

WebSphere Application Server



Edge Components Konzepte, Planung und Installation

Version 6.1

WebSphere Application Server



Edge Components Konzepte, Planung und Installation

Version 6.1

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die allgemeinen Informationen unter „Bemerkungen“ auf Seite 85 gelesen werden.

Erste Ausgabe (Mai 2006)

Diese Ausgabe gilt für:

WebSphere Application Server Version 6.1

Außerdem gilt diese Ausgabe für alle nachfolgenden Releases und Änderungen, sofern in den neuen Ausgaben keine anderen Hinweise enthalten sind.

Veröffentlichungen können über den zuständigen IBM Ansprechpartner oder die zuständige IBM Geschäftsstelle bezogen werden.

Diese Veröffentlichung ist eine Übersetzung des Handbuchs

IBM WebSphere Application Server Edge Components Concepts, Planning, and Installation, Version 6.1,

IBM Form GC31-6918-00,

herausgegeben von International Business Machines Corporation, USA

© Copyright International Business Machines Corporation 2006

© Copyright IBM Deutschland GmbH 2006

Informationen, die nur für bestimmte Länder Gültigkeit haben und für Deutschland, Österreich und die Schweiz nicht zutreffen, wurden in dieser Veröffentlichung im Originaltext übernommen.

Möglicherweise sind nicht alle in dieser Übersetzung aufgeführten Produkte in Deutschland angekündigt und verfügbar; vor Entscheidungen empfiehlt sich der Kontakt mit der zuständigen IBM Geschäftsstelle.

Änderung des Textes bleibt vorbehalten.

Herausgegeben von:

SW TSC Germany

Kst. 2877

Mai 2006

Inhaltsverzeichnis

Abbildungsverzeichnis v

Zu diesem Handbuch	vii
Zielgruppe	vii
Eingabehilfen	vii
Konventionen und Terminologie in diesem Handbuch	vii

Teil 1. Übersicht 1

Kapitel 1. Einführung in WebSphere Application Server Edge Components	3
Caching Proxy	4
Load Balancer	5
Dispatcher	6
Content Based Routing	6
Site Selector	7
Cisco CSS Controller	7
Nortel Alteon Controller	7
Metric Server	7

Kapitel 2. Edge Components und die WebSphere-Produktfamilie	9
Tivoli Access Manager	9
WebSphere Portal Server	9
WebSphere Site Analyzer	10
WebSphere Transcoding Publisher	10

Kapitel 3. Weitere Informationen zu Application Server und Edge Components	11
---------------------------------------------------------------------------------------------	-----------

Teil 2. Edge Components - Konzepte und Erläuterungen 13

Kapitel 4. Caching	15
Caching-Proxy-Basiskonfigurationen	15
Reverse Caching Proxy (Standardkonfiguration)	15
Forward Caching Proxy	16
Erweitertes Caching	19
Caching-Proxy-Cluster mit Lastausgleich	19
Dynamischen Inhalt zwischenspeichern	20
Zusätzliche Caching-Funktionen	21

Kapitel 5. Netzleistung	23
Netzhardware	23
Überlegungen zum Speicher	23
Überlegungen zur Festplatte	24
Überlegungen zum Netz	24
Überlegungen zur CPU	24
Netzarchitektur	24

Überlegungen zu Popularität der Website und Arbeitslast des Proxy-Servers	24
Überlegungen zur Art des Datenverkehrs	25

Kapitel 6. Verfügbarkeit	27
Lastausgleich	27
Lastausgleich für mehrere Inhaltshosts	27
Lastausgleich für mehrere Reverse-Proxy-Server	29
Load Balancer mit mehreren Forward-Proxy-Servern	30
Unterstützung der Lastübernahme	33

Kapitel 7. Content Based Routing 35

Teil 3. Szenarios 39

Kapitel 8. B2C-Netz	41
Phase 1	41
Phase 2	42
Phase 3	44

Kapitel 9. Online-Banking-Lösung 45

Kapitel 10. Web-Portal-Netz 47

Teil 4. Installation von Edge Components 49

Kapitel 11. Voraussetzungen für Edge Components	51
Hardware- und Softwarevoraussetzungen	51
Verwendung der Konfigurations- und Verwaltungsfomulare von Caching Proxy in Browsern	51
Verwendung von Browsern für die Anzeige der Online-Hilfe von Load Balancer	53

Kapitel 12. Installation von Edge Components mit dem Installationsprogramm	55
Verwendung des Installationsprogramms auf Windows-Systemen	55
Verwendung des Installationsprogramms auf Linux- und UNIX-Systemen	57

Kapitel 13. Installation von Caching Proxy mit den Paketverwaltungstools des Betriebssystems	59
Caching Proxy mit Systemtools deinstallieren	61

Kapitel 14. Installation von Load Balancer mit den Paketverwaltungstools des Betriebssystems 63

Installation unter AIX	64
Installationsvorbereitung	64
Installationsverfahren	65
Installation unter HP-UX	67
Installationsvorbereitung	67
Installationsverfahren	67
Installation unter Linux	69
Installationsvorbereitung	69
Installationsschritte	69
Installation unter Solaris	71
Installationsvorbereitung	71
Installationsschritte	71

Teil 5. Aufbau von Netzen mit Edge Components 73

Kapitel 15. Aufbau eines Caching-Proxy-Netzes 75

Arbeitsablauf	75
-------------------------	----

Erforderliche Computersysteme und Software überprüfen	76
Server 1 erstellen (Linux- und UNIX-Systeme).	76
Server 1 erstellen (Windows-System)	76
Server 1 konfigurieren	76
Das Caching-Proxy-Netz testen	77

Kapitel 16. Aufbau eines Load-Balancer-Netzes 79

Arbeitsablauf	79
Erforderliche Computersysteme und Software überprüfen	79
Das Netz konfigurieren	80
Den Dispatcher konfigurieren	81
Konfiguration über die Befehlszeile	81
Konfiguration mit dem Konfigurationsassistenten	82
Konfiguration über die grafische Benutzerschnittstelle (GUI)	83
Das Load-Balancer-Netz testen	83

Bemerkungen. 85

Marken.	87
-----------------	----

Abbildungsverzeichnis

1. Caching Proxy als Reverse Proxy	16	10. Verwendung eines primären und eines Backup-Load-Balancer, um die Verfügbarkeit von Webinhalten zu erhöhen	33
2. Caching Proxy als Forward Proxy	17	11. Installation eines Backup-Load-Balancer auf einem Inhaltshost	34
3. Caching Proxy als transparenter Forward Proxy	19	12. Routing von HTTP-Anforderungen mit CBR	36
4. Caching Proxy als Proxy-Server für einen Cluster mit Lastausgleich	20	13. Mit CBR weitergeleitete HTTP-Anforderungen verteilen	37
5. Lastausgleich für mehrere Inhaltshosts	28	14. B2C-Netz (Phase 1)	42
6. Lastausgleich für mehrere Reverse-Proxy-Server und Inhaltshosts	29	15. B2C-Netz (Phase 2)	43
7. Dispatcher für den Lastausgleich für mehrere Caching-Proxy-Server verwenden.	31	16. B2C-Netz (Phase 3)	44
8. Verwendung eines primären und eines Backup-Dispatcher zur Unterstützung eines Internet-Zugangs mit hoher Verfügbarkeit.	32	17. Online-Banking-Lösung	46
9. Installation des Backup-Dispatcher auf einer Caching-Proxy-Maschine.	33	18. Web-Portal.	48
		19. Beispiel für ein Caching-Proxy-Netz	75
		20. Beispiel für ein Load-Balancer-Netz	79

Zu diesem Handbuch

Das Handbuch *WebSphere Application Server Edge Components Konzepte, Planung und Installation* dient als Einführung in WebSphere Application Server Edge Components. Es enthält Produktübersichten, detaillierte Erläuterungen der Funktionalität von Schlüsselkomponenten, Szenarien für den Einsatz der Edge-Komponenten im Netz, Informationen zur Installation und Erstkonfiguration sowie Beispielnetze.

Zielgruppe

Das Handbuch *WebSphere Application Server Edge Components Konzepte, Planung und Installation* wurde für erfahrene Netz- und Systemadministratoren geschrieben, die mit ihrem Betriebssystem und dem Bereitstellen von Internet-Services vertraut sind. Vorkenntnisse bezüglich WebSphere Application Server oder WebSphere Application Server Edge Components sind nicht erforderlich.

Eingabehilfen

Eingabehilfen unterstützen Benutzer mit körperlichen Behinderungen wie eingeschränkter Motorik oder eingeschränktem Sehvermögen bei der Arbeit mit Softwareprodukten. Im Folgenden sind die wichtigsten Eingabehilfen von WebSphere Application Server Version 6.1 beschrieben:

- Sie können so genannte Bildschirmleseprogramme (Screen-Reader) und einen digitalen Sprachsynthesizer verwenden, um sich die Bildschirmanzeige vorlesen zu lassen. Mit einer Spracherkennungssoftware wie IBM ViaVoice können Sie Daten eingeben und in der Benutzerschnittstelle navigieren.
- Alle Funktionen sind neben der Maus auch über die Tastatur ausführbar.
- Die Funktionen von Application Server können mit Standardtexteditoren oder Befehlszeilenschnittstellen anstatt über die bereitgestellten grafischen Oberflächen konfiguriert und verwaltet werden. Nähere Informationen zu den speziellen Eingabehilfen finden Sie in der zugehörigen Dokumentation.

Konventionen und Terminologie in diesem Handbuch

Diese Dokumentation richtet sich in Bezug auf Typografie und Hervorhebung nach den folgenden Konventionen.

Tabelle 1. In diesem Handbuch verwendete Konventionen

Konvention	Bedeutung
Fettschrift	Bei Bezugnahme auf grafische Benutzerschnittstellen (GUIs) werden Menüs, Menüpunkte, Titel, Knöpfe (Schaltflächen), Symbole und Ordner in Fettschrift dargestellt. Die Fettschrift kann auch zum Hervorheben von Befehlsnamen verwendet werden, die sonst mit dem Begleittext verwechselt werden könnten.
Monospace-Schrift	Kennzeichnet Text, der an der Eingabeaufforderung eingegeben werden muss. In Monospace-Schrift werden auch Anzeigetexte, Codebeispiele und Dateiauszüge hervorgehoben.
<i>Kursivschrift</i>	Kennzeichnet Variablenwerte, die eingegeben werden müssen (z. B. müssen Sie <i>Dateiname</i> durch den Namen einer Datei ersetzen). Kursivschrift wird außerdem für Hervorhebungen und Handbuchtitel verwendet.

Tabelle 1. In diesem Handbuch verwendete Konventionen (Forts.)

Konvention	Bedeutung
Strg- <i>x</i>	Diese Angabe kennzeichnet eine Tastenkombination mit der Steuerungstaste. <i>x</i> steht hier für eine Tastenbezeichnung. Beispielsweise bedeutet die Angabe <Strg-c>, dass Sie die Taste Strg gedrückt halten und gleichzeitig die Taste c drücken sollen.
Eingabetaste	Bei dieser Angabe müssen Sie die Eingabetaste drücken.
%	Steht in der Linux- und UNIX-Befehlsumgebung für die Aufforderung zur Eingabe eines Befehls, der keine Root-Berechtigung erfordert.
#	Steht in der Linux- und UNIX-Befehlsumgebung für die Aufforderung zur Eingabe eines Befehls, der Root-Berechtigung erfordert.
C:\	Steht für die Eingabeaufforderung in der Windows-Umgebung.
Befehlseingabe	Wenn Sie aufgefordert werden, einen Befehl einzugeben, geben Sie den Befehl ein und drücken Sie dann die Eingabetaste. Beispiel: Die Anweisung "Geben Sie den Befehl ls ein" bedeutet, dass Sie an der Eingabeaufforderung ls eingeben und anschließend die Eingabetaste drücken müssen.
[]	In eckigen Klammern werden optionale Elemente in Syntaxbeschreibungen angegeben.
{ }	In geschweiften Klammern werden Listen in Syntaxbeschreibungen angegeben, aus denen Sie einen Eintrag auswählen können.
	Dieses Zeichen trennt in Syntaxbeschreibungen die Einträge in einer Auswahlliste, die in geschweiften Klammern ({ }) angegeben ist.
...	Drei Punkte in Syntaxbeschreibungen bedeuten, dass der vorherige Eintrag einmal oder mehrmals wiederholt werden kann. Drei Punkte in Beispielen bedeuten, dass Informationen weggelassen wurden, um die Darstellung zu vereinfachen.

Teil 1. Übersicht

Dieser Teil enthält eine Einführung in die Komponenten Caching Proxy und Load Balancer von WebSphere Application Server Edge Components und erläutert ihre Verwendung zusammen mit Application Server. Darüber hinaus werden in diesem Teil andere zugehörige Produkte der WebSphere-Produktfamilie vorgestellt.

Dieser Teil enthält folgende Kapitel:

- Kapitel 1, „Einführung in WebSphere Application Server Edge Components“, auf Seite 3
- Kapitel 2, „Edge Components und die WebSphere-Produktfamilie“, auf Seite 9
- Kapitel 3, „Weitere Informationen zu Application Server und Edge Components“, auf Seite 11

Kapitel 1. Einführung in WebSphere Application Server Edge Components

WebSphere ist eine Internet-Infrastruktursoftware, mit deren Unterstützung Unternehmen e-business-Anwendungen der nächsten Generation, z. B. Anwendungen für B2B-E-Commerce, entwickeln, einsetzen und integrieren können. WebSphere-Middleware unterstützt Geschäftsanwendungen vom einfachen Web-Publishing bis hin zur unternehmensweiten Transaktionsverarbeitung.

Als Grundlage der WebSphere-Plattform stellt WebSphere Application Server umfassende Middleware bereit, mit deren Hilfe die Benutzer Geschäftsanwendungen entwerfen, implementieren, einsetzen und verwalten können. Diese Anwendungen können vom einfachen virtuellen Schaufenster auf einer Website bis hin zur vollständigen Überarbeitung der Datenverarbeitungsinfrastruktur eines Unternehmens reichen.

Prozessorintensive Funktionen wie Personalisierung bringen jedem e-business einen Wettbewerbsvorteil. Weil diese Funktionen jedoch für gewöhnlich an zentrale Server übertragen werden, stehen wertvolle Funktionen nicht auf Internet-Ebene zur Verfügung. Folglich müssen Umfang und Leistung der Internet-Infrastruktur eines Unternehmens zusammen mit der Zahl der neuen Webanwendungen wachsen. Außerdem sind für ein e-business die Zuverlässigkeit und die Sicherheit zwei Aspekte von außerordentlicher Bedeutung. Selbst die geringste Serviceunterbrechung kann Geschäftsverluste zur Folge haben.

Edge Components (früher Edge Server) ist jetzt im Produktumfang von WebSphere Application Server enthalten. Edge Components kann zusammen mit WebSphere Application Server eingesetzt werden, um den Clientzugriff auf die Webserver zu steuern. Außerdem ermöglicht es den Unternehmen, Benutzern, die über das Internet oder ein Unternehmens-Intranet auf webbasierte Inhalte zugreifen, einen besseren Service zu bieten. Durch den Einsatz von Edge Components kann die Last auf den Webservern verringert, die Verfügbarkeit der Inhalte erhöht und die Leistung der Webserver verbessert werden. Wie der Name bereits andeutet, wird Edge Components normalerweise auf Maschinen eingesetzt, die sich (in Bezug auf die Netzkonfiguration) nahe der Grenze (Edge) zwischen dem Unternehmens-Intranet und dem Internet befinden.

WebSphere Application Server umfasst die Edge-Komponenten Caching Proxy und Load Balancer.

Wichtig: Caching Proxy ist mit folgender Ausnahme in allen Edge-Components-Installationen verfügbar:

- Caching Proxy ist nicht verfügbar in Edge-Components-Installationen auf 64-Bit-Plattformen mit Itanium-2- oder AMD-Opteron-Prozessoren.
- Caching Proxy ist nicht verfügbar in Edge-Components-Installationen von Load Balancer for IPv4 and IPv6.

Caching Proxy

Caching Proxy verringert die Belastung des Netzes und verbessert Geschwindigkeit und Zuverlässigkeit einer Website durch die Bereitstellung eines POP-Knotens (Point-of-Presence, Zugangspunkt) für einen oder mehrere Back-End-Inhaltsserver. Caching Proxy kann statische Inhalte und Inhalte, die von WebSphere Application Server dynamisch generiert wurden, zwischenspeichern und bereitstellen.

Caching Proxy kann als Reverse-Proxy-Server (Standardkonfiguration) oder als Forward-Proxy-Server konfiguriert werden und damit entweder einen so genannten Point-of-Presence für ein Netz oder einen internen Netzserver darstellen, dessen Aufgabe es ist, Anforderungs- und Antwortzeiten zu verbessern. Weitere Informationen zu Reverse- und Forward-Proxy-Konfigurationen finden Sie im Abschnitt „Caching-Proxy-Basiskonfigurationen“ auf Seite 15.

Der Proxy-Server fängt Datenanforderungen von Clients ab, ruft die angeforderten Informationen von den Maschinen ab, auf denen Inhalte bereitgestellt werden, und liefert sie an die Clients. Im Allgemeinen handelt es sich bei den Anforderungen um Anforderungen für Dokumente, die auf Webserver-Maschinen (auch *Ursprungsserver* oder *Inhaltshosts* genannt) gespeichert sind und die über das Protokoll HTTP (Hypertext Transfer Protocol) zugestellt werden. Sie können den Proxy-Server jedoch auch für die Verwendung anderer Protokolle wie File Transfer Protocol (FTP) und Gopher konfigurieren.

Der Proxy-Server legt Inhalte, die zwischengespeichert werden können, in einem lokalen Cache ab, bevor er sie an den Requester liefert. Beispiele für solche Inhalte, die im Cache zwischengespeichert werden können, sind statische Webseiten und JSP-Dateien (JavaServer Pages) mit Fragmenten, die dynamisch generiert werden, sich aber nur selten ändern. Durch die Zwischenspeicherung (Caching) ist der Proxy-Server in der Lage, nachfolgende Anforderungen für denselben Inhalt direkt aus dem Cache abzurufen. Das ist sehr viel schneller als ein erneuter Abruf des Inhalts vom Inhaltshost.

Die Plug-ins für Caching Proxy erweitern die Funktionalität des Proxy-Servers.

- Das Plug-in ICP erlaubt es einem Proxy-Server, bei der Suche nach HTML-Seiten oder anderen Ressourcen, die im Cache gespeichert werden können, ICP-kompatible Caches (ICP = Internet Caching Protocol) abzufragen.
- Das Plug-in Tivoli Access Manager (früher Policy Director) ermöglicht dem Proxy-Server, die integrierten Berechtigungs- und Authentifizierungsservices von Access Manager zu verwenden.
- Mit dem PAC-LDAP-Authentifizierungsmodul ist der Proxy-Server in der Lage, beim Ausführen von Berechtigungs- und Authentifizierungsroutinen auf einen LDAP-Server zuzugreifen.
- Das Plug-in WebSphere Transcoding Publisher erlaubt es dem Proxy-Server, mehrere Versionen von konvertiertem Inhalt für mobile Einheiten zwischenspeichern.

Darüber hinaus können Sie die Funktionen von Caching Proxy erweitern, indem Sie eigene Plug-in-Module für eine API (Application Programming Interface) schreiben. Die API ist flexibel, einfach zu verwenden und plattformunabhängig. Der Proxyserver führt für jede von ihm verarbeitete Clientanforderung eine Reihe von Schritten aus. Eine Plug-in-Anwendung ändert oder ersetzt einen Schritt der Anforderungsverarbeitung, z. B. die Clientauthentifizierung oder das Filtern der Anforderungen.

Die leistungsfähige Schnittstelle TransmogriFY unterstützt beispielsweise den Zugriff auf HTTP-Daten und das Ersetzen oder Umwandeln von URLs und Webinhalten. Plug-ins können bestimmte Verarbeitungsschritte ändern oder ersetzen. Außerdem können für einen bestimmten Schritt mehrere Plug-ins aufgerufen werden.

Load Balancer

Mit Load Balancer werden Systeme an der Grenze (Edge) des Netzes erstellt, die die Datenübertragungen auf dem Netz steuern. Auf diese Weise kann eine Überlastung des Netzes weitgehend vermieden und die Arbeitslast auf verschiedene andere Services und Systeme verteilt werden. Load Balancer unterstützt Site-Auswahl, Laststeuerung (WLM, Workload Management), Sitzungsaffinität und transparente Übernahme von Arbeitslasten.

Load Balancer wird zwischen dem Internet und den Back-End-Servern des Unternehmens installiert, bei denen es sich um Inhaltshosts oder Caching-Proxy-Maschinen handeln kann. Load Balancer fungiert als zentraler POP-Knoten (Point-of-Presence, Zugangspunkt) des Unternehmens im Internet, selbst wenn das Unternehmen auf Grund hoher Nachfrage oder großer Inhaltsmengen mehrere Back-End-Server verwendet. Eine hohe Verfügbarkeit ist garantiert, wenn Sie einen Load Balancer als Backup installieren, der bei temporärem Ausfall des primären Load Balancer dessen Aufgaben übernimmt.

Load Balancer fängt Datenanforderungen von Clients ab und leitet jede Anforderung an den Server weiter, der zum gegebenen Zeitpunkt am besten für die Bearbeitung der Anforderung geeignet ist. Anders ausgedrückt, die Last eingehender Anforderungen wird auf eine definierte Menge von Maschinen aufgeteilt, die dieselbe Art von Anforderungen bearbeiten. Load Balancer kann Anforderungen auf viele Servertypen verteilen, darunter WebSphere Application Server und Caching-Proxy-Maschinen. Der Lastausgleich kann für eine bestimmte Anwendung oder Plattform mit benutzerdefinierten Advisor-Funktionen angepasst werden. Es werden spezielle Advisor-Funktionen bereitgestellt, mit denen Informationen für den Lastausgleich in WebSphere Application Server abgerufen werden können.

Wird die Komponente Content Based Routing zusammen mit Caching Proxy installiert, können HTTP- und HTTPS-Anforderungen sogar auf der Grundlage der URLs oder anderer, vom Administrator festgelegter Merkmale verteilt werden. Dadurch entfällt das Speichern identischer Inhalte auf allen Back-End-Servern. Die Komponente Dispatcher kann dieselbe Funktion auch für HTTP-Anforderungen bereitstellen.

