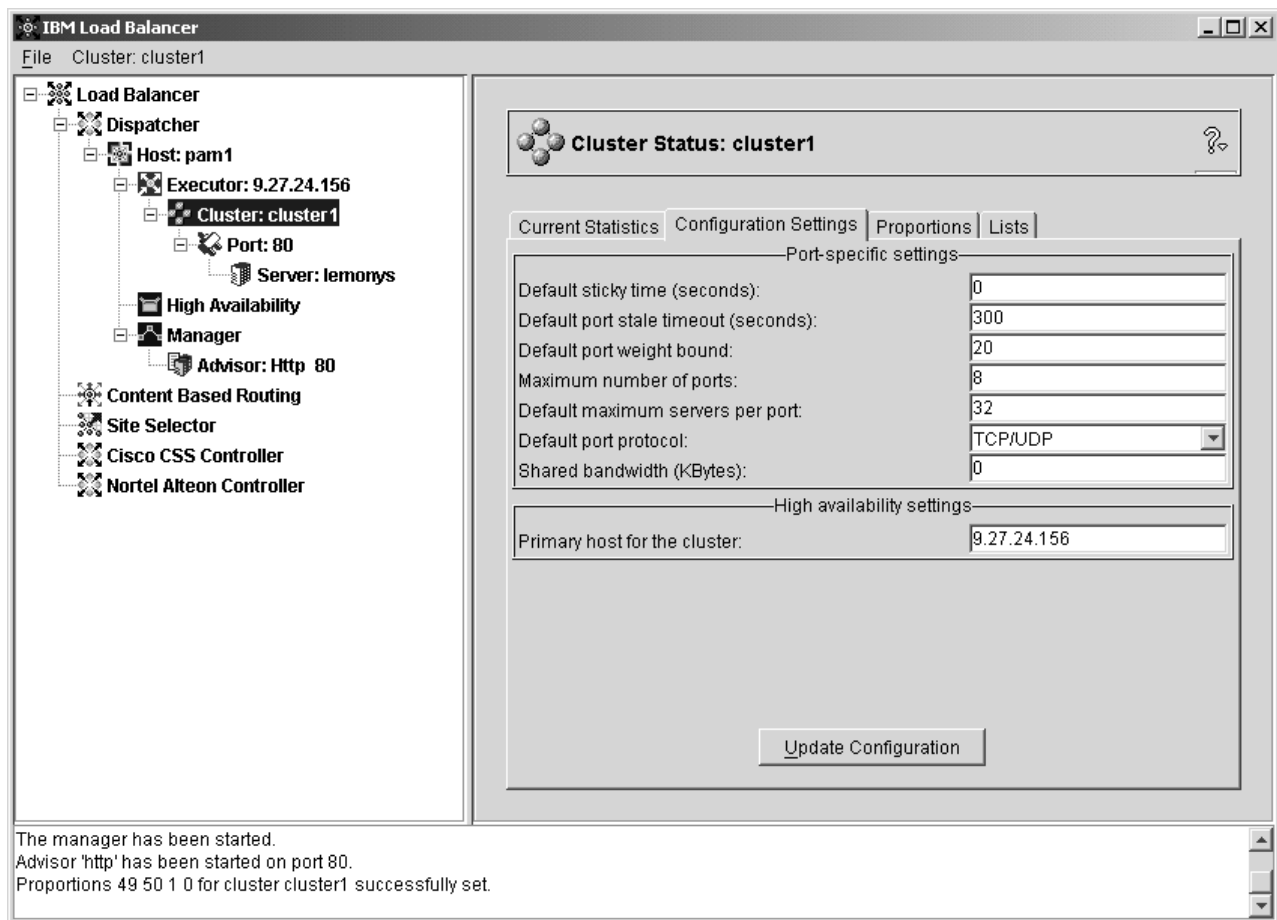


Figura 41. La interfaz gráfica de usuario (GUI) que muestra la expansión de la estructura de árbol de la GUI del componente Dispatcher.

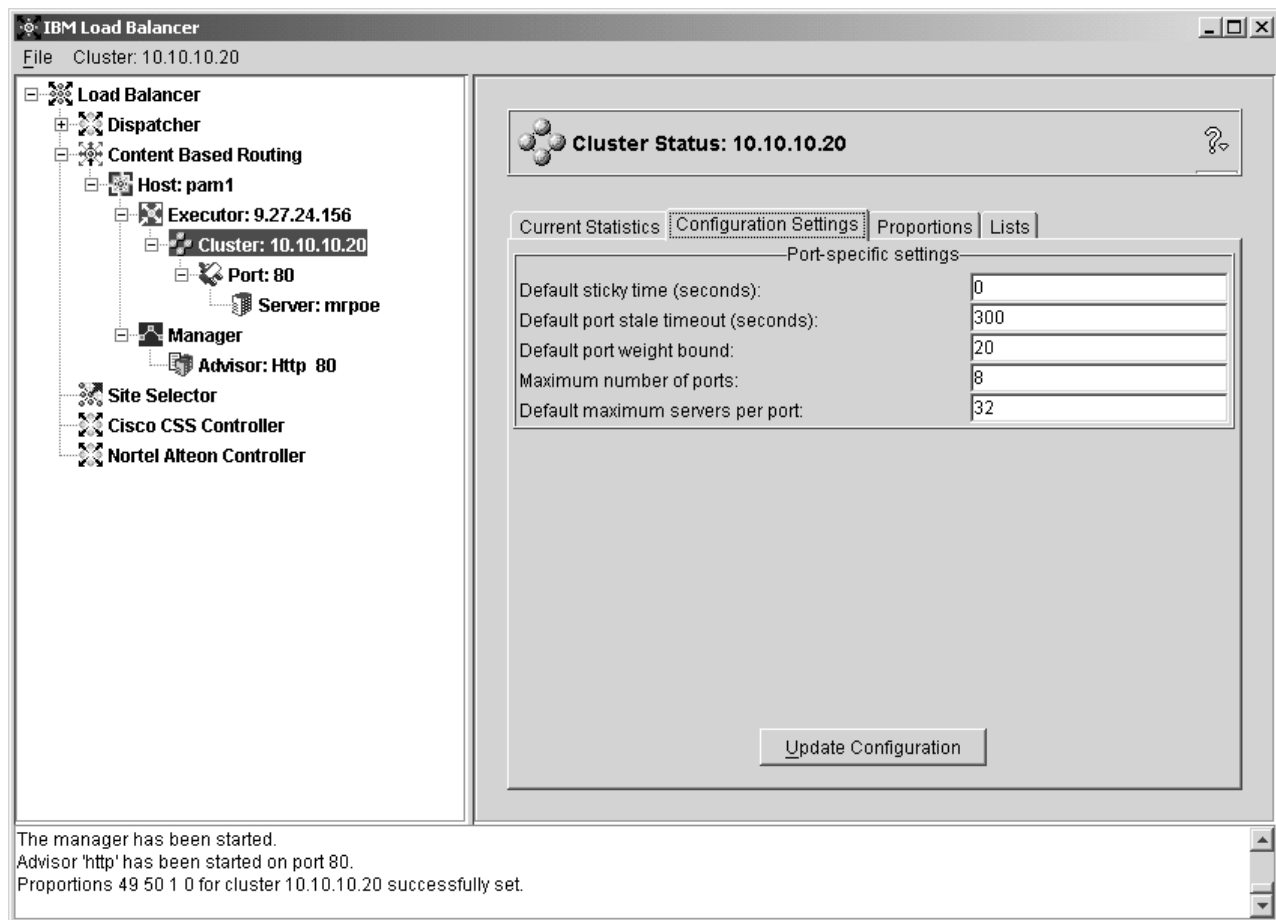


Figura 42. La interfaz gráfica de usuario (GUI) que muestra la expansión de la estructura de árbol de la GUI del componente CBR.

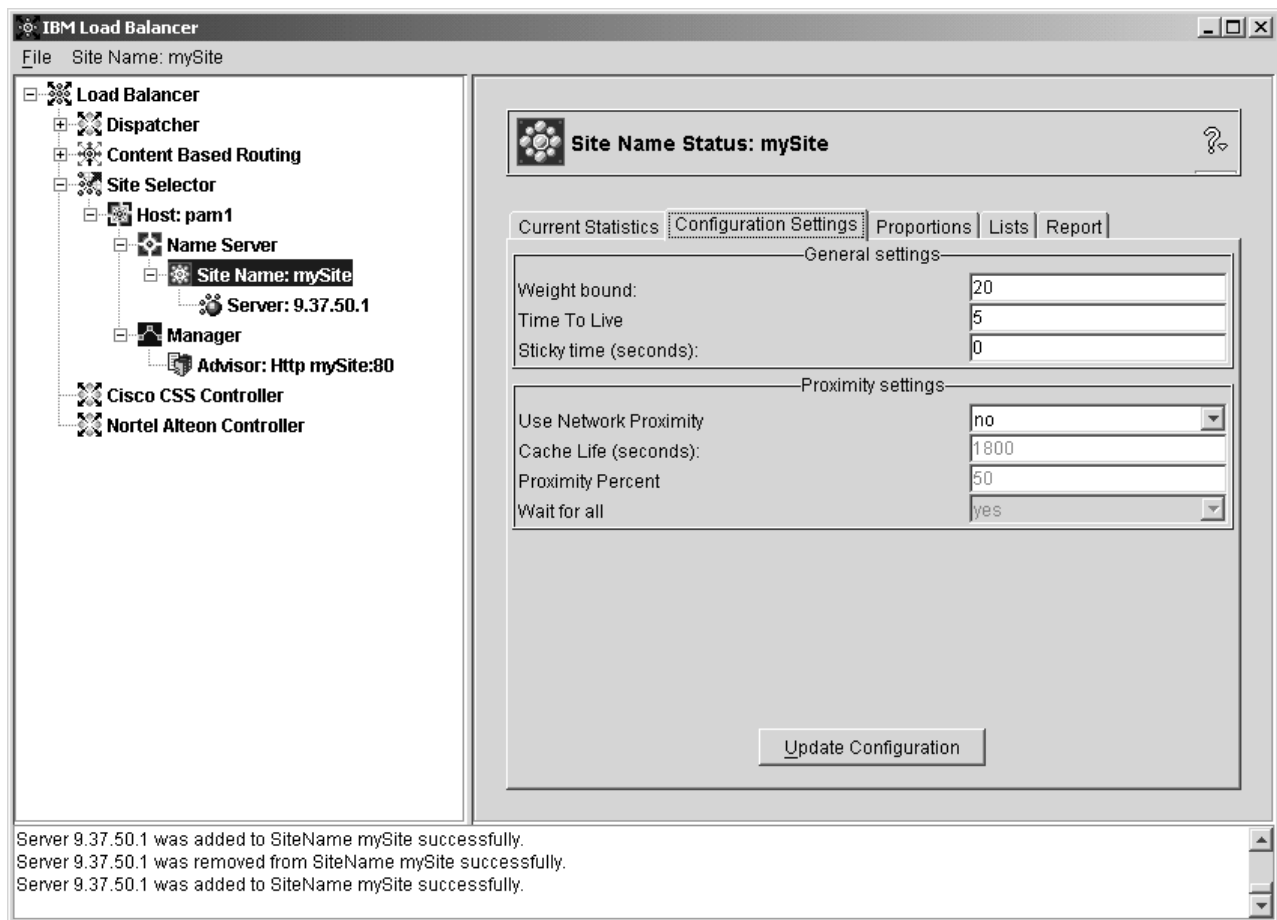


Figura 43. La interfaz gráfica de usuario (GUI) que muestra la expansión de la estructura de árbol de la GUI del componente Site Selector.

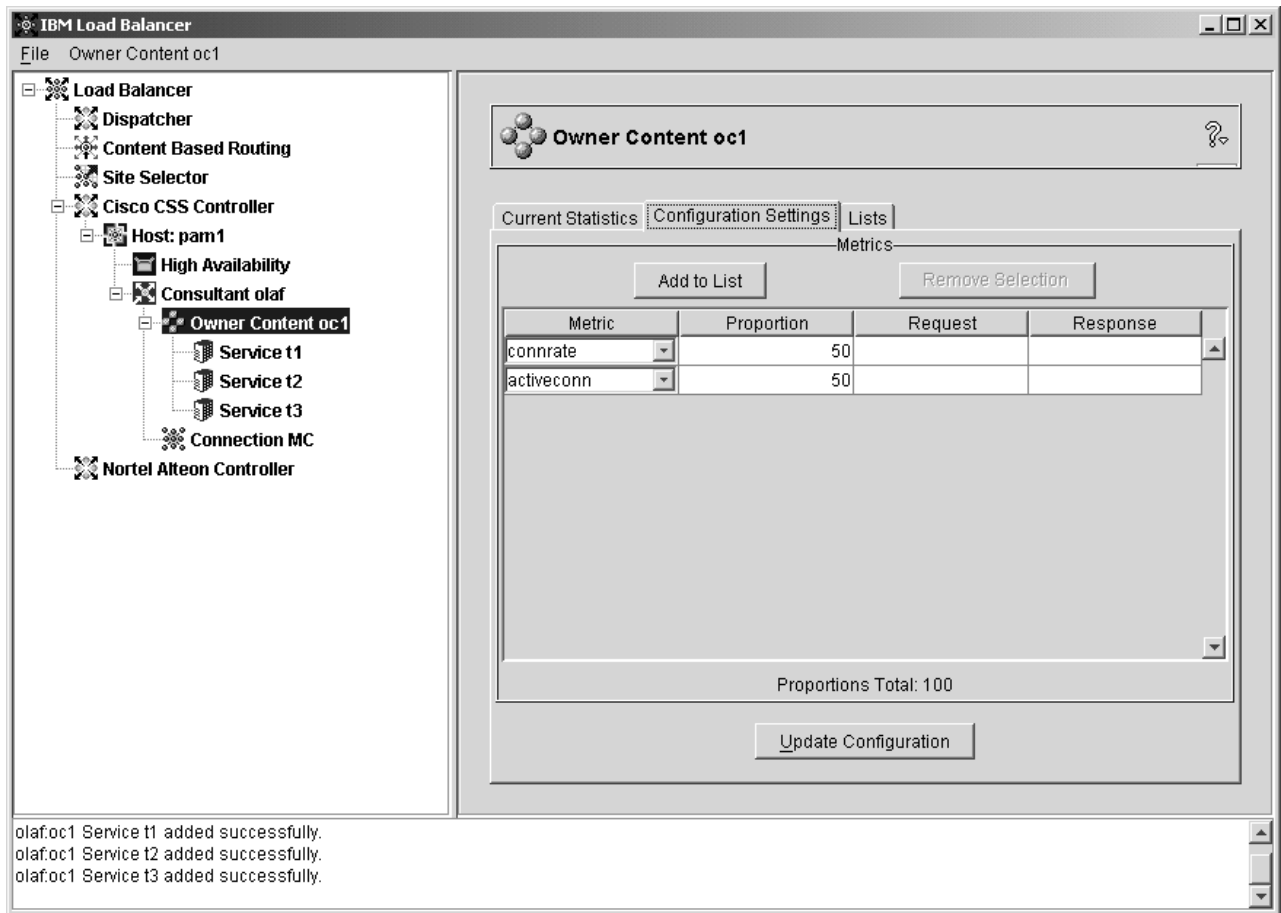


Figura 44. La interfaz gráfica de usuario (GUI) que muestra la expansión de la estructura de árbol de la GUI del componente Cisco CSS Controller.

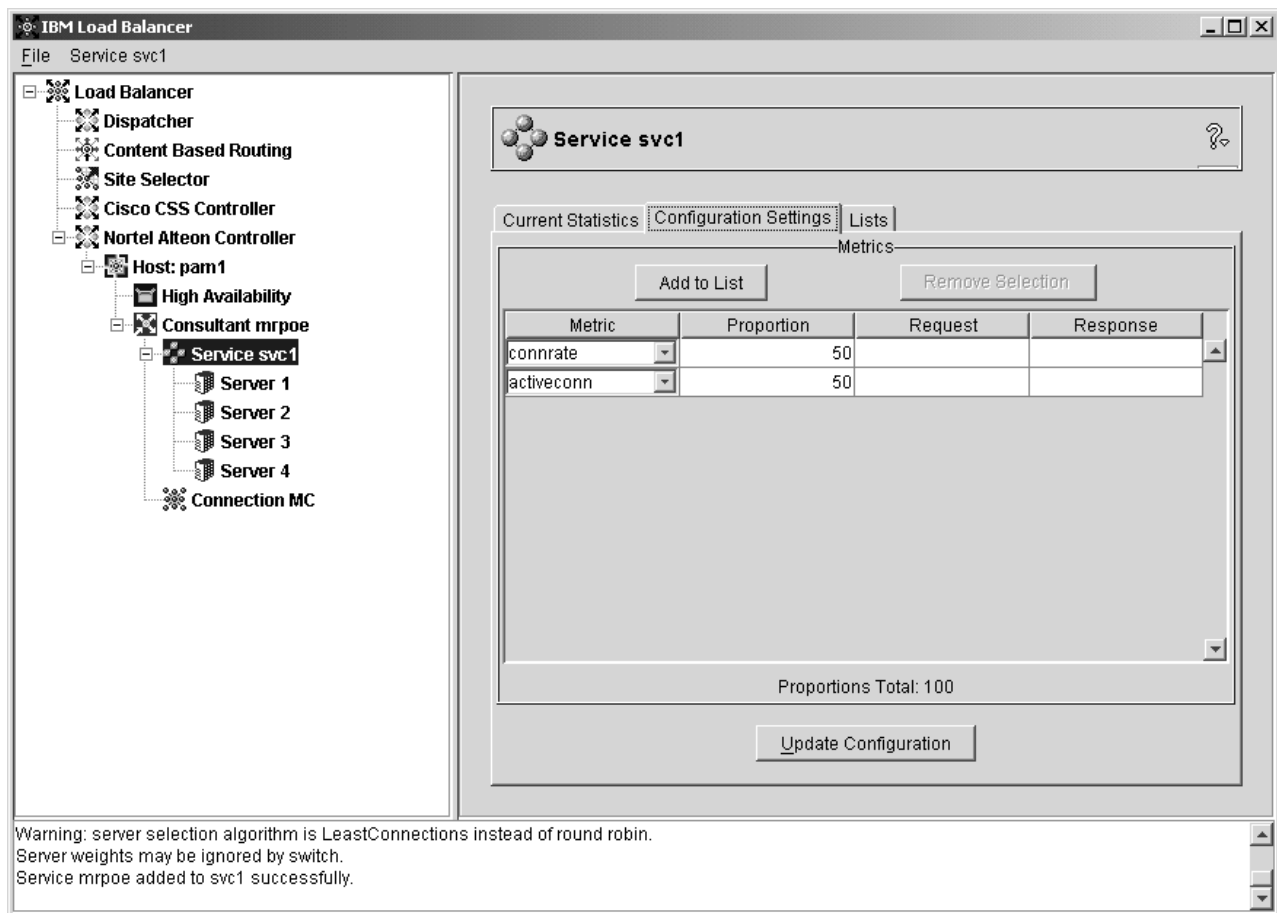


Figura 45. La interfaz gráfica de usuario (GUI) que muestra la expansión de la estructura de árbol de la GUI del componente Nortel Alteon Controller.