Der Lastausgleich verbessert die Verfügbarkeit und Skalierbarkeit Ihrer Website, indem Inhaltsserver, einschließlich HTTP-Server, Anwendungsserver und Proxyserver, die stellvertretend für die Inhaltsserver auftreten, transparent zusammengefasst werden. Durch Parallelschaltung, Lastausgleich und Lastübernahme wird eine hohe Verfügbarkeit sichergestellt. Der Ausfall eines Servers hat keine Unterbrechung von Geschäftsaktivitäten zur Folge. Die Skalierbarkeit einer Infrastruktur verbessert sich erheblich, weil Back-End-Verarbeitungsleistung transparent hinzugefügt werden kann.

Unterstützung für IPv6: Die Unterstützung für das erweiterte IP-Adressierungsschema IPv6 ist in "Load Balancer for IPv4 and IPv6" verfügbar. Load Balancer for IPv4 and IPv6 ist ein gesondertes Installations-Image, das *nur* die Komponente Dispatcher enthält. Dieser Installationstyp unterstützt den Lastausgleich für IPv4- und IPv6-Datenverkehr mit Servern, die im Netz konfiguriert sind, unter Verwendung der MAC-basierten Paketweiterleitung der Komponente Dispatcher. Alle früheren Versionen von Load Balancer müssen unbedingt deinstalliert werden, bevor Load Balancer for IPv4 and IPv6 installiert wird. Es ist nicht möglich, zwei Versionen von Load Balancer auf einer Maschine zu installieren. (Der Abschnitt „Dispatcher“ enthält eine Kurzübersicht über die Komponente Dispatcher.)

Load Balancer umfasst folgende Komponenten:

Dispatcher

Die Komponente Dispatcher führt den Lastausgleich für alle Internet-Services, wie z. B. HTTP, FTP, HTTPS und Telnet, auf den Servern eines lokalen Netzes (LAN) oder eines Weitverkehrsnetzes (WAN) durch. Für HTTP-Services kann Dispatcher den Lastausgleich zwischen den Servern basierend auf dem URL-Inhalt der Clientanforderung durchführen.

Die Komponente Dispatcher erlaubt eine stabile, effiziente Verwaltung eines großen skalierbaren Servernetzes. Mit Hilfe von Dispatcher können Sie viele einzelne Server so miteinander verknüpfen, dass sie als einzelner virtueller Server erscheinen. Den Besuchern stellt sich Ihre Site daher als eine einzelne IP-Adresse dar.

Wenn Sie eine Installation von Load Balancer for IPv4 and IPv6 verwenden, lesen Sie das Kapitel zur Implementierung von Dispatcher in Load Balancer for IPv4 and IPv6 im *WebSphere Application Server Load Balancer Administratorhandbuch*, das Informationen zu den Einschränkungen und Konfigurationsunterschieden enthält.

Content Based Routing

Die Komponente Content Based Routing führt den Lastausgleich zwischen den Servern für die Services HTTP und HTTPS basierend auf dem Inhalt der Clientanforderung durch. Die Komponente Content Based Routing arbeitet mit der Komponente Application Server Caching Proxy zusammen.

Wichtig: Die Komponente Content Based Routing (CBR) ist mit folgenden Ausnahmen auf allen unterstützten Plattformen verfügbar:

- CBR ist nicht verfügbar in Load-Balancer-Installationen auf Plattformen mit einer 64-Bit-JVM.

Für diese Art von Installation können Sie alternativ die Weiterleitungsmethode `cbr` der Load-Balancer-Komponente Dispatcher verwenden, um das inhaltsbasierte Routing von HTTP- und HTTPS-Anforderungen ohne Verwendung von Caching Proxy zu unterstützen. Nähere Informationen hierzu finden Sie im *WebSphere Application Server Load Balancer Administratorhandbuch*.

- CBR ist nicht verfügbar in Installationen von Load Balancer for IPv4 and IPv6. Load Balancer for IPv4 and IPv6 unterstützt nur die Weiterleitungsmethode `mac` der Komponente Dispatcher. Die Weiterleitungsmethoden `nat` und `cbr` werden nicht unterstützt.

Site Selector

Die Komponente Site Selector erweitert ein Lastausgleichssystem, indem sie ihm erlaubt, als POP-Knoten (Point-of-Presence, Zugangspunkt) für ein Netz zu fungieren und ankommende Anforderungen durch Zuordnung von DNS-Namen zu IP-Adressen zu verteilen. Zusammen mit Metric Server kann Site Selector die Aktivitäten eines Servers überwachen, den Server mit der geringsten Auslastung herausfinden und einen Server, der ausgefallen ist, erkennen.

Diese Komponente wird mit folgender Ausnahme in allen Edge-Components-Installationen unterstützt:

- Diese Komponente ist in Edge-Components-Installationen von Load Balancer for IPv4 and IPv6 nicht verfügbar.

Cisco CSS Controller

Die Komponente Cisco CSS Controller generiert Metrikangaben für die Servergewichtung, die zwecks Serverauswahl, Lastoptimierung und Fehlertoleranz an einen Cisco CSS Switch weitergeleitet werden.

Diese Komponente wird mit folgender Ausnahme in allen Edge-Components-Installationen unterstützt:

- Diese Komponente ist in Edge-Components-Installationen von Load Balancer for IPv4 and IPv6 nicht verfügbar.

Nortel Alteon Controller

Die Komponente Nortel Alteon Controller generiert Metrikangaben für die Servergewichtung, die zwecks Serverauswahl, Lastoptimierung und Fehlertoleranz an einen Nortel Alteon Switch weitergeleitet werden.

Diese Komponente wird mit folgender Ausnahme in allen Edge-Components-Installationen unterstützt:

- Diese Komponente ist in Edge-Components-Installationen von Load Balancer for IPv4 and IPv6 nicht verfügbar.

Metric Server

Die Komponente Metric Server wird als Dämon auf einem Server mit Lastausgleich ausgeführt und liefert der Komponente Load Balancer Informationen über die Systembelastung.

Kapitel 2. Edge Components und die WebSphere-Produktfamilie

Die IBM WebSphere-Produktfamilie unterstützt Benutzer bei der Realisierung eines eigenen e-business. Es handelt sich bei dieser Produktfamilie um eine Gruppe von Softwareprodukten, die den Benutzer dabei unterstützen, extrem leistungsfähige Websites zu entwickeln und zu verwalten sowie Websites in neue oder vorhandene Informationssysteme außerhalb des Web-Business zu integrieren.

Die WebSphere-Produktfamilie setzt sich zusammen aus WebSphere Application Server mit Edge Components und anderer WebSphere-Software, die eng mit WebSphere Application Server verbunden ist und dessen Leistungsspektrum erweitert. Eine Übersicht über WebSphere Application Server und seine Komponenten enthält Kapitel 1, „Einführung in WebSphere Application Server Edge Components“, auf Seite 3.

Tivoli Access Manager

Tivoli Access Manager (früher Tivoli Policy Director) ist ein eigenständig verfügbares Produkt. Dieses Produkt ermöglicht die Zugriffssteuerung und zentrale Sicherheitsverwaltung in vorhandenen Webanwendungen und den Zugriff auf mehrere Webressourcen nach einmaliger Authentifizierung. Ein Caching-Proxy-Plug-in nutzt die Sicherheitsfunktionen von Access Manager und erlaubt dadurch dem Proxy-Server, die integrierten Berechtigungs- und Authentifizierungsservices von Access Manager zu verwenden.

WebSphere Portal Server

WebSphere Portal Server ist ein eigenständig verfügbares Produkt, das ein Gerüst für die Präsentation, Sicherheit, Skalierbarkeit und Verfügbarkeit von Portalen bietet. Mit Hilfe von Portal Server können Unternehmen eigene angepasste Portal-Websites erstellen, um den Anforderungen ihrer Angestellten, Geschäftspartner und Kunden gerecht zu werden. Benutzer können sich am Portal anmelden und erhalten personalisierte Webseiten, die ihnen den Zugang zu den gewünschten Informationen, Personen und Anwendungen liefern. Durch diesen personalisierten, zentralen Zugangspunkt zu allen erforderlichen Ressourcen wird eine Informationsüberflutung verringert, die Produktivität verbessert und die Nutzung der Website erhöht.

WebSphere Portal Server wird zur Gewährleistung von Skalierbarkeit und Zuverlässigkeit in einem WebSphere-Application-Server-Cluster ausgeführt. Ein besserer Lastausgleich und eine noch höhere Verfügbarkeit können durch die zusätzliche Verwendung der Komponente Load Balancer von Application Server erreicht werden.

WebSphere Site Analyzer

WebSphere Site Analyzer ist ein eigenständig verfügbares Produkt, das Unternehmen bei der frühzeitigen Erkennung von Kapazitäts- und Leistungsproblemen unterstützt. Mit Site Analyzer können die Protokolle von Caching Proxy und Load Balancer sowie weitere Verwaltungshilfen dazu herangezogen werden, den Bedarf an zusätzlichen Ressourcen festzustellen, indem die Auslastung der Website überwacht, analysiert und in Berichten gespeichert wird. Außerdem unterstützen die Verwaltungskomponenten von Site Analyzer den Benutzer bei Installation und Upgrade von Edge Components, beim Verwalten und Speichern von Konfigurationen, bei der fernen Ausführung von Edge Components sowie beim Anzeigen und Berichten von Ereignissen.

WebSphere Transcoding Publisher

WebSphere Transcoding Publisher ist ein eigenständig verfügbares Produkt, das eine Website so konvertieren kann, dass sie auf einer mobilen Einheit, z. B. auf einem Telefon mit Internet-Unterstützung, anzeigbar ist, Webinhalte (durch Aufruf von WebSphere Translation Server) in die gewünschte Landessprache des Benutzers übersetzen und Markup-Sprachen konvertieren kann. Durch die Möglichkeit, Inhalte für verschiedene Einheiten und Benutzer bereitzustellen, erweitert Transcoding Publisher das Leistungsspektrum von Caching Proxy. Nach dem Zugriff auf die Inhalte eines Webservers kann die Schnittstelle Transmogrify Caching Proxy so konfiguriert werden, dass Transcoding Publisher aufgerufen wird, um die Daten umzuwandeln und für Caching und mögliche Wiederverwendung zu kennzeichnen. An der Schnittstelle von Caching Proxy, die nach der Authentifizierung aufgerufen wird, prüft Transcoding Publisher anschließend den Proxy-Server auf Inhalte, die mit den Benutzer- und Einheitenvoraussetzungen übereinstimmen, und stellt bei Übereinstimmung die Inhalte aus dem Cache des Proxy-Servers bereit.

Kapitel 3. Weitere Informationen zu Application Server und Edge Components

Im Information Center von Edge Components finden Sie die folgenden Veröffentlichungen zu WebSphere Application Server Edge Components:

- *Programming Guide for Edge Components*, IBM Form GC31-6919-00
- *Caching Proxy Administration Guide*, IBM Form GC12-3679-00
- *Load Balancer Administration Guide*, IBM Form GC12-3680-00

Weitere Veröffentlichungen zu WebSphere Application Server finden Sie auf der Bibliotheksseite von WebSphere Application Server.

Technische Unterstützungsinformationen zu Edge Components finden Sie auf der Unterstützungsseite von WebSphere Application Server.

In der folgenden Liste sind die Websites aufgeführt, die Informationen zu Edge Components oder zugehörige Informationen enthalten:

- Homepage der IBM Website: <http://www.ibm.com/>
- IBM WebSphere Application Server: <http://www.ibm.com/software/webservers/appserv/>
- Website mit der Bibliothek zu IBM WebSphere Application Server: <http://www.ibm.com/software/webservers/appserv/library.html>
- Website mit Unterstützungsinformationen zu IBM WebSphere Application Server: <http://www.ibm.com/software/webservers/appserv/support.html>
- IBM WebSphere Application Server Information Center <http://www.ibm.com/software/webservers/appserv/infocenter.html>
- IBM WebSphere Application Server Edge Components Information Center <http://www.ibm.com/software/webservers/appserv/ecinfocenter.html>

Teil 2. Edge Components - Konzepte und Erläuterungen

In den detaillierten Erläuterungen in diesem Teil werden einige Funktionen von Edge Components besonders hervorgehoben. Eine Übersicht über die Komponente Caching Proxy von Application Server finden Sie in Kapitel 1, „Einführung in WebSphere Application Server Edge Components“, auf Seite 3.

Dieser Teil enthält folgende Kapitel:

Kapitel 4, „Caching“, auf Seite 15

Kapitel 5, „Netzleistung“, auf Seite 23

Kapitel 6, „Verfügbarkeit“, auf Seite 27

Kapitel 7, „Content Based Routing“, auf Seite 35

Kapitel 4. Caching

Mit den Caching-Funktionen von Caching Proxy können Sie die Belastung des Netzes verringern und den Endbenutzern einen schnelleren und zuverlässigeren Service gewährleisten. Dies erfolgt durch Entlastung der Back-End-Server und Peer-Links durch das vom Proxy-Server durchgeführte Caching. Caching Proxy kann statische Inhalte und Inhalte, die von WebSphere Application Server dynamisch generiert werden, zwischenspeichern. Zur Verbesserung des Caching arbeitet Caching Proxy außerdem mit der Komponente Application Server Load Balancer zusammen. Eine Einführung in diese Systeme finden Sie in Kapitel 1, „Einführung in WebSphere Application Server Edge Components“, auf Seite 3.

Wichtig: Caching Proxy ist mit folgender Ausnahme in allen Edge-Components-Installationen verfügbar:

- Caching Proxy ist nicht verfügbar in Edge-Components-Installationen auf 64-Bit-Plattformen mit Itanium-2- oder AMD-Opteron-Prozessoren.
- Caching Proxy ist nicht verfügbar in Edge-Components-Installationen von Load Balancer for IPv4 and IPv6.

Caching-Proxy-Basiskonfigurationen

Caching Proxy kann als Reverse-Caching-Proxy-Server (Standardkonfiguration) oder als Forward-Caching-Proxy-Server konfiguriert werden. Für die Verwendung durch Inhaltshosts wird Caching Proxy als Reverse-Caching-Proxy-Server zwischen dem Internet und den Inhaltshosts des Unternehmens konfiguriert. Für die Verwendung durch Internet-Zugriffspower wird Caching Proxy als Forward-Caching-Proxy-Server zwischen einem Client und dem Internet konfiguriert.

Reverse Caching Proxy (Standardkonfiguration)

Wenn Sie eine Reverse-Proxy-Konfiguration verwenden, befinden sich die Caching-Proxy-Maschinen zwischen dem Internet und den Inhaltshosts des Unternehmens. Der Proxy-Server fängt stellvertretend die aus dem Internet ankommenden Benutzeranforderungen ab, leitet diese an den geeigneten Inhaltshost weiter, speichert die zurückgegebenen Daten im Cache und übermittelt sie dann über das Internet an die Benutzer. Durch das Caching ist Caching Proxy in der Lage, nachfolgende Anforderungen für denselben Inhalt direkt aus dem Cache abzurufen. Das ist sehr viel schneller als ein erneuter Abruf des Inhalts vom Inhaltshost. Entscheidungsfaktoren für das Caching von Daten können das Verfallsdatum der Daten, die Größe des Cache und der erforderliche Aktualisierungszeitpunkt für die Daten sein. Schnellere Download-Zeiten für Daten, die bereits im Cache gespeichert sind, bedeuten eine bessere Servicequalität für die Kunden. Abb. 1 auf Seite 16 stellt diese grundlegende Funktionalität von Caching Proxy dar.

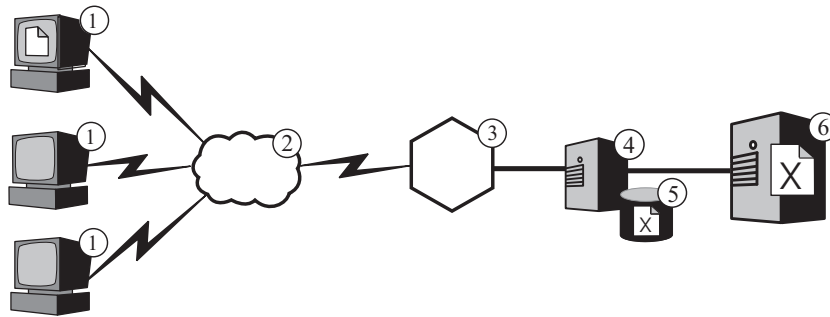


Abbildung 1. Caching Proxy als Reverse Proxy. Legende:
 1—Client 2—Internet 3—Router/Gateway 4—Caching
 Proxy 5—Cache 6—Inhaltshost

In dieser Konfiguration fängt der Proxy-Server (4) die Anforderungen ab, deren URL den Hostnamen des Inhaltshost (6) enthalten. Wenn ein Client (1) die Datei X anfordert, wird die Anforderung über das Internet (2) gesendet und erreicht das interne Unternehmensnetz über das Internet-Gateway (3) des Unternehmens. Der Proxy-Server fängt die Anforderung ab, generiert eine neue Anforderung mit seiner eigenen IP-Adresse als Ursprungsadresse und sendet die neue Anforderung an den Inhaltshost (6).

Der Inhaltshost gibt die Datei X nicht direkt an den Endbenutzer, sondern an den Proxy-Server zurück. Wenn die Datei für Caching geeignet ist, speichert der Caching-Proxy-Server eine Kopie der Datei in seinem Cache (5), bevor er die Datei an den Endbenutzer übergibt. Statische Webseiten sind das bekannteste Beispiel für Inhalte, die für Caching geeignet sind. Allerdings erlaubt Caching Proxy auch das Caching und Bereitstellen von Inhalten, die WebSphere Application Server dynamisch generiert.

Forward Caching Proxy

Die Bereitstellung eines direkten Internet-Zugangs für Endbenutzer kann sehr ineffizient sein. Jeder Benutzer, der eine bestimmte Datei von einem Webserver abrufen, generiert dasselbe Datenverkehrsvolumen in Ihrem Netz und über das Internet-Gateway wie der erste Benutzer, der die Datei abgerufen hat, selbst wenn diese Datei nicht geändert wurde. Die Lösung ist die Installation eines Forward Caching Proxy in der Nähe des Gateway.

Wenn Sie eine Forward-Proxy-Konfiguration verwenden, befinden sich die Caching-Proxy-Maschinen zwischen dem Client und dem Internet. Caching Proxy leitet eine Clientanforderung an Inhaltshosts im Internet weiter, stellt die abgerufenen Daten in den Cache und stellt die abgerufenen Daten dem Client zu.

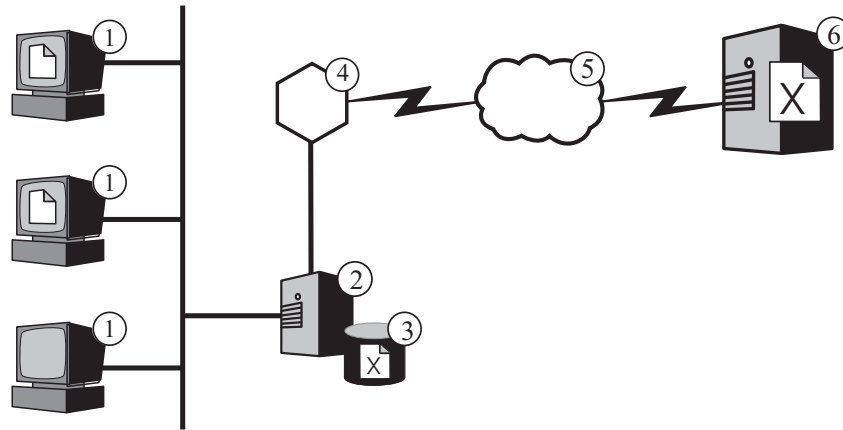


Abbildung 2. Caching Proxy als Forward Proxy. Legende: 1—Client 2—Caching Proxy 3—Cache 4—Router/Gateway 5—Internet 6—Inhaltshost

Abb. 2 zeigt die Forward-Caching-Proxy-Konfiguration. Die Browser-Programme des Clients (auf den mit 1 gekennzeichneten Maschinen) sind so konfiguriert, dass sie Anforderungen an den Forward Caching Proxy (2) weiterleiten, der die Anforderungen abfängt. Wenn ein Endbenutzer Datei X anfordert, die auf dem Inhaltshost (6) gespeichert ist, fängt der Forward Caching Proxy die Anforderung ab, generiert eine neue Anforderung mit seiner eigenen IP-Adresse als Ursprungsadresse und sendet die neue Anforderung über den Router (4) des Unternehmens über das Internet (5).

Der Ursprungsserver gibt die Datei X an den Forward Caching Proxy und nicht direkt an den Endbenutzer zurück. Wenn die Caching-Funktion des Forward Caching Proxy aktiviert ist, ermittelt Caching Proxy, ob die Datei X zwischengespeichert werden kann, indem er die Einstellungen im zurückgegebenen Header, z. B. das Verfallsdatum und etwaige Angaben zur dynamischen Generierung der Datei, prüft. Wenn die Datei zwischenspeicherbar ist, speichert Caching Proxy eine Kopie der Datei in seinem Cache (3), bevor die Datei an den Endbenutzer übergeben wird. Standardmäßig ist das Caching aktiviert, und der Forward Caching Proxy verwendet einen Hauptspeicher-Cache. Sie können jedoch auch andere Typen von Caching konfigurieren.

Für die erste Anforderung der Datei X bietet der Forward Caching Proxy keinen wesentlich effizienteren Zugang zum Internet. In der Tat ist die Antwortzeit für den ersten Benutzer, der auf die Datei X zugreift, wahrscheinlich länger als ohne den Forward Caching Proxy, weil es geringfügig länger dauert, bis der Forward Caching Proxy das ursprüngliche Anforderungspaket verarbeitet und den empfangenen Header der Datei X nach Caching-Informationen durchsucht hat. Die Verwendung des Forward Caching Proxy bringt dann Vorteile, wenn weitere Benutzer die Datei X anfordern. Der Forward Caching Proxy prüft, ob seine zwischengespeicherte Kopie der Datei X noch gültig ist (nicht verfallen ist), und stellt bei positivem Ergebnis dieser Prüfung die Datei X direkt aus dem Cache bereit, ohne die Anforderung über das Internet an den Inhaltshost weiterzuleiten.

Selbst wenn der Forward Caching Proxy feststellt, dass eine angeforderte Datei verfallen ist, ruft er die Datei nicht zwingenderweise erneut vom Inhaltshost ab. Stattdessen sendet er eine spezielle Statusprüfnachricht an den Inhaltshost. Wenn der Inhaltshost anzeigt, dass die Datei nicht geändert wurde, kann der Forward Caching Proxy die zwischengespeicherte Version dem anfordernden Benutzer bereitstellen.

Eine solche Konfiguration von Caching Proxy wird als Forward Proxy bezeichnet, weil Caching Proxy für die Browser auftritt und ihre Anforderungen über das Internet an Inhaltshosts weiterleitet. Die Vorteile eines Forward Proxy sind im Folgenden aufgeführt:

- Wenn eine Datei zwischengespeichert ist, erhalten die Endbenutzer sie wesentlich schneller, als wenn ihre Anforderungen über das Internet gesendet werden müssen, weil sich Forward Caching Proxy im lokalen Netz befindet. Je mehr Dateien zwischengespeichert werden, desto mehr sinkt die Gesamtantwortzeit für Internet-Anforderungen für diese Benutzer.
- Es wird kein Datenverkehr außerhalb des lokalen Netzes des Unternehmens generiert. Damit erhöht sich die Kapazität (verfügbare Bandbreite) des Unternehmens-Gateway zum Internet effektiv, weil das Gateway damit für die Bearbeitung von Anforderungen für Dateien, die nicht zwischengespeichert sind, verfügbar ist. Außerdem reduzieren sich die Internet-Zugriffsgebühren, was insbesondere in Umgebungen, in denen diese Gebühren auf der Anzahl der Pakete basieren, wichtig ist.

Caching Proxy kann mehrere Netzübertragungsprotokolle unterstützen, z. B. HTTP (Hypertext Transfer Protocol, FTP (File Transfer Protocol) und Gopher.

Transparenter Forward Caching Proxy (nur Linux-Systeme)

Eine Variante von Caching Proxy als Forward-Proxy-Server ist ein transparenter Caching Proxy. In dieser Rolle führt Caching Proxy dieselbe Funktion wie ein Basis-Forward-Caching-Proxy aus, aber der Client ist sich seiner Präsenz nicht bewusst. Die transparente Caching-Proxy-Konfiguration wird nur auf Linux-Systemen unterstützt.

In der im Abschnitt „Forward Caching Proxy“ auf Seite 16 beschriebenen Konfiguration wird jeder Client-Browser separat konfiguriert, um Anforderungen an einen bestimmten Forward Caching Proxy weiterzuleiten. Die Pflege einer solchen Konfiguration kann aufwendig werden, insbesondere wenn viele Clientmaschinen beteiligt sind. Caching Proxy unterstützt mehrere Alternativen, die die Verwaltung vereinfachen. Eine Möglichkeit ist die Konfiguration von Caching Proxy als transparenter Proxy, wie in Abb. 3 auf Seite 19 gezeigt wird. Wie ein regulärer Forward Caching Proxy wird der transparente Caching Proxy auf einer Maschine in der Nähe des Gateway installiert, aber die Browser-Programme der Clients werden nicht so konfiguriert, dass sie Anforderungen an einen Forward Caching Proxy weiterleiten. Die Clients sind sich nicht bewusst, dass ein Proxy-Server in der Konfiguration vorhanden ist. Stattdessen wird ein Router konfiguriert, der die Clientanforderungen abfängt und an den transparenten Caching Proxy weiterleitet. Wenn ein Client, der auf einer der mit 1 gekennzeichneten Maschinen arbeitet, die Datei X anfordert, die auf einem Inhaltshost (6) gespeichert ist, übergibt der Router (2) die Anforderung an Caching Proxy. Caching Proxy generiert eine neue Anforderung mit seiner eigenen IP-Adresse als Ursprungsadresse und sendet die neue Anforderung über den Router (2) über das Internet (5). Wenn die Datei X ankommt, stellt Caching Proxy die Datei in den Cache (sofern die im Abschnitt „Forward Caching Proxy“ auf Seite 16 beschriebenen Bedingungen zutreffen) und übergibt die Datei anschließend an den anfordernden Client.

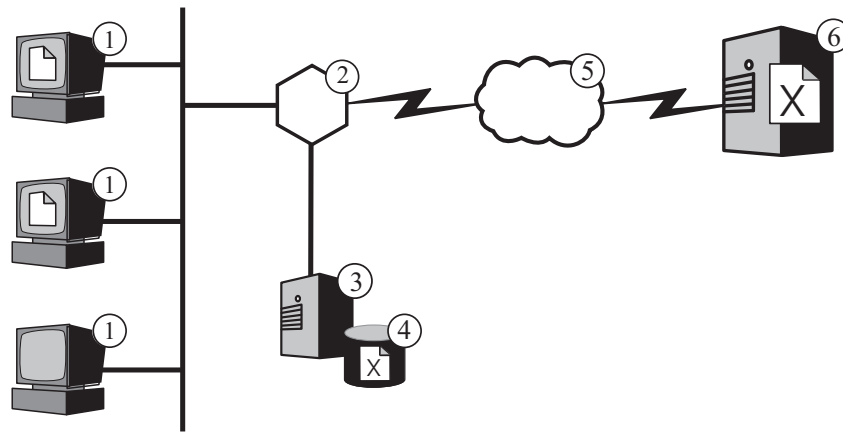


Abbildung 3. Caching Proxy als transparenter Forward Proxy. Legende:
 1—Client 2—Router/Gateway 3—Caching
 Proxy 4—Cache 5—Internet 6—Inhaltshost

Für HTTP-Anforderungen ist eine weitere mögliche Alternative für die Pflege der Proxy-Konfigurationsdaten in jedem Browser die Verwendung der Funktion für automatische Proxy-Konfiguration, die in mehreren Browser-Programmen, einschließlich Netscape Navigator ab Version 2.0 und Microsoft Internet Explorer ab Version 4.0 verfügbar ist. In diesem Fall erstellen Sie eine oder mehrere zentrale PAC-Dateien (Proxy Automatic Configuration) und zeigen in den Browsern auf eine dieser Dateien anstatt auf die lokalen Proxy-Konfigurationsdaten. Der Browser erkennt Änderungen an der PAC-Datei automatisch und passt die Proxy-Verwendung entsprechend an. Diese Methode macht nicht nur die Verwaltung separater Konfigurationsdaten in jedem Browser überflüssig, sondern vereinfacht auch die Weiterleitung von Anforderungen, wenn ein Proxy-Server nicht verfügbar ist.

Eine dritte Alternative ist die Verwendung des Mechanismus Web Proxy Auto Discovery (WPAD), der in einigen Browser-Programmen, z. B. Internet Explorer ab Version 5.0 verfügbar ist. Wenn Sie diese Funktion im Browser aktivieren, sucht der Browser automatisch einen WPAD-kompatiblen Proxy-Server in seinem Netz und leitet seine Webanforderungen dorthin weiter. In diesem Fall müssen Sie keine zentralen Proxy-Konfigurationsdateien verwalten. Caching Proxy ist WPAD-kompatibel.

Erweitertes Caching

Caching-Proxy-Cluster mit Lastausgleich

Eine erweiterte Caching-Funktionalität erhalten Sie, wenn Sie Caching Proxy als Reverse Proxy zusammen mit der Komponente Load Balancer verwenden. Durch die Kombination von Caching- und Lastausgleichsfunktionen erhalten Sie eine effiziente und einfach zu handhabende Infrastruktur für Webauftritte.

Abb. 4 auf Seite 20 zeigt, wie Sie Caching Proxy mit Load Balancer kombinieren können, um Webinhalte selbst bei hohem Bedarf effizient bereitzustellen. In dieser Konfiguration ist der Proxy-Server (4) so konfiguriert, dass er die Anforderungen abfängt, deren URL den Hostnamen eines Cluster von Inhaltshosts (7) enthält, in dem Load Balancer (6) für den Lastausgleich zuständig ist.

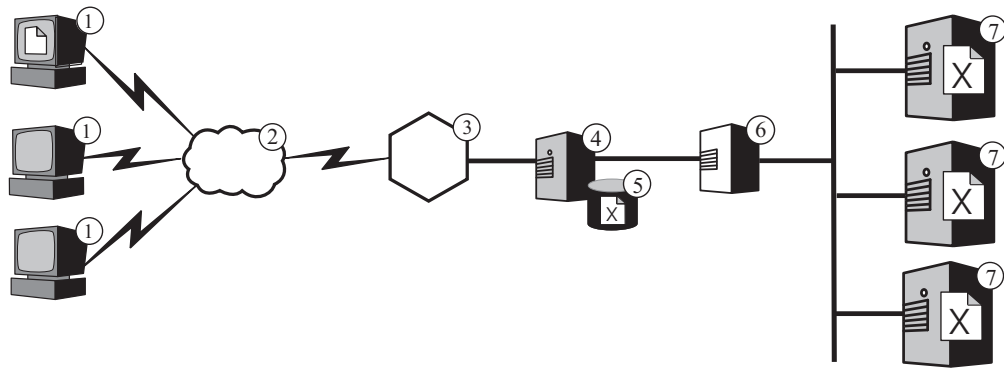


Abbildung 4. Caching Proxy als Proxy-Server für einen Cluster mit Lastausgleich. Legende:
 1—Client 2—Internet 3—Router/Gateway 4—Caching
 Proxy 5—Cache 6—Load Balancer 7—Inhaltshost

Wenn ein Client (1) die Datei X anfordert, wird die Anforderung über das Internet (2) gesendet und erreicht das interne Unternehmensnetz über das Internet-Gateway (3) des Unternehmens. Der Proxy-Server fängt die Anforderung ab, generiert eine neue Anforderung mit seiner eigenen IP-Adresse als Ursprungsadresse und sendet die neue Anforderung an den Load Balancer an die Adresse des Clusters. Load Balancer verwendet seinen Algorithmus für Lastausgleich, um den Inhaltshost zu ermitteln, der zum gegebenen Zeitpunkt am besten für die Verarbeitung der Anforderung von Datei X geeignet ist. Der Inhaltshost gibt die Datei X an den Proxy-Server zurück, anstatt sie über Load Balancer weiterzuleiten. Der Proxy-Server bestimmt, ob die Datei im Cache gespeichert wird, und liefert die Datei wie zuvor beschrieben an den Endbenutzer.

Dynamischen Inhalt zwischenspeichern

Erweiterte Caching-Funktionen werden auch vom Plug-in Dynamic Caching von Caching Proxy bereitgestellt. Zusammen mit WebSphere Application Server verwendet, kann Caching Proxy dynamische Inhalte in Form von JSPs (JavaServer Pages) und Servlet-Antworten, die von einem WebSphere Application Server generiert werden, im Cache speichern, bereitstellen und ungültig machen (invalidieren).

Im Allgemeinen müssen dynamische Inhalte mit unbegrenzter Verfallszeit als "nicht Cache-fähig" gekennzeichnet werden, weil die zeitbasierte Standardverfallslogik für Cache-Einträge nicht sicherstellen kann, dass derartige Inhalte in angemessener Zeit aus dem Cache entfernt werden. Die ereignisgesteuerte Verfallslogik des Plug-in Dynamic Caching hingegen unterstützt das Caching von Inhalten mit unbestimmter Verfallszeit durch Proxy-Server. Das Caching solcher Inhalte an den Grenzen (Edge) des Netzes entlastet die Inhaltshosts insofern, dass Application Server nicht wiederholt abgefragt werden müssen, um Clientanforderungen zu bedienen. Dies kann folgende Vorteile haben:

- Geringere Arbeitsbelastung von Webservern, WebSphere Application Server und Back-End-Inhaltshosts
- Schnellere Bedienung von Benutzern durch Vermeiden von Netzverzögerungen
- Geringere Belastung des Netzes aufgrund einer geringeren Anzahl von Internet-Abfragen
- Bessere Skalierbarkeit von Websites, die dynamisch generierte Inhalte bereitstellen

Das Caching von Servlet-Antworten eignet sich ideal für dynamisch erstellte Webseiten, deren Verfallszeit auf der Anwendungslogik oder auf einem Ereignis, z. B. der Nachricht von einer Datenbank, basiert. Obwohl die Lebensdauer einer solchen Seite begrenzt ist, kann der Wert für die Lebensdauer (TTL, Time-to-Live) zum Zeitpunkt der Erstellung nicht festgelegt werden, weil der Auslöser für den Verfall nicht im Vorhinein bekannt ist. Wird die Lebensdauer für solche Seiten auf null gesetzt, wirkt sich das Bereitstellen dynamischer Inhalte extrem nachteilig auf die Inhaltshosts aus.

Zuständig für die Synchronisation des dynamischen Cache von Caching Proxy und Application Server sind beide Systeme. Beispielsweise kann eine öffentliche Webseite, die von einer Anwendung dynamisch erstellt wurde, die aktuelle Wettervorhersagen meldet, von Application Server exportiert und von Caching Proxy im Cache gespeichert werden. Caching Proxy kann anschließend die Ausführungsergebnisse der Anwendung so oft an viele verschiedene Benutzer liefern, bis er darüber benachrichtigt wird, dass die Seite ungültig ist. Der Inhalt im Caching-Proxy-Cache für Servlet-Antworten bleibt so lange gültig, bis der Proxy-Server einen Eintrag löscht, weil der Cache überlastet ist, bis das von der Anweisung ExternalCacheManager in der Konfigurationsdatei von Caching Proxy gesetzte Standardzeitlimit abläuft oder Caching Proxy eine Invalidierungsnachricht empfängt, in der er zum Löschen des Inhalts aus dem Cache angewiesen wird. Invalidierungsnachrichten stammen immer vom WebSphere Application Server, der Eigentümer des Inhalts ist, und werden an jeden konfigurierten Caching Proxy weitergegeben.

Anmerkung: Dynamisch generierte private Seiten (beispielsweise eine Seite, die den Inhalt des elektronischen Warenkorbs eines Benutzers anzeigt) können und sollten im Allgemeinen von Caching Proxy nicht im Cache gespeichert werden. Caching Proxy kann private Seiten nur dann im Cache speichern und bereitstellen, wenn er für die Übernahme von Authentifizierungs- und Berechtigungsaufgaben konfiguriert ist und auf diese Weise sicherstellen kann, dass die privaten Seiten nur den vorgesehenen Benutzern bereitgestellt werden.

Zusätzliche Caching-Funktionen

Caching Proxy stellt weitere wichtige Funktionen für erweitertes Caching bereit:

- die Möglichkeit, sehr große Caches zu verwenden
- eine Option zur automatischen Aktualisierung des Cache mit den am häufigsten aufgerufenen Seiten
- die Möglichkeit, selbst die Seiten im Cache zu speichern, deren Header-Informationen eigentlich vorsehen, dass sie immer neu abgerufen werden müssen
- konfigurierbare tägliche Garbage-Collection, um die Serverleistung zu verbessern und die Cache-Pflege zu gewährleisten
- Remote Cache Access (RCA) - eine Funktion, die es erlaubt, dass mehrere Caching-Proxy-Maschinen denselben Cache gemeinsam benutzen, und die auf diese Weise die Anzahl redundanter Informationen im Cache verringert
- das Plug-in ICP, das es Caching Proxy erlaubt, bei der Suche nach HTML-Seiten und anderen Ressourcen, die im Cache gespeichert werden können, ICP-kompatible Caches (ICP = Internet Caching Protocol) abzufragen

Kapitel 5. Netzleistung

Die Einführung der Caching-Proxy-Funktionalität wirkt sich auf die Netzleistung aus. Sie können die Leistung Ihres Netzes verbessern, indem Sie Caching Proxy allein oder zusammen mit Load Balancer verwenden. Eine Einführung in diese Systeme finden Sie in Kapitel 1, „Einführung in WebSphere Application Server Edge Components“, auf Seite 3.

Die Leistung der Software Caching Proxy in Ihrem Unternehmen ist jedoch direkt abhängig von der Hardware, auf der sie ausgeführt wird, und von der Gesamtarchitektur des Systems, in dem sie eingesetzt wird. Zur Optimierung der Netzleistung sollten Sie die Hardware- und Gesamtnetzarchitektur gemäß den Anforderungen der Proxy-Server gestalten.

Die Basiskonfiguration und -verwaltung der Software Caching Proxy sowie die Optimierung auf Betriebssystemebene können in erheblichem Maße zur Leistung von Caching Proxy beitragen. Sie können zahlreiche Softwarekonfigurationsänderungen vornehmen, die eine bessere Leistung zur Folge haben. Dazu gehören unter anderem das Anpassen von Protokollanweisungen, Zuordnungsregeln, Plug-ins, Zeitlimitwerten, Cache-Konfigurationswerten und Werten für aktive Threads. Detaillierte Angaben zur Konfiguration der Caching-Proxy-Software enthält das *Caching Proxy Administratorhandbuch*.

Viele Änderungen an der Konfiguration des Betriebssystems können die Leistung ebenfalls verbessern. Dazu gehören unter anderem die Optimierung von TCP und ARP, höhere Grenzwerte für Dateideskriptoren, Synchronisation der Systemuhren, Optimierung der Network Interface Cards (NICs) und Befolgen der empfohlenen Praktiken zur Ausführung von Systemverwaltungs-Tasks.

Wichtig: Caching Proxy ist mit folgender Ausnahme in allen Edge-Components-Installationen verfügbar:

- Caching Proxy ist nicht verfügbar in Edge-Components-Installationen auf 64-Bit-Plattformen mit Itanium-2- oder AMD-Opteron-Prozessoren.
- Caching Proxy ist nicht verfügbar in Edge-Components-Installationen von Load Balancer for IPv4 and IPv6.

Netzhardware

In diesem Abschnitt werden Aspekte der Netzhardware beschrieben, die Sie bei Einführung der Caching-Proxy-Funktionalität in Ihr Netz beachten müssen.

Überlegungen zum Speicher

Dem Proxy-Server muss eine große Menge an Speicher zugeordnet werden. Caching Proxy kann 2 GB virtuellen Adressraum belegen, wenn ein großer Speicher-Cache konfiguriert wird. Außerdem wird Speicherplatz für den Kernel, gemeinsam benutzte Bibliotheken und Netzpuffer benötigt. Daher ist ein physischer Speicherbedarf von 3 oder 4 GB für einen Proxy-Server nicht ungewöhnlich. Beachten Sie, dass ein Speicher-Cache erheblich schneller ist als ein Rohplatten-Cache und eine solche Konfigurationsänderung allein schon eine Leistungsverbesserung darstellt.

Überlegungen zur Festplatte

Auf der Maschine, auf der Caching Proxy installiert wird, muss viel Platten-speicherplatz verfügbar sein. Dies gilt insbesondere dann, wenn Platten-Caches verwendet werden. Das Lesen von einer und Schreiben auf eine Festplatte sind für einen Computer rechenintensive Prozesse. Obwohl Caching Proxy effiziente E/A-Prozeduren verwendet, können die mechanischen Grenzen von Festplatten die Leistung beeinträchtigen, wenn in der Konfiguration von Caching Proxy die Verwendung eines Platten-Cache vorgesehen ist. Der Engpass, der aus der Platten-E/A resultiert, kann beispielsweise durch Verwendung mehrerer Festplatten für Cache-Roheiten (Raw Cache Devices) und durch Protokolldateien sowie durch Verwendung von Plattenlaufwerken mit kurzen Suchzeiten, hohen Umdrehungsgeschwindigkeiten und hohen Übertragungsgeschwindigkeiten beseitigt werden.

Überlegungen zum Netz

Die Anforderungen des Netzes wie Geschwindigkeit, Art und Zahl der NICs und Geschwindigkeit der Netzverbindung zum Proxy-Server beeinflussen die Leistung von Caching Proxy. Im Allgemeinen ist es der Leistung dienlich, wenn auf einer Proxyservermaschine zwei NICs verwendet werden: eine für ankommende Datenübertragungen und eine für abgehende Datenübertragungen. Eine einzelne NIC erreicht ihr Limit wahrscheinlich bereits allein durch die HTTP-Anforderungen und -Antworten. Außerdem sollten NICs mindestens eine Kapazität von 100 MB besitzen und immer für Vollduplexbetrieb konfiguriert sein, weil bei einer automatischen Vereinbarung zwischen Routing- und Switching-Einheiten Fehler auftreten können, die sich negativ auf den Durchsatz auswirken. Schließlich ist die Übertragungsgeschwindigkeit in der Netzverbindung von großer Bedeutung. Sie können beispielsweise nicht erwarten, eine hohe Anforderungslast zu verarbeiten und gleichzeitig einen optimalen Durchsatz zu erzielen, wenn die Verbindung zur Caching-Proxy-Maschine über einen ausgelasteten T1-Träger erfolgt.

Überlegungen zur CPU

Die Zentraleinheit (Central Processing Unit, CPU) einer Caching-Proxy-Maschine kann eventuell zu einem einschränkenden Faktor für die Leistung werden. Die CPU-Leistung wirkt sich aus auf die Zeit, die zur Verarbeitung von Anforderungen benötigt wird, und die Anzahl der CPUs im Netz hat Auswirkungen auf die Skalierbarkeit. Es ist von großer Bedeutung, dass Sie die CPU-Anforderungen des Proxyserver an die Umgebung anpassen, wobei Sie insbesondere die Spitzenauslastung berücksichtigen müssen, die vom Proxy-Server bewältigt werden soll.

Netzarchitektur

Für die Gesamtleistung ist es im Allgemeinen vorteilhaft, die Architektur als Ganzes zu skalieren und nicht nur einzelne Hardwarekomponenten. Unabhängig davon, wie viel Hardware Sie einer einzelnen Maschine hinzufügen, diese Hardware hat trotzdem eine maximale Leistungsgrenze.

In diesem Abschnitt werden Aspekte der Netzarchitektur beschrieben, die Sie bei Einführung der Caching-Proxy-Funktionalität in Ihr Netz beachten müssen.

Überlegungen zu Popularität der Website und Arbeitslast des Proxy-Servers

Ist die Website Ihres Unternehmens sehr populär, besteht unter Umständen eine höhere Nachfrage nach Inhalten, als ein einzelner Proxy-Server verarbeiten kann, was lange Antwortzeiten zur Folge haben kann. Zur Optimierung der Netzleistung sollten Sie in Erwägung ziehen, Cluster von Proxyserver-Maschinen mit Lastaus-

gleich oder eine Architektur mit gemeinsamem Cache und RCA (Remote Cache Access) in Ihrer Gesamtnetzarchitektur einzusetzen.