Todos los componentes pueden configurarse desde la GUI. Puede seleccionar elementos en la estructura de árbol pulsando el botón del ratón (normalmente el botón izquierdo) y, a continuación, mostrar los menús emergentes pulsando el botón dos del ratón (normalmente el botón derecho). También se puede acceder a los menús emergentes de los tres elementos desde la barra de menús situada en la parte superior del panel.

Pulse los signos más o menos para expandir o contraer los elementos de la estructura de árbol.

Para ejecutar un mandato desde la GUI: resalte el nodo Sistema principal en el árbol de la GUI y seleccione **Enviar mandato....** en el menú emergente Sistema principal. En el campo de entrada de mandatos, escriba el mandato que desea ejecutar, por ejemplo: **executor report**. El resultado y el historial de los mandatos que se ejecutan en la sesión actual aparece en la ventana que se proporciona.

En la parte derecha del panel se muestran pestañas que indican el estado del elemento seleccionado actualmente.

- La pestaña **Estadísticas actuales** presenta información estadística sobre el elemento. Esta pestaña no aparece para todos los elementos de la estructura de árbol.

- El botón **Renovar estadísticas** muestra los datos estadísticos más recientes. Si el botón **Renovar estadísticas** no aparece, los datos estadísticos se renuevan automáticamente y siempre están actualizados.
- La pestaña **Valores de configuración** muestra parámetros de configuración que pueden establecerse utilizando los procedimientos descritos en los capítulos de configuración para cada uno de los componentes. Esta pestaña no aparece para todos los elementos de la estructura de árbol.
- El botón **Actualizar configuración** se aplica a los últimos cambios realizados en la configuración que se está ejecutando actualmente.
- La pestaña **Proporciones** muestra los parámetros de proporción (o peso) que pueden establecerse utilizando la información de Capítulo 22, “Características avanzadas para Dispatcher, CBR y Site Selector”, en la página 201. Esta pestaña no aparece para todos los elementos de la estructura de árbol.
- La pestaña **Listas** muestra detalles adicionales sobre el elemento de árbol seleccionado. Esta pestaña no aparece para todos los elementos de la estructura de árbol.
- El botón **Eliminar** suprime de la lista los elementos seleccionados.
- La pestaña **Informe** presenta la información del informe del gestor sobre el elemento. Esta pestaña no aparece para todos los elementos de la estructura de árbol.
- El botón **Renovar informe** muestra los datos más recientes del informe del gestor.

Para acceder a la **Ayuda**, pulse el signo de interrogación (?) situado en la esquina superior derecha de la ventana Load Balancer.

- **Ayuda: Nivel de campo** — describe cada campo, los valores por omisión
- **Ayuda: Cómo puedo** — lista las tareas que pueden llevarse a cabo desde la pantalla actual
- **InfoCenter**: proporciona acceso a la siguiente información del producto: visión general y los elementos más destacados de la información de característica nueva, enlace al sitio Web del producto, índice de los archivos de ayuda en línea, glosario de términos.

Apéndice B. Sintaxis de la norma de contenido (patrón)

En este apéndice se describe cómo utilizar la sintaxis de la norma de contenido (patrón) para el componente CBR y el método de reenvío CBR del componente Dispatcher, junto con los escenarios y ejemplos de su uso.

Sintaxis de la norma de contenido (patrón):

Aplicable sólo si se ha seleccionado "contenido" para el tipo de norma.

Entre la sintaxis de patrón que desea utilizar, con las siguientes restricciones

- no se pueden indicar espacios dentro del patrón
- caracteres especiales, a menos que preceda el carácter con una barra inclinada invertida (\):
 - * comodín ((sustituye a cualquier número de caracteres o a ninguno)
 - (paréntesis izquierdo utilizado para agrupación lógica
 -) paréntesis derecho utilizado para agrupación lógica
 - & AND lógico
 - | OR lógico
 - ! NOT lógico

Palabras clave reservadas

Las palabras claves reservadas siempre van seguidas de un signo igual "=".

Method

Método HTTP de la petición, por ejemplo GET, POST, etc

URI vía de acceso de la petición URL (sensible a las mayúsculas/minúsculas)

Version

versión específica de la petición, HTTP/1.0 o HTTP/1.1

Host valor de la cabecera host: (no es sensible a las mayúsculas/minúsculas)

Nota: Opcional en los protocolos HTTP/1.0

<clave>

cualquier nombre de cabecera HTTP válido que Dispatcher pueda buscar. Ejemplos de cabeceras HTTP son User-Agent, Connection, Referer, etc.

Un valor con destino `http://www.empresa.com/path/webpage.htm` podría mostrar los valores siguientes:

```
Method=GET
URI=/path/webpage.htm
Version=HTTP/1.1
Host=www.empresa.com
Connection=Keep-Alive
Referer=http://www.empresa.com/path/parentwebpage.htm
```

Nota: El shell del sistema operativo puede interpretarlos como caracteres especiales, como "&", y convertirlos en texto alternativo antes de que **cbrcontrol** los evalúe.

Por ejemplo, el siguiente mandato sólo es válido cuando se utiliza el indicador **cbrcontrol**>>.

```
rule add 10.1.203.4:80:cbr_prod_rule_ek type content pattern uri=/nipoe/*
```

Cuando se utilizan caracteres especiales, para que este mismo mandato funcione en el indicador del sistema operativo (o en el archivo de configuración), el patrón debe indicarse entre dos signos de comillas (" ") tal como se indica a continuación:

```
cbrcontrol rule add 10.1.203.4:80:cbr_prod_rule_ek type content  
pattern "uri=/nipoe/*"
```

Si no se utilizan las comillas, alguna parte del patrón puede truncarse cuando la norma se guarda en CBR. Tenga en cuenta que las comillas no están soportadas cuando se utiliza el indicador de mandatos **cbrcontrol**>>.

A continuación se muestra una recopilación de posibles casos y ejemplos para el uso de sintaxis de patrón

Caso de ejemplo 1:

La configuración de un nombre de clúster incluye un conjunto de servidores Web para el contenido HTML estándar, otro conjunto para servidores Web con WebSphere Application Server para peticiones de servlet, otro conjunto de servidores Lotus Notes para archivos NSF, etc. Para distinguir entre estas páginas solicitadas es necesario tener acceso al cliente. También es necesario enviarlas a los servidores adecuados. Las normas de coincidencia de patrones de contenido proporcionan la separación necesaria para llevar a cabo estas tareas. Para que la separación de las peticiones necesaria se produzca automáticamente, se configura una serie de normas. Por ejemplo, los siguientes mandatos realizan las tres separaciones antes mencionadas:

```
>>rule add cluster1:80:servlets type content pattern uri=*/servlet/* priority 1  
>>rule uses cluster1:80:servlets server1+server2  
  
>>rule add cluster1:80:notes type content pattern uri=*.nsf* priority 2  
>>rule uses cluster1:80:notes server3+server4  
  
>>rule add cluster1:80:regular type true priority 3  
>>rule uses cluster1:80:regular server5+server6
```

Si una petición para un archivo NSF llega a Load Balancer, primero la examina la norma de servlets, pero no coincide. A continuación, la petición la examina la norma de notes y devuelve una coincidencia. La carga del cliente está equilibrada entre server3 y server4.

Caso de ejemplo 2:

Otro ejemplo común es cuando el sitio Web principal controla varios grupos internos distintos. Por ejemplo, www.empresa.com/software incluye un conjunto de servidores y un contenido distinto de la división www.empresa.com/hardware. Puesto que las peticiones están basadas en el clúster de www.empresa.com raíz, las normas de contenido tienen que encontrar las diferencias de URI y completar el equilibrio de carga. La norma del caso de ejemplo se parece a la siguiente:

```
>>rule add cluster1:80:div1 type content pattern uri=/software/* priority 1  
>>rule uses cluster1:80:div1 server1+server2  
  
>>rule add cluster1:80:div2 type content pattern uri=/hardware/* priority 2  
>>rule uses cluster1:80:div2 server3+server4
```

Caso de ejemplo 3:

Determinadas combinaciones son susceptibles al orden en el que se realiza la búsqueda en las normas. Por ejemplo, en el caso de ejemplo 2, los clientes se separaron en función de un directorio de su vía de acceso de peticiones; sin embargo, el directorio de destino puede aparecer en varios niveles de la vía de acceso e indicar cosas distintas dependiendo del lugar en que se encuentren. Por ejemplo, `www.empresa.com/pcs/fixed/software` es un destino distinto de `www.empresa.com/mainframe/fixed/software`. Las normas deben definirse de forma que tengan prevista esta posibilidad y no identifique demasiados casos a la vez. Por ejemplo, la prueba `"uri=*/software/*"` es una búsqueda con comodín demasiado amplia en este caso. Pueden estructurarse normas alternativas de la siguiente forma:

Una búsqueda de combinación puede limitarla:

```
>>rule add cluster1:80:pcs type content pattern (uri=/pcs/*)&(uri=*/software/*)
>>rule uses cluster 1:80:pcs server1
```

En los casos en los que no haya combinaciones, el orden pasa a ser importante:

```
>>rule add cluster1:80:pc1 type content pattern uri=/pcs/*
>>rule uses cluster1:80:pc1 server2
```

La segunda norma detecta cuando `"pcs"` aparece en lugares de directorios posteriores en lugar del primero.

```
>>rule add cluster1:80:pc2 type content pattern uri=*/pcs/*
>>rule uses cluster1:80:pc2 server3
```

En casi cada caso, desea completar las normas con una norma **siempre cierta** por omisión para identificar todo lo que no puedan detectar otras normas. Esto también puede ser un servidor "Lo sentimos, el sitio está inactivo actualmente, inténtelo más adelante" para los casos en los que los demás servidores no pueden aceptar la petición de este cliente.

```
>>rule add cluster1:80:sorry type true priority 100
>>rule uses cluster1:80:sorry server5
```

Apéndice C. Archivos de configuración de ejemplo

Este apéndice contiene archivos de configuración de ejemplo para el componente Dispatcher de Load Balancer.

IMPORTANTE: si utiliza la instalación de Load Balancer para IPv4 y IPv6, recuerde sustituir el símbolo de arroba (@) por dos puntos (:) como el delimitador dentro de mandatos dscontrol en estos archivos de configuración de ejemplo.

Archivos de configuración de Load Balancer de ejemplo

Los archivos de ejemplo se ubican en el directorio ...ibm/edge/lb/servers/samples/.

Archivo de configuración de Dispatcher — Sistemas AIX, Linux y Solaris

```
#!/bin/bash
#
# configuration.sample - Archivo de configuración de ejemplo para el
# componente Dispatcher
#
#
# Asegúrese de ejecutar este script como usuario root.
#
# iam=`whoami`

# if [ "$iam" != "root" ]if [ "$iam" != "root" ]
# then
# echo "Debe iniciar la sesión como root para ejecutar este script"
# exit 2
# fi

#
# Primero, inicie el servidor
#
# dsserver start
# sleep 5

#
# Después inicie el ejecutor
#
# dscontrol executor start

#
# Dispatcher puede eliminarse en cualquier momento con los
# mandatos "dscontrol executor stop" y "dsserver stop" para
# detener respectivamente el ejecutor y servidor antes de eliminar
# el software de Dispatcher.
#
# En el siguiente paso de la configuración de Dispatcher se establecerá la
# NFA (dirección de no reenvío) y las direcciones del clúster.
#
# La NFA se usa para acceder de forma remota a la máquina Dispatcher
# para fines de administración o configuración. Esta
# dirección es necesaria puesto que Dispatcher enviará paquetes
# a las direcciones de clúster.
#
# La dirección de clúster es el nombre de sistema principal (o dirección IP) al
# que se conectarán los clientes remotos.
```

```

#
# En todo este archivo puede utilizar los nombres de sistema principal y
# las direcciones IP de manera intercambiable.
#

# NFA=hostname.domain.name
# CLUSTER=www.suempresa.com

# echo "Cargando la dirección de no reenvío"
# dscontrol executor set nfa $NFA

#
# En el siguiente paso de la configuración de Dispatcher se creará
# un clúster. Dispatcher direccionará las peticiones enviadas a
# la dirección del clúster a las correspondientes máquinas servidor
# definidas para dicho clúster. Puede configurar y atender a
# varias direcciones de clúster con Dispatcher.

# Emplee una configuración parecida para CLUSTER2, CLUSTER3, etc.
#

# echo "Cargando primero la dirección de clúster"
# dscontrol cluster add $CLUSTER

#
# Ahora, tenemos que definir los puertos que usará este clúster. Todas
# las peticiones recibidas por Dispatcher en un puerto definido se
# reenviarán al correspondiente puerto de una de las
# máquinas servidor.
#

# echo "Creando puertos para clúster: $CLUSTER"

# dscontrol port add $CLUSTER:20+21+80

#
# En el último paso se añadirá cada una de las máquinas servidor a los
# puertos de este clúster.
# De nuevo, puede usar el nombre de sistema principal o la dirección IP
# de las máquinas servidor.
#

# SERVER1=server1name.domain.name
# SERVER2=server2name.domain.name
# SERVER3=server3name.domain.name

# echo "Añadiendo máquinas servidor"
# dscontrol server add $CLUSTER:20+21+80:
# $SERVER1+$SERVER2+$SERVER3

#
# Ahora empezará el equilibrio de carga de los componentes de
# Dispatcher. El principal componente del equilibrio de carga se denomina
# gestor y el segundo componente del equilibrio de carga son los
# asesores. Si el gestor y los asesores no están ejecutándose,
# Dispatcher envía peticiones de forma de turno rotativo. Una vez que
# se inicia el gestor, se emplea la ponderación de decisiones en base al
# número de conexiones nuevas y activas, y las peticiones entrantes
# se envían al mejor servidor. Los asesores ofrecen al
# gestor una mejor comprensión de la capacidad de los servidores para atender
# peticiones así como detectar si un servidor está activo. Si
# un asesor detecta que un servidor está inactivo, se marcará como inactivo
# (siempre que las proporciones del gestor se hayan establecido
# de forma que incluyan la entrada del asesor) y no se direccionarán
# más peticiones al servidor.

# En el último paso de la configuración de los componentes del equilibrio de carga

```

```

# se establecerán las proporciones del gestor. El gestor actualiza el
# peso de cada uno de los servidores basándose en cuatro políticas:
# 1. El número de conexiones activas en cada servidor.
# 2. El número de nuevas conexiones en cada servidor.
# 3. La entrada de datos desde los asesores.
# 4. La entrada de datos desde el asesor del nivel del sistema.
# La suma de estas proporciones debe ser 100. Como ejemplo, si se establecen
# las proporciones del gestor en
# dscontrol manager proportions 48 48 0 0
# otorgará a las conexiones activas y nuevas el 48% de entrada en la
# ponderación de decisiones, los asesores contribuirán un 4% y
# no se tendrá en cuenta la entrada del sistema.
#
# NOTA: por omisión, las proporciones del gestor están establecidas en 50 50 0 0
#

# echo "Iniciando el gestor..."
# dscontrol manager start

# echo "Iniciando el asesor FTP en puerto 21 ..."
# dscontrol advisor start ftp 21
# echo "Iniciando el asesor HTTP en puerto 80 ..."
# dscontrol advisor start http 80
# echo "Iniciando el asesor Telnet en puerto 23 ..."
# dscontrol advisor start telnet 23
# echo "Iniciando el asesor SMTP en puerto 25 ..."
# dscontrol advisor start smtp 25
# echo "Iniciando el asesor POP3 en puerto 110 ..."
# dscontrol advisor start pop3 110
# echo "Iniciando el asesor NNTP en puerto 119 ..."
# dscontrol advisor start nntp 119
# echo "Iniciando el asesor SSL en puerto 443 ..."
# dscontrol advisor start ssl 443
#

# echo "Definiendo las proporciones del gestor..."
# dscontrol manager proportions 58 40 2 0

#
# El último paso de la configuración de la máquina Dispatcher es crear un
# alias para la tarjeta de interfaz de red (NIC).
#
# NOTA: NO utilice este mandato en un entorno de alta
# disponibilidad. Los scripts go* configurarán la NIC y
# el bucle de retorno según sea necesario.
# dscontrol executor configure $CLUSTER

# Si la dirección de clúster está en una NIC o subred distinta
# de la de NFA, utilice el siguiente formato para el mandato cluster
# configure.
# dscontrol executor configure $CLUSTER tr0 0xfffff800
# donde tr0 es la NIC (tr1 para la segunda tarjeta token ring, en0
# para la primera tarjeta ethernet) y 0xfffff800 es una
# máscara de subred válida para el sitio.
#

#
# Los siguientes mandatos se establecen en los valores por omisión.
# Utilice estos mandatos como guía para cambiar los valores por omisión.
# dscontrol manager loglevel 1
# dscontrol manager logsize 1048576
# dscontrol manager sensitivity 5
# dscontrol manager interval 2
# dscontrol manager refresh 2
#
# dscontrol advisor interval ftp 21 5
# dscontrol advisor loglevel ftp 21 1

```

```
# dscontrol advisor logsize ftp 21 1048576
# dscontrol advisor timeout ftp 21 unlimited
# dscontrol advisor interval telnet 23 5
# dscontrol advisor loglevel telnet 23 1
# dscontrol advisor logsize telnet 23 1048576
# dscontrol advisor timeout telnet 23 unlimited
# dscontrol advisor interval smtp 25 5
# dscontrol advisor loglevel smtp 25 1
# dscontrol advisor logsize smtp 25 1048576
# dscontrol advisor timeout smtp 25 unlimited
# dscontrol advisor interval http 80 5
# dscontrol advisor loglevel http 80 1
# dscontrol advisor logsize http 80 1048576
# dscontrol advisor timeout http 80 unlimited
# dscontrol advisor interval pop3 110 5
# dscontrol advisor loglevel pop3 110 1
# dscontrol advisor logsize pop3 110 1048576
# dscontrol advisor timeout pop3 110 unlimited
# dscontrol advisor interval nntp 119 5
# dscontrol advisor loglevel nntp 119 1
# dscontrol advisor logsize nntp 119 1048576
# dscontrol advisor timeout nntp 119 unlimited
# dscontrol advisor interval ssl 443 5
# dscontrol advisor loglevel ssl 443 1
# dscontrol advisor logsize ssl 443 1048576
# dscontrol advisor timeout ssl 443 unlimited
#
```

Archivo de configuración de Dispatcher — Sistemas Windows

A continuación se muestra un archivo de configuración de Load Balancer de ejemplo denominado **configuration.cmd.sample** para puede utilizarse con Windows.

```
@echo off
rem configuration.cmd.sample - Archivo de configuración de ejemplo para el
rem componente Dispatcher.
rem

rem dsserver debe iniciarse a través de Servicios

rem

rem
rem Después inicie el ejecutor
rem
rem call dscontrol executor start

rem

rem En el siguiente paso de la configuración de Dispatcher se establecerá la
rem NFA (dirección de no reenvío) y las direcciones
rem del clúster.
rem

rem La NFA se usa para acceder de forma remota a la máquina
rem Dispatcher para fines de configuración de administración. Esta
rem dirección es necesaria puesto que Dispatcher enviará
rem paquetes a las direcciones de clúster.

rem
rem La dirección de clúster es el nombre de sistema principal (o dirección IP) al
rem que se conectarán los clientes remotos.
rem

rem En todo este archivo puede utilizar los nombres de sistema principal y
rem las direcciones IP de manera intercambiable.
```



```

rem NFA=[dirección de no reenvío]
rem CLUSTER=[el nombre de clúster]
rem

rem set NFA=hostname.domain.name
rem set CLUSTER=www.suempresa.com

rem echo "Cargando la dirección de no reenvío"
rem call dscontrol executor set nfa %NFA%

rem
rem Los siguientes mandatos se establecen en los valores por omisión.
rem Utilice estos mandatos para cambiar los valores por omisión

rem call dscontrol executor set fintimeout 30
rem
rem En el siguiente paso de la configuración de Dispatcher se creará
rem un clúster. Dispatcher direccionará las peticiones enviadas a
rem la dirección del clúster a las correspondientes máquinas servidor
rem definidas para dicho clúster. Puede configurar y atender a
rem varias direcciones de clúster con Dispatcher.
rem Emplee una configuración parecida para CLUSTER2, CLUSTER3, etc.
rem

rem echo "Cargando primero la dirección de clúster"
rem call dscontrol cluster add %CLUSTER%

rem
rem Ahora, tenemos que definir los puertos que usará este clúster. Todas
rem las peticiones recibidas por Dispatcher en un puerto definido se
rem reenviará al correspondiente
rem puerto de una de las máquinas servidor.
rem

rem echo "Creando puertos para clúster: %CLUSTER%"
rem call dscontrol port add %CLUSTER%:20+21+80

rem
rem En el último paso se añadirá cada una de las máquinas servidor a
rem los puertos de este clúster. De nuevo, puede utilizar el
rem nombre de sistema principal o la dirección IP de las máquinas servidor.
rem

rem set SERVER1=server1name.domain.name
rem set SERVER2=server2name.domain.name
rem set SERVER3=server3name.domain.name

rem echo "Añadiendo máquinas servidor"
rem call dscontrol server add %CLUSTER%:20+21+80:
rem %SERVER1%+%SERVER2%+%SERVER3%

rem
rem Ahora empezará el equilibrio de carga de los componentes de
rem Dispatcher. El principal componente del equilibrio de carga se denomina
rem gestor y el segundo componente del equilibrio de carga son los
rem asesores. Si el gestor y los asesores no están
rem ejecutándose, Dispatcher envía peticiones en forma de turno rotativo.
rem Una vez que se inicia el gestor, se emplea la ponderación de decisiones
rem en base al número de conexiones nuevas y activas
rem y las peticiones entrantes se envían al mejor
rem servidor. Los asesores ofrecen al gestor una mejor comprensión
rem de la capacidad de los servidores para atender peticiones así como
rem detectar si un servidor está activo. Si un asesor detecta
rem que un servidor está inactivo, se marcará como inactivo (siempre que las
rem proporciones del gestor se hayan establecido de forma que incluyan
rem la entrada del asesor) y no se direccionarán más peticiones al servidor.
rem En el último paso de la configuración de los componentes del equilibrio

```

```

rem de carga se establecerán las proporciones del gestor. El
rem gestor actualiza el peso de cada uno de los servidores basándose
rem en cuatro políticas:

rem 1. El número de conexiones activas en cada servidor
rem 2. El número de nuevas conexiones en cada servidor
rem 3. La entrada de datos desde los asesores.
rem 4. La entrada de datos desde el asesor del nivel del sistema.
rem
rem La suma de estas proporciones debe ser 100. Como ejemplo, si se
rem establecen las proporciones de clúster mediante
rem dscontrol cluster set <cluster> proportions 48 48 4 0
rem otorgará a las conexiones activas y nuevas el 48% de entrada en la
rem ponderación de decisiones, el asesor contribuirá un 4% y
rem no se tendrá en cuenta la entrada del sistema.
rem
rem NOTA: por omisión, las proporciones del gestor están establecidas en
rem 50 50 0 0

rem echo "Iniciando el gestor..."
rem call dscontrol manager start

rem echo "Iniciando el asesor FTP en puerto 21 ..."
rem call dscontrol advisor start ftp 21
rem echo "Iniciando el asesor HTTP en puerto 80 ..."
rem call dscontrol advisor start http 80
rem echo "Iniciando el asesor Telnet en puerto 23 ..."
rem call dscontrol advisor start telnet 23
rem echo "Iniciando el asesor SMTP en puerto 25 ..."
rem call dscontrol advisor start smtp 25
rem echo "Iniciando el asesor POP3 en puerto 110 ..."
rem call dscontrol advisor start pop3 110
rem echo "Iniciando el asesor NNTP en puerto 119 ..."
rem call dscontrol advisor start nntp 119
rem echo "Iniciando el asesor SSL en puerto 443 ..."
rem call dscontrol advisor start ssl 443
rem

rem echo "Definiendo las proporciones del clúster..."
rem call dscontrol cluster set %CLUSTER% proportions 58 40 2 0

rem
rem El último paso de la configuración de la máquina Dispatcher es
rem crear un alias para la tarjeta de interfaz de red (NIC).
rem
rem NOTA: NO utilice este mandato en un entorno de alta
rem disponibilidad. Los scripts go* configurarán la NIC y
rem el bucle de retorno según sea necesario.
rem
rem dscontrol executor configure %CLUSTER%

rem Si la dirección de clúster está en una NIC o subred distinta
rem de la de NFA, utilice el siguiente formato para el mandato cluster
rem configure.
rem dscontrol executor configure %CLUSTER% tr0 0xfffff800
rem donde tr0 es la NIC (tr1 para la segunda tarjeta token ring,
rem en0 para la primera tarjeta ethernet) y 0xfffff800 es
rem una máscara de subred válida para el sitio.
rem

rem
rem Los siguientes mandatos se establecen en los valores por omisión.
rem Utilice estos mandatos como orientación para cambiar los valores por omisión.
rem call dscontrol manager loglevel 1
rem call dscontrol manager logsize 1048576
rem call dscontrol manager sensitivity 5
rem call dscontrol manager interval 2

```

```

rem call dscontrol manager refresh      2
rem
rem call dscontrol advisor interval ftp 21 5
rem call dscontrol advisor loglevel ftp 21 1
rem call dscontrol advisor logsize ftp 21 1048576
rem call dscontrol advisor timeout ftp 21 unlimited
rem call dscontrol advisor interval telnet 23 5
rem call dscontrol advisor loglevel telnet 23 1
rem call dscontrol advisor logsize telnet 23 1048576
rem call dscontrol advisor timeout telnet 23 unlimited
rem call dscontrol advisor interval smtp 25 5
rem call dscontrol advisor loglevel smtp 25 1
rem call dscontrol advisor logsize smtp 25 1048576
rem call dscontrol advisor timeout smtp 25 unlimited
rem call dscontrol advisor interval http 80 5
rem call dscontrol advisor loglevel http 80 1
rem call dscontrol advisor logsize http 80 1048576
rem call dscontrol advisor timeout http 80 unlimited
rem call dscontrol advisor interval pop3 110 5
rem call dscontrol advisor loglevel pop3 110 1
rem call dscontrol advisor logsize pop3 110 1048576
rem call dscontrol advisor timeout pop3 110 unlimited
rem call dscontrol advisor interval nntp 119 5
rem call dscontrol advisor loglevel nntp 119 1
rem call dscontrol advisor logsize nntp 119 1048576
rem call dscontrol advisor timeout nntp 119 unlimited
rem call dscontrol advisor interval ssl 443 5
rem call dscontrol advisor loglevel ssl 443 1
rem call dscontrol advisor logsize ssl 443 1048576
rem call dscontrol advisor timeout ssl 443 unlimited
rem

```

Asesor de ejemplo

A continuación se muestra un archivo de asesor de ejemplo denominado **ADV_sample**.

```

/**
 * ADV_sample: Asesor HTTP de Load Balancer
 *
 *
 * Esta clase define un asesor personalizado de ejemplo para Load Balancer. Como
 * todos los asesores, este asesor personalizado amplía la función de la base del
 * asesor, denominada ADV_Base. Es la base del asesor que en realidad realiza la
 * mayoría de las funciones del asesor, como informar de las cargas a Load Balancer
 * para su uso en el algoritmo de peso de Load Balancer. La base del asesor también
 * realiza operaciones de cierre y conexión de sockets, y proporciona métodos
 * de envío y recepción para que el asesor los emplee. El asesor sólo se utiliza
 * para enviar y recibir datos del puerto del servidor que se está asesorando.
 * Se calcula la duración de los métodos TCP incluidos en la base del asesor para
 * calcular la carga. Un distintivo interno del constructor de ADV_base escribe
 * sobre la carga existente la nueva carga devuelta desde el asesor, si se desea.
 *
 * Nota: en función de un valor fijado en el constructor, la base del asesor
 * suministra la carga al algoritmo de peso a intervalos especificados. Si el
 * asesor real no se ha completado y puede devolver una carga válida, la base del
 * asesor utiliza la carga anterior.
 *
 * DENOMINACIÓN
 *
 * El convenio de denominación es el siguiente:
 *
 * - El archivo debe estar en el siguiente directorio de Load Balancer:
 *
 *    lb/servers/lib/CustomAdvisors/ (lb\servers\lib\CustomAdvisors en Windows)
 *
 * - El nombre del asesor debe ir precedido de "ADV_". Sin embargo, el asesor

```

```

* sólo puede empezar con el nombre; por ejemplo, el asesor "ADV_sample"
* puede empezar con "sample".
*
* - El nombre del asesor debe indicarse en minúsculas.
*
* Por lo tanto, teniendo presente estas normas, este ejemplo se denomina:
*
*         <directorio base>/lib/CustomAdvisors/ADV_sample.class
*
* Los asesores, al igual que el resto de Load Balancer, deben compilarse con la
* versión prereq de Java. Para garantizar el acceso a las clases de Load Balancer,
* asegúrese de que el archivo ibmlb.jar (que se encuentra en el directorio lib
* del directorio base) está incluido en la CLASSPATH del sistema.
*
* Métodos proporcionados por ADV_Base:
*
* - ADV_Base (Constructor):
*
*   - Parámetros
*     - String sName = Nombre del asesor
*     - String sVersion = Versión del asesor
*     - int iDefaultPort = Número de puerto por omisión sobre el que asesorar
*     - int iInterval = Intervalo sobre el que asesorar sobre los servidores
*     - String sDefaultName = No se utiliza. Debe pasarse como "".
*     - boolean replace = True - sustituye el valor de carga que calcula
*                           la base del asesor
*                           False - añade el valor de carga que calcula
*                           la base del asesor
*   - Retorno
*     - Los constructores no tienen valores de retorno.
*
* Puesto que la base del asesor se basa en hebras, tiene otros métodos
* disponibles que un asesor puede usar. Se puede hacer referencia a estos métodos
* con el parámetro CALLER pasado en getLoad().
*
* Estos métodos son los siguientes:
*
* - send - Envía un paquete de información en la conexión de socket establecida
*         al servidor del puerto especificado.
*   - Parámetros
*     - String sDataString - Los datos que deben enviar en el formato de serie
*   - Retorno
*     - int RC - Si los datos se han enviado satisfactoriamente; cero indica que
*               los datos se han enviado; un entero negativo indica un error.
*
* - receive - Recibe información de la conexión del socket.
*   - Parámetros
*     - StringBuffer sbDataBuffer - Los datos recibidos durante la llamada de
*                                   recepción
*   - Retorno
*     - int RC - Si los datos se recibieron satisfactoriamente; cero
*               indica que los datos se enviaron; un entero negativo indica
*               un error.
*
* Si la función que proporciona la base del asesor no es suficiente,
* puede crear la función adecuada dentro del asesor y
* se ignorarán los métodos que proporciona la base del asesor.
*
* Una pregunta importante en relación a la carga devuelta es si se debe aplicar
* si la carga que se genera dentro de la base del asesor,
* o se debe sustituir; hay instancias válidas para las dos situaciones.
*
* Este ejemplo es fundamentalmente el asesor HTTP de Load Balancer. Funciona de una
* forma muy simple: se emite una petición de envío: una petición de cabecera HTTP.
* Una vez que se recibe la respuesta, el método getLoad finaliza, indicando a la
* base del asesor que detenga la medición del tiempo de la petición. Entonces el

```

```

* método finaliza. La información devuelta no se analiza; la carga se basa en el
* tiempo necesario en realizar las operaciones de envío y recepción.
*/

```

```

package CustomAdvisors;
import com.ibm.internet.nd.advisors.*;

public class ADV_sample extends ADV_Base implements ADV_MethodInterface
{
    String COPYRIGHT =
        "(C) Copyright IBM Corporation 1997, All Rights Reserved.\n";

    static final String  ADV_NAME          = "Sample";
    static final int     ADV_DEF_ADV_ON_PORT = 80;
    static final int     ADV_DEF_INTERVAL  = 7;

    // Nota: la mayoría de los protocolos de servidor requieren un retorno de
    //        carro ("\r") y un salto de línea ("\n") al final de los mensajes.
    //        Si es así, inclúyalos en la serie aquí.
    static final String  ADV_SEND_REQUEST  =
        "HEAD / HTTP/1.0\r\nAccept: */*\r\nUser-Agent: " +
        "IBM_Load_Balancer_HTTP_Advisor\r\n\r\n";

    /**
     * Constructor.
     *
     * Parámetros: Ninguno; pero el constructor de ADV_Base tiene varios parámetros
     *             que deben pasarse.
     */
    public ADV_sample()
    {
        super( ADV_NAME,
              "2.0.0.0-03.27.98",
              ADV_DEF_ADV_ON_PORT,
              ADV_DEF_INTERVAL,
              "", // no se utiliza
              false);
        super.setAdvisor( this );
    }

    /**
     * ADV_AdvisorInitialize
     *
     * Se inicia cualquier inicialización específica del asesor que debe tener lugar
     * después de la base del asesor. Este método sólo se invoca una vez y
     * normalmente no se utiliza.
     */
    public void ADV_AdvisorInitialize()
    {
        return;
    }

    /**
     * getLoad()
     *
     * La base del asesor llama a este método para completar la operación del
     * asesor, basándose en detalles específicos del protocolo. En este ejemplo del
     * asesor, sólo es necesario emitir un sólo envío y recepción; si es necesario
     * usa una lógica más compleja, se pueden emitir varios envíos y recepciones.
     * Por ejemplo, una respuesta puede recibirse y analizarse. Basándose en la
     * información que se obtiene, se podría emitir otro envío y recepción.
     *
     * Parámetros:
     */
}

```

```

* - iConnectTime - La carga actual relativa al intervalo de tiempo que ha
*                  tardado en llevarse a cabo la conexión con el servidor en
*                  el puerto especificado.
*
* - caller - Una referencia a la clase base del asesor donde los métodos
*             que proporciona Load Balancer van a realizar peticiones TCP,
*             principalmente envíos y recepciones.
*
* Resultados:
*
* - La carga, un valor expresado en milisegundos, que puede añadirse a la
*   carga existente o que puede sustituir a la misma, según lo
*   determina el distintivo "replace" del constructor.
*
*   Cuánto mayor sea la carga, más tiempo se necesitará para que el servidor
*   responda; por lo tanto, menor será el peso dentro de Load Balancer.
*
*   Si el valor es negativo, se da por supuesto un error. Un error de un asesor
*   indica que el servidor al que el asesor intenta llegar no es accesible y
*   que se ha identificado como inactivo. Load Balancer no intentará equilibrar la
*   carga en un servidor que está inactivo. Load Balancer reanudará el equilibrio
*   de carga en el servidor cuando se reciba un valor positivo.
*
*/
public int getLoad(int iConnectTime, ADV_Thread caller)
{
    int iRc;
    int iLoad = ADV_HOST_INACCESSIBLE; // -1

    // Enviar petición TCP
    iRc = caller.send(ADV_SEND_REQUEST);
    if (iRc >= 0)
    {
        // Realizar una recepción
        StringBuffer sbReceiveData = new StringBuffer("");
        iRc = caller.receive(sbReceiveData);

        /**
         * En una modalidad de asesor (el distintivo "replace" es false), la carga
         * devuelta es 0 o 1, lo que indica que el servidor está activo o inactivo.
         * Si la recepción es satisfactoria, se devuelve una carga de cero, lo
         * que indica que se va a usar la carga incluida dentro del asesor base.
         *
         * De lo contrario (el distintivo "replace" es true), devuelva el valor de
         * carga que desee.
         */

        if (iRc >= 0)
        {
            iLoad = 0;
        }
    }
    return iLoad;
}

} // Final de - ADV_sample

```

Apéndice D. Ejemplo de configuración de alta disponibilidad de 2 niveles con Dispatcher, CBR y Caching Proxy

En este apéndice se describe cómo establecer una configuración de alta disponibilidad de 2 niveles combinando las posibilidades de dos componentes de Load Balancer (el componente Dispatcher y el componente CBR) junto con Caching Proxy.