- **Cluster mit Lastausgleich**

Eine Möglichkeit zum Skalieren der Architektur besteht darin, dass Sie Cluster von Proxy-Servern bilden und die Komponente Load Balancer für die Verteilung der Arbeitslast auf diese Proxyserver verwenden. Das Clustering von Proxy-Servern ist eine nützliche Designmaßnahme, die sich nicht nur auf Leistung und Skalierbarkeit vorteilhaft auswirkt, sondern auch Redundanzen vermeidet und die Zuverlässigkeit erhöht. Ein einzelner Proxy-Server stellt einen Single Point of Failure dar. Falls er ausfällt oder aufgrund eines Netzfehlers nicht mehr zugänglich ist, können die Benutzer nicht mehr auf die Website zugreifen.

- **Architektur mit gemeinsamem Cache**

Sie sollten auch eine Architektur mit gemeinsamem Cache und RCA in Erwägung ziehen. In einer Architektur mit gemeinsamem Cache wird der gesamte virtuelle Cache auf mehrere Caching-Proxy-Server verteilt. Diese Server verwenden in der Regel ein Inter-cache-Protokoll wie Internet Cache Protocol (ICP) oder Cache Array Routing Protocol (CARP). RCA dient dazu, die Trefferquoten im Cache eines Clusters zu erhöhen, indem ein großer virtueller Cache bereitgestellt wird.

Leistungsverbesserungen werden erzielt, indem anstelle einer einzelnen Standalone-Caching-Proxy-Maschine oder auch eines Clusters von Standalone-Caching-Proxy-Maschinen eine RCA-Gruppe von Proxy-Servern verwendet wird. In der Regel werden die Leistungsverbesserungen durch die höhere insgesamt verfügbare virtuelle Cache-Kapazität erzielt, wodurch sich die Cache-Trefferquote erhöht und Abweichungen und Verzögerungen im Cache auf ein Minimum reduziert werden. Bei Verwendung von RCA wird nur eine Kopie eines gegebenen Dokuments im Cache gespeichert. Bei einem Cluster von Proxy-Servern erhöht sich zwar die Cache-Kapazität insgesamt, aber wahrscheinlich werden jedoch mehrere Proxyserver dieselben Informationen abrufen und zwischenspeichern. Die Gesamttrefferquote im Cache erhöht sich folglich nicht.

RCA wird in der Regel in großen Unternehmen eingesetzt, die Inhaltshosts verwenden. Allerdings sind die Vorteile von RCA nicht nur auf den Einsatz in sehr großen Unternehmen beschränkt. Sie können RCA beispielsweise auch dann einsetzen, wenn die Arbeitslast im Netz die Verwendung eines Clusters von Cache-Servern erfordert und die Mehrzahl der Anforderungen sich auf im Cache gespeicherte Informationen beziehen. In bestimmten Netzkonfigurationen führt der Einsatz von RCA jedoch nicht zu einer besseren Leistung im Unternehmen. Dies hängt mit der größeren Zahl von TCP-Verbindungen zusammen, die ein Client verwendet, wenn RCA konfiguriert wird. Ein RCA-Member ist nämlich nicht nur dafür verantwortlich, die URLs bereitzustellen, für die es selbst die höchste Trefferquote aufweist, sondern es muss auch Anforderungen an andere Member oder Cluster weiterleiten, wenn es eine URL-Anforderung erhält, für die es selbst nicht die höchste Trefferquote hat. Dies bedeutet, dass ein bestimmtes Member einer RCA-Gruppe mehr offene TCP-Verbindungen haben kann, als dies der Fall wäre, wenn es als Standalone-Server arbeiten würde.

Überlegungen zur Art des Datenverkehrs

Einen großen Beitrag zur Leistungsverbesserung leisten die Caching-Funktionen von Caching Proxy. Der Cache des Proxy-Servers kann jedoch einen Engpass darstellen, wenn er nicht ordnungsgemäß konfiguriert ist. Um die beste Cache-Konfiguration zu bestimmen, ist es notwendig, einen größeren Aufwand zu betreiben und die Merkmale des Datenverkehrs genau zu analysieren. Art, Größe, Menge und Attribute des Inhalts haben Auswirkungen auf die Leistung des Proxy-Servers, was sich in der Zeit, die zum Abrufen eines Dokuments von den Ursprungsservern

benötigt wird, und in der Arbeitslast des Servers bemerkbar macht. Wenn Sie die Art des Datenverkehrs bestimmen können, den Caching Proxy weiterleitet oder aus seinem Cache bedient, dann können Sie diese Merkmale bei der Konfiguration des Proxy-Servers berücksichtigen. Wenn Sie beispielsweise wissen, dass 80 % der im Cache gespeicherten Objekte Bilder sind (*.gif oder *.jpg) und ungefähr eine Größe von 200 KB aufweisen, dann ist diese Information für Sie sicher nützlich bei der Optimierung der Caching-Parameter und beim Festlegen der Cache-Größe. Wenn Sie darüber hinaus wissen, dass die meisten Inhalte angepasste dynamische Seiten sind, die nicht im Cache gespeichert werden, dann kann Ihnen dies ebenfalls bei der Optimierung von Caching Proxy helfen.

Indem Sie die Merkmale des Datenverkehrs analysieren, können Sie bestimmen, ob Sie die Leistung des Cache eher durch einen Speicher-Cache oder eher durch einen Platten-Cache optimieren können. Außerdem hilft Ihnen die Kenntnis der Merkmale des Netzverkehrs bei der Entscheidung, ob durch das dynamische Caching von Caching Proxy eine Leistungsverbesserung erzielt werden könnte.

- **Speicher-Cache versus Platten-Cache**

Platten-Caches eignen sich für Sites, für die große Datenmengen zwischengespeichert werden müssen. Wenn der Inhalt der Site umfangreich (mehr als 5 GB) ist und eine Cache-Trefferquote von 80 bis 90 % aufweist, dann ist die Verwendung eines Platten-Cache zu empfehlen. Allerdings ist bekannt, dass ein Speicher-(RAM)-Cache schneller ist, und es gibt viele Szenarios, in denen sich ein Speicher-Cache auch für große Sites eignet. Wenn die Cache-Trefferquote von Caching Proxy beispielsweise nicht so wichtig ist oder eine Konfiguration mit gemeinsamem Cache verwendet wird, empfiehlt sich die Verwendung eines Speicher-Cache.

- **Caching von dynamisch erstelltem Inhalt**

Caching Proxy kann dynamische Inhalte (JSPs und Servlet-Antworten), die vom dynamischen Cache des WebSphere Application Server generiert werden, zwischenspeichern und ungültig machen (invalidieren) und ermöglicht auf diese Weise eine virtuelle Erweiterung des Cache von Application Server auf netzgestützte Caches. Das Caching von dynamisch generierten Inhalten verbessert die Netzleistung in einer Umgebung, in der viele Anforderungen nach dynamisch generierten öffentlichen Webseiten gestellt werden, wobei diese Webseiten auf der Basis der Anwendungslogik oder auf der Basis eines Ereignisses, z. B. einer Nachricht von einer Datenbank, verfallen. Die Lebensdauer der Seite ist zwar begrenzt, aber zum Zeitpunkt ihrer Erstellung kann kein Verfallsauslöser definiert werden. Aus diesem Grund müssen Hosts ohne dynamisches Caching und Invalidierungsfunktion einer solchen Seite eine Lebensdauer von null zuweisen.

Wird eine solche dynamisch generierte Seite während ihrer Lebensdauer von einem oder mehreren Benutzern häufiger angefordert, dann bietet das dynamische Caching eine wertvolle Entlastung und verringert die Arbeitslast der Inhaltshosts im Netz. Mit dynamischem Caching verbessert sich auch die Netzleistung, weil Benutzer aufgrund der geringeren Netzverzögerungen und der geringeren Arbeitslast im Netz, die durch weniger Internet-Abfragen erreicht wird, schneller bedient werden können.

Kapitel 6. Verfügbarkeit

Durch die Verwendung der Komponente Load Balancer von Application Server zusammen mit Inhaltshosts wie WebSphere Application Server oder mit der Komponente Caching Proxy von Application Server können Sie Verfügbarkeit und Skalierbarkeit Ihres Netzes verbessern. (Eine Einführung in diese Komponenten von Edge Components finden Sie in Kapitel 1, „Einführung in WebSphere Application Server Edge Components“, auf Seite 3.) Load Balancer wird in Unternehmensnetzen verwendet und zwischen dem Internet und den Back-End-Servern des Unternehmens installiert. Load Balancer fungiert als Zugangspunkt (POP, Point-of-Presence) des Unternehmens im Internet, selbst wenn das Unternehmen auf Grund des hohen Bedarfs oder großer Inhaltsmengen mehrere Back-End-Server verwendet.

Die Verfügbarkeit wird durch Lastausgleich und Übernahme der Arbeitslast bei Ausfall eines Servers (Failover) erzielt.

Wichtig: Caching Proxy ist mit folgender Ausnahme in allen Edge-Components-Installationen verfügbar:

- Caching Proxy ist nicht verfügbar in Edge-Components-Installationen auf 64-Bit-Plattformen mit Itanium-2- oder AMD-Opteron-Prozessoren.
- Caching Proxy ist nicht verfügbar in Edge-Components-Installationen von Load Balancer for IPv4 and IPv6.

Lastausgleich

Der Lastausgleich verbessert die Verfügbarkeit und Skalierbarkeit Ihrer Website, indem Proxyserver und Anwendungsserver transparent zu einem Cluster zusammengefasst werden. Die Skalierbarkeit einer IT-Infrastruktur verbessert sich in hohem Maße, weil Back-End-Verarbeitungsleistung transparent hinzugefügt werden kann.

Lastausgleich für mehrere Inhaltshosts

Wenn Ihr System eine große Anzahl von Anforderungen verarbeiten muss, können Sie den Inhalt auf mehreren Hosts duplizieren. In diesem Fall müssen Sie jedoch dafür sorgen, dass die Arbeitslast gleichmäßig auf die einzelnen Hosts verteilt wird. DNS (Domain Name Service) bietet zwar einen grundlegenden Lastausgleich nach dem Round-Robin-Verfahren, aber es gibt verschiedene Situationen, in denen sich dieses Verfahren nicht eignet.

Eine ausgereifere Lösung für die Lastverteilung auf mehrere Inhaltshosts bietet die Verwendung der Komponente Dispatcher von Load Balancer, die in Abb. 5 auf Seite 28 veranschaulicht ist. Bei dieser Konfiguration ist auf allen Inhaltshosts (die mit 5 gekennzeichneten Maschinen) derselbe Inhalt gespeichert. Die Maschinen bilden einen *Cluster* mit Lastausgleich, und einer der Netzschnittstellen auf der Load-Balancer-Maschine (4) ist ein Hostname und eine IP-Adresse für diesen Cluster zugewiesen. Wenn ein Endbenutzer, der auf einer der Maschinen 1 arbeitet, die Datei X anfordert, wird die Anforderung über das Internet (2) gesendet und erreicht das interne Netz des Unternehmens über das Internet-Gateway (3). Der Dispatcher fängt die Anforderung ab, weil der URL der Anforderung dem Hostnamen und der IP-Adresse des Dispatcher zugeordnet wird. Der Dispatcher ermittelt, welcher der Inhaltshosts im Cluster derzeit am besten geeignet ist, die Anforderung

ung zu bearbeiten, und leitet die Anforderung an diesen Host weiter. Ist die MAC-gestützte Weiterleitung konfiguriert, gibt der Host die Datei X direkt an den Client zurück (d. h., die Datei X wird nicht über den Load Balancer weitergeleitet).

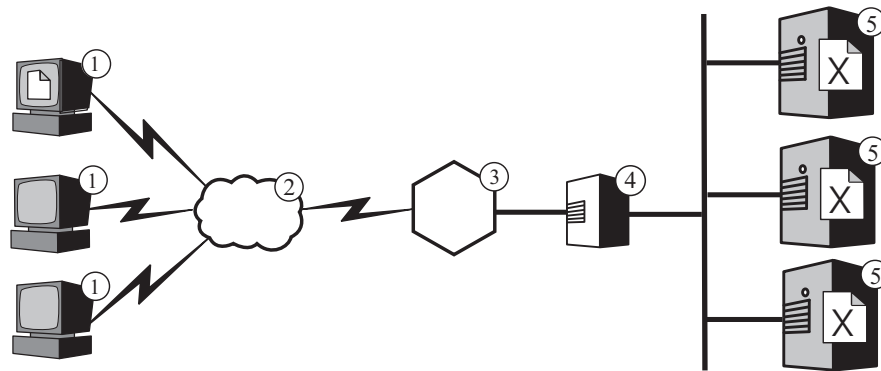


Abbildung 5. Lastausgleich für mehrere Inhaltshosts. Legende:
1—Client 2—Internet 3—Router/Gateway 4—Dispatcher 5—Inhaltshost

Anmerkung: Der Dispatcher unterstützt drei Weiterleitungsmethoden:

- Die MAC-gestützte Weiterleitungsmethode wird verwendet, um die ankommenden Anforderungen für den Server an die Inhaltshosts zu verteilen. Antworten werden direkt an den Client zurückgegeben.
- Die Weiterleitungsmethode NAT/NAPT wird für ferne Server verwendet. Der Dispatcher verteilt die ankommenden Anforderungen an die Inhaltshosts, empfängt die Antworten vom Server und gibt diese an die Clients zurück. (In Installationen von Load Balancer for IPv4 and IPv6 wird diese Weiterleitungsmethode nicht unterstützt.)
- Die Methode Content-Based Routing (CBR) unterstützt die inhaltsabhängige Weiterleitung von HTTP- und HTTPS-Anforderungen ohne Verwendung von Caching Proxy. Die inhaltsabhängige Weiterleitung für HTTP-Anforderungen wird gemäß der Regel für Inhaltsarten und für HTTPS-Anforderungen auf der Basis der SSL-Sitzungsaffinität durchgeführt. (In Installationen von Load Balancer for IPv4 and IPv6 wird diese Weiterleitungsmethode nicht unterstützt.)

Standardmäßig verwendet der Dispatcher wie DNS den Lastausgleich nach dem Round-Robin-Prinzip. Trotzdem weist der Lastausgleich mit Dispatcher nicht dieselben Unzulänglichkeiten auf wie der Lastausgleich mit DNS. Anders als bei DNS wird protokolliert, ob ein Inhaltshost nicht verfügbar oder nicht zugänglich ist. Es werden keine Clients an einen nicht verfügbaren Inhaltshost weitergeleitet. Darüber hinaus wird die aktuelle Belastung der Inhaltshosts durch Protokollieren neuer, aktiver und beendeter Verbindungen berücksichtigt. Sie können den Lastausgleich weiter optimieren, indem Sie die optionalen Advisor- und Managerkomponenten von Load Balancer aktivieren. Diese Komponenten überwachen den Status der Inhaltshosts noch genauer und bringen zusätzliche Informationen in den Entscheidungsprozess für den Lastausgleich ein. Mit dem Manager können Sie den unterschiedlichen Faktoren, die beim Entscheidungsprozess verwendet werden, verschiedene Gewichtungen zuweisen und somit den Lastausgleich für Ihre Site weiter anpassen.

Lastausgleich für mehrere Reverse-Proxy-Server

Dispatcher von Load Balancer kann auch den Lastausgleich für mehrere Caching-Proxy-Maschinen durchführen. Ist die Website Ihres Unternehmens sehr populär, besteht unter Umständen eine höhere Nachfrage nach Inhalten, als ein einzelner Proxy-Server effektiv verarbeiten kann. Aufgrund einer solchen Situation kann sich die Leistung des Proxyservers verschlechtern.

Sie können mehrere Caching-Proxy-Systeme verwenden, die Proxyfunktionen für einen einzelnen Inhaltshost ausführen (ähnlich wie in der Konfiguration in Abb. 1 auf Seite 16). Falls Ihre Site jedoch so populär ist, dass Sie mehrere Proxy-Server benötigen, brauchen Sie wahrscheinlich auch mehrere Inhaltshosts, deren Arbeitslast von Load Balancer verteilt werden muss. Diese Konfiguration wird in Abb. 6 dargestellt. Der Dispatcher 4 verteilt die Arbeitslast in einem Cluster mit zwei Proxyservern (5), und der Dispatcher 7 verteilt die Arbeitslast in einem Cluster mit drei Inhaltshosts (8).

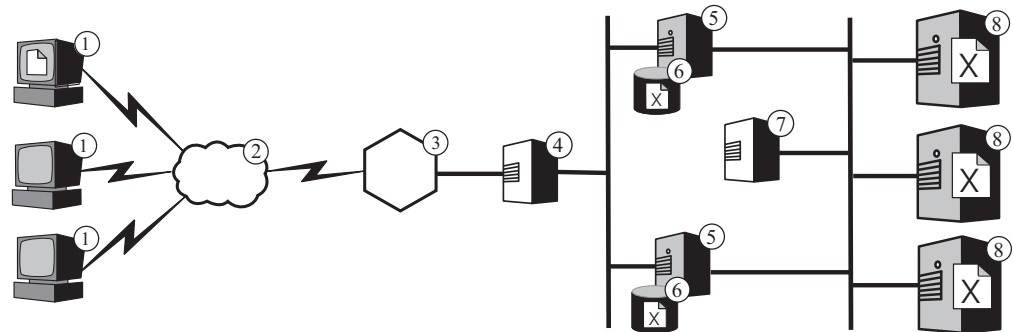


Abbildung 6. Lastausgleich für mehrere Reverse-Proxy-Server und Inhaltshosts. Legende: 1—Client 2—Internet 3—Router/Gateway 4—Dispatcher Proxy 5—Caching Proxy 6—Cache 7—Dispatcher 8—Inhaltshost

Beim Cluster-Hostnamen des Dispatcher 4 handelt es sich um den Hostnamen, der in den URLs für Webinhalte des Unternehmens angezeigt wird (d. h., es ist der Name der Website, wie er im Internet sichtbar ist). Der Cluster-Hostname für den Dispatcher 7 ist im Internet nicht sichtbar und kann daher beliebig gewählt werden. Beispiel: Für das Unternehmen ABC wäre `www.abc.com` ein geeigneter Hostname für den Dispatcher 4, während für den Dispatcher 7 ein Name wie `http-balancer.abc.com` festgelegt werden könnte.

Angenommen, ein Browser auf einer der Clientmaschinen 1 muss auf die Datei X zugreifen, die auf den Inhaltsservern (8) gespeichert ist. Die HTTP-Anforderung wird über das Internet (2) gesendet und erreicht das interne Unternehmensnetz über das Gateway (3). Der Router leitet die Anforderung an den Dispatcher 4 weiter, der sie an den Proxy-Server (5) übergibt, der gemäß dem Algorithmus für Lastausgleich zum gegebenen Zeitpunkt am besten für die Verarbeitung der Anforderung geeignet ist. Wenn sich die Datei X im Cache (6) des Proxy-Servers befindet, wird sie unter Umgehung des Dispatcher 4 direkt an den Browser zurückgegeben.

Befindet sich im Cache des Proxy-Servers keine Kopie der Datei X, erstellt der Proxyserver eine neue Anforderung mit seinem eigenen Hostnamen im Feld "origin" des Header und sendet diese an den Dispatcher 7. Load Balancer bestimmt, welcher Inhaltshost (8) zurzeit am besten für die Bearbeitung der Anforderung geeignet ist, und leitet dann die Anforderung an diesen Host weiter. Der Inhalts-

host ruft die Datei X aus dem Speicher ab und übergibt sie direkt an den Proxy-Server, wobei er den Dispatcher 7 übergeht. Der Proxy-Server speichert die Datei X gegebenenfalls im Cache und leitet sie dann unter Umgehung des Dispatcher 4 an den Browser weiter.

Load Balancer mit mehreren Forward-Proxy-Servern

Wenn Sie einer großen Anzahl von Clients Internet-Zugriffe ermöglichen, generieren diese einen höheren Bedarf an Internet-Zugriffen, als ein einzelner Proxy-Server effizient bewältigen kann. Da Caching Proxy mit Anforderungen überladen wird, können die Clients unter Umständen schlechtere Antwortzeiten erleben als bei einem direkten Internet-Zugriff. Wenn ein Fehler in Caching Proxy auftritt oder Caching Proxy aufgrund eines Netzfehlers vorübergehend ausfällt, sind keine Internet-Zugriffe mehr möglich. Die Lösung besteht in der Installation mehrerer Caching-Proxy-Maschine und der Verwendung der Komponente Dispatcher von Load Balancer, die die Last gleichmäßig auf diese Maschinen verteilt.

Ohne den Dispatcher können Sie einen echten transparenten Proxy-Server mit mehreren Caching-Proxy-Maschinen nur dann bereitstellen, wenn Ihre Router denselben Typ von Datenverkehr an mehrere Caching-Proxy-Server weiterleiten können. Nicht alle Router unterstützen dies. Es ist möglich, einen regulären Forward-Proxy-Service auf mehreren Caching-Proxy-Maschinen ohne den Dispatcher bereitzustellen, aber in diesem Fall müssen Sie eine der Caching-Proxy-Maschinen als primären Proxy explizit in den Client-Browsern konfigurieren. Wenn in diesem Caching Proxy ein Fehler auftritt oder Caching Proxy überlastet oder nicht verfügbar ist, sind die Endbenutzer möglicherweise nicht mehr in der Lage, auf das Internet zuzugreifen. Sie können diese Situation vermeiden, indem Sie eine PAC-Datei (Proxy Automatic Configuration) erstellen (siehe Beschreibung im Abschnitt „Transparenter Forward Caching Proxy (nur Linux-Systeme)“ auf Seite 18), die den Browser anweist, auf eine oder mehrere sekundäre Caching-Proxy-Maschinen umzuschalten. Eine PAC-Datei befasst sich nicht mit dem Bedarf nach Lastausgleich zwischen den Caching-Proxy-Maschinen. Wenn jedoch ein Caching Proxy mehr Anforderungen empfängt als ein anderer, lässt seine Leistung wahrscheinlich nach, was längere Antwortzeiten für seine Browser-Clients bedeutet. Damit allen Clients dieselbe Leistung zur Verfügung gestellt wird, müssen Sie für jeden Caching Proxy ungefähr dieselbe Anzahl an Browsern konfigurieren und die Verteilung manuell überwachen, damit die Last auch dann weiter gleichmäßig verteilt wird, wenn Sie Browser hinzufügen oder entfernen.