Configuración de la máquina servidor

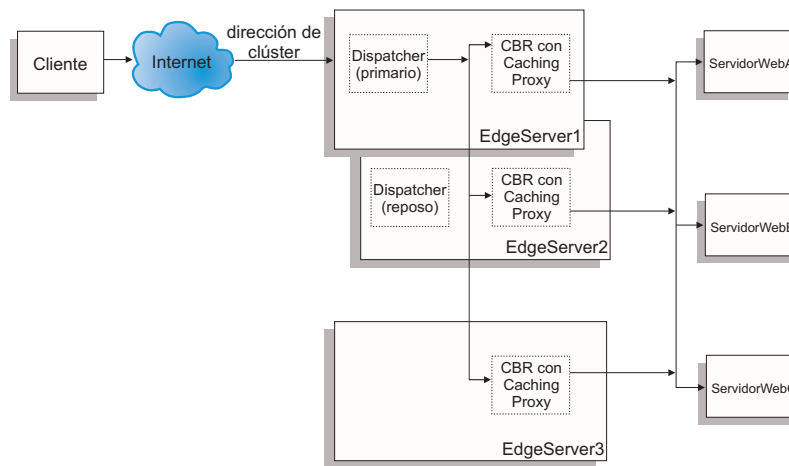


Figura 46. Ejemplo de configuración de alta disponibilidad de 2 niveles con Dispatcher, CBR y Caching Proxy

A continuación se detalla la configuración de máquina servidor para la Figura 46:

- EdgeServer1: máquina de Dispatcher primaria (de alta disponibilidad) con ubicación compartida con CBR y Caching Proxy que equilibran la carga entre servidores Web
- EdgeServer2: máquina de Dispatcher de reserva (de alta disponibilidad) con ubicación compartida con CBR y Caching Proxy
- EdgeServer3: máquina CBR y Caching Proxy
- WebServerA, WebServerB, WebServerC: servidores Web finales

La Figura 46 muestra una representación básica de varios servidores (EdgeServer1, EdgeServer2, EdgeServer3) que equilibran la carga entre varios servidores Web finales. El componente CBR utiliza Caching Proxy para reenviar peticiones según el contenido del URL a los servidores Web finales. El componente Dispatcher su utiliza para equilibrar la carga de componentes CBR entre los servidores EdgeServers. Se utiliza la función de alta disponibilidad del componente Dispatcher para asegurarse de que continúen las peticiones a los servidores finales aún cuando la máquina primaria de alta disponibilidad (EdgeServer1) diera un error en algún momento.

Instrucciones básicas de configuración:

- Configure Caching Proxy para que sea el mismo en todos los servidores EdgeServers. Con el fin de mejorar la accesibilidad global a las páginas Web en los servidores finales, configure Caching Proxy para realizar la colocación en

antememoria de la memoria. Esto permitirá a los servidores EdgeServers colocar en antememoria las páginas Web que más se solicitan. Para obtener más información sobre cómo configurar Caching Proxy, consulte el manual *Guía de administración de Caching Proxy*.

- Defina la dirección del clúster y los puertos para que sean iguales en los dos componentes: CBR y Dispatcher de Load Balancer.
- Configure el componente CBR para que sea igual entre todos los servidores EdgeServers. Utilice los servidores Web A, B y C como los servidores en los puertos que desea definir para el clúster. Para obtener más información para configurar CBR, consulte el Capítulo 11, “Configuración de CBR (Content Based Routing)”, en la página 109.
- Configure el componente Dispatcher para que sea igual en EdgeServer1 y EdgeServer2. Defina todos los EdgeServers como los servidores en los puertos que desea que se definan en el clúster para que el Dispatcher los equilibre la carga. Para obtener más información sobre cómo configurar el Dispatcher, consulte el Capítulo 7, “Configuración de Dispatcher”, en la página 63.
- Configure EdgeServer1 como la máquina primaria de alta disponibilidad y EdgeServer2 como la máquina de reserva (respaldo) de alta disponibilidad. Para obtener más información, consulte el apartado “Alta disponibilidad” en la página 204.

Nota:

1. Para evitar que se muestren las direcciones del servidor final en el URL en un cliente, tendrá que establecer la directiva ReversePass para cada dirección de servidor final en el archivo de configuración de Caching Proxy.
2. Para asegurarse de que se utiliza eficazmente la colocación en antememoria de la Web, establezca la directiva “Caching” en “ON” y aumente el valor de la directiva “CacheMemory” al tamaño necesario en el archivo de configuración de Caching Proxy.
3. Líneas de ejemplo a las que se hace referencia en las notas 1 a 2 (anteriores):

```
Caching                ON
CacheMemory            128000 K
ReversePass /* http://websrvA.empresa.com/* http://www.empresa.com/*
```
4. Recuerde poner un alias a la dirección del clúster en la tarjeta de interfaz de red para EdgeServer1 y un alias a la dirección del clúster en el dispositivo de bucle de retorno en los EdgeServers restantes.
5. Si utiliza la plataforma Linux para los EdgeServers, quizá tenga que instalar un parche para el kernel Linux o utilizar una alternativa a poner un alias al dispositivo de bucle de retorno. Para obtener más información, consulte el apartado “Alternativas de alias de bucle de retorno de Linux cuando se utiliza el reenvío MAC de Load Balancer” en la página 78.
6. Para CBR, no se debe utilizar la afinidad de puerto (tiempo de permanencia en memoria) cuando se utilizan normas de contenido, de lo contrario, no se activarán dichas normas mientras se procesan peticiones a los servidores Web finales.

Archivos de configuración de ejemplo:

Los archivos de configuración de ejemplo siguientes son similares a los archivos que se crean cuando se establece una configuración de Edge Components como se detalla en la Figura 46 en la página 489. Los archivos de configuración de ejemplo

representan los archivos para los componentes Dispatcher y CBR de Load Balancer. En la configuración de ejemplo, se utiliza un solo adaptador Ethernet para cada una de las máquinas EdgeServer y todas las direcciones se representan dentro de una subred privada. Los archivos de configuración de ejemplo utilizan las siguientes direcciones IP para las máquinas especificadas:

- EdgeServer1 (EdgeServer primario de alta disponibilidad): 192.168.1.10
- EdgeServer2 (EdgeServer de reserva de alta disponibilidad): 192.168.1.20
- EdgeServer3 (EdgeServer de colocación en antememoria de la Web): 192.168.1.30
- Dirección de clúster del sitio Web: 192.168.1.11
- WebServersA-C (servidores Web de reserva): 192.168.1.71, 192.168.1.72 y 192.168.1.73

Archivo de configuración de ejemplo para el componente Dispatcher en EdgeServer primario de alta disponibilidad:

```
dscontrol executor start

dscontrol cluster add 192.168.1.11 primaryhost 192.168.1.10

dscontrol port add 192.168.1.11:80

dscontrol server add 192.168.1.11:80:edgeserver1 address 192.168.1.10
dscontrol server add 192.168.1.11:80:edgeserver2 address 192.168.1.20
dscontrol server add 192.168.1.11:80:edgeserver3 address 192.168.1.30

dscontrol manager start manager.log 10004

dscontrol highavailability heartbeat add 192.168.1.10 192.168.1.20
dscontrol highavailability backup add primary auto 4567
```

Archivo de configuración de ejemplo para el componente CBR en los EdgeServers:

```
cbrcontrol set loglevel 1
cbrcontrol executor start

cbrcontrol cluster add 192.168.1.11

cbrcontrol port add 192.168.1.11:80

cbrcontrol server add 192.168.1.11:80:webserverA address 192.168.1.71
cbrcontrol server add 192.168.1.11:80:webserverB address 192.168.1.72
cbrcontrol server add 192.168.1.11:80:webserverC address 192.168.1.73

cbrcontrol rule add 192.168.1.11:80:webA_rule type content
  pattern (URI=*WSA*)|(URI=*wsA*) priority 21
cbrcontrol rule useserver 192.168.1.11:80:webA_rule webserverA

cbrcontrol rule add 192.168.1.11:80:webB_rule type content
  pattern (URI=/WS_B*) priority 22
cbrcontrol rule useserver 192.168.1.11:80:webB_rule webserverB

cbrcontrol rule add 192.168.1.11:80:webC_rule type content
  pattern URI=*webC* priority 23
cbrcontrol rule useserver 192.168.1.21:80:webC_rule webserverC
```

Apéndice E. Avisos

Esta información se ha desarrollado para productos y servicios proporcionados en los Estados Unidos.

Es posible que IBM no ofrezca los productos, servicios o funciones que se tratan en este documento en otros países. Consulte el representante de IBM de su localidad para obtener información acerca de los productos y servicios que están disponibles actualmente en su localidad. Cualquier referencia que se haga a un producto, programa o servicio de IBM no implica que sólo se pueda utilizar dicho producto, programa o servicio de IBM. En su lugar, se puede utilizar cualquier producto, programa o servicio funcionalmente equivalente que no vulnere ningún derecho de propiedad intelectual de IBM. Sin embargo, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o aplicaciones pendientes de patente que conciernan al tema descrito en este documento. La posesión de este documento no le da ninguna licencia sobre estas patentes. Puede enviar preguntas acerca de licencias por escrito a:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594
Estados Unidos

Para preguntas acerca de licencias referentes a información de doble byte (DBCS), póngase en contacto con el Departamento de propiedad intelectual de IBM de su país o envíe sus preguntas por escrito a:

IBM World Trade Asia Corporation Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japón

El siguiente párrafo no se aplica al Reino Unido ni a ningún otro país donde estas disposiciones no coincidan con la legislación local:

INTERNATIONAL BUSINESS MACHINES CORPORATION LE PROPORCIONA ESTE DOCUMENTO "TAL CUAL", SIN GARANTÍAS DE NINGÚN TIPO, NI EXPLÍCITAS NI IMPLÍCITAS, INCLUIDAS, AUNQUE SIN LIMITARSE A LAS MISMAS, LAS GARANTÍAS O CONDICIONES IMPLÍCITAS DE NO INFRINGIMIENTO, COMERCIALIZACIÓN O ADECUACIÓN A UN PROPÓSITO DETERMINADO. Algunas legislaciones no contemplan la exclusión de garantías, explícitas o implícitas en algunas transacciones, por lo que puede haber usuarios a los que no les afecte dicha regla.

Esta publicación puede contener imprecisiones técnicas o errores tipográficos. Se realizan cambios periódicos en la información aquí contenida; estos cambios se incorporarán en nuevas ediciones o en el documento. IBM se reserva el derecho de realizar mejoras y/o cambios en los productos y/o programas descritos en esta publicación en cualquier momento sin previo aviso.

Cualquier referencia en esta información a sitios Web que no son de IBM se proporciona solamente para su comodidad y no equivale de ninguna manera a una aprobación de esos sitios Web. El material de dichos sitios Web no forma parte del material correspondiente a este producto IBM y el uso de estos sitios Web se realiza bajo riesgo del usuario.

IBM puede utilizar o distribuir cualquier información que el usuario le proporcione de la manera que considere adecuada sin incurrir en ninguna obligación con el usuario.

Los usuarios autorizados de este programa que deseen tener información sobre éste con el propósito de posibilitar: (i) el intercambio de información entre programas creados independientemente y otros programas (incluyendo éste) y (ii) la utilización mutua de la información que se ha intercambiado, deben ponerse en contacto con:

IBM Corporation
Attn.: G7IA./503.
P.O. Box 12195
3039 Cornwallis Rd.
Research Triangle Park, N.C. 27709-2195
Estados Unidos

Es posible que esta información esté disponible, sujeta a los términos y condiciones adecuados, y que en algunos casos incluya el pago de una tarifa.

El programa con licencia descrito en este documento y todos los materiales con licencia disponibles para el mismo son proporcionados por IBM bajo los términos del acuerdo IBM International Program License Agreement o cualquier acuerdo equivalente entre nosotros.

Los datos sobre rendimiento aquí contenidos se han determinado en un entorno controlado. Por tanto, los resultados obtenidos en otros entornos operativos pueden variar de forma significativa. Es posible que algunas medidas se hayan tomado en sistemas de nivel de desarrollo y no existe ninguna garantía de que dichas medidas se repitan en sistemas disponibles a nivel general. Además, es posible que algunas medidas se hayan estimado mediante extrapolación. Los resultados reales pueden variar. Los usuarios de este documento deben verificar los datos aplicables para su entorno específico.

La información referente a productos que no son de IBM se ha obtenido de los suministradores de estos productos, sus anuncios publicados u otras fuentes disponibles para el público. IBM no ha probado estos productos y no puede confirmar la precisión del rendimiento, compatibilidad y otras afirmaciones relacionadas con productos que no son de IBM. Las preguntas acerca de las posibilidades de productos que no son de IBM deben dirigirse a los suministradores de estos productos.

Todas las declaraciones referentes a acciones e intenciones futuras de IBM pueden cambiar o ser retiradas sin aviso previo y solamente representan objetivos.

Esta información contiene ejemplos de datos e informes utilizados en operaciones comerciales diarias. Para ilustrarlos de la forma más completa posible, los ejemplos pueden incluir nombres de particulares, empresas, marcas y productos. Todos estos nombres son ficticios y cualquier parecido con nombres y direcciones utilizadas por una empresa de negocios real es mera coincidencia.

Si consulta esta información en copia de software, muchas de las fotografías y las ilustraciones en color no aparecerán.

Marcas registradas

Los siguientes términos son marcas registradas o marcas comerciales de IBM Corporation en Estados Unidos y/o en otros países.

AFS
AIX
DFS
IBM
iSeries
NetView
OS/2
Redbooks
RS/6000
SecureWay
ViaVoice
WebSphere
zSeries

Java y todas las marcas registradas y logotipos basados en Java son marcas registradas de Sun Microsystems, Inc. en Estados Unidos y/o en otros países.

Microsoft, Windows, Windows NT y el logotipo de Windows son marcas registradas de Microsoft Corporation en los Estados Unidos y/o en otros países.

Intel, Intel Inside (logotipos), MMX y Pentium son marcas registradas de Intel Corporation en los Estados Unidos y/o en otros países.

UNIX es una marca registrada de The Open Group en los Estados Unidos y en otros países.

Linux es una marca registrada de Linus Torvalds en los Estados Unidos y en otros países.

Otros nombres de empresas, productos o servicios pueden ser marcas registradas o marcas de servicio de terceros.

Glosario

A

ACK. Bit de control (acuse de recibo) que no ocupa ningún espacio de secuencia e indica que el campo de acuse de recibo de este segmento especifica que el siguiente número de secuencia de este segmento está esperando recibir, esto es, acusar recibo de, todos los números de secuencia anteriores.

afinidad entre puertos. La afinidad entre puertos es la característica de afinidad (permanencia en memoria) avanzada que permite abarcar varios puertos. Consulte también tiempo de permanencia en memoria.

agente. (1) En gestión de sistemas, usuario que, para una interacción determinada, ha asumido la función de un agente. (2) Entidad que representa uno o más objetos gestionados por medio de (a) la emisión de notificaciones relacionadas con objetos y (b) el manejo de peticiones de los gestores de operaciones de gestión para modificar o consultar los objetos.

alcance. En Dispatcher, asesor que emite mandatos ping a un destino determinado e informa de si el destino está respondiendo.

alias. Nombre adicional asignado a un servidor. Un alias independiza al servidor del nombre de su sistema principal. El alias debe estar definido en el servidor de nombres de dominio.

alias de bucle. Dirección IP alternativa asociada a la interfaz de bucle. La dirección alternativa tiene como efecto secundario la ventaja de que no se anuncia en interfaz real.

alta disponibilidad. Función de Load Balancer por medio de la cual una máquina Load Balancer puede tomar el control de las funciones de otra si sufre alguna anomalía.

alta disponibilidad mutua. Permite que dos máquinas Dispatcher puedan ser entre sí tanto la máquina primaria como la máquina de reserva. Consulte también, reserva, alta disponibilidad, primaria.

ancho de banda. La diferencia entre las frecuencias superiores e inferiores de un canal de transmisión; la cantidad de datos que se envían a través de un circuito de comunicaciones dado por segundo.

API. Interfaz de programación de aplicaciones. Interfaz mediante la cual un programa de aplicación accede al sistema operativo o a otros servicios. Una API se define a nivel de código fuente y proporciona un nivel de abstracción entre la aplicación y el núcleo (u otros programas de utilidad privilegiados) para asegurar la portabilidad del código.

asesor. Los asesores son una función de Load Balancer. Los asesores reúnen y analizan la información de retorno de los servidores individuales e informan la función de gestor.

asistente. Diálogo dentro de una aplicación que utiliza instrucciones paso a paso para guiar al usuario en una tarea específica.

C

Caching Proxy. Servidor proxy de colocación en antememoria que puede ayudar a acelerar el tiempo de respuesta del usuario final a través de esquemas de gestión de antememoria altamente eficaces. El filtrado PICS flexible ayuda a los administradores de redes a acceder a información basada en Web en una ubicación central.

Calidad del servicio (QoS). Las propiedades de rendimiento de un servicio de red, incluyendo rendimiento, retraso de la transmisión y prioridad. Algunos protocolos permiten que los paquetes o el flujo de datos incluyan los requisitos QoS.

CBR. Content Based Routing de WTE. Componente de Load Balancer. CBR funciona junto con Caching Proxy para realizar el equilibrio de carga de las peticiones entrantes, en base al contenido de las páginas Web utilizando tipos de normas específicos, a servidores HTTP o HTTPS.

cbrcontrol. Proporciona la interfaz para el componente CBR (Content Based Router) de Load Balancer.

cbrserver. En CBR (Content Based Router), maneja las peticiones desde la línea de mandatos para el ejecutor, gestor y asesores.

ccocontrol. En Cisco CSS Controller, proporciona la interfaz con el Conmutador Cisco CSS.

ccoserver. En Cisco CSS Controller, maneja las peticiones desde la línea de mandatos para los consultores.

CGI. Common Gateway Interface. Estándar para el intercambio de información entre un servidor Web y un programa externo. El programa externo puede estar escrito en cualquier lenguaje soportado por el sistema operativo y ejecuta tareas que el servidor no realiza habitualmente, como el proceso de formularios.

Cisco CSS Controller. Componente de IBM Load Balancer. Cisco CSS Controller utiliza la tecnología de Load Balancer para proporcionar información en tiempo real sobre el equilibrio de carga al Conmutador Cisco Content Services.

cliente. Sistema o proceso que solicita un servicio de otro sistema o proceso. Por ejemplo, una estación de trabajo o un PC que solicita documentos HTML de Lotus Domino Go Webserver es un cliente de dicho servidor.

clúster. En Dispatcher, es un grupo de servidores TCP o UDP que se utilizan para el mismo propósito y que se identifican por el mismo nombre de sistema principal. Consulte también célula.

Conmutador Cisco CSS. Cualquiera de los conmutadores CSS 11000 de Cisco, utilizados para el reenvío de paquetes y el direccionamiento de contenido.

Conmutador Nortel Alteon Web. Conmutador Nortel Alteon ACE Director Series y Conmutador Nortel Alteon 180 Series de la cartera de Alteon Web Switching, utilizados para el reenvío de paquetes y el direccionamiento de contenidos.

consultor. Recopila métricas de servidor de los servidores de los que se está realizando equilibrio de carga y envía la información de peso del servidor al conmutador que realiza el equilibrio de carga.

Contenido de propietario. Representa el nombre de propietario y la norma de contenido de un propietario, definidos ambos en nidos Conmutador Cisco CSS.

controlador. Conjunto de uno o más consultores.

Conversión de direcciones de red. NAT, o conversor de direcciones de red, LAN virtual. Dispositivo de hardware que se está desarrollando actualmente y que se utiliza para ampliar las direcciones de Internet que ya se utilizan. Permite utilizar direcciones IP duplicadas dentro de una empresa y direcciones exclusivas fuera.

Conversión de puertos de direcciones de red (NAPT). NAPT, también conocido como correlación de puerto. Permite configurar múltiples daemons de servidor en un servidor físico para escuchar a diferentes números de puerto.

cortafuegos. Sistema que conecta una red privada, como la de una empresa, a una red pública, como Internet. Contiene programas que limitan el acceso entre dos redes. Consulte también *pasarela proxy*.

D

daemon. Supervisor de disco y ejecución. Programa que no se entra en acción explícitamente sino que permanece en estado suspendido esperando que suceda(n) determinada(s) condición(es). La idea es que quien realiza la acción de la condición no necesita saber que un daemon está esperando (aunque a menudo un programa realizará una acción sólo porque sabe que invocará implícitamente a un daemon).

dirección. Código exclusivo asignado a cada dispositivo o estación de trabajo conectado a una red. Una dirección IPv4 estándar es un campo de dirección de 32 bits que contiene dos partes. La primera parte es la dirección de red, la segunda el número del sistema principal. Una dirección IPv6 es un campo de dirección de 128 bits que admite un número de direcciones mucho mayor que IPv4. También admite características adicionales como el direccionamiento "multicast" y "anycast".

dirección de alcance. En alta disponibilidad para el componente Dispatcher, dirección del destino al que debe enviar el asesor los mandatos PING para determinar si el destino está respondiendo.

dirección de destino. Dirección de la máquina asociada de alta disponibilidad a la que se envían los pulsos y las respuestas.

dirección de métrica. La dirección en la que se conecta la métrica del sistema.

dirección de no reenvío (NFA). Dirección IP primaria de la máquina Load Balancer, utilizada para administración y configuración.

dirección de retorno. Una dirección IP o nombre de sistema principal exclusivo. Se configura en la máquina Dispatcher y Dispatcher lo utiliza como su dirección origen al realizar el equilibrio de carga de las peticiones del cliente al servidor.

dirección de servidor. El código exclusivo asignado a cada sistema que proporciona servicios compartidos a otros sistemas a través de una red; por ejemplo un servidor de archivos, un servidor de impresión o un servidor de correo. La dirección del servidor puede ser la dirección IP o el nombre del sistema principal.

dirección del clúster. En el componente Dispatcher, dirección a la que se conectan los clientes.

dirección IP. Dirección del protocolo Internet (IP). Dirección exclusiva que especifica la ubicación real de cada dispositivo o estación de trabajo de una red. También se conoce como una dirección de Internet.

dirección MAC. Dirección de control de acceso al medio. La dirección de hardware de un dispositivo conectado a un medio de red compartido.

dirección origen. En alta disponibilidad para el componente Dispatcher, dirección de la máquina asociada de alta disponibilidad que envía los pulsos.

direccionador. Dispositivo que reenvía paquetes entre redes. La decisión del reenvío se basa en la información en la capa de red y en las tablas de direccionamiento, a menudo construidas por productos de direccionamiento.

Dispatcher. Componente de Load Balancer que equilibra eficazmente el tráfico TCP o UDP entre grupos de servidores individuales enlazados. La máquina Dispatcher es el servidor que ejecuta el código de Dispatcher.

dscontrol. Proporciona la interfaz para el componente Dispatcher de Load Balancer.

dsserver. En Dispatcher, maneja las peticiones desde la línea de mandatos para el ejecutor, gestor y asesores.

E

ejecutor. Una de las funciones de Load Balancer. El ejecutor direcciona las peticiones a los servidores TCP o UDP y también supervisa el número de conexiones nuevas, activas y finalizadas y realiza el proceso de recogida de basura de las conexiones completadas o restablecidas. El ejecutor suministra las conexiones nuevas a la función de gestor.

escalable. Relativo a la posibilidad que poseen los sistemas de adaptarse fácilmente a una mayor o menor intensidad de uso, volumen o demanda. Por ejemplo, un sistema escalable puede adaptarse eficazmente para que pueda funcionar con redes mayores o menores efectuando tareas de diversa complejidad.

estación de gestión de red. En SNMP (Protocolo simple de gestión de red), estación que ejecuta los programas de aplicación de gestión que supervisan y controlan los elementos de red.

estado FIN. Estado de una transacción que ha finalizado. Una vez que una transacción se encuentra en estado FIN, los procesos de recogida de basura de Load Balancer pueden vaciar la memoria reservada para la conexión.

estrategia. En alta disponibilidad de Dispatcher, palabra clave para especificar de qué modo se efectuará la recuperación cuando se produzca una anomalía en la máquina activa.

Ethernet. El tipo estándar para redes de área local (LAN). Permite que múltiples estaciones accedan a un medio de transmisión cuando lo deseen sin coordinación previa, evita la contención al utilizar detención de portadora y deferencia y resuelve la contención utilizando la detección de colisiones y la transmisión. Los protocolos de software utilizados por Ethernet pueden variar pero incluyen TCP/IP.

F

FIN. Bit de control (final) que ocupa un número de secuencia y que indica que el remitente no enviará mas datos o controles que ocupen espacio de secuencia.

final del rango. En el equilibrio de carga basado en normas, valor superior especificado en una norma. El valor por omisión depende del tipo de norma.

FQDN. Nombre de dominio calificado al completo. El nombre completo de un sistema, que consiste de su nombre de sistema local y su nombre de dominio, incluyendo el dominio de nivel superior (TLD). Por ejemplo, "venera" es un nombre de sistema principal y "venera.isi.edu" es un FQDN. Un FQDN debería ser suficiente para determinar una dirección de Internet exclusiva para cualquier sistema principal de Internet. Este proceso, llamado "resolución de nombres", utiliza el sistema de nombres de dominio (DNS).

FTP (File Transfer Protocol). Protocolo de aplicaciones utilizado para transferir archivos a y desde sistemas en redes. FTP requiere un ID de usuario y a veces una contraseña para permitir el acceso a los archivos de un sistema principal remoto.

G

gestor. Una de las funciones de Load Balancer. El gestor establece los pesos basándose en contadores internos del ejecutor y en la realimentación proporcionada por los asesores. El ejecutor utilizará los pesos para efectuar el equilibrio de carga.

GRE. Encapsulamiento genérico de direccionamiento. Un protocolo que permite a un protocolo de red arbitrario A ser transmitido mediante cualquier otro protocolo arbitrario B, encapsulando los paquetes de A dentro de paquetes GRE, que, a su vez, se contienen dentro de paquetes de B.

H

HTML (Lenguaje de marcación de hipertexto). Es el lenguaje que se utiliza para crear documentos de hipertexto. Los documentos de hipertexto incluyen enlaces con otros documentos que contienen información adicional acerca del término o tema resaltado. HTML controla el formato del texto y la posición de las áreas de entrada de formularios, por ejemplo, al igual que los enlaces navegables.

HTTP (Protocolo de transferencia de hipertexto). Protocolo utilizado para transferir y visualizar documentos de hipertexto.

HTTPS (Protocolo de transferencia de hipertexto, seguro). Protocolo utilizado para transferir y visualizar documentos de hipertexto utilizando SSL.

I

ICMP. Protocolo de control de mensajes de Internet. Control de mensajes y protocolo de notificación de errores entre un servidor principal y una pasarela con Internet.

IMAP. Protocolo de acceso de mensajes de Internet. Protocolo que permite a un cliente acceder y manipular mensajes de correo electrónico en un servidor. Permite manipular las carpetas de mensajes remotos, de un modo equivalente a nivel funcional a los buzones locales.

inicio del rango. En el equilibrio de carga basado en normas, un valor inferior especificado en una norma. El valor por omisión depende del tipo de norma.

inmovilizar. Finalizar un proceso permitiendo que las operaciones se lleven a término normalmente.

interfaz de bucle de retorno. Interfaz que ignora las funciones de comunicación innecesarias cuando la información está dirigida a una entidad dentro del mismo sistema.

Internet. Conjunto mundial de redes interconectadas que utiliza el conjunto de protocolos Internet y permiten el acceso público.

intranet. Red segura y privada que integra los estándares y las aplicaciones de Internet (como por ejemplo los navegadores Web) en la estructura de red informática existente de una organización.

IP. Protocolo Internet. Protocolo sin conexión que dirige datos a través de una red o redes interconectadas. IP actúa como un intermediario entre las capas superiores de protocolo y la capa física.

IPSEC. Seguridad del protocolo de Internet. Estándar de seguridad para garantizar la seguridad en la red o en la capa de proceso de paquetes de las comunicaciones de red.

L

LAN. Red de área local. Una red de dispositivos conectada dentro de un área geográfica limitada para las comunicaciones que puede conectarse a una red mayor.

M

máquina servidor. Servidor que Dispatcher agrupa con otros servidores para formar un solo servidor virtual. Dispatcher equilibra el tráfico entre las máquinas servidor. Sinónimo de servidor en clúster.

máquina servidor TCP. Servidor que Load Balancer agrupa con otros servidores para formar un solo servidor virtual. Load Balancer equilibra el tráfico TCP entre las máquinas servidor TCP. Sinónimo de servidor en clúster.

marcar como activo. Permitir que un servidor reciba nuevas conexiones.

marcar como inactivo. Interrumpir todas las conexiones activas con un servidor y detener cualquier conexión o paquete nuevo que se envíe a ese servidor.

máscara de subred. Para IPv4, máscara de 32 bits que se utiliza para identificar los bits de dirección de subred en la parte correspondiente al sistema principal de una dirección IP.

Metric Server. Anteriormente conocido como Server Monitor Agent (SMA). Metric Server proporciona métrica específica del sistema al gestor de Load Balancer.

métrica. Un proceso o mandato que devuelve un valor numérico que puede utilizarse para el equilibrio de carga en la red; por ejemplo, el número de usuarios conectados actualmente.

MIB. (1) Management Information Base. Conjunto de objetos a los que se puede acceder por medio de un protocolo de gestión de red. (2) Definición para la información de gestión que especifica la información que hay disponible en un sistema principal o en una pasarela y las operaciones permitidas.

N

nalcontrol. Proporciona la interfaz para el componente Nortel Alteon Controller de Load Balancer.

nalserver. En Nortel Alteon Controller, maneja las peticiones desde la línea de mandatos para los consultores.

netmask. Para IPv4, máscara de 32 bits que se utiliza para identificar los bits de dirección de subred en la parte correspondiente al sistema principal de una dirección IP.

NIC. Tarjeta de interfaz de red. Una placa de circuitos adaptadores instalada en un sistema que proporciona conexión a una red.

NNTP. Protocolo de transferencia de noticias de red. Protocolo TCP/IP para transferir nuevos artículos.

nodo gestionado. En comunicaciones Internet, una estación de trabajo, un servidor o un direccionador que contiene un agente de gestión de red. En el protocolo Internet (IP), el nodo gestionado contiene generalmente un agente SNMP (Protocolo simple de gestión de red).

nombre de sistema principal. Nombre simbólico asignado a un sistema principal. Los nombres de sistema principal se resuelven en direcciones IP a través de un servidor de nombres de dominio.

nombre de sitio. Un nombre de sitio es un nombre de sistema principal que no es posible resolver y que solicitará el cliente. Por ejemplo, un sitio Web con 3 servidores (1.2.3.4, 1.2.3.5 y 1.2.3.6) configurado con el nombre de sitio *www.dnsload.com*. Cuando un cliente solicita este nombre de sitio, se devolverá una de las tres direcciones IP de servidor como resolución. El nombre del sitio debe ser un nombre de dominio calificado al completo, por ejemplo, *dnsload.com*. Un espacio de nombres no cualificado, por ejemplo, *dnsload* no es válido para un nombre de sitio.

norma. En el equilibrio de carga basado en normas, mecanismo para agrupar servidores de modo que se pueda seleccionar un servidor basándose en una información distinta de la dirección de destino y el puerto.

Nortel Alteon Controller. Componente de IBM Load Balancer. Nortel Alteon Controller utiliza tecnología de Load Balancer para proporcionar información en tiempo real sobre el equilibrio de carga a Conmutador Nortel Alteon Web.

notación decimal con puntos. Representación sintáctica de un entero de 32 bits que consiste en cuatro números de 8 bits, escritos en base 10 y separados por puntos. Se utiliza para representar las direcciones IPv4.

P

paquete. Unidad de datos que se dirige entre un origen y un destino en Internet o en cualquier red conmutada de paquetes.

pasarela. Unidad funcional que interconecta dos redes de sistemas con distintas arquitecturas.

PICS. Plataforma para la selección de contenidos de Internet. Los clientes habilitados para PICS permiten a los usuarios determinar qué servicios de tarifas desean utilizar y, para cada servicio de tarifas, qué tarifas se aceptan y cuáles no.

ping. Mandato que envía paquetes de petición de eco del protocolo ICMP (Control Message Protocol) a un sistema principal, una pasarela o un direccionador, a la espera de recibir una respuesta.

POP3. Post Office Protocol 3. Un protocolo utilizado para intercambiar correo en la red y para acceder a los buzones de correo.

primaria. En alta disponibilidad para Dispatcher, la máquina que se inicia como máquina que dirige paquetes activamente. Su asociada, la máquina de reserva, supervisa el estado de la máquina primaria y asume el control si es necesario. Consulte también máquina de reserva, alta disponibilidad.

prioridad. En el equilibrio de carga basado en normas, el nivel de importancia asignado a una norma dada. Dispatcher evalúa normas desde el primer nivel de prioridad hasta el último nivel de prioridad.

protocolo. Conjunto de normas que rigen la operación de las unidades funcionales de un sistema de comunicación para que tenga lugar dicha comunicación. Los protocolos pueden determinar los detalles de nivel inferior de las interfaces entre máquina y máquina, tales como el orden en el que se envían los bits de un byte; también puede determinar intercambios de alto nivel entre programas de aplicación como, por ejemplo, la transferencia de archivos.

proximidad de red. Proximidad de dos entidades de red, como un cliente y un servidor, que Site Selector determina midiendo el tiempo de ida y vuelta.

puerto. Número que identifica un dispositivo de comunicación abstracto o un protocolo TCP/IP. Por omisión, los servidores Web utilizan el puerto 80.

pulso. Paquete simple que se envía entre dos máquinas Load Balancer en modalidad de alta disponibilidad y que utiliza Load Balancer en reposo para supervisar el estado de la máquina Load Balancer activa.

R

recopilador de métricas. Reside en el consultor y es el responsable de recopilar una métrica o métricas.

red. Sistema de comunicación de datos basado en hardware y software. Las redes se suelen clasificar de acuerdo con su extensión geográfica, redes de área local (LAN), redes de área metropolitana (MAN), redes de área amplia (WAN) y también de acuerdo con los protocolos que dichas redes utilizan.

red privada. Red independiente a través de la que Dispatcher se comunica con servidores en clúster por motivos de rendimiento.

registro cronológico en binario. Permite que la información del servidor sea almacenada en archivos binarios y procesada a continuación para analizar la información del servidor recopilada a lo largo del tiempo.

reserva. En alta disponibilidad para el componente Dispatcher, la máquina asociada a la máquina primaria. Supervisa el estado de la máquina primaria y asume el control si es necesario. Consulte también alta disponibilidad, primaria.

RMI. Remote Method Invocation. Parte de la biblioteca de lenguajes de programación Java que habilita a un programa Java que se ejecuta en un sistema para acceder a los objetos de otro programa Java que se ejecuta en otro sistema.

RPM. Red Hat Package Manager.

ruta. El recorrido que sigue el tráfico de la red desde el punto de origen al punto de destino.

S

script CGI. Programa CGI escrito en un lenguaje de scripts, como por ejemplo Perl o REXX, que utiliza Common Gateway Interface para ejecutar tareas que el servidor no realiza habitualmente, como el proceso de formularios.

servicio. (1) Función que ofrecen uno o más nodos; por ejemplo, HTTP, FTP y Telnet. (2) En el caso de Nortel Alteon Controller, un servicio es la función o información solicitada por un usuario final desde un sitio. Se identifica mediante una dirección IP virtual y un número de puerto virtual en una petición de usuario final. En el conmutador, se define mediante un identificador de servidor virtual, que es un entero y un número de puerto virtual o nombre de servicio. (3) En el caso de Cisco CSS Consultant, un servicio es una ubicación de destino donde reside físicamente una parte del contenido. Por ejemplo, un servidor local o remoto y un puerto.

servidor. Sistema que proporciona servicios compartidos a otros sistemas de una red, por ejemplo un servidor de archivos, un servidor de impresión o un servidor de correo.

servidor de nombres de dominio. DNS. Un servicio de consulta de datos, duplicado y distribuido, de propósito general utilizado principalmente en Internet para convertir los nombres de sistema principal en direcciones de Internet. Es, además, el estilo de nombre de sistema principal utilizado en Internet, aunque el nombre adecuado sea el de un nombre de dominio calificado al completo. Es posible configurar DNS para que utilice una secuencia de servidores de nombres, basado en los dominios contenidos en el nombre que se busca, hasta que se encuentre una coincidencia.

servidor en clúster. Servidor que Dispatcher agrupa con otros servidores para formar un solo servidor virtual. Load Balancer equilibra el tráfico TCP o UDP entre dichos servidores agrupados.

shell. Software que acepta y procesa las líneas de mandatos de la estación de trabajo de un usuario. Bash es uno de los diferentes shell disponibles para UNIX.

sistema principal. Sistema conectado a una red que proporciona un punto de acceso a dicha red. Un sistema principal puede ser un cliente, un servidor o ambas cosas a la vez.

Site Selector. Componente de equilibrio de carga basado en DNS de Load Balancer. Site Selector equilibra la carga en los servidores dentro de una red de área amplia (WAN) utilizando las medidas y pesos que ha reunido el componente Metric Server ejecutándose en dichos servidores.

SMTP. Protocolo simple de transferencia de correo. En el conjunto de protocolos de Internet, un protocolo de aplicación para transferir correo entre usuarios del entorno de Internet. SMTP especifica las secuencias de intercambio de correo y el formato de los mensajes. Presupone que el Protocolo de control de transmisión (TCP) es el protocolo subyacente.

SNMP. Protocolo simple de gestión de red. El protocolo estándar de Internet, definido en STD 15, RFC 1157 y desarrollado para gestionar los nodos en una red IP. SNMP no está limitado a TCP/IP. Puede utilizarse para gestionar y supervisar todo tipo de equipos incluyendo sistemas, direccionadores, concentradores de cableado, grabadoras y bibliotecas de discos.