Abb. 7 auf Seite 31 zeigt eine Netzkonfiguration, in der der Dispatcher den Lastausgleich für einen Cluster von Caching-Proxy-Maschinen durchführt. Eine der Netzschnittstellen der Dispatcher-Maschine ist mit dem Hostnamen und der IP-Adresse des Cluster konfiguriert. Client-Browser sind so konfiguriert, dass sie ihre Internet-Anforderungen an den Hostnamen des Cluster weiterleiten. Wenn beispielsweise ein Browser auf einer der Clientmaschinen, die mit 1 gekennzeichnet ist, auf die Datei X auf einem Inhaltshost (7) zugreifen muss, leitet er seine Anforderung an den Hostnamen oder die Adresse des Cluster weiter. Dispatcher (2) fängt diese Anforderung ab und leitet sie an den entsprechenden Caching Proxy (3) weiter. Caching Proxy erstellt eine neue Anforderung, übergibt sie über das Unternehmens-Gateway (5) und über das Internet (6) und speichert die zurückgegebene Datei gegebenenfalls in seinem Cache (4). Eine ausführlichere Beschreibung finden Sie im Abschnitt „Forward Caching Proxy“ auf Seite 16

Anmerkung: Das Feature für transparente Proxy-Server ist nur auf Linux-Systemen verfügbar.

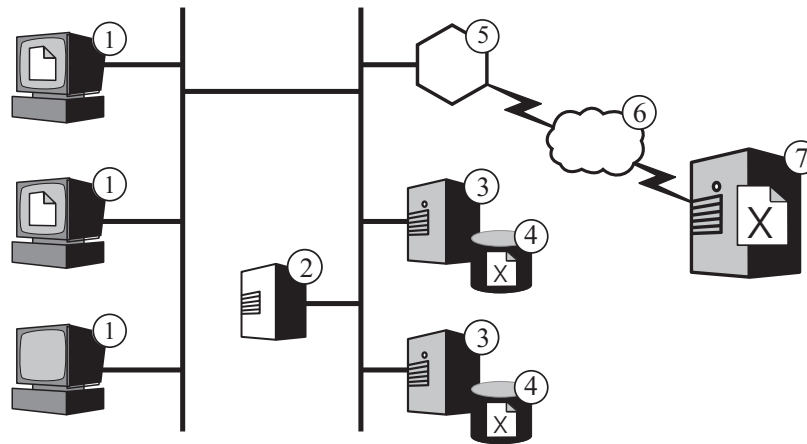


Abbildung 7. Dispatcher für den Lastausgleich für mehrere Caching-Proxy-Server verwenden.. Legende: 1—Client 2—Dispatcher 3—Caching Proxy 4—Cache 5—Router/Gateway 6—Internet 7—Inhaltshost

Der Dispatcher erkennt, wenn eine der Caching-Proxy-Maschinen nicht verfügbar ist, und leitet die Anforderungen automatisch an die andere weiter. Dies ermöglicht Ihnen, eine Caching-Proxy-Maschine zu Wartungszwecken herunterzufahren, ohne die Internet-Zugriffe zu beeinträchtigen. Der Dispatcher hat zahlreiche Konfigurationsoptionen, mit denen Sie die Faktoren steuern können, die der Dispatcher bei Lastausgleichentscheidungen berücksichtigt. Außerdem können Sie Dispatcher-Hilfsprogramme auf den Caching-Proxy-Maschinen installieren, um ihren Status zu überwachen und die Informationen an den Dispatcher zurückzugeben. Nähere Einzelheiten finden Sie im *WebSphere Application Server Load Balancer Administratorhandbuch*. Die Verwendung mehrerer Caching-Proxy-Server kann eine potenzielle Ineffizienz mit sich bringen, da mehrere Caching-Proxy-Maschinen dieselbe Datei zwischenspeichern können, wenn unterschiedliche Clients dieselbe Datei über eine jeweils andere Caching-Proxy-Maschine anfordern. Zur Vermeidung von Redundanzen können Sie RCA (Remote Cache Access, ferner Cache-Zugriff) konfigurieren, das allen Proxy-Servern in einer definierten Gruppe ermöglicht, den Inhalt ihres Cache mit den anderen zu teilen. Die Proxy-Server in der RCA-Gruppe verwenden alle denselben Algorithmus, um festzustellen, welcher Caching Proxy für einen bestimmten URL verantwortlich ist. Wenn ein Caching Proxy einen URL abfängt, für den er nicht verantwortlich ist, übergibt er die Anforderung an den verantwortlichen Caching Proxy. Der verantwortliche Caching Proxy führt die erforderlichen Aufgaben zur Bearbeitung der Anforderung aus, d. h. er ruft die Anforderung aus seinem Cache ab oder er leitet die Anforderung an den relevanten Inhaltshost weiter und stellt gegebenenfalls die zurückgegebene Datei in seinen Cache. Der verantwortliche Caching Proxy übergibt anschließend die Datei an den ursprünglichen Caching Proxy, der sie dem anfordernden Endbenutzer bereitstellt.

Wenn in dem für einen bestimmten URL verantwortlichen Caching Proxy in der RCA-Gruppe ein Fehler auftritt, greift der ursprüngliche Caching Proxy, der die Clientanforderung empfangen hat, direkt auf den Inhaltshost (oder den Caching-Proxy-Backup-Server, sofern ein solcher definiert ist) zu. Dies impliziert, dass Benutzer auf Dateien zugreifen können, solange mindestens ein Caching Proxy in einer RCA-Gruppe ordnungsgemäß funktioniert.

Diese Konfiguration erfüllt den hohen Bedarf an Internet-Zugriffen, weil der Dispatcher verwendet wird, um die Anforderungslast auf mehrere Caching-Proxy-Maschinen zu verteilen. Ein potenzielles Problem ist, dass der Dispatcher einen Single Point of Failure darstellt.

Wenn im Dispatcher ein Fehler auftritt oder der Dispatcher aufgrund eines Netzfehlers nicht mehr zugänglich ist, können die Browser-Clients die Caching-Proxy-Maschinen oder das Internet nicht erreichen. Die Lösung besteht darin, einen weiteren Dispatcher zu konfigurieren, der als Backup für den primären Dispatcher dient. Diese Lösung ist in Abb. 8 veranschaulicht.

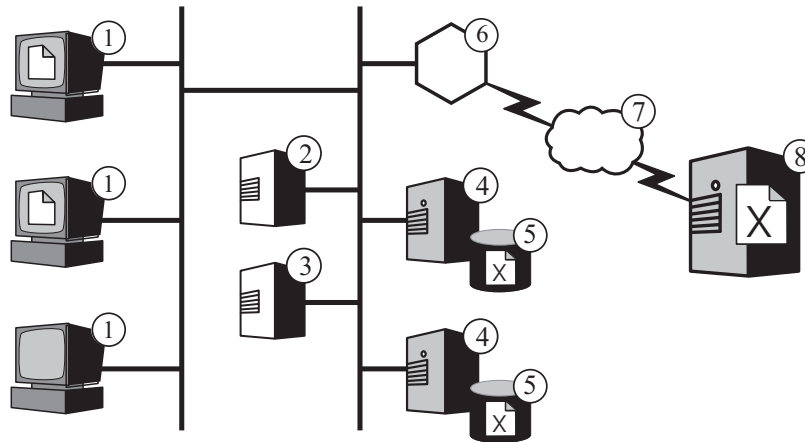


Abbildung 8. Verwendung eines primären und eines Backup-Dispatchers zur Unterstützung eines Internet-Zugangs mit hoher Verfügbarkeit.. Legende: 1—Client 2—Primärer Dispatcher 3—Backup-Dispatcher 4—Caching Proxy 5—Cache 6—Router/Gateway 7—Internet 8—Inhaltshost

Hier leitet ein Browser, der auf einer der mit 1 gekennzeichneten Maschinen ausgeführt wird, seine Anforderung für eine Datei X gewöhnlich an den primären Dispatcher (2) weiter, der die Anforderung an den Caching Proxy (4) weiterleitet, der auf der Basis der Lastausgleichskriterien des Dispatcher ausgewählt wird. Der Caching Proxy erstellt eine neue Anforderung, leitet sie über das Unternehmens-Gateway (6) über das Internet (7) an den Inhaltshost (8) weiter und speichert gegebenenfalls die zurückgegebene Datei X in seinem Cache (5). Eine ausführlichere Beschreibung dieses Teils des Prozesses finden Sie im Abschnitt „Forward Caching Proxy“ auf Seite 16.

In dieser Konfiguration führt der Backup-Dispatcher (3) keinen Lastausgleich durch, solange der primäre Dispatcher funktionsfähig ist. Der primäre und der Backup-Dispatcher überwachen jeweils den Status des anderen durch den regelmäßigen Austausch von Nachrichten. Diese Nachrichten werden als Überwachungssignale bezeichnet. Wenn der Backup-Dispatcher feststellt, dass der primäre Dispatcher ausgefallen ist, übernimmt er automatisch den Lastausgleich, indem er Anforderungen an den Hostnamen oder die IP-Adresse des primären Dispatcher abfängt. Es ist außerdem möglich, zwei Dispatcher für wechselseitige hohe Verfügbarkeit zu konfigurieren. In diesem Fall führt jeder Dispatcher aktiv den Lastausgleich für einen separaten Cluster von Caching-Proxy-Maschinen aus und fungiert gleichzeitig als Backup für den jeweils anderen. Nähere Einzelheiten finden Sie im *WebSphere Application Server Load Balancer Administratorhandbuch*.

In der Regel verbraucht der Dispatcher nicht sehr viele Verarbeitungs- und Speicherressourcen, und auf der Dispatcher-Maschine können andere Anwendungen aktiv sein. Sollte es erforderlich sein, die Kosten für Geräte so gering wie möglich zu halten, kann der Backup-Dispatcher sogar auf derselben Maschine wie Caching Proxy ausgeführt werden. Abb. 9 auf Seite 33 zeigt eine solche Konfiguration, in der der Backup-Dispatcher auf derselben Maschine (3) wie Caching Proxy ausgeführt wird.

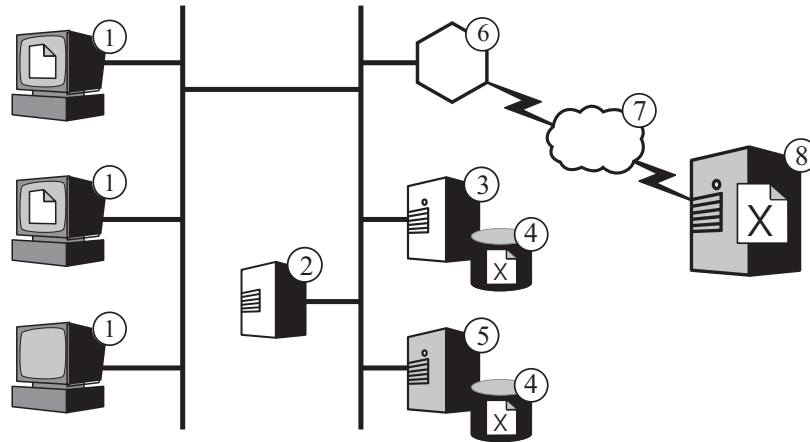


Abbildung 9. Installation des Backup-Dispatchers auf einer Caching-Proxy-Maschine.
 Legende: 1—Client 2—Primärer Dispatcher 3—Backup-Dispatcher und Caching Proxy 4—Caching Proxy 5—Cache 6—Router/Gateway 7—Internet 8—Inhaltshost

Unterstützung der Lastübernahme

Load Balancer tritt als zentraler Zugangspunkt (POP, Point-of-Presence) für die Inhaltshosts Ihres Unternehmens auf. Ein zentraler Zugangspunkt erweist sich als vorteilhaft, weil Sie den Hostnamen und die Adresse des Clusters im DNS veröffentlichen und nicht die Hostnamen und Adressen der einzelnen Inhaltshosts. Dies bietet einen gewissen Schutz vor unbefugten Zugriffen und die Möglichkeit einer einheitlichen Darstellung der Website Ihres Unternehmens. Um die Verfügbarkeit der Website zu verbessern, sollten Sie einen weiteren Load Balancer konfigurieren, der als Backup für den primären Load Balancer fungiert (siehe Abb. 10). Falls ein Load Balancer ausfällt oder aufgrund eines Netzfehlers nicht mehr zugänglich ist, können die Endbenutzer trotzdem auf die Inhaltshosts zugreifen.

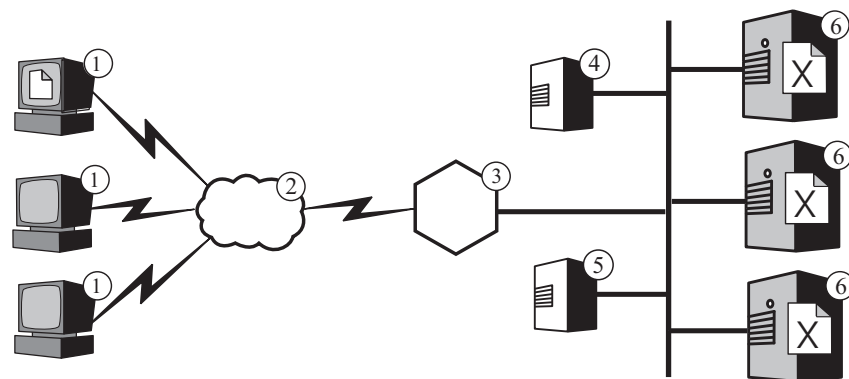


Abbildung 10. Verwendung eines primären und eines Backup-Load-Balancers, um die Verfügbarkeit von Webinhalten zu erhöhen. Legende: 1—Client 2—Internet 3—Router/Gateway 4—Primärer Dispatcher 5—Backup-Dispatcher 6—Inhaltshost

In der Regel sendet ein Browser, der auf einer der Maschinen 1 ausgeführt wird, seine Anforderung für die Datei X an den Cluster-Hostnamen, der dem primären Load Balancer (4) zugeordnet ist.

Der Dispatcher leitet die Anforderung an den Inhaltshost (6) weiter, der auf der Grundlage der Kriterien für Lastausgleich vom Dispatcher ausgewählt wurde. Der Inhaltshost sendet die Datei X über das Gateway des Unternehmens (3) durch das Internet (2) direkt an den Browser weiter, wobei Load Balancer übergangen wird.

Der Backup-Dispatcher (5) führt keinen Lastausgleich durch, solange der primäre Dispatcher ordnungsgemäß funktioniert. Der primäre und der Backup-Dispatcher überwachen jeweils den Status des anderen durch den regelmäßigen Austausch von Nachrichten. Diese Nachrichten werden als *Überwachungssignale* bezeichnet. Wenn der Backup-Dispatcher feststellt, dass der primäre Dispatcher ausgefallen ist, übernimmt er automatisch den Lastausgleich, indem er Anforderungen an den Cluster-Hostnamen oder die IP-Adresse des primären Dispatcher abfängt.

Es ist außerdem möglich, zwei Dispatcher für *wechselseitige hohe Verfügbarkeit* zu konfigurieren. In diesem Fall führt jeder Dispatcher aktiv den Lastausgleich für einen separaten Cluster von Inhaltshosts aus und fungiert gleichzeitig als Backup für den jeweils anderen. (In Installationen von Load Balancer for IPv4 and IPv6 wird die einfache hohe Verfügbarkeit unterstützt, die gegenseitige hohe Verfügbarkeit jedoch nicht.)

In der Regel verbraucht der Dispatcher nicht sehr viele Verarbeitungs- und Speicherressourcen, und auf der Load-Balancer-Maschine können andere Anwendungen aktiv sein. Sollte es erforderlich sein, die Kosten für Geräte so gering wie möglich zu halten, kann der Backup-Dispatcher sogar auf einer der Maschinen im Cluster ausgeführt werden, für die der Lastausgleich durchgeführt wird. Abb. 11 veranschaulicht eine Konfiguration, in der der Backup-Dispatcher auf einem der Inhaltshosts (5) im Cluster ausgeführt wird.

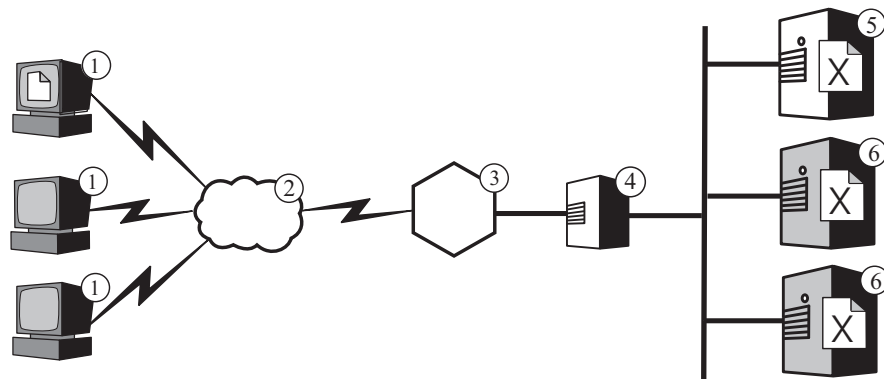


Abbildung 11. Installation eines Backup-Load-Balancer auf einem Inhaltshost. Legende:
 1—Client 2—Internet 3—Router/Gateway 4—Primärer Dispatcher 5—Backup-Dispatcher und Inhaltshost 6—Inhaltshost

Kapitel 7. Content Based Routing

Wichtig: Die Komponente Content Based Routing (CBR) ist mit folgenden Ausnahmen auf allen unterstützten Plattformen verfügbar:

- CBR ist nicht verfügbar in Load-Balancer-Installationen auf Plattformen mit einer 64-Bit-JVM.

Für diese Art von Installation können Sie alternativ die Weiterleitungsmethode *cbr* der Load-Balancer-Komponente Dispatcher verwenden, um das inhaltsbasierte Routing von HTTP- und HTTPS-Anforderungen ohne Verwendung von Caching Proxy zu unterstützen. Nähere Informationen hierzu finden Sie im *WebSphere Application Server Load Balancer Administratorhandbuch*.

- CBR ist nicht verfügbar in Installationen von Load Balancer for IPv4 and IPv6. Load Balancer for IPv4 and IPv6 unterstützt nur die Weiterleitungsmethode *mac* der Komponente Dispatcher. Die Weiterleitungsmethoden *nat* und *cbr* werden nicht unterstützt.

Bei Verwendung zusammen mit der Komponente Application Server Caching Proxy erlaubt Ihnen die Komponente Application Server Load Balancer, die Anforderungen an mehrere Back-End-Server zu verteilen, auf denen unterschiedliche Inhalte gespeichert sind. (Eine Einführung in diese Komponenten von Edge Components finden Sie in Kapitel 1, „Einführung in WebSphere Application Server Edge Components“, auf Seite 3.)

Wenn die Komponente CBR (Content Based Routing) von Load Balancer zusammen mit Caching Proxy installiert wird, können HTTP-Anforderungen auf der Basis des URL oder auf der Basis von anderen vom Administrator festgelegten Merkmalen verteilt werden, wodurch das Speichern identischer Inhalte auf allen Back-End-Servern entfällt.

Die Verwendung von CBR ist insbesondere dann zu empfehlen, wenn Ihre Webserver unterschiedliche Funktionen ausführen oder verschiedene Arten von Services anbieten. So muss z. B. die Website eines Onlinehändlers sowohl den Katalog anzeigen, der zum großen Teil statisch ist, als auch Aufträge annehmen, was bedeutet, dass eine interaktive Anwendung, z. B. ein CGI-Script (CGI = Common Gateway Interface), ausgeführt werden muss, die Artikelnummern und Kundendaten bearbeitet. Häufig ist es effektiver, zwei Gruppen von Maschinen für die Durchführung unterschiedlicher Funktionen einzusetzen und CBR für die Weiterleitung der unterschiedlichen Arten von Datenverkehr an die Maschinen zu verwenden. In ähnlicher Weise kann ein Unternehmen CBR verwenden, um zahlenden Kunden einen besseren Service zu bieten als Gelegenheitsbesuchern, indem die "bezahlten" Anforderungen an leistungsfähigere Webserver geleitet werden.

CBR leitet Anforderungen auf der Grundlage von Regeln weiter, die Sie festlegen. Die bekannteste Regelart ist die *Inhaltsregel*, die Anforderungen abhängig vom Pfadnamen im URL weiterleitet. Beispielsweise kann das Unternehmen ABC Regeln schreiben, die Anforderungen für den URL `http://www.abc.com/catalog_index.html` an einen Server-Cluster und Anforderungen für den URL `http://www.abc.com/orders.html` an einen anderen Cluster leiten. Es gibt außerdem Regeln, die Anforderungen abhängig von der IP-Adresse des sendenden Clients oder auf der Grundlage anderer Merkmale weiterleiten. Eine Beschreibung dieser Regeln finden Sie im *WebSphere Application Server Load Balancer Administratorhandbuch* in den Kapiteln über die Konfiguration von CBR und über

die komplexeren Funktionen von Load Balancer und CBR. Die Syntaxdefinitionen für die Regeln finden Sie im *WebSphere Application Server Load Balancer Administratorhandbuch* im Anhang über die Arten von CBR-Regeln.

Abb. 12 zeigt eine einfache Konfiguration, in der die Komponente CBR von Load Balancer und Caching Proxy zusammen auf der Maschine 4 installiert sind und Anforderungen an die drei Inhaltshosts (6, 7 und 8) weiterleiten, wobei auf jedem Inhaltshost andere Inhalte gespeichert sind. Wenn ein Endbenutzer an einer der mit 1 markierten Maschinen die Datei X anfordert, wird die Anforderung über das Internet (2) gesendet. Die Anforderung erreicht das interne Unternehmensnetz über das Internet-Gateway (3) des Unternehmens. Der Proxy-Server fängt die Anforderung ab und übergibt sie an die Komponente CBR auf derselben Maschine. Dort wird der URL in der Anforderung syntaktisch analysiert, und es wird ermittelt, dass der Inhaltshost 6 die Datei X enthält. Anschließend generiert der Proxy-Server eine neue Anforderung für die Datei X und stellt, sofern die Caching-Funktion aktiviert ist, fest, ob sich die Datei für die Speicherung im Cache eignet, sobald sie von Host 6 zurückgegeben wird. Wenn eine Speicherung der Datei im Cache möglich ist, speichert der Proxyserver eine Kopie der Datei in seinem Cache (5), bevor er die Datei an den Endbenutzer übergibt. Das Routing für andere Dateien erfolgt auf dieselbe Weise: Anforderungen für die Datei Y werden an den Inhaltshost 7 weitergeleitet, und Anforderungen für Datei Z werden an den Inhaltshost 8 weitergeleitet.