SPARC. Arquitectura de procesador escalable.

sscontrol. Proporciona la interfaz para el componente Site Selector de Load Balancer.

SSL. Capa de sockets seguros. Plan de seguridad muy popular desarrollado por Netscape Communications Corp. en colaboración con RSA Data Security Inc. SSL permite a la máquina cliente autenticar el servidor, así como todos los datos y peticiones que deben cifrarse. El URL de un servidor protegido mediante SSL comienza por https (y no por http).

ssserver. En Site Selector, maneja las peticiones desde la línea de mandatos para el nombre del sitio, el gestor y los asesores.

SYN. Bit de control en el segmento de entrada que ocupa un número de secuencia y que se utiliza en la inicialización de una conexión para indicar dónde comenzará la numeración de la secuencia.

T

TCP. Protocolo de control de transmisión. Protocolo de comunicaciones que se utiliza en Internet. TCP proporciona un intercambio de información fiable entre varios sistemas principales. Utiliza IP como el protocolo subyacente.

TCP/IP. Protocolo de control de transmisión/Protocolo Internet. Conjunto de protocolos diseñados para permitir la comunicación entre redes sin tener en cuenta las tecnologías de comunicación utilizadas en cada red.

Telnet. Protocolo de emulación de terminal; se trata de un protocolo de aplicación TCP/IP para el servicio de conexión remota. Telnet permite a un usuario situado en una ubicación acceder a un sistema principal remoto como si la estación de trabajo del usuario estuviera conectada directamente a dicho sistema principal remoto.

tiempo de espera. Intervalo de tiempo permitido para que se lleve a cabo una operación.

tiempo de permanencia en memoria. El período de permanencia en memoria es el intervalo entre el cierre de una conexión y la apertura de una conexión nueva, durante el cual un cliente se volverá a enviar al mismo servidor utilizado durante la primera conexión. Una vez transcurrido el tiempo de permanencia en memoria, puede enviarse el cliente a un servidor distinto del primero.

tipo de norma. En el equilibrio de carga basado en normas, indicador de la información que debe evaluarse para determinar si una norma es cierta.

TOS. Tipo del servicio. Campo de un byte en la cabecera IP del paquete SYN.

TTL. UN TTL de DNS (tiempo de duración) es el número de segundos que un cliente puede almacenar en antememoria la respuesta de resolución de nombres.

U

ubicación compartida. Cuando Load Balancer se instala en la misma máquina en la que está efectuando el equilibrio de carga.

ubicación compartida de varias direcciones. La ubicación compartida de varias direcciones permite al cliente especificar la dirección del servidor con ubicación compartida de modo que sea diferente de la dirección de no reenvío (NFA) en la configuración. Consulte también, ubicación compartida.

UDP. User Datagram Protocol. En la suite de protocolos de Internet, protocolo de aplicación que proporciona un servicio de datagramas sin conexión y no fiable. Permite que un programa de aplicación de una máquina o proceso envíe un datagrama a un programa de aplicación de otra máquina o proceso. UDP utiliza el protocolo IP (Protocolo Internet) para enviar los datagramas.

URI. Identificador universal de recurso. Dirección codificada para cualquier recurso de la Web, tales como documento HTML, imagen, vídeo clip, programa, etc.

URL. Localizador universal de recursos. Una manera estándar de especificar la ubicación de un objeto, normalmente una página Web, en Internet. Los URL son el formato de dirección utilizado en la World Wide Web. Se utilizan en documentos HTML para especificar el destino de un hiperenlace que normalmente es otro documento HTML (posiblemente almacenado en otro sistema).

usuario root. Autorización sin limitaciones para modificar y acceder a cualquier parte del sistema operativo AIX, Red Hat Linux o Solaris, asociada generalmente al usuario que gestiona el sistema.

V

valor por omisión. Valor, atributo u opción que se presupone cuando no se indica ninguno explícitamente.

VPN. Red privada virtual (VPN). Red formada por uno o varios túneles IP protegidos que conectan dos o varias redes.

W

WAN. Red de área amplia. Red que provee servicios de comunicaciones a un área geográfica mayor que la servida por una red de área local o metropolitana. Puede utilizar o proporcionar recursos de comunicaciones públicas.

WAP. Protocolo de aplicación inalámbrico. Un estándar internacional abierto para aplicaciones que utilizan comunicaciones inalámbricas, por ejemplo, acceder a Internet mediante un teléfono móvil.

WAS. WebSphere Application Server.

Web. Red de servidores HTTP que contienen programas y archivos, muchos de ellos documentos hipertexto que contienen enlaces con otros documentos en servidores HTTP. También World Wide Web.

WLM. Gestor de carga de trabajo. Asesor que se proporciona con Dispatcher. Está diseñado para funcionar únicamente junto con servidores en sistemas principales OS/390 que ejecutan el componente Gestor de carga de trabajo (WLM) de MVS.

Índice

A

- accesibilidad xvii
- activo, marcar un servidor como 396, 423, 424
- add
 - Cisco CSS Controller 432
 - Nortel Alteon Controller 450
- administración remota 35, 38, 40
- administración basada en la Web 261, 263
- RMI 261, 262
- administración remota (basada en la Web) renovar 265
- afinidad (permanencia en memoria)
 - afinidad entre puertos 222, 223, 380
 - alteración temporal de afinidad entre puertos 219
 - cómo funciona 221
 - cookie activo 225, 389
 - cookie pasivo 225, 227, 389
 - desactivar temporalmente ahora 224, 374, 378
 - ID de SSL (reenvío cbr) 55
 - máscara de dirección de afinidad 223
 - opción de norma 224
 - permanencia en memoria (alteración temporal de afinidad entre puertos) 219, 393
 - stickymask 222, 223, 381
 - stickytime 381, 389
 - tiempo de permanencia en memoria 55, 221, 222
 - URI 225, 228, 389
- afinidad de cookies activos 225, 389
- afinidad de cookies pasivos 225, 227, 389
- afinidad de URI 225, 228, 389
- afinidad entre puertos 222, 380
- AIX
 - instalación 32
 - requisitos 31
- alertas
 - controladores 257
 - Dispatcher, CBR, Site Selector 184
- alias
 - dispositivo de bucle de retorno 72
 - la NIC 69, 116
- alta disponibilidad 5, 6, 60, 204
 - Cisco CSS Controller 243
 - configuración 153, 175
 - configurar 205
 - dscontrol 367, 457
 - IPv6, consideración 85
 - Linux para S/390 211
 - mutua 61, 206, 357, 358, 369
 - ndcontrol 439
 - Nortel Alteon Controller 243
 - primaryhost 357, 358
 - reenvío NAT 210
 - scripts 209
 - goActive 210
- alta disponibilidad (*continuación*)
 - scripts (*continuación*)
 - goldle 210
 - goInOp 210
 - goStandby 210
 - highavailChange 210
- alta disponibilidad mutua 61, 205, 206
 - primaryhost 357, 358
 - scripts 209
 - tomar control 209
- alteración temporal de afinidad entre puertos
 - servidor 219, 393, 396
- anotaciones cronológicas
 - archivo, establecer el nombre
 - del asesor 406
 - del gestor 415
 - binarias, para estadísticas de servidor 241
 - nivel, establecer
 - del asesor 265, 352, 407
 - del gestor 413
 - para el consultor 267
 - para el gestor 265
 - para el servidor 265, 267
 - para el subagente 265
 - tamaño, establecer
 - para el asesor 265, 352, 405, 407
 - para el consultor 267
 - para el gestor 265, 376, 413, 415
 - para el servidor 265, 267
 - para el subagente 265, 267
 - utilizar archivos de anotaciones cronológicas de CBR 278
 - utilizar archivos de anotaciones cronológicas de Cisco CSS Controller 279
 - utilizar archivos de anotaciones cronológicas de Load Balancer 265
 - utilizar archivos de anotaciones cronológicas de Metric Server 280
 - utilizar archivos de anotaciones cronológicas de Site Selector 278
- anotaciones cronológicas binarias para estadísticas del servidor 266, 268
- añadir
 - clúster 358
 - puerto a clústeres 70, 384
 - servidor a puertos 70, 396, 424
- archivo
 - cbrcontrol 111
 - dscontrol 64
 - sscontrol 132
- archivo de correlación de direcciones
 - ejemplo 236
- archivos de configuración de
 - ejemplo 479
 - asesor 485
 - componente Dispatcher (AIX) 479
 - componente Dispatcher (Windows) 482
- asesor Caching Proxy 189
- asesor DB2 190
- asesor del gestor de carga de trabajo (WLM) 198, 255
- asesor personalizado (personalizable) 192, 250
 - ejemplo 485
- asesor ssl2http 108, 189
- asesor WAS 190, 194
- asesores
 - archivo de configuración de
 - ejemplo 485
 - cbrcontrol 349
 - componente CBR
 - asesor ssl2http 189
 - componente Dispatcher 185
 - asesor automático 190, 192
 - asesor Caching Proxy 189
 - detección rápida de anomalía 188
 - detención 352
 - informe sobre el estado de 353
 - inicio 71, 352
 - inicio/detención 186
 - intervalo para 187, 352
 - lista de 188, 352
 - nombre de 349
 - personalizar 192
 - puerto para 356
 - reintento de servidor 182, 188, 351
 - report 353
 - tiempo de espera de conexión del servidor 188, 349, 352
 - tiempo de espera de informe 187, 352
 - tiempo de espera de recepción del servidor 188, 350, 353
 - versión de 353
 - controladores 248
 - detección rápida de anomalía 249
 - personalizar 250
 - reintento de servidor 249
 - tiempo de espera de conexión del servidor 249
 - tiempo de espera de recepción del servidor 249
 - tiempo de inactividad 249
 - dscontrol 349
 - ejemplo personalizado 485
 - IPv6, consideración 84
 - limitación en Solaris 185
 - lista de 351
 - opción URL, asesor HTTP 190
 - petición/respuesta del asesor HTTP 190
 - Site Selector
 - detección rápida de anomalía 188
 - detención 406, 408
 - informe sobre el estado de 405, 407
 - inicio 406, 407

asesores (*continuación*)
 Site Selector (*continuación*)
 interval 404
 intervalo para 407
 list 404
 lista de 406, 407
 loglevel 404
 nombre de 404
 puerto para 349, 404
 reintento de servidor 188
 reintentos de servidor 405
 tiempo de espera de conexión del servidor 188, 404, 407
 tiempo de espera de informe 406, 408
 tiempo de espera de recepción del servidor 188, 405, 407
 versión de 407, 408
 sscontrol 404, 411
 asesores, componente de Load Balancer
 inicio 71
 asistente, configuración
 CBR 113
 Dispatcher 66
 Site Selector 134
 avisos 493

B

binlog
 anotaciones cronológicas en binario,
 para estadísticas de servidor 354
 cbrcontrol 354
 dscontrol 354
 bucle de retorno
 crear alias para alternativas para
 Linux 78

C

Caching Proxy 107
 configurar para CBR 113
 CBR
 aparecen caracteres nacionales Latin-1
 dañados (Windows) 328
 asesores y destinos de alcance marcan
 todos los servidores como inactivos
 (Windows) 328
 cbrcontrol da un error 326
 cbrcontrol da un error en Solaris 327
 comportamiento de la GUI inesperado
 con tarjetas Matrox AGP 327
 con Caching Proxy
 asesor ssl2http 108
 conexiones SSL 107
 configurar 118
 mapport, palabra clave 108
 visión general 106
 con el componente Dispatcher 55
 configuración
 configuración de la máquina
 CBR 113
 visión general de tareas 109
 crear alias para la NIC 116
 desconexión del sistema principal, con
 administración Web 328

CBR (*continuación*)
 determinar las características que se
 van a utilizar 23
 ejemplo de inicio rápido 99
 error de memoria/hebra Java
 (HP-UX) 328
 error sintáctico o de
 configuración 327
 iniciar y detener 277
 lbadm da un error 326
 mandato ifconfig 116
 no se ejecutará 326
 no se equilibra la carga de las
 peticiones 327
 planificar 105
 problema al resolver la dirección IP
 con el nombre de sistema principal
 (Windows) 329
 resolución de problemas, tabla 292
 valores de equilibrio de carga 180
 reintento de servidor de
 asesor 188
 cbr, método de reenvío 55, 57
 tiempo de permanencia en
 memoria 55
 cbrserver
 inicio 100
 ccoserver
 inicio 140
 no se iniciará 301, 302, 332
 Cisco CSS Controller
 alertas 257
 alta disponibilidad 243
 Asesor del gestor de carga de
 trabajo 255
 asesores 248
 ccocontrol da un error 332
 comportamiento de la GUI inesperado
 con tarjetas Matrox AGP 333
 conexión del consultor, error 333
 configuración
 configuración de la máquina
 CSS 152
 ejemplo 16
 visión general de tareas 149
 desconexión del sistema principal, con
 administración Web 333
 determinar las características que se
 van a utilizar 27
 ejemplo de inicio rápido 139
 el conmutador no actualiza los
 pesos 333
 error de memoria/hebra Java
 (HP-UX) 334
 iniciar y detener 278
 inicio 278
 lbadm da un error 332
 mandatos 431
 Metric Server 253
 no se ha podido crear el registro en el
 puerto 13099 332
 no se iniciará 332
 planificar 143
 refresh (mandato) no actualiza la
 configuración 333
 registro cronológico en binario para
 estadísticas de servidor 256

Cisco CSS Controller (*continuación*)
 report
 controller 435
 requisitos de hardware y
 software 143
 resolución de problemas, tabla 295
 ubicación compartida 243
 utilizar 278
 valores de equilibrio de carga 246
 Cisco CSS Controller, componente
 aparecen caracteres nacionales Latin-1
 dañados (Windows) 334
 clave privada
 para autenticación remota 262
 clave pública
 para autenticación remota 262
 claves
 lbkeys 197, 253, 262
 clúster
 añadir 358
 cbrcontrol 355
 comodín 69
 configurar la dirección 69
 definir 69, 358
 definir proporciones 71
 dscontrol 355
 eliminar 358, 427
 mostrar
 estado de este clúster 358
 proportions 355
 clúster comodín 69, 358
 con Caching Proxy para un proxy
 transparente 238
 para combinar configuraciones de
 servidores 237
 para equilibrar la carga de
 cortafuegos 238
 collocated (palabra clave) 203, 396
 componente Dispatcher
 configuración
 configuración de la máquina Load
 Balancer 66
 configuración de una red
 privada 236
 visión general de tareas 63
 En Linux, Dispatcher reenvía
 paquetes, pero el servidor de
 programa de fondo no los
 recibe 323
 En Linux, existen limitaciones cuando
 se utilizan servidores zSeries o
 S/390 321
 En Linux, se produce una pérdida de
 memoria cuando se utilizan el gestor
 y los asesores 323
 En sistemas Windows, hay un
 problema con la toma de control de
 alta disponibilidad 324
 En Solaris, no se puede añadir
 servidores IPv6 a la
 configuración 325
 restablecer servidores inactivos 383
 restaurar un servidor inactivo 182
 valores de equilibrio de carga 180
 índice de suavizado 183
 intervalos de asesor 187
 intervalos del gestor 183

- componente Dispatcher (*continuación*)
 - valores de equilibrio de carga (*continuación*)
 - pesos 181
 - proporción de importancia dada a la información de estado 180
 - reintento de servidor de asesor 182, 188
 - tiempo de espera de informe del asesor 187
 - tiempo de espera de servidor de asesor 188
 - umbral de sensibilidad 183
- componentes del producto 51
- comprobación
 - ruta adicional 76
- conexiones, establecer proporción de importancia 181, 358
- conexiones SSL
 - asesor HTTPS 188
 - asesor SSL 189
 - configurar ibmproxy 108
 - para CBR 107, 108
 - problema con la habilitación 305
- configuración
 - alta disponibilidad 153, 175
 - archivos de ejemplo 479
 - cbrwizard 113
 - Cisco CSS Controller 149
 - componente Dispatcher 63
 - Content Based Routing 109
 - definir consultor de conmutador 175
 - dswizard 66
 - inicio del consultor 153, 175
 - métodos
 - asistente (CBR) 113
 - asistente (Dispatcher) 66
 - asistente (Site Selector) 134
 - GUI (CBR) 111
 - GUI (Cisco CSS Controller) 151
 - GUI (Dispatcher) 64
 - GUI (Nortel Alteon Controller) 173
 - GUI (Site Selector) 132
 - línea de mandatos (CBR) 110
 - línea de mandatos (Cisco CSS Controller) 149
 - línea de mandatos (Dispatcher) 63
 - línea de mandatos (Nortel Alteon Controller) 171
 - línea de mandatos (Site Selector) 131
 - scripts (CBR) 111
 - scripts (Cisco CSS Controller) 150
 - scripts (Dispatcher) 64
 - scripts (Nortel Alteon Controller) 172
 - scripts (Site Selector) 132
 - métrica 153, 175
 - Nortel Alteon Controller 171
 - probar 154, 176
 - servicio 175
 - Site Selector 131
 - sswizard 134
 - tareas, avanzadas 179, 201
 - verificar 77

- connecttimeout
 - Site Selector 404
- consultant
 - ccocontrol 432, 435
 - nalcontrol 450, 453
 - Nortel Alteon Controller
 - add 450
 - binarylog 450
 - report 450
- consultor
 - Cisco CSS Controller
 - add 432
 - binarylog 432
 - report 432
 - inicio 153, 175
- consultor de conmutador
 - definir 175
- Content Based Routing 5
 - con el componente Dispatcher 55
 - configuración
 - configuración de la máquina CBR 113
 - visión general de tareas 109
 - planificar 105
 - resolución de problemas, tabla 292
 - utilizar 277
 - valores de equilibrio de carga 180
- controlador
 - peso fijo 247
- controladores
 - asesor personalizado (personalizable) 250
 - valores de equilibrio de carga
 - importancia dada a información métrica 246
 - pesos 247
 - reintento de servidor de asesor 249
 - tiempo de espera de servidor de asesor 249
 - tiempos de inactividad 247
 - tiempos de inactividad del asesor 249
 - umbral de sensibilidad 248
- controller
 - Cisco CSS Controller
 - loglevel 433, 435
 - logsize 433, 435
 - report 435
 - set 435
 - Nortel Alteon Controller
 - loglevel 451, 453
 - logsize 451, 453
 - report 453
 - set 453

D

- default.cfg 68, 115, 134
- definir
 - clúster 358
 - dirección de no reenvío 68, 363
 - puerto a clústeres 70, 384
 - servidor a puertos 70, 396, 424
- desactivar temporalmente un servidor 224, 374, 376, 378