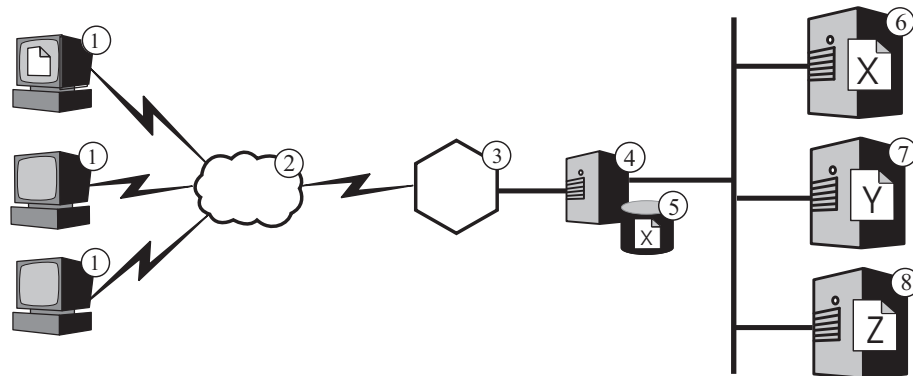


Abbildung 12. Routing von HTTP-Anforderungen mit CBR. Legende:
 1—Client 2—Internet 3—Router/Gateway 4—Caching Proxy und die Komponente CBR von Load Balancer 5—Cache 6, 7, 8—Inhaltshost

Abb. 13 auf Seite 37 veranschaulicht eine komplexere Konfiguration, die sich unter Umständen für Onlinehändler eignet. Die Komponente CBR von Load Balancer und der Proxy-Server werden gemeinsam auf der Maschine 4 installiert und leiten Anforderungen an zwei Load-Balancer-Maschinen weiter. Die Load-Balancer-Maschine 6 führt den Lastausgleich in einem Cluster von Inhaltshosts (8) durch, die den zum größten Teil statischen Inhalt des Katalogs enthalten, wohingegen die Load-Balancer-Maschine 7 den Lastausgleich für einen Cluster von Webservern durchführt, die für die Auftragsabwicklung (9) verantwortlich sind.

Wenn ein Endbenutzer, der an einer der beiden mit 1 markierten Maschinen arbeitet, auf den URL des Händlerkatalogs zugreift, wird die Anforderung über das Internet (2) gesendet und erreicht das interne Unternehmensnetz über das Internet-Gateway (3) des Unternehmens. Der Proxy-Server fängt die Anforderung ab und leitet sie an die Komponente CBR auf derselben Maschine weiter.

CBR führt eine Syntaxanalyse der URL aus und bestimmt, dass die Load-Balancer-Maschine 6 den URL verarbeiten soll. Der Proxy-Server erstellt eine neue Zugriffsanforderung und sendet sie an Load Balancer, der (auf der Grundlage der von Ihnen definierten Kriterien) ermittelt, welcher der Inhaltshosts (8) derzeit am besten geeignet ist, die Anforderung zu verarbeiten. Der Inhaltshost übergibt den Kataloginhalt unter Umgehung von Load Balancer direkt an den Proxy-Server. Wie im vorherigen Beispiel ermittelt der Proxy-Server, ob der Inhalt im Cache gespeichert werden kann, und speichert ihn ggf. in seinem Cache (5).

Der Endbenutzer sendet seine Bestellung, indem er auf den Bestell-URL des Händlers zugreift, in der Regel über einen Hyperlink im Katalog. Die Anforderung wird über dieselbe Route geleitet wie die Anforderung für Katalogzugriff. Allerdings leitet die Komponente CBR auf der Maschine 4 die Anforderung jetzt an die Load-Balancer-Maschine 7 weiter. Load Balancer wiederum leitet die Anforderung an den am besten geeigneten Server weiter, hier Webserver 9, der seine Antwort direkt an den Proxy-Server sendet. Weil Bestellinformationen in der Regel dynamisch generiert werden, speichert der Proxy-Server die Daten wahrscheinlich nicht im Cache.

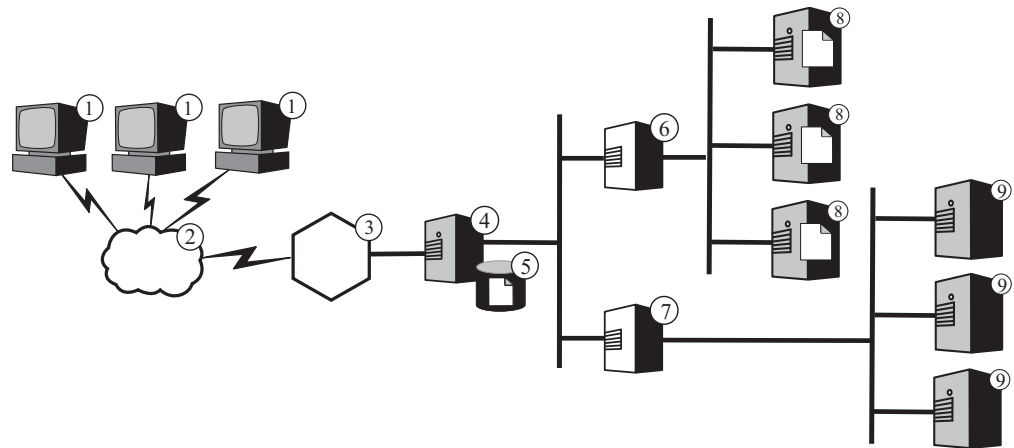


Abbildung 13. Mit CBR weitergeleitete HTTP-Anforderungen verteilen. Legende:
 1—Client 2—Internet 3—Router/Gateway 4—Caching Proxy und die Komponente
 CBR von Load Balancer 5—Cache 6, 7—Load
 Balancer 8—Inhaltshost 9—Webserver

Die Funktion CBR von Load Balancer unterstützt *Cookie-Affinität*. Dies bedeutet, dass die Identität des Servers, der die erste Anforderung eines Endbenutzers verarbeitet, in einem speziellen Datenpaket (einem so genannten *Cookie*) aufgezeichnet wird, das in die Antwort des Servers aufgenommen wird. Wenn der Endbenutzer innerhalb eines von Ihnen festgelegten Zeitraums erneut auf denselben URL zugreift und die Anforderung das Cookie enthält, leitet CBR die Anforderung an den ursprünglichen Server weiter und wendet seine Standardregeln nicht erneut an. Im Allgemeinen verkürzen sich die Antwortzeiten, wenn auf dem Server Informationen über den Endbenutzer gespeichert sind, die nicht erneut ermittelt werden müssen (z. B. die Kreditkartennummer).

Teil 3. Szenarios

In diesem Teil werden Geschäftsszenarios beschrieben, in denen IBM WebSphere Application Server Edge Components verwendet wird. Es handelt sich um Lösungen mit stabiler und geprüfter Architektur, die eine hervorragende Leistung, Verfügbarkeit, Skalierbarkeit und Zuverlässigkeit bieten.

Dieser Teil enthält folgende Kapitel:

Kapitel 8, „B2C-Netz“, auf Seite 41

Kapitel 9, „Online-Banking-Lösung“, auf Seite 45

Kapitel 10, „Web-Portal-Netz“, auf Seite 47

Kapitel 8. B2C-Netz

Die Basis-Website für E-Commerce ist ein B2C-Netz (B2C = Business-to-Consumer). In der ersten Phase ihres Wachstums im Internet konzentrieren sich die Unternehmen in der Regel darauf, lediglich eine Präsenz im Web aufzubauen. Informationen zum Unternehmen und Produktkataloge werden in digitale Formate konvertiert und auf der Website verfügbar gemacht. Das Einkaufen wird durch Angabe von E-Mail-Adressen, Telefon und Faxnummern oder sogar von automatisierten Formularen ermöglicht. Ein echtes Online-Shopping ist jedoch nicht verfügbar. Alle Transaktionen erfolgen mit einer zeitlichen Verzögerung, weil die Bestellungen von Personen verarbeitet werden müssen.

In Phase zwei wird diese Verzögerungszeit beseitigt. Die Verkaufsoperationen werden rationalisiert, indem sichere elektronische Warenkörbe für direkte Onlinekäufe implementiert werden. Entscheidend für die Ausführung dieser Verkaufstransaktionen sind die Synchronisation mit Warehouse-Datenbanken und die Einführung von Zahlungssystemen. Ein Produkt, das nicht verfügbar ist, kann nicht verkauft werden, und das Konto des Kunden kann für diesen Artikel nicht belastet werden. Genauso wenig kann ein Produkt aus dem Inventar entnommen und an einen Kunden geliefert werden, bevor eine gültige finanzielle Transaktion stattgefunden hat.

In der dritten Phase entwickelt sich die Website des Unternehmens zu einer Site mit dynamischer Präsentation, in der der Kunde allmählich als Client behandelt wird, indem ihm Inhalte angezeigt werden, die speziell für ihn angepasst wurden.

Das folgende Szenario umfasst Load Balancer und Caching Proxy.

Wichtig: Caching Proxy ist mit folgender Ausnahme in allen Edge-Components-Installationen verfügbar:

- Caching Proxy ist nicht verfügbar in Edge-Components-Installationen auf 64-Bit-Plattformen mit Itanium-2- oder AMD-Opteron-Prozessoren.
- Caching Proxy ist nicht verfügbar in Edge-Components-Installationen von Load Balancer for IPv4 and IPv6.

Phase 1

Abb. 14 auf Seite 42 zeigt eine kleine kommerzielle Website, die für eine effiziente Katalogsuche aufgebaut wurde. Alle Clientanforderungen werden über die Firewall an einen Dispatcher übergeben, der die Anforderungen an einen Cluster von Proxy-Servern mit aktiven Caches weiterleitet, die stellvertretend für die Webserver auftreten. Den Proxy-Servern sind Metrikserver zugeordnet, die Lastausgleichsdaten für den Dispatcher bereitstellen. Diese Anordnung verringert die Netzlast auf den Webservern und isoliert sie vom direkten Kontakt mit dem Internet.

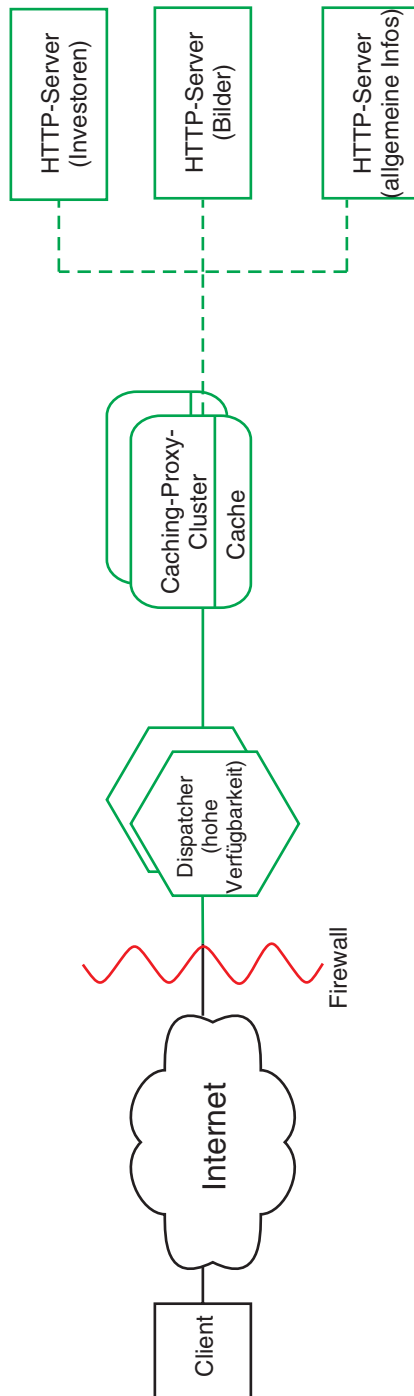


Abbildung 14. B2C-Netz (Phase 1)

Phase 2

Abb. 15 auf Seite 43 zeigt die zweite Phase der Entwicklung einer E-Commerce-Website, die ihren potenziellen Kunden eine effektive Katalogsuche ermöglicht sowie schnelle und sichere elektronische Warenkörbe zur Verfügung stellt. Alle Anforderungen von Kunden werden durch einen Dispatcher, der die Anforderungen auf der Grundlage eines Internet-Protokolls aufteilt, an den geeigneten Zweig

des Netzes weitergeleitet. HTTP-Anforderungen werden an die statische Website, HTTPS-Anforderungen an das Einkaufsnetz übermittelt. Die primäre, statische Website wird weiterhin von einem Cluster von Proxy-Servern mit aktiven Caches bedient, die stellvertretend für die Webserver auftreten. Dieser Teil des Netzes spiegelt das Netz in der ersten Phase wider.

Der E-Commerce-Teil der Website wird ebenfalls von einem Cluster von Proxy-Servern bedient. Allerdings werden die Caching-Proxy-Knoten durch mehrere Plug-in-Module ergänzt. Das SSL-Handshaking wird an eine Verschlüsselungskarte ("Cryptocard" in der folgenden Abbildung) ausgelagert. Die Authentifizierung erfolgt über das Plug-in Access Manager (früher Policy Director). Das Plug-in Dynamic Caching verringert die Arbeitslast im WebSphere Application Server, weil häufig benötigte Daten gespeichert werden. Ein Plug-in im Anwendungsserver macht Objekte im dynamischen Cache ungültig, wenn dies erforderlich ist.

Alle Anwendungen mit elektronischen Warenkörben sind in die Kundendatenbank eingebunden, die zur Authentifizierung des Benutzers verwendet wird. Dies verhindert, dass der Benutzer mehrmals persönliche Informationen eingeben muss, einmal zur Authentifizierung und einmal zum Einkaufen.

In diesem Netz wird der Datenverkehr entsprechend der Clientnutzung verteilt. Die primäre Website wird von der prozessorintensiven SSL-Authentifizierung und den E-Commerce-Warenkörben befreit. Diese zweigleisige Website ermöglicht es dem Netzadministrator, die verschiedenen Server so einzustellen, dass sie in Abhängigkeit von ihrem jeweiligen Aufgabenbereich im Netz eine optimale Leistung erzielen.

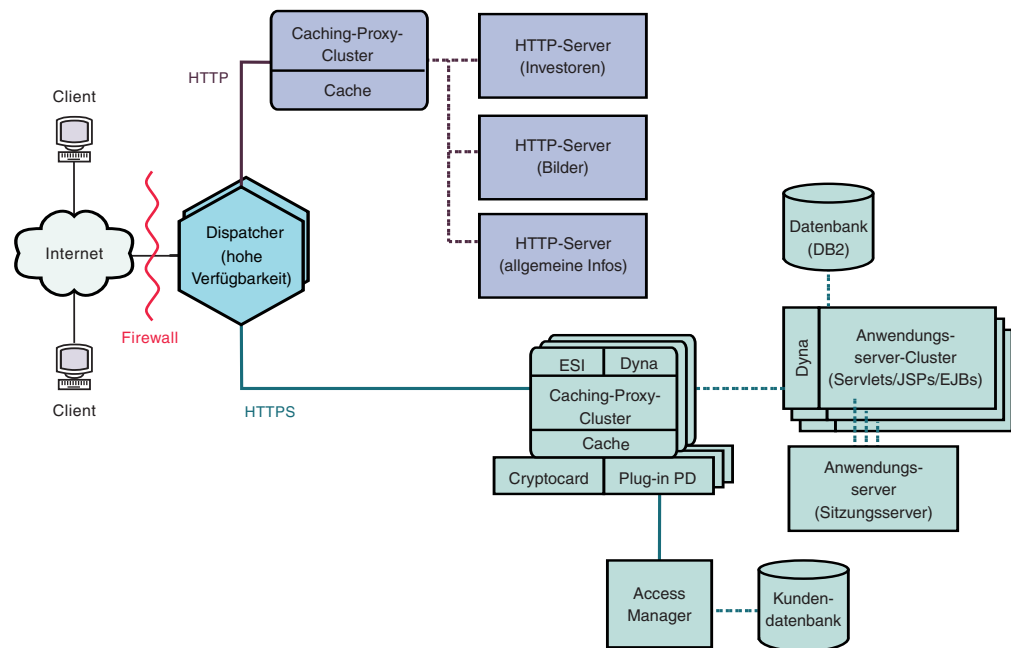


Abbildung 15. B2C-Netz (Phase 2)

Phase 3

Abb. 16 zeigt die dritte Phase in der Entstehung eines B2C-Netzes, in der die statische Website eine Methode für dynamische Präsentation verwendet. Der Cluster aus Proxyservern wurde in der Weise erweitert, dass er das Caching dynamischer Webinhalte unterstützt sowie die Assemblierung von Seitenfragmenten, die gemäß den Regeln des Protokolls ESI (Edge Side Includes) geschrieben wurden. Anstatt mit Server-Side Includes Webseiten auf den Inhaltsservern zu erstellen und diese clientspezifischen, unveränderlichen Seiten dann im gesamten Netz weiterzugeben, können mit dem Protokoll ESI Seiten aus zwischengespeicherten Inhalten an den Grenzen (Edge) des Netzes assembliert werden, wodurch sich die Belastung des Netzes und die Antwortzeiten verringern.

Das Protokoll ESI ist in dieser dritten Phase von entscheidender Bedeutung, in der jeder Client von der Website eine personalisierte Homepage erhält. Die Bausteine für diese Seiten werden von einer Reihe von WebSphere Application Servern abgerufen. Anwendungsserver, die kritische Geschäftslogik und Verknüpfungen mit geschützten Datenbanken enthalten, werden hinter einer Firewall isoliert.

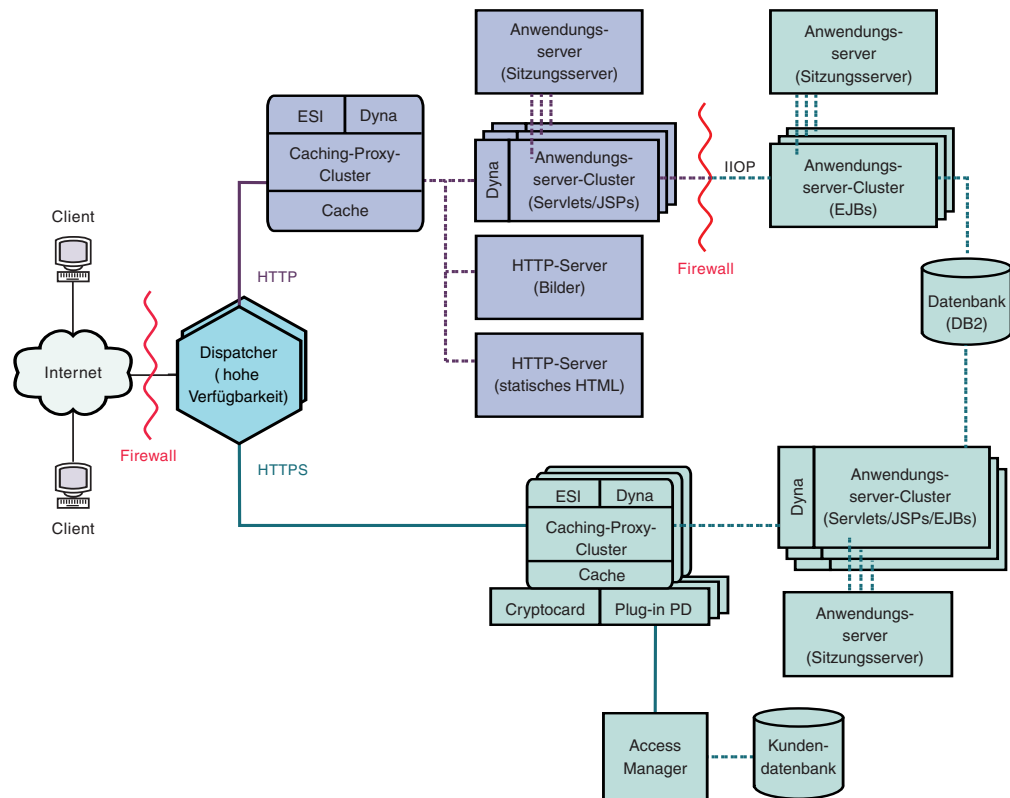


Abbildung 16. B2C-Netz (Phase 3)

Kapitel 9. Online-Banking-Lösung

Abb. 17 auf Seite 46 zeigt eine effiziente Lösung für Online-Banking, die ähnlich aufgebaut ist wie das in Kapitel 8, „B2C-Netz“, auf Seite 41 beschriebene B2C-Netz. Alle Clientanforderungen werden durch die Firewall an einen Dispatcher übertragen, der die Übertragungen gemäß dem Internet-Protokoll verteilt. HTTP-Anforderungen werden an einen Cluster von Proxyservern mit aktiven Caches übermittelt, die stellvertretend für die Webserver auftreten. Den Proxyservern sind Metrikserver zugeordnet, die Lastausgleichsdaten für den Dispatcher bereitstellen. Diese Anordnung verringert die Netzlast auf den Webservern und erstellt einen zusätzlichen Puffer zwischen ihnen und dem Internet.

HTTPS-Anforderungen werden an ein sicheres Netz weitergeleitet, das für die Clients persönliche Finanzinformationen bereitstellt und die Ausführung von Online-Banking-Transaktionen erlaubt. Ein Cluster von erweiterten Proxyservern erlaubt die Skalierbarkeit der Site. Diese Proxyserver unterstützen das Caching von dynamischen Webinhalten und das Assemblieren von Seitenfragmenten, die gemäß den Regeln des Protokolls ESI (Edge Side Includes) geschrieben wurden. Eine Verschlüsselungskarte (Cryptocard in der folgenden Abbildung) verwaltet die SSL-Handshakes, wodurch sich der Verarbeitungsaufwand für den Proxyserver-Host erheblich verringert. Access Manager (früher Policy Director) steuert die Clientauthentifizierung.

Eine Gruppe von Anwendungsserver-Clustern verteilt die Verarbeitung von Anforderungen, indem die in den EJB-Komponenten enthaltene Geschäftslogik von der in Servlets und JSP-Dateien enthaltenen Präsentationsschicht getrennt wird. Jeder dieser Cluster wird von einem eigenen Sitzungsserver verwaltet.

Das folgende Szenario umfasst Load Balancer und Caching Proxy.

Wichtig: Caching Proxy ist mit folgender Ausnahme in allen Edge-Components-Installationen verfügbar:

- Caching Proxy ist nicht verfügbar in Edge-Components-Installationen auf 64-Bit-Plattformen mit Itanium-2- oder AMD-Opteron-Prozessoren.
- Caching Proxy ist nicht verfügbar in Edge-Components-Installationen von Load Balancer for IPv4 and IPv6.

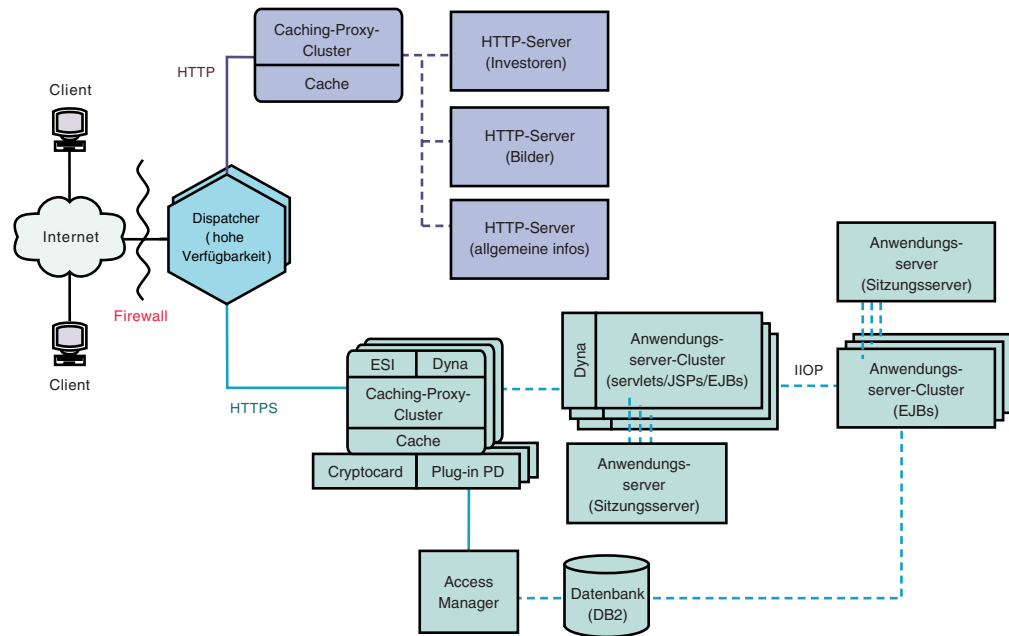


Abbildung 17. Online-Banking-Lösung

Kapitel 10. Web-Portal-Netz

Abb. 18 auf Seite 48 zeigt ein Web-Portal-Netz, das zur Unterstützung eines hohen Datenübertragungsaufkommens dient und gleichzeitig jedem Client personalisierte Inhalte bereitstellt. Damit die Verarbeitungslast auf den verschiedenen Servern verringert wird, werden in keinem Teil des Netzes SSL-Datenübertragungen durchgeführt. Weil das Portal keine sensiblen Daten bereitstellt, ist die Sicherheit hierbei kein wichtiger Aspekt. Es ist wichtig, dass die Datenbank, in der die Client-IDs, -Kennwörter und -Einstellungen gespeichert sind, sicher und unbeschädigt bleibt. Diese Voraussetzung beeinträchtigt jedoch nicht die Leistung der restlichen Website.

Alle Clientanforderungen werden durch die Firewall an einen Dispatcher übermittelt, der die Netzlast auf einen Cluster von Proxyservern mit aktiven Caches verteilt, die stellvertretend für die Webserver fungieren. Den Proxyservern sind Metrikserver zugeordnet, die Lastausgleichsdaten für den Dispatcher bereitstellen.

Die eigentliche dynamische Website ist ein Cluster von Anwendungsservern, die ESI-Fragmente generieren, die zur Assemblierung an die Proxyserver übermittelt werden. Aufgrund der Tatsache, dass die Sicherheit eine untergeordnete Rolle spielt, kann jeder Anwendungsserver alle erforderlichen Funktionen zur Konstruktion der Website ausführen. Alle Anwendungsserver sind identisch. Fällt ein Anwendungsserver aus, kann der Sitzungsserver die Anforderungen an andere Server weiterleiten und auf diese Weise für die gesamte Site eine hohe Verfügbarkeit gewährleisten. Diese Konfiguration erlaubt auch eine schnelle Eskalation der Website, falls eine unerwartet hohe Menge an Datenübertragungen zu bewältigen ist, z. B. das Hosting eines speziellen Ereignisses durch das Portal. In diesem Fall können zusätzliche Proxyserver und Anwendungsserver schnell für die Site konfiguriert werden.

Alle statischen Inhalte, z. B. Bilddateien und Standardtexte, werden auf separaten Webservern gespeichert, so dass diese aktualisiert werden können, ohne zu riskieren, dass einer der komplexeren Anwendungsserver beschädigt wird.

Das folgende Szenario umfasst Load Balancer und Caching Proxy.

Wichtig: Caching Proxy ist mit folgender Ausnahme in allen Edge-Components-Installationen verfügbar:

- Caching Proxy ist nicht verfügbar in Edge-Components-Installationen auf 64-Bit-Plattformen mit Itanium-2- oder AMD-Opteron-Prozessoren.
- Caching Proxy ist nicht verfügbar in Edge-Components-Installationen von Load Balancer for IPv4 and IPv6.

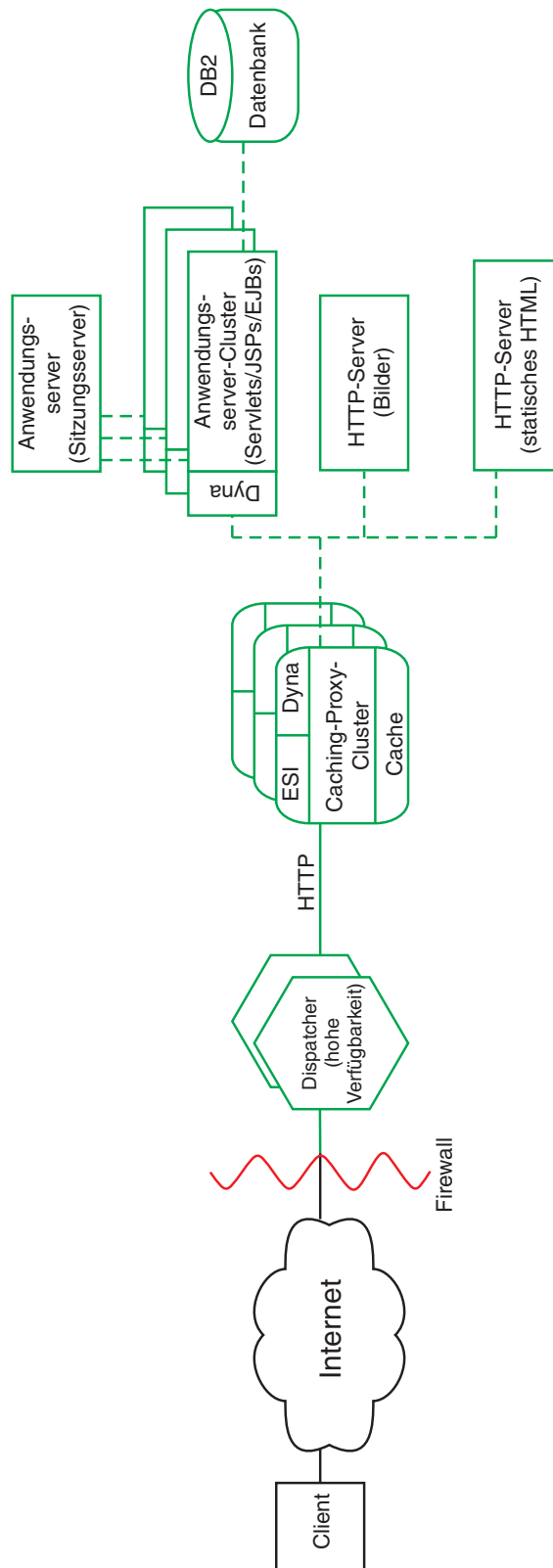


Abbildung 18. Web-Portal

Teil 4. Installation von Edge Components

Dieser Teil beschreibt die Prozeduren für die Installation von Edge Components.

Dieser Teil enthält folgende Kapitel:

Kapitel 11, „Voraussetzungen für Edge Components“, auf Seite 51

Kapitel 12, „Installation von Edge Components mit dem Installationsprogramm“, auf Seite 55

Kapitel 13, „Installation von Caching Proxy mit den Paketverwaltungstools des Betriebssystems“, auf Seite 59

Kapitel 14, „Installation von Load Balancer mit den Paketverwaltungstools des Betriebssystems“, auf Seite 63

Kapitel 11. Voraussetzungen für Edge Components

Dieses Kapitel enthält einen Link zu den Hardware- und Softwarevoraussetzungen für Edge Components sowie Richtlinien für die Verwendung von Webbrowsern mit den Konfigurations- und Verwaltungsformularen von Caching Proxy und mit der Online-Hilfe von Load Balancer.

Hardware- und Softwarevoraussetzungen

Informationen zur unterstützten Hardware und zu den Softwarevoraussetzungen für WebSphere Application Server Version 6.1 Edge Components finden Sie auf der folgenden Webseite: <http://www.ibm.com/support/docview.wss?rs=180&uid=swg27006921>.

SDK-Installation: Das Java 2 SDK wird auf allen Plattformen automatisch mit Load Balancer installiert.

Verwendung der Konfigurations- und Verwaltungsformulare von Caching Proxy in Browsern

Mindestvoraussetzungen für Browser

Zum Konfigurieren von Caching Proxy mit den Konfigurations- und Verwaltungsformularen muss der Browser folgende Voraussetzungen erfüllen:

- Es werden Frames unterstützt.
- JavaScript und Java sind aktiviert.
- Es wird eine Farbauflösung von mindestens 256 Farben (Einstellung im Betriebssystem) unterstützt.
- Dokumente werden im Cache gespeichert und bei jedem Abruf mit den Dokumenten im Netz verglichen.

Für Linux- und UNIX-Systeme: Informationen zu den empfohlenen Versionen der Browser Mozilla und Firefox finden Sie auf der folgenden Website. Folgen Sie auf dieser Website den Links zur Webseite mit Informationen zur unterstützten Software: <http://www.ibm.com/support/docview.wss?rs=180&uid=swg27006921>.

Für Windows-Systeme: Informationen zu den empfohlenen Versions der Browser Internet Explorer, Mozilla und Firefox finden Sie auf der folgenden Website. Folgen Sie auf dieser Website den Links zur Website mit Informationen zur unterstützten Software: <http://www.ibm.com/support/docview.wss?rs=180&uid=swg27006921>.

Anmerkung: Auf Linux-Systemen des Typs 64-Bit-PowerPC ist es nicht möglich, mit dem Browser Mozilla auf die Konfigurations- und Verwaltungsformulare zuzugreifen, weil kein SDK für diese Architektur verfügbar ist. Sie können jedoch von einer anderen Maschine mit einem unterstützten Webbrowser auf die Konfigurations- und Verwaltungsformulare zugreifen.

Einschränkung: Die vertikale Schiebeleiste links in den Administrationsformularen wird möglicherweise vom Browser nicht angezeigt, wenn die Anzahl der eingeblendeten Elemente die Darstellungsmöglichkeiten des Browser-Fensters überschreitet. In diesem Fall schieben sich die unten in der Liste enthaltenen Elemente aus dem derzeit angezeigten Browser-Fenster und können nicht ausgewählt werden. Sie können dieses Problem beheben, indem Sie die Anzahl der einzublendenden Elemente im linken Menü einschränken. Wenn die Anzahl der eingeblendeten Elemente zu groß ist, müssen Sie so viele Elemente ausblenden, bis die Elemente unten in der Liste im Browser-Fenster sichtbar werden.

Damit die Formulare ordnungsgemäß angezeigt werden, muss das Betriebssystem, unter dem die Formulare angezeigt werden (d. h. das Betriebssystem, auf dem der Browser installiert ist), die erforderlichen Schriftarten für die Sprache besitzen, in der die Formulare geschrieben sind. Die Browser-Schnittstelle muss allerdings nicht unbedingt dieselbe Sprache verwenden wie die Formulare.

Beispiel: Die chinesische Version des Proxyserver läuft auf einem Solaris-9-System. Ein Mozilla-Browser mit englischer Schnittstelle wird auf den Solaris-Host geladen. Der Browser kann dazu verwendet werden, die Konfigurations- und Verwaltungsformulare lokal zu editieren. (Die Formulare werden dem Browser in dem Zeichensatz übermittelt, der vom Proxyserver verwendet wird - in diesem Beispiel Chinesisch. Allerdings werden die Formulare möglicherweise nicht korrekt angezeigt, wenn der Browser und das verwendete Betriebssystem nicht ordnungsgemäß für die Darstellung des vom Proxyserver übermittelten Zeichensatzes konfiguriert sind.)

Wenn eine Windows-Workstation mit Unterstützung der chinesischen Sprache verfügbar ist, die eine ferne Verbindung zum Proxyserver herstellen kann, wäre es auch möglich, die chinesische Version eines Netscape-Browsers auf die Windows-Workstation zu laden und die Formulare in diesem Browser zu bearbeiten. Diese zweite Lösung hat den Vorteil, dass sich dem Administrator eine einheitliche Sprachenschnittstelle bietet.

Die betriebssystemspezifischen Schriftarten haben einen großen Einfluss auf die Darstellung der verschiedenen Sprachen in den Browsern, insbesondere bei Sprachen mit Doppelbytezeichen. Beispielsweise sieht eine chinesische Schriftart unter AIX nicht genauso aus wie auf Windows-Plattformen. Dies verursacht einige Unregelmäßigkeiten in der Darstellung von HTML-Text und Java-Applets in den Konfigurations- und Verwaltungsformularen. Daher werden für eine optimale Darstellung nur Browser empfohlen, die unter dem Betriebssystem Windows ausgeführt werden.

Anmerkung zum Browser Mozilla 1.4 auf Systemen des Typs S/390 und PowerPC

Das mit Mozilla 1.4 installierte Java-Plug-in muss auf Version 1.4.2 oder höher aktualisiert werden, damit die Administrationsformulare ordnungsgemäß angezeigt werden. Gehen Sie zum Aktualisieren des Plug-in wie folgt vor:

1. Rufen Sie die Webseite <http://plugindoc.mozdev.org> auf.
2. Wählen Sie im Abschnitt "Documentation" die gewünschte Plattform aus.
3. Folgen Sie den Anweisungen im Abschnitt "Java Runtime Environment", um das Plug-in zu aktualisieren.

Verwendung von Browsern für die Anzeige der Online-Hilfe von Load Balancer

Zur Anzeige der Online-Hilfe von Load Balancer muss der Browser Folgendes unterstützen:

- HTML 4
- Cascading Style Sheets
- JavaScript-Technologie
- Java-Applets

Bei Verwendung eines Browsers, der diese Voraussetzungen nicht erfüllt, werden möglicherweise falsch formatierte Seiten angezeigt und Funktionen nicht richtig ausgeführt.

- **Für Linux- und UNIX-Systeme:** Die Standard-Browser sind Mozilla und Firefox. Informationen zu den empfohlenen Versionen dieser Browser finden Sie auf der folgenden Website. Folgen Sie auf dieser Website den Links zur Webseite mit Informationen zur unterstützten Software: <http://www.ibm.com/support/docview.wss?rs=180&uid=swg27006921>.
- **Für Windows-Systeme:** Der Standard-Browser ist der System-Browser. Informationen zu den empfohlenen Versions der Browser Internet Explorer, Mozilla und Firefox finden Sie auf der folgenden Website. Folgen Sie auf dieser Website den Links zur Website mit Informationen zur unterstützten Software: <http://www.ibm.com/support/docview.wss?rs=180&uid=swg27006921>.

Kapitel 12. Installation von Edge Components mit dem Installationsprogramm

Dieses Kapitel enthält Anweisungen für die Installation von Edge Components mit dem Installationsprogramm.

Das Java 2 SDK wird auf allen Plattformen automatisch mit Load Balancer installiert.

Nach der Installation versuchen Scripts aus dem Caching-Proxy-Paket, den Proxy-Server mit der Standardkonfiguration zu starten. Ist Port 80 belegt, beispielsweise von einem anderen Webserver, schlägt das Starten des Proxy-Servers fehl.

Wichtig: Caching Proxy ist mit folgender Ausnahme in allen Edge-Components-Installationen verfügbar:

- Caching Proxy ist nicht verfügbar in Edge-Components-Installationen auf 64-Bit-Plattformen mit Itanium-2- oder AMD-Opteron-Prozessoren.
- Caching Proxy ist nicht verfügbar in Edge-Components-Installationen von Load Balancer for IPv4 and IPv6.

Verwendung des Installationsprogramms auf Windows-Systemen

Mit dem Installationsprogramm können Sie Edge Components wie folgt auf Ihrem Windows-System installieren:

1. Vergewissern Sie sich, dass das Windows-System alle in Kapitel 11, „Voraussetzungen für Edge Components“, auf Seite 51 beschriebenen Hardware- und Softwarevoraussetzungen erfüllt.
2. Melden Sie sich als Benutzer mit Administratorrechten an.
3. Legen Sie die Edge-Components-CD in das CD-ROM-Laufwerk ein. Daraufhin wird das LaunchPad automatisch gestartet.
4. Klicken Sie auf **Installationsassistenten für WebSphere Application Server starten – Edge Components**. Das Installationsprogramm wird automatisch gestartet. Es bereitet den InstallShield-Assistenten vor und öffnet das Fenster "Willkommen".

Anmerkung: Wenn Ihre Maschine die Autoplay-Funktion nicht unterstützt oder diese Funktion inaktiviert ist, starten Sie das Installationsprogramm manuell. Führen Sie dazu das Programm `setup.exe` im Ausgangsverzeichnis der CD aus.

5. Klicken Sie auf **Weiter**, um die Installation fortzusetzen. Das Fenster "Softwarelizenzvereinbarung" wird geöffnet.
6. Lesen Sie die Lizenzvereinbarung und klicken Sie auf **Ja**, wenn Sie alle Bedingungen akzeptieren. Das Fenster "Komponentenauswahl" wird geöffnet.
Sind bereits Komponenten von Edge Components installiert, wird vor dem Fenster "Komponentenauswahl" das Fenster "Verwaltungsoptionen" angezeigt. Wählen Sie den Radioknopf **Ändern** aus und klicken Sie dann auf **Weiter**. Das Fenster "Komponentenauswahl" wird geöffnet.
7. Wählen Sie die zu installierenden Komponenten aus.
8. Wenn Sie für eine Komponente die Auswahl zu installierender Teilkomponenten ändern wollen, klicken Sie auf den Namen der Komponente. Klicken

Sie anschließend auf **Teilkomponenten ändern**. Daraufhin wird ein weiteres Fenster "Komponentenauswahl" geöffnet, in dem die Teilkomponenten der aktiven Komponente angezeigt werden. Wählen Sie jetzt gemäß der zuvor beschriebenen Vorgehensweise die zu installierenden Teilkomponenten, die Sprache der Komponenten und das Installationsverzeichnis aus.

9. Wählen Sie in den Menüs **Aktuelle Sprache** die Sprache bzw. die Sprachen aus, in denen Edge Components installiert werden soll. Im linken Menü werden die verfügbaren Sprachen aufgelistet. Die ausgewählten Sprachen werden im rechten Menü aufgelistet.
10. Überprüfen Sie im Fenster "Komponentenauswahl" den Installationspfad für Edge Components. Sie können entweder die Standardeinstellung übernehmen oder einen anderen Ordner angeben, indem Sie auf **Ordner ändern** klicken.

Anmerkung: Wenn Sie einen anderen Installationspfad angeben, verwenden Sie im Pfadnamen keine Leerzeichen. Vermeiden Sie Pfadnamen wie C:\Meine Dateien\Edgeserver\.

11. Überprüfen Sie im Komponentenauswahlfenster, ob im ausgewählten Installationspfad genügend Speicherplatz verfügbar ist. Ist dies nicht der Fall, klicken Sie auf **Ordner ändern** und geben Sie einen anderen Installationspfad an.
12. Nachdem Sie die Komponenten von Edge Components, den Installationspfad und die Sprachen ausgewählt haben, klicken Sie auf **Weiter**. Überprüfen Sie die Angaben, die im Fenster "Installationsbestätigung" angezeigt werden. Wenn Sie eine oder mehrere Angaben ändern möchten, klicken Sie auf **Zurück**, um zum Komponentenauswahlfenster zurückzukehren, in dem Sie Ihre Änderungen vornehmen können. Nachdem Sie die Richtigkeit Ihrer Angaben sichergestellt haben, klicken Sie auf **Fertig stellen**.
13. Das Produktinstallationsprogramm von Edge Components beginnt damit, die ausgewählten Komponenten von Edge Components und gegebenenfalls das GSK in dem angegebenen Installationspfad zu installieren.
14. Das Fenster "Installation beendet" wird angezeigt. Wenn Sie die Readme-Datei von Edge Components lesen möchten, achten Sie darauf, dass das Markierungsfeld **Ja, die Readme-Datei anzeigen** ausgewählt ist. Die Readme-Datei wird im Standard-Browser geöffnet.
15. Vergewissern Sie sich, dass das Markierungsfeld **Ja, den Computer jetzt neu starten** ausgewählt ist, und klicken Sie dann auf **Fertig stellen**. Wenn Sie die Option zum Anzeigen der Readme-Datei ausgewählt haben, wird die Maschine neu gestartet, sobald Sie das Browser-Fenster mit der Readme-Datei schließen. Andernfalls wird das Produktinstallationsprogramm von Edge Components sofort beendet und die Maschine wird neu gestartet. Damit Sie eine der neu installierten Komponenten von Edge Components verwenden können, müssen Sie die Maschine neu starten.

Einschränkung: Wenn Sie im Fenster mit der Lizenzvereinbarung die Tabulatortaste verwenden, wechselt der Fokus zwischen den Optionen **Ich akzeptiere** und **Ich akzeptiere nicht**. Mit der Tabulatortaste können Sie jedoch nicht die Navigationsoptionen **Zurück**, **Weiter** und **Abbrechen** erreichen. Verwenden Sie die Ausweichtastenkombination Umschalttaste+Tab, um diese Navigationsoptionen zu erreichen. Außerdem funktioniert die Eingabetaste nur bei den Navigationsschaltflächen. Zur Auswahl der Option **Ich akzeptiere** oder **Ich akzeptiere nicht** müssen Sie deshalb die Leertaste verwenden.

Verwendung des Installationsprogramms auf Linux- und UNIX-Systemen

Wenn Sie die Installation von CD durchführen, können Sie mit dem Installationsprogramm Edge Components wie folgt auf Ihrem Linux- bzw. UNIX-System installieren:

1. Vergewissern Sie sich, dass der Server alle in Kapitel 11, „Voraussetzungen für Edge Components“, auf Seite 51 beschriebenen Hardware- und Softwarevoraussetzungen erfüllt.
 - Außerdem muss auf Linux-Systemen das Paket `compat-libstdc++-33` installiert werden, das die Bibliotheken für die Kompatibilität mit GCC 3.3 C++ enthält.
2. Melden Sie sich als lokaler Superuser (normalerweise "root") an.
3. Legen Sie die Edge-Components-CD in das CD-ROM-Laufwerk ein. Hängen Sie das CD-ROM-Laufwerk gegebenenfalls per Mount an.
4. Wechseln Sie aus Ihrem Arbeitsverzeichnis in das Basisverzeichnis der CD.
5. Rufen Sie das Installationsprogramm mit dem folgenden Befehl auf:

```
# ./install
```

Das Fenster "Willkommen" wird geöffnet.

6. Klicken Sie auf **Weiter**, um die Installation fortzusetzen. Das Fenster "Softwarelizenzvereinbarung" wird geöffnet.
7. Lesen Sie die Lizenzvereinbarung und klicken Sie auf **Ja**, wenn Sie alle Bedingungen akzeptieren. Das Fenster "Sprachauswahl" wird geöffnet.
8. Wählen Sie die Sprachen aus, die in dieser Installation von Edge Components unterstützt werden sollen. Klicken Sie auf **Weiter**. Das Fenster "Komponentenauswahl" wird geöffnet.
9. Wählen Sie die zu installierenden Komponenten aus.
10. Klicken Sie auf **Weiter**. Das Fenster "Installation beendet" wird geöffnet.
11. Überprüfen Sie die Informationen in diesem Fenster. Wenn Sie eine Einstellung ändern möchten, klicken Sie auf **Zurück**. Daraufhin wird das Komponentenauswahlfenster wieder angezeigt, in dem Sie Ihre Änderungen vornehmen können. Nachdem Sie die Richtigkeit Ihrer Angaben sichergestellt haben, klicken Sie auf **Weiter**.

Das Installationsprogramm beginnt mit der Installation der ausgewählten Komponenten von Edge Components und der erforderlichen Pakete.

12. Das Fenster "Installationsergebnisse" wird angezeigt. Überprüfen Sie die Ergebnisse und klicken Sie dann auf **Fertig stellen**.

Einschränkung: Wenn Sie im Fenster mit der Lizenzvereinbarung die Tabulatortaste verwenden, wechselt der Fokus zwischen den Optionen **Ich akzeptiere** und **Ich akzeptiere nicht**. Mit der Tabulatortaste können Sie jedoch nicht die Navigationsoptionen **Zurück**, **Weiter** und **Abbrechen** erreichen. Verwenden Sie die Ausweichtastenkombination Umschalttaste+Tab, um diese Navigationsoptionen zu erreichen. Außerdem funktioniert die Eingabetaste nur bei den Navigationsschaltflächen. Zur Auswahl der Option **Ich akzeptiere** oder **Ich akzeptiere nicht** müssen Sie deshalb die Leertaste verwenden.

Hinweis zu Red Hat Linux 3.0 Update 3: Wenn Sie das Installationsprogramm für Edge Components ausführen, funktionieren die Schaltflächen nicht, wenn die GUI-Anzeige auf Maximalgröße eingestellt und anschließend in Originalgröße wiederhergestellt wird. Sie können dieses Problem wie folgt beheben:

1. Klicken Sie auf das **X** oben rechts in der Anzeige, um das Installationsprogramm zu schließen.
2. Beantworten Sie die Frage "Do you want to exit?" mit **Yes**.
3. Starten Sie das Installationsprogramm erneut, ohne die Anzeige auf Maximalgröße einzustellen und anschließend die Originalgröße wiederherzustellen.

Auf Linux- und UNIX-Systemen: Wenn das Programm setup zum Installieren von Edge Components verwendet wird, kann das Deinstallationsprogramm der GUI für die Deinstallation von Edge Components verwendet werden. Mit dem Deinstallationsprogramm der GUI von Edge Components können jedoch keine Aktualisierungspakete deinstalliert werden, die mit nativen Befehlen installiert wurden. In diesem Fall müssen Sie das Aktualisierungspaket zuerst mit den nativen Befehlen (Befehle des Betriebssystems) deinstallieren, damit Sie Edge Components mit dem Deinstallationsprogramm der GUI deinstallieren können.

Informationen zur Verwendung nativer Befehle finden Sie in Kapitel 13, „Installation von Caching Proxy mit den Paketverwaltungstools des Betriebssystems“, auf Seite 59 und Kapitel 14, „Installation von Load Balancer mit den Paketverwaltungstools des Betriebssystems“, auf Seite 63.

Kapitel 13. Installation von Caching Proxy mit den Paketverwaltungstools des Betriebssystems

Dieses Kapitel enthält Anweisungen für die Installation von Caching Proxy mit den Paketverwaltungstools des Systems.

Nach der Installation versuchen Scripts aus dem Caching-Proxy-Paket, den Proxy-Server mit der Standardkonfiguration zu starten. Ist Port 80 belegt, beispielsweise von einem anderen Webserver, schlägt das Starten des Proxy-Servers fehl.

Wichtig: Caching Proxy ist mit folgender Ausnahme in allen Edge-Components-Installationen verfügbar:

- Caching Proxy ist nicht verfügbar in Edge-Components-Installationen auf 64-Bit-Plattformen mit Itanium-2- oder AMD-Opteron-Prozessoren.
- Caching Proxy ist nicht verfügbar in Edge-Components-Installationen von Load Balancer for IPv4 and IPv6.

Wenn Sie das Installationssystem für Softwarepakete des Betriebssystems verwenden, müssen Sie die Pakete in der Reihenfolge installieren, die in Tabelle 2 auf Seite 60 vorgegeben ist. Nachfolgend werden die Schritte, die Sie in der Regel bei der Installation ausführen müssen, ausführlich beschrieben.

1. Legen Sie die Edge-Components-CD in das CD-ROM-Laufwerk ein und hängen Sie das Laufwerk gegebenenfalls per Mount an.
2. Melden Sie sich als lokaler Superuser "root" an:

```
su - root  
Password: Kennwort
```

3. Wechseln Sie in das gewünschte Verzeichnis der CD:
cd Mount-Punkt/Paketverzeichnis/

4. Installieren Sie die Pakete:

Unter AIX:

```
installp -acXd ./Paketname
```

Unter HP-UX:

```
swinstall -s source/ Paketname
```

Unter Linux:

```
rpm -i ./Paketname
```

Unter Solaris:

```
pkgadd -d ./Paketname
```

Tabelle 2. Caching-Proxy-Komponenten

Komponente	Installierte Pakete (empfohlene Reihenfolge)
Caching Proxy	1. gskit7 2. icu 3. admin 4. msg-cp- <i>Sprache</i> 5. cp
Dokumentation zu Edge Components	doc-en_US ¹
Anmerkungen: 1. Die Dokumentation zu Load Balancer wird in zwei Paketen bereitgestellt. Das Paket doc-en_US enthält die gesamte Dokumentation zu Edge Components, einschließlich der Dokumente zu Load Balancer, und legt diese im Verzeichnis ../edge/doc/ ab. Das Dokumentationspaket für Load-Balancer-Installationen (Kapitel 14, „Installation von Load Balancer mit den Paketverwaltungstools des Betriebssystems“, auf Seite 63) installiert nur die Dokumente zu Load Balancer und legt sie in einem Unterverzeichnis des Verzeichnisses ../edge/lb/ ab.	

Tabelle 3. Dateinamen der Pakete unter AIX, HP-UX und Solaris

Generischer Paket-name	AIX-Dateigruppe	HP-UX-Dateigruppe	Solaris-Dateiname
admin	wses_admin.rte	WSES-ADMIN	WSESadmin
cp	wses_cp.base	WSES-CP	WSEScp
doc	wses_doc.en_US	WSES-DOC-en_US	WSESdocen
gskit7	gskkm.rte	gsk7bas	gsk7bas
icu	wses_icu.rte	WSES-ICU	WSESicu
msg-cp- <i>Sprache</i>	wses_cp.msg. <i>Sprache</i> ¹ .base	WSES-cpm <i>Sprache</i> ²	WSEScpm <i>Sprache</i> ³
Anmerkungen: 1. Unter AIX muss die Variable <i>Sprache</i> durch einen der folgenden sprachspezifischen Codes ersetzt werden: 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. 2. Unter HP-UX muss die Variable <i>Sprache</i> durch einen der folgenden sprachspezifischen Codes ersetzt werden: de_DE, en_US, es_ES, fr_FR, it_IT, ja_JP, ko_KR, zh_CN, zh_TW. (HP-UX bietet keine Unterstützung für brasilianisches Portugiesisch (pt_BR).) 3. Unter Solaris muss die Variable <i>Sprache</i> durch einen der folgenden sprachspezifischen Codes ersetzt werden: br, cn, cw, de, en, es, fr, it, ja, kr.			

Tabelle 4. Dateinamen der Pakete unter Linux

Generischer Paketname	Linux-Dateiname
admin	WSES_Admin_Runtime-Release-Version ¹ .Hardware ² .rpm
cp	WSES_CachingProxy-Release-Version ¹ .Hardware ² .rpm
doc	WSES_Doc_en_US-release-version ¹ .Hardware ² .rpm
gskit7	gsk7bas.rpm

Tabelle 4. Dateinamen der Pakete unter Linux (Forts.)

Generischer Paketname	Linux-Dateiname
icu	WSES_ICU_Runtime-Release-Version ¹ .Hardware ² .rpm
msg-cp-Sprache	WSES_CachingProxy_msg_Sprache ³ -Release-Version ¹ .Hardware ² .rpm
Anmerkungen: <ol style="list-style-type: none"> 1. <i>Release-Version</i> steht für das aktuelle Release, z. B. 6.1.0-0. 2. Die Variable <i>Hardware</i> muss durch einen der folgenden Werte ersetzt werden: i686, s390, ppc64. 3. Die Variable <i>Sprache</i> muss durch einen der folgenden sprachspezifischen Codes ersetzt werden: de_DE, en_US, es_ES, fr_FR, it_IT, ja_JP, ko_KR, pt_BR, zh_CN, zh_TW. 	

Das Dokumentationspaket enthält nur englische Dateien. Die übersetzten Versionen der Dokumentation zu Edge Components finden Sie auf der folgenden Website:
www.ibm.com/software/webervers/appserv/ecinfocenter.html.

Caching Proxy mit Systemtools deinstallieren

Geben Sie zum Deinstallieren der Pakete Folgendes ein:

Unter AIX:

```
installp -u Paketname
```

Verwenden Sie zum Deinstallieren aller Caching-Proxy-Pakete den folgenden Befehl:

```
installp -u wses
```

Unter HP-UX:

```
swremove Paketname
```

Verwenden Sie zum Abfragen der installierten Pakete für Caching Proxy folgenden Befehl:

```
swlist | grep WSES
```

Die Pakete müssen in umgekehrter Installationsreihenfolge deinstalliert werden.

Unter Linux:

```
rpm -e Paketname
```

Verwenden Sie zum Abfragen der installierten Pakete für Caching Proxy folgenden Befehl:

```
rpm -qa |grep -i wses
```

Die Pakete müssen in umgekehrter Installationsreihenfolge deinstalliert werden.

Unter Solaris:

```
pkgrm Paketnam
```

Verwenden Sie zum Abfragen der installierten Pakete für Caching Proxy folgenden Befehl:

```
pkginfo | grep WSES
```

Die Pakete müssen in umgekehrter Installationsreihenfolge deinstalliert werden.

Kapitel 14. Installation von Load Balancer mit den Paketverwaltungstools des Betriebssystems

Dieses Kapitel beschreibt die Installation von Load Balancer auf AIX-, HP-UX-, Linux- und Solaris-Systemen:

- „Installation unter AIX“ auf Seite 64
- „Installation unter HP-UX“ auf Seite 67
- „Installation unter Linux“ auf Seite 69
- „Installation unter Solaris“ auf Seite 71

Je nach Installationstyp werden unter Umständen nicht alle Load-Balancer-Komponentenpaket, die in diesem Abschnitt aufgelistet sind, bereitgestellt.

- Für Edge-Components-Installationen, die Load Balancer und Caching Proxy bereitstellen können, sind alle Installationskomponentenpakete für Load Balancer verfügbar.
- Für Edge-Components-Installationen, die nur Load Balancer bereitstellen können, ist das CBR-Komponentenpaket nicht in Load Balancer enthalten.
- Für Installationen von Edge Components for IPv6 (Load Balancer for IPv4 and IPv6) ist das Dispatcher-Komponentenpaket in Load Balancer enthalten. Die CBR-, Site-Selector- und Controller-Komponentenpakete sind nicht enthalten.

Die empfohlene Reihenfolge für die Installation der Pakete ist für Installationen von Load Balancer for IPv4 and IPv6 geringfügig anders. Das Paket für die Verwaltungskomponente muss unbedingt nach dem Paket für die Dispatcher-Komponente installiert werden. Die empfohlene Reihenfolge für die Installation der Pakete für Load Balancer for IPv4 and IPv6 mit den Systemtools ist Basis, Lizenz, Dispatcher, Verwaltung, Dokumentation, Metric Server.

Wenn Sie eine frühere Version von Load Balancer auf die neue Version migrieren oder ein Betriebssystem erneut installieren, können Sie vor der Installation die früheren Konfigurationsdateien oder Script-Dateien für Load Balancer sichern.

- Kopieren Sie nach der Installation die Konfigurationsdateien in das Verzeichnis `.../ibm/edge/lb/servers/configurations/Komponente` (**Komponente** steht hier für `dispatcher`, `cbr`, `ss`, `cco` oder `nal`).
- Kopieren Sie nach der Installation die Script-Dateien (wie z. B. `goIdle` und `goStandby`) in das Verzeichnis `.../ibm/edge/lb/servers/bin`, wenn Sie diese ausführen möchten.

Wenn Sie sich nach der Installation von Load Balancer von einer Maschine abmelden, müssen Sie nach einer erneuten Anmeldung alle Load-Balancer-Dienste neu starten.

Installation unter AIX

Tabelle 5 enthält eine Liste der AIX-Dateigruppen für Load Balancer und die empfohlene Installationsreihenfolge unter Verwendung des Paketinstallationstools des Systems auf.

Tabelle 5. AIX-Dateigruppen

Load-Balancer-Komponenten	AIX-Dateigruppen
Basis	ibmlb.base.rte
Verwaltung (mit Nachrichten)	<ul style="list-style-type: none">ibmlb.admin.rteibmlb.msg.<i>Sprache</i>.admin
Einheitentreiber	ibmlb.lb.driver
Lizenz	ibmlb.lb.license
Load-Balancer-Komponenten (mit Nachrichten)	<ul style="list-style-type: none">ibmlb.<i>Komponente</i>.rteibmlb.msg.<i>Sprache</i>.lb
Dokumentation (mit Nachrichten)	<ul style="list-style-type: none">ibmlb.doc.rteibmlb.msg.en_US.doc
Metric Server	ibmlb.ms.rte

Anmerkungen:

1. Die Variable *Komponente* kann durch eines der folgenden Komponentenkürzel ersetzt werden: disp (Dispatcher), cbr (CBR), ss (Site Selector), cco (Cisco CSS Controller) oder nal (Nortel Alteon Controller).
2. Die Variable *Sprache* kann durch einen der folgenden sprachspezifischen Codes ersetzt werden: 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.

Das Dokumentationspaket enthält nur englische Dateien. Die übersetzten Versionen der Dokumentation zu Edge Components finden Sie auf der folgenden Website: www.ibm.com/software/webservers/appserv/ecinfocenter.html.

Installationsvorbereitung

Vergewissern Sie sich vor der Installation von Load Balancer unter AIX, dass folgende Voraussetzungen erfüllt sind:

- Sie sind als Benutzer root angemeldet.
- Sie haben die Edge-Components-CD in das CD-ROM-Laufwerk eingelegt bzw. die Installations-Images in ein Verzeichnis kopiert, falls Sie das Produkt aus dem Web heruntergeladen haben. Sie haben alle früheren Versionen des Produkts deinstalliert. Vergewissern Sie sich vor der Deinstallation, dass alle Steuerprogramme (Executor) und Server gestoppt wurden. Geben Sie anschließend den folgenden Befehl ein, um das vollständige Produkt zu deinstallieren:

```
installp -u ibmlb
```

Geben Sie den folgenden Befehl ein, um frühere Versionen zu deinstallieren:

```
installp -u ibmnd
```

Wenn Sie bestimmte Dateigruppen deinstallieren möchten, listen Sie diese anstelle des Paketnamens `ibmlb` einzeln auf.

Bei der Installation des Produkts können Sie auswählen, ob Sie nur bestimmte oder alle in der folgenden Liste aufgeführten Komponenten installieren möchten:

- Basisverwaltung
- Verwaltung (mit Nachrichten)
- Einheitentreiber (erforderlich)
- Lizenz (erforderlich)
- Komponente Dispatcher (mit Nachrichten)
- Komponente CBR (mit Nachrichten)
- Komponente Site Selector (mit Nachrichten)
- Komponente Cisco CSS Controller (mit Nachrichten)
- Komponente Nortel Alteon Controller (mit Nachrichten)
- Dokumentation (mit Nachrichten)
- Metric Server

Installationsverfahren

Es wird empfohlen, Load Balancer unter AIX mit SMIT zu installieren, da in diesem Fall alle Nachrichten automatisch installiert werden.

Load Balancer unter AIX mit SMIT installieren

1. Wählen Sie **Softwareinstallation und -wartung** aus.
2. Wählen Sie **Software installieren und aktualisieren** aus.
3. Wählen Sie **Installation und Aktualisierung der zuletzt verfügbaren Software** aus.
4. Geben Sie die Einheit oder das Verzeichnis mit den Dateigruppen ein.
5. Geben Sie im Feld **Zu installierende Software** die gewünschten Komponenten an (oder wählen Sie "Liste" aus).
6. Klicken Sie auf **OK**.
7. Nach Ausführung des Befehls klicken Sie auf **Fertig**.
8. Beenden Sie SMIT, indem Sie im Menü **Beenden** die Option **SMIT beenden** auswählen oder die Taste **F12** drücken. Falls Sie SMITTY verwenden, drücken Sie die Taste **F10**, um das Programm zu beenden.

Load Balancer über die Befehlszeile installieren

1. Falls Sie das Produkt von einer CD installieren, geben Sie die folgenden Befehle ein, um das CD-ROM-Laufwerk per Mount anzuhängen:

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

2. In der folgenden Tabelle sind die Befehle aufgeführt, die Sie eingeben müssen, um die gewünschten Pakete von Load Balancer unter AIX zu installieren:

Tabelle 6. AIX-Installationsbefehle

Pakete	Befehle
Basis	installp -acXgd <i>Einheit</i> ibmlb.base.rte
Verwaltung (mit Nachrichten)	installp -acXgd <i>Einheit</i> ibmlb.admin.rte ibmlb.msg. <i>Sprache</i> .admin
Einheitentreiber	installp -acXgd <i>Einheit</i> ibmlb.lb.driver
Lizenz	installp -acXgd <i>Einheit</i> ibmlb.lb.license
Load-Balancer-Komponenten (mit Nachrichten): Dispatcher, CBR, Site Selector, Cisco CSS Controller und Nortel Alteon Controller	installp -acXgd <i>Einheit</i> ibmlb. <i>Komponente</i> .rte ibmlb.msg. <i>Sprache</i> .lb
Dokumentation (mit Nachrichten)	installp -acXgd <i>Einheit</i> ibmlb.doc.rte ibmlb.msg.en_US.lb
Metric Server	installp -acXgd <i>Einheit</i> ibmlb.ms.rte

Einheit kann durch Folgendes ersetzt werden:

- /cdrom bei Installation von einer CD
- /dir (das Verzeichnis mit den Dateigruppen) bei Installation aus einem Dateisystem.

3. Vergewissern Sie sich, dass die Ergebnisspalte in der Zusammenfassung für alle installierten Komponenten von Load Balancer die Angabe ERFOLGREICH enthält. Fahren Sie erst fort, wenn alle zu installierenden Komponenten erfolgreich installiert wurden.

Anmerkung: Wenn Sie für eine ausgewählte Einheit eine Liste der Dateigruppen einschließlich aller verfügbaren Nachrichtenkataloge generieren möchten, geben Sie Folgendes ein:

```
installp -ld Einheit
```

Wenn Sie die Installation von CD durchführen, geben Sie den folgenden Befehl ein, um das CD-ROM-Laufwerk abzuhängen:

```
umount /cdrom
```

Überprüfen Sie, ob das Produkt installiert wurde. Geben Sie dazu folgenden Befehl ein:

```
lsipp -h | grep ibmlb
```

Wenn Sie das vollständige Produkt installiert haben, gibt der Befehl Folgendes zurück:

```
ibmlb.base.rte
ibmlb.admin.rte
ibmlb.lb.driver
ibmlb.lb.license
ibmlb.Komponente.rte
ibmlb.doc.rte
```

ibmlb.ms.rte
ibmlb.msg.*Sprache*.admin
ibmlb.msg.en_US.doc
ibmlb.msg.*Sprache*.lb

Load Balancer verwendet folgende Installationspfade:

- Verwaltung: /opt/ibm/edge/lb/admin
- Load-Balancer-Komponenten: /opt/ibm/edge/lb/servers
- Metric Server: /opt/ibm/edge/lb/ms
- Dokumentation (*Administratorhandbuch*): /opt/ibm/edge/lb/documentation

Installation unter HP-UX

In diesem Abschnitt wird erläutert, wie Load Balancer unter HP-UX von der Produkt-CD installiert wird.

Installationsvorbereitung

Vergewissern Sie sich vor Beginn der Installation, dass Sie die zum Installieren der Software erforderliche Root-Berechtigung besitzen.

Sollte bereits eine frühere Version des Produkts installiert sein, müssen Sie diese Kopie vor der Installation der aktuellen Version deinstallieren. Stellen Sie zuerst sicher, dass das Steuerprogramm (Executor) und der Server gestoppt sind. Deinstallieren Sie anschließend Load Balancer gemäß den Anweisungen im Abschnitt „Anweisungen für die Deinstallation der Pakete“ auf Seite 68.

Installationsverfahren

Die Tabelle 7 enthält eine Liste der Installationspakete für Load Balancer und die empfohlene Reihenfolge, in der diese Pakete mit dem Paketinstallationsstool des Systems installiert werden sollten.

Tabelle 7. Einzelheiten zur Installation der Pakete für Load Balancer unter HP-UX

Paketbeschreibung	Name des Pakets unter