- desinstalar
 - en AIX 32
 - en HP-UX 36
 - en Linux 37
 - en Solaris 39
 - en Windows 41
- Detección de ataques para rechazo de servicio (DoS) 239
 - halfopenaddressreport 384
 - maxhalfopen 383
- detener
 - asesor 352, 406, 408
 - Cisco CSS Controller 278
 - ejecutor 363
 - gestor 378, 415, 417
 - Nortel Alteon Controller 279
- diagnosticar problemas
 - Actualización de Java proporcionada con la instalación 326
 - alta disponibilidad, consejos para configurar 319
 - alta disponibilidad, no funciona en la modalidad de área amplia de Load Balancer 308
 - aparecen caracteres nacionales Latin-1 dañados (Windows) 313, 328, 331, 334, 336
 - archivo de anotaciones cronológicas de Metric Server informa de que "Es necesaria la firma para acceder al agente" 337
 - asesores y destinos de alcance marcan todos los servidores como inactivos (Windows) 313, 328, 331
 - cbrcontrol da un error en Solaris 327
 - cbrcontrol o lbadm (mandato) da un error 326
 - ccocontrol o lbadm (mandato) da un error 332
 - comportamiento de la GUI inesperado con tarjetas Matrox AGP 311, 327, 330, 333, 335
 - comportamiento inesperado al cargar un archivo de configuración de gran tamaño 309
 - comportamiento inesperado con "rmmod ibmlb" 311
 - conexión del consultor, error 333, 336
 - configurar Metric Server en una configuración de dos niveles 338
 - conflicto de dirección IP cuando se utiliza la alta disponibilidad 317
 - desaparecen los paneles de ayuda 307
 - desconexión del sistema principal, con administración Web 312, 328, 331, 333, 335
 - dirección del direccionador no especificada o no válida para el método del puerto 316
 - Dispatcher, Microsoft IIS y SSL no funcionan 305
 - dscontrol o lbadm (mandato) da un error 305
 - el conmutador no actualiza los pesos 333, 336

- diagnosticar problemas (*continuación*)
 - en AIX, se daña la salida del mandato ps -vg 338
 - En Linux, Dispatcher reenvía paquetes, pero el servidor de programa de fondo no los recibe 323
 - En Linux, es posible que Dispatcher de HA se pueda sincronizar 319
 - En Linux, existen limitaciones cuando se utilizan servidores zSeries o S/390 321
 - En sistemas Linux, no se pueden recuperar valores de Metric Server 340
 - En sistemas Windows, hay un problema con la toma de control de alta disponibilidad 324
 - en Solaris, los scripts producen mensajes de consola no deseados 339
 - En Solaris, no se puede añadir servidores IPv6 a la configuración 325
 - En Windows, se produce el error "el servidor no responde" 318
 - enlace del servidor Web a 0.0.0.0 312
 - error al ejecutar Dispatcher con Caching Proxy instalado 306
 - error de memoria/hebra Java (HP-UX) 313, 328, 331, 334, 337
 - Error sintáctico o de configuración 327
 - fin de los procesos de Load Balancer (Solaris) 317
 - fonts coreanos no deseados en AIX y Linux 310
 - GUI no se inicia correctamente 306
 - GUI no se muestra correctamente 306
 - la dirección IP no se resuelve en la conexión remota 310
 - lbadmin desconecta del servidor después de actualizar la configuración 309
 - Load Balancer no puede procesar y reenviar una trama 307
 - los asesores no funcionan en una configuración de alta disponibilidad después de una caída de la red (Windows) 315
 - máquinas primaria y de reserva activas en una configuración de alta disponibilidad 318
 - mensaje de aviso Java aparece al instalar arreglos de servicio 325
 - mensaje de error al intentar consultar la ayuda en línea 306
 - Metric Server IOException en Windows 337
 - Metric Server no informa de las cargas 337
 - nalcontrol o lbadmin (mandato) da un error 334
 - no funciona la alta disponibilidad de Dispatcher 304
 - no funcionan los asesores 304
- diagnosticar problemas (*continuación*)
 - no registra cargas del servidor 312
 - no responderán Dispatcher y el servidor 303
 - no se direccionan las peticiones de Dispatcher 303
 - no se ejecutará CBR 326
 - no se ejecutará Dispatcher 303
 - no se ejecutará Site Selector 329
 - no se equilibra la carga de las peticiones 327
 - no se ha podido crear el registro en el puerto 13099 332
 - no se ha podido crear el registro en el puerto 14099 335
 - no se han podido añadir pulsos 304
 - no se iniciará ccoserver 332
 - no se iniciará nalsver 334
 - no se pueden realizar las peticiones del cliente cuando el sistema intenta devolver respuestas de páginas de gran tamaño 318
 - no utilice el mandato IP address add para crear alias de bucle de retorno (Linux) 316
 - números de puerto utilizados por CBR 300
 - números de puerto utilizados por Cisco CSS Controller 301
 - números de puerto utilizados por Dispatcher 299
 - números de puerto utilizados por Nortel Alteon Controller 302
 - números de puerto utilizados por Site Selector 301
 - pantalla azul al iniciar el ejecutor de Load Balancer 307
 - problema al resolver la dirección IP con el nombre de sistema principal (Windows) 314, 329
 - problemas comunes y soluciones 303, 305, 326, 329, 332, 334, 337
 - refresh (mandato) no actualiza la configuración 333, 336
 - retardo al cargar la configuración de Load Balancer 317
 - rutas adicionales 304
 - se devuelve un alias en lugar de la dirección local 310
 - Site Selector no equilibra la carga correctamente 330
 - Site Selector no utiliza el algoritmo de turno rotativo (Solaris) 329
 - sscontrol o lbadmin (mandato) da un error 329
 - ssserver no se ha podido iniciar en Windows 330
 - tiempo de respuesta lento 311
 - Valor de métrica devuelve -1 después de iniciar Metric Server 340
 - vía de acceso al descubrimiento impide el tráfico de retorno con Load Balancer 307
- diagnóstico de problemas
 - En Linux, se produce una pérdida de memoria cuando se utilizan el gestor y los asesores 323
- diagramas de sintaxis
 - ejemplos 345
 - leer 345
 - parámetros 345
 - puntuación 345
 - símbolos 345
- dirección de no reenvío
 - definir 68
 - establecer 363
- Dispatcher
 - configuración
 - configuración de servidores de programas de fondo 72
 - determinar las características que se van a utilizar 19
- Dispatcher, componente
 - Actualización de Java proporcionada con la instalación 326
 - alta disponibilidad, consejos para configurar 319
 - alta disponibilidad, no funciona en la modalidad de área amplia de Load Balancer. 308
 - aparecen caracteres nacionales Latin-1 dañados (Windows) 313
 - asesores y destinos de alcance marcan todos los servidores como inactivos (Windows) 313
 - comportamiento de la GUI inesperado con tarjetas Matrox AGP 311
 - comportamiento inesperado al cargar un archivo de configuración de gran tamaño 309
 - comportamiento inesperado con "rmmod ibmlb" 311
 - conexión con una máquina remota 305
 - conflicto de dirección IP cuando se utiliza la alta disponibilidad 317
 - desaparecen las ventanas de ayuda 307
 - desconexión del sistema principal, con administración Web 312
 - dirección del direccionador no especificada o no válida para el método del puerto 316
 - direccionamiento basado en contenido 55
 - dscontrol da un error 305
 - En Linux, es posible que Dispatcher de HA se pueda sincronizar 319
 - En Windows, se produce el error "el servidor no responde" 318
 - enlace del servidor Web a 0.0.0.0 312
 - error cuando está instalado Caching Proxy 306
 - error de memoria/hebra Java (HP-UX) 313
 - fin de los procesos de Load Balancer (Solaris) 317
 - fonts coreanos no deseados en AIX y Linux 310
 - GUI no se inicia correctamente 306

Dispatcher, componente (*continuación*)

GUI no se muestra

correctamente 306

inicio 268

IPv6, soporte 81

la dirección IP no se resuelve en la
conexión remota 310

lbadm da un error 305

lbadm desconecta del servidor

después de actualizar la

configuración 309

los asesores no funcionan en una
configuración de alta disponibilidad
después de una caída de la red
(Windows) 315

máquinas primaria y de reserva
activas en una configuración de alta
disponibilidad 318

mensaje de aviso Java aparece al
instalar arreglos de servicio 325

MS IIS y SSL no funcionan 305

NAT / NAPT 53

no funciona la alta

disponibilidad 304

no funcionan los asesores 304

no puede reenviar una trama 307

no registra cargas del servidor 312

no responderá el servidor 303

no se ejecutará 303

no se equilibran las peticiones 303

no se han podido añadir pulsos 304

no se puede abrir la ventana de
ayuda 306

no se pueden realizar las peticiones
del cliente cuando el sistema intenta
devolver respuestas de páginas de
gran tamaño 318

no utilice el mandato IP address add
para crear alias de bucle de retorno
(Linux) 316

pantalla azul al iniciar el

ejecutor 307

planificar 51

problema al resolver la dirección IP
con el nombre de sistema principal
(Windows) 314

reenvío MAC 53

resolución de problemas, tabla 286

retardo al cargar la configuración de
Load Balancer 317

rutas adicionales (Windows) 304

se devuelve un alias en lugar de la
dirección local 310

tiempo de respuesta lento 311

utilizar 268

vía de acceso al descubrimiento
impide el tráfico de retorno con
Load Balancer 307

dispositivo de bucle de retorno

alias 72

DPID2 271

dscontrol, mandato

asesor 71

ejecutor 68

gestor 71

puerto 70

servidor 70

dsserver

inicio 47

E

ejecutor

detener 363

inicio 363

ejemplo de inicio rápido 45

CBR 99

Cisco CSS Controller 139

Nortel Alteon Controller 157

Site Selector 121

ejemplos

gestión de servidores locales 10, 11,
13, 14, 16

inicio rápido 45

CBR 99

Cisco CSS Controller 139

Nortel Alteon Controller 157

Site Selector 121

eliminar

clúster 358, 427

puerto de clústeres 384

ruta adicional 77

servidor de puertos 396, 423, 424

enlace explícito 236

equilibrio de carga basado en
normas 212

ancho de banda compartido 216, 387,
391

ancho de banda reservado 216, 387,
391

conexiones activas para puerto 215,
387

conexiones por segundo 215, 387

contenido de la petición 55

contenido de petición 219, 387

dirección IP de cliente 213, 386, 391,
420, 422

elección de normas, por
componente 212

hora del día 214, 386, 391, 420, 422

media de la métrica 218

metricall 420

metricavg 420

opción de evaluación 220

opción de evaluación del
servidor 220

puerto cliente 214, 387

siempre cierta 218, 387, 391, 420, 422

tipo de servicio (TOS) 214, 387, 391

toda la métrica 217

específico de clúster

proportions 426

establecer

dirección de clúster 70

dirección de no reenvío 66

frecuencia con la que el gestor debe
consultar el ejecutor 183, 376

índice de suavizado 184, 377, 414,
416

nivel de anotaciones

del asesor 265, 352, 407

del gestor 413

nombre del archivo de anotaciones
cronológicas 406

establecer (*continuación*)

para el gestor 415

peso máximo

para servidores en un puerto
específico 181, 384

peso para un servidor 376, 378, 396,
423

proporción de importancia en
equilibrio de carga 358

sensibilidad a actualización de
pesos 183, 377, 414, 416

tamaño máximo del archivo de
anotaciones cronológicas

para el asesor 265, 352, 405, 407

para el gestor 376, 413, 415

tiempo del intervalo

para que el asesor consulte los
servidores 352, 407

para que el gestor actualice el
ejecutor 183, 376, 413, 415

estado, mostrar

servidores en un puerto concreto 384

Ethernet NIC

ibmlb.conf

configuración para Solaris 67

executor

cbrcontrol 359

dscontrol 359

F

file

cbrcontrol 364

ccocontrol 437

dscontrol 364

nalcontrol 455

sscontrol 409

Firewall (restricción) 41

ftp, asesor 349, 404

G

gestionar Load Balancer 261

gestor

detener 378, 415, 417

inicio 71, 377, 414, 416

peso fijo 182

proporciones 180

versión 378, 415, 417

goActive 210

goIdle 210

goInOp 210

goStandby 210

GRE (Encapsulamiento genérico de
direccionamiento)

Linux 235

OS/390 234

soporte de área amplia 234

GUI

CBR 111

Cisco CSS Controller 151

Dispatcher 64

instrucciones generales 467

Nortel Alteon Controller 173

resolución 306

Site Selector 132

H

help

- cbrcontrol 366
- cococontrol 438
- dscontrol 366
- nalcontrol 456

highavailChange 210

host

- cbrcontrol 371
- cococontrol 444
- dscontrol 371
- nalcontrol 464

HP-UX

- instalación 35
- mandato arp publish 70
- requisitos 35

http, asesor 349, 404

I

IBM Firewall (restricción) 41

ibmlb.conf

- configuración para Solaris 67

ibmproxy 108, 113

ifconfig, mandato 73

inactivo, marcar un servidor como 396, 423, 424

índice de suavizado, establecer 184, 377, 414, 416

información, recopilar 281

informe de instantánea de estadísticas, mostrar 376, 414, 415

iniciar y detener

- CBR 277
- Dispatcher 268

inicio

- asesor 71, 352, 406, 407
- CBR 100
- Cisco CSS Controller 140, 278
- Dispatcher 47
- ejecutor 68, 363
- gestor 71, 377, 414, 416
- Metric Server 280
- Nortel Alteon Controller 158, 279
- servidor 68
- Site Selector 122, 278

instalación

- en AIX 32
- en HP-UX 35
- en Linux 37
- en Solaris 39
- en Windows 40, 41
- Load Balancer 31

interfaz gráfica de usuario (GUI)

- CBR 111
- Cisco CSS Controller 151
- Dispatcher 64
- instrucciones generales 467
- Nortel Alteon Controller 173
- Site Selector 132

intervalo, establecer la frecuencia con la que

- el asesor consulta los servidores 352, 407
- el gestor actualiza los pesos en el ejecutor 183, 376, 413, 415

intervalo, establecer la frecuencia con la que (*continuación*)

- el gestor consulta el ejecutor 183, 376

IPv6, soporte 81

- alta disponibilidad 85

- asesores, utilizar 84

- autoconf6, AIX 88

- características no admitidas 84

- consideraciones de configuración 83

- dirección local de enlace 84

- dsconfig 88

- dscontrol, mandatos 92

- habilitar paquetes IPv6 88

- ifconfig 88

- ip, dirección 88

- Metric Server 87

- modprobe, Linux 88

- poner un alias a NIC 88

- sintaxis de mandato, diferencias 92

- soporte de plataforma 82

- ubicación compartida 86

L

lbkeys 197, 254, 262

lbwebaccess 264

línea de mandatos

- ejemplo de configuración

- CBR 100

- Cisco CSS Controller 140

- Dispatcher 47

- Nortel Alteon Controller 158

- Site Selector 122

- Enviar mandato (GUI) 472

Linux

- alta disponibilidad en S/390 211

- instalación 37

- requisitos 37

Load Balancer

- configurar

- CBR 109

- Cisco CSS Controller 149

- Dispatcher, componente 66, 113, 134

- Nortel Alteon Controller 171

- Site Selector 131

- ejemplo de inicio rápido 45

- CBR 99

- Cisco CSS Controller 139

- Nortel Alteon Controller 157

- Site Selector 121

- funciones 3, 9

- instalación 31

- IPv6, soporte 81

- operar y gestionar 261, 278, 279

- planificar consideraciones 51, 125

- resolución de problemas 281

- tareas de configuración,

- avanzadas 179, 201

- ventajas 5

- visión general 3, 9

Load Balancer para IPv4 y IPv6 81

- alta disponibilidad 85

- asesores, utilizar 84

- autoconf6, AIX 88

- características no admitidas 84

- consideraciones de configuración 83

Load Balancer para IPv4 y IPv6 (*continuación*)

- dirección local de enlace 84

- dsconfig 88

- dscontrol, mandatos 92

- habilitar paquetes IPv6 88

- ifconfig 88

- ip, dirección 88

- Metric Server 87

- modprobe, Linux 88

- poner un alias al dispositivo de bucle de retorno 88

- sintaxis de mandato, diferencias 92

- soporte de plataforma 82

- ubicación compartida 86

logstatus

- cbrcontrol 372

- dscontrol 372

- sscontrol 412

M

mac, método de reenvío 53

manager

- cbrcontrol 373

- dscontrol 373

- sscontrol 413

mandato cbrcontrol

- advisor 349

- binlog 354

- clúster 355

- ejecutor 359

- file 364

- help 366

- host 371

- logstatus 372

- manager 373

- metric 379

- puerto 380

- rule 386

- server 392

- set 398

- status 399

mandato cococontrol

- consultant 432, 435

- file 437

- help 438

- host 444

- indicador de mandatos 431

- métrica 442

- servidor 447

mandato dscontrol

- advisor 349

- binlog 354

- clúster 355

- ejecutor 359

- file 364

- help 366

- highavailability 367, 457

- host 371

- indicador de mandatos 348

- logstatus 372

- manager 373

- metric 379

- minimizar parámetros de

- mandato 348

- puerto 380

- mandato dscontrol *(continuación)*
 - rule 386
 - server 392
 - set 398
 - status 399
 - subagent 400
- mandato ifconfig 70, 116, 232
- mandato nalcontrol
 - consultant 450, 453
 - file 455
 - help 456
 - host 464
 - indicador de mandatos 449
 - metric 460
 - servidor 462
- mandato ndcontrol
 - highavailability 439
- mandato sscontrol
 - advisor 404
 - file 409
 - help 411
 - logstatus 412
 - manager 413
 - metric 418
 - nameserver 419
 - rule 420
 - server 423
 - set 425
 - sitename 426
 - status 429
- mandatos
 - cbrcontrol
 - advisor 349
 - binlog 354
 - clúster 355
 - executor 359
 - file 364
 - help 366
 - host 371
 - logstatus 372
 - manager 373
 - metric 379
 - puerto 380
 - rule 386
 - server 392
 - set 398
 - status 399
 - cococontrol
 - consultant 432, 435
 - file 437
 - help 438
 - host 444
 - indicador 431
 - métrica 442
 - servidores, configurar 447
- Cisco CSS Controller 431
- dscontrol
 - advisor 349
 - alta disponibilidad, control 367, 457
 - binlog 354
 - clúster 355
 - controlar el asesor 71
 - controlar el gestor 71
 - definir la dirección de no reenvío 68, 363
 - definir puertos 70

- mandatos *(continuación)*
 - dscontrol *(continuación)*
 - definir servidores 70
 - executor 359
 - file 364
 - help 366
 - host 371
 - indicador 348
 - logstatus 372
 - manager 373
 - metric 379
 - puerto 380
 - rule 386
 - server 392
 - set 398
 - status 399
 - subagent, configurar SNMP 400
- ifconfig 70, 232
 - poner un alias al dispositivo de bucle de retorno 73
- nalcontrol
 - consultant 450, 453
 - file 455
 - help 456
 - host 464
 - indicador 449
 - metric 460
 - servidores, configurar 462
- ndcontrol
 - alta disponibilidad, control 439
- netstat
 - comprobar direcciones IP y los alias 76
- Nortel Alteon Controller 449
- ruta
 - suprimir rutas adicionales 76, 77
- Site Selector 403
- sscontrol
 - advisor 404
 - file 409
 - help 411
 - logstatus 412
 - manager 413
 - metric 418
 - nameserver 419
 - rule 420
 - server 423
 - set 425
 - sitename 426
 - status 429
- marcar el servidor como
 - activo 396, 423, 424
 - inactivo 396, 423, 424
- marcas registradas 495
- máscara de dirección de afinidad 223, 381
- método de reenvío
 - cbr 55, 57
 - mac 53, 54
 - mac, nat o cbr 56, 382
 - nat 57
 - NAT 53
- método de reenvío NAT
 - scripts de alta disponibilidad 210
- metric
 - cbrcontrol 379
 - dscontrol 379

- metric *(continuación)*
 - nalcontrol 460
 - sscontrol 418
- Metric Server
 - archivo de anotaciones cronológicas de Metric Server informa de que "Es necesaria la firma para acceder al agente" 337
 - configurar Metric Server en una configuración de dos niveles 338
 - en AIX, se daña la salida del mandato ps -vg 338
 - En sistemas Linux, no se pueden recuperar valores de Metric Server 340
 - en Solaris, los scripts producen mensajes de consola no deseados 339
 - iniciar y detener 280
 - IPv6, consideración 87
 - Metric Server IOException en Windows 337
 - Metric Server no informa de las cargas 337
 - resolución de problemas, tabla 298
 - utilizar 280
 - Valores de métrica devuelven -1 después de iniciar Metric Server 340
 - visión general 196, 253
- métrica
 - cococontrol 442
 - configuración 153, 175
- métrica del sistema
 - configurar 379, 418, 442, 460
 - establecer proporción de importancia 181, 246, 355, 356
- migración 31
- mostrar
 - contadores internos 362
 - estado
 - servidores en un puerto 384
 - un clúster o todos los clústeres 358
 - informe sobre el estado de un asesor 353, 405, 407
 - informes de estadísticas 376, 414, 415
 - lista
 - asesores que proporcionan medidas actualmente 352, 407
 - número de versión
 - de asesor 353, 407, 408
 - de gestor 378, 415, 417
 - valores globales y sus valores por omisión
 - para el gestor 377, 415, 416
 - para un asesor 353, 406, 407
- N
 - nalserv
 - inicio 158
 - no se iniciará 334
 - nameserver
 - sscontrol 419
 - NAPT, Network Address Port Translation 53

- nat, método de reenvío 57
- NAT, método de reenvío 53
- NAT, Network Address Translation 53
- NAT, ubicación compartida de servidor con 204
- netstat, mandato 76
- NIC
 - alias 69
 - correlación (para Windows) 69
 - ethernet (para Solaris) 67
- norma de contenido 55, 219
- Nortel Alteon Consultant
 - determinar las características que se van a utilizar 28
- Nortel Alteon Controller
 - alertas 257
 - alta disponibilidad 243
 - aparecen caracteres nacionales Latin-1 dañados (Windows) 336
 - Asesor del gestor de carga de trabajo 255
 - asesores 248
 - comportamiento de la GUI inesperado con tarjetas Matrox AGP 335
 - conexión del consultor, error 336
 - configuración
 - configuración de la máquina Nortel Alteon Controller 174
 - visión general de tareas 171
 - desconexión del sistema principal, con administración Web 335
 - ejemplo de inicio rápido 157
 - el conmutador no actualiza los pesos 336
 - error de memoria/hebra Java (HP-UX) 337
 - iniciar y detener 279
 - lbadm da un error 334
 - mandatos 449
 - Metric Server 253
 - nalcontrol da un error 334
 - no se ha podido crear el registro en el puerto 14099 335
 - no se iniciará 334
 - planificar 161
 - refresh (mandato) no actualiza la configuración 336
 - registro cronológico en binario para estadísticas de servidor 256
 - report
 - controller 453
 - requisitos de hardware y software 161
 - resolución de problemas, tabla 297
 - ubicación compartida 243
 - utilizar 279
 - valores de equilibrio de carga 246
- nuevas características, V6.1
 - asesor SIP 7
 - configuración de cliente con ubicación compartida 7
 - soporte de espacio de usuario 6
 - soporte para el navegador Firefox 7
 - soporte para HP-UX Itanium 64-bit 7
 - soporte para Linux zSeries de 64 bits 7
 - soporte sin kernel 6

- nuevas conexiones, establecer proporción de importancia 180, 356

O

- opciones de proximidad 128
- operar Load Balancer 261
- OS/390
 - soporte de GRE 234

P

- permanencia en memoria (afinidad)
 - afinidad entre puertos 222, 223, 380
 - alteración temporal de afinidad entre puertos 219
 - cómo funciona 221
 - cookie activo 225, 389
 - cookie pasivo 225, 227, 389
 - desactivar temporalmente ahora 224, 374, 378
 - máscara de dirección de afinidad 223
 - permanencia en memoria (alteración temporal de afinidad entre puertos) 219, 393
 - stickymask 222, 223, 381
 - stickytime 381, 389
 - tiempo de permanencia en memoria 55, 221, 222
 - URI 225, 389
- peso
 - cómo establece el gestor 182
 - controladores 247
 - establecer
 - el límite para todos los servidores en un puerto 181, 384
 - para un servidor 396, 423
- peso máximo, establecer
 - para servidores en un puerto específico 181, 384
- planificar
 - CBR 105
 - Cisco CSS Controller 143
 - Dispatcher, componente 51
 - Nortel Alteon Controller 161
 - Site Selector 125
- planificar la instalación 3, 9, 51, 125
- primaryhost 206, 358
- probar
 - configuración 154, 176
- proporción de importancia para el equilibrio de carga, establecer 180, 358
- Protocolo simple de gestión de red, SNMP 269
- proximidad de red 128
- puerto
 - cbrcontrol 380
 - dscontrol 380
- puerto comodín 70, 384
 - asesor ping 189
 - para dirigir tráfico de puerto no configurado 239
 - para manejar el tráfico FTP 239
- puertos
 - añadir 384
 - comodín 70

- puertos (*continuación*)
 - definir en un clúster 70, 384
 - eliminar 384
 - establecer el peso máximo 181, 384
 - mostrar
 - estado de servidores en este puerto 384
 - para asesores 349, 404

R

- recopilar información 281
- red privada, utilizar con Dispatcher 236
- referencias de mandato
 - cómo leer 345
- registro cronológico en binario para estadísticas de servidor 241
- controladores 256
- reiniciar todos los servidores a sus pesos normalizados 377, 414, 416
- renovar la configuración de forma remota 265
- report
 - Cisco CSS Controller 435
 - Nortel Alteon Controller 453
- requisitos
 - AIX 31
 - HP-UX 35
 - Linux 37
 - Solaris 39
 - Windows 40
- requisitos de hardware
 - Cisco CSS Controller 143
 - Nortel Alteon Controller 161
- requisitos de software
 - Cisco CSS Controller 143
 - Nortel Alteon Controller 161
- reserva, alta disponibilidad 60, 367, 439, 457
 - configurar 205
- resolución, GUI 306
- resolución de problemas 281
 - Actualización de Java proporcionada con la instalación 326
 - alta disponibilidad, consejos para configurar 319
 - alta disponibilidad, no funciona en la modalidad de área amplia de Load Balancer. 308
 - aparecen caracteres nacionales Latin-1 dañados (Windows) 313, 328, 331, 334, 336
 - archivo de anotaciones cronológicas de Metric Server informa de que "Es necesaria la firma para acceder al agente" 337
 - asesores y destinos de alcance marcan todos los servidores como inactivos (Windows) 313, 328, 331
 - cbrcontrol da un error en Solaris 327
 - cbrcontrol o lbadm (mandato) da un error 326
 - cococontrol o lbadm (mandato) da un error 332
 - comportamiento de la GUI inesperado con tarjetas Matrox AGP 311, 327, 330, 333, 335

resolución de problemas (*continuación*)
 comportamiento inesperado al cargar un archivo de configuración de gran tamaño 309
 comportamiento inesperado con "rmmod ibmlb" 311
 conexión del consultor, error 333, 336
 configurar Metric Server en una configuración de dos niveles 338
 conflicto de dirección IP cuando se utiliza la alta disponibilidad 317
 desaparecen los paneles de ayuda 307
 desconexión del sistema principal, con administración Web 312, 328, 331, 333, 335
 dirección del direccionador no especificada o no válida para el método del puerto 316
 Dispatcher, Microsoft IIS y SSL no funcionan 305
 dscontrol o lbadm (mandato) da un error 305
 el conmutador no actualiza los pesos 333, 336
 en AIX, se daña la salida del mandato ps -vg 338
 En Linux, Dispatcher reenvía paquetes, pero el servidor de programa de fondo no los recibe 323
 En Linux, es posible que Dispatcher de HA se pueda sincronizar 319
 En Linux, existen limitaciones cuando se utilizan servidores zSeries o S/390 321
 En Linux, se produce una pérdida de memoria cuando se utilizan el gestor y los asesores 323
 En sistemas Linux, no se pueden recuperar valores de Metric Server 340
 En sistemas Windows, hay un problema con la toma de control de alta disponibilidad 324
 en Solaris, los scripts producen mensajes de consola no deseados 339
 En Solaris, no se puede añadir servidores IPv6 a la configuración 325
 En Windows, se produce el error "el servidor no responde" 318
 enlace del servidor Web a 0.0.0.0 312
 error al ejecutar Dispatcher con Caching Proxy instalado 306
 error de memoria/hebra Java (HP-UX) 313, 328, 331, 334, 337
 Error sintáctico o de configuración 327
 fin de los procesos de Load Balancer (Solaris) 317
 fonts coreanos no deseados en AIX y Linux 310
 GUI no se inicia correctamente 306
 GUI no se muestra correctamente 306

resolución de problemas (*continuación*)
 la dirección IP no se resuelve en la conexión remota 310
 lbadm desconecta del servidor después de actualizar la configuración 309
 Load Balancer no puede procesar y reenviar una trama 307
 los asesores no funcionan en una configuración de alta disponibilidad después de una caída de la red (Windows) 315
 máquinas primaria y de reserva activas en una configuración de alta disponibilidad 318
 mensaje de aviso Java aparece al instalar arreglos de servicio 325
 mensaje de error al intentar consultar la ayuda en línea 306
 Metric Server IOException en Windows 337
 Metric Server no informa de las cargas 337
 nalcontrol o lbadm (mandato) da un error 334
 no funciona la alta disponibilidad de Dispatcher 304
 no funcionan los asesores 304
 no registra cargas del servidor 312
 no responderán Dispatcher y el servidor 303
 no se direccionan las peticiones de Dispatcher 303
 no se ejecutará CBR 326
 no se ejecutará Dispatcher 303
 no se ejecutará Site Selector 329
 no se equilibra la carga de las peticiones 327
 no se ha podido crear el registro en el puerto 13099 332
 no se ha podido crear el registro en el puerto 14099 335
 no se han podido añadir pulsos 304
 no se iniciará ccserver 332
 no se iniciará nalserv 334
 no se pueden realizar las peticiones del cliente cuando el sistema intenta devolver respuestas de páginas de gran tamaño 318
 no utilice el mandato IP address add para crear alias de bucle de retorno (Linux) 316
 números de puerto utilizados por CBR 300
 números de puerto utilizados por Cisco CSS Controller 301
 números de puerto utilizados por Dispatcher 299
 números de puerto utilizados por Nortel Alteon Controller 302
 números de puerto utilizados por Site Selector 301
 pantalla azul al iniciar el ejecutor de Load Balancer 307
 problema al resolver la dirección IP con el nombre de sistema principal (Windows) 314, 329

resolución de problemas (*continuación*)
 problemas comunes y soluciones 303, 305, 326, 329, 332, 334, 337
 refresh (mandato) no actualiza la configuración 333, 336
 retardo al cargar la configuración de Load Balancer 317
 rutas adicionales 304
 se devuelve un alias en lugar de la dirección local 310
 Site Selector no equilibra la carga correctamente 330
 Site Selector no utiliza el algoritmo de turno rotativo (Solaris) 329
 sscontrol o lbadm (mandato) da un error 329
 ssserver no se ha podido iniciar en Windows 330
 tiempo de respuesta lento 311
 Valor de métrica devuelve -1 después de iniciar Metric Server 340
 vía de acceso al descubrimiento impide el tráfico de retorno con Load Balancer 307
 RMI (Remote Method Invocation) 35, 38, 40, 261, 262
 route, mandato 76, 77
 rule
 cbrcontrol 386
 dscontrol 386
 sscontrol 420
 rutas, adicionales 76
 rutas, suprimir adicionales 77
 rutas adicionales 76, 77

S

scripts 209
 ccserverdown 257
 goActive 210
 goldle 210
 goInOp 210
 goStandby 210
 highavailChange 210
 salida de usuario 184, 257
 scripts de salidas de usuario 184, 257
 ccoallserversdown 257
 ccserverdown 257
 ccserverup 257
 detección de rechazo de servicio (DoS) 240
 managerAlert 184
 managerClear 184
 nalallserversdown 257
 nalserv 257
 nalservdown 257
 serverDown 184
 serverUp 184
 Secure Sockets Layer 70
 sensibilidad a actualización de pesos, establecer 183, 377, 414, 416
 server
 cbrcontrol 392
 dscontrol 392
 nalcontrol 462
 sscontrol 423

- servicio
 - configuración 175
- servidor
 - advisorrequest 395
 - advisorresponse 395
 - añadir 396, 424
 - ccocontrol 447
 - collocated 393, 396
 - cookievalue 393
 - definir en un puerto 70, 396, 424
 - desactivar temporalmente 224, 374, 376, 378
 - dirección 392
 - eliminar 396, 423, 424
 - establecer el peso 396, 423
 - físico 58
 - fixedweight 393
 - lógico 58
 - mapport 108, 394
 - marcar como activo 396, 423, 424
 - marcar como inactivo 396, 423, 424
 - no de permanencia en memoria (alteración temporal de afinidad entre puertos) 393, 396
 - particiones 58
 - peso 393
 - protocol 394
 - reiniciar a todos los pesos
 - normalizados 377, 414, 416
 - restaurar un servidor inactivo 182
 - returnaddress 394
 - router 394
 - ubicación compartida con NAT 204
 - volver a activar 378
- servidores específicos del enlace 70, 71, 185, 231
- set
 - cbrcontrol 398
 - dscontrol 398
 - sscontrol 425
- Site Selector
 - aparecen caracteres nacionales Latin-1 dañados (Windows) 331
 - asesores y destinos de alcance marcan todos los servidores como inactivos (Windows) 331
 - comportamiento de la GUI inesperado con tarjetas Matrox AGP 330
 - configuración
 - configuración de la máquina 134
 - visión general de tareas 131
 - desconexión del sistema principal, con administración Web 331
 - determinar las características que se van a utilizar 26
 - ejemplo de configuración 14
 - ejemplo de inicio rápido 121
 - error de memoria/hebra Java (HP-UX) 331
 - iniciar y detener 278
 - lbadmin da un error 329
 - mandatos 403
 - no se ejecutará 329
 - no se equilibra la carga correctamente con rutas duplicadas 330

- Site Selector (*continuación*)
 - no utilizará el algoritmo de turno rotativo en el tráfico de clientes Solaris 329
 - planificar 125
 - resolución de problemas, tabla 294
 - sistemas Dispatcher de HA de equilibrio de carga 211
 - sscontrol da un error 329
 - ssserver no se ha podido iniciar en Windows 330
 - utilizar 278
 - valores de equilibrio de carga 180
 - reintento de servidor de asesor 188
 - tiempo de espera de servidor de asesor 188
 - visión general 14
- sitename
 - sscontrol 426
- SNMP 265, 269
- Solaris
 - configuración de la máquina Dispatcher 67
 - instalación 39
 - mandato arp publish 70
 - requisitos 39
- soporte de área amplia 229
 - ejemplo de configuración 232
 - Linux 235
 - utilización de asesores remotos 230
 - utilización de Dispatcher remoto 229
 - utilización de GRE 234
- soporte de espacio de usuario 82
- soporte sin kernel 82
- SSL 70
- ssserver
 - inicio 122
- status
 - cbrcontrol 399
 - dscontrol 399
- subagentes 265, 270
 - dscontrol 400
- Supervisar, opción de menú 269
- suprimir
 - clúster 358, 427
 - puerto de clústeres 384
 - ruta adicional 77
 - servidor de puertos 396, 423, 424

T

- tablas de resolución de problemas
 - CBR 292
 - Cisco CSS Controller 295
 - Dispatcher, componente 286
 - Metric Server 298
 - Nortel Alteon Controller 297
 - Site Selector 294
- tiempo de espera sin actividad 268, 357, 360, 382

U

- ubicación compartida
 - Cisco CSS Controller 243

- ubicación compartida (*continuación*)
 - IPv6, consideración 86
 - Nortel Alteon Controller 243
- ubicación compartida, Load Balancer y cliente 242
- ubicación compartida, Load Balancer y servidor 66, 71, 203, 231, 393, 396
- ubicación compartida con NAT 204
- ubicación compartida de varias direcciones 71
- umbral de sensibilidad 248

V

- valores, mostrar todos los valores global
 - para el gestor 377, 415, 416
 - para un asesor 353, 406, 407
- valores de equilibrio de carga (optimización) 180, 246
- versión, mostrar
 - asesor 353, 407, 408
 - gestor 378, 415, 417
- visión general
 - configuración de CBR 109
 - configuración de Cisco CSS Controller 149
 - configuración de Nortel Alteon Controller 171
 - configuración de Site Selector 131
 - configuración del componente Dispatcher 63

W

- WAS (WebSphere Application Server)
 - asesor WAS 190, 194
- Web, administración basada en 261, 263
 - renovar 265
- Windows
 - configuración de la máquina Dispatcher 67
 - instalación 40
 - mandato executor configure 69
 - requisitos 40



Printed in Denmark by IBM Danmark A/S

GC11-3240-00



Spine information:



WebSphere Application Server

Guía de administración de Load Balancer

Versión 6.1

GC11-3240-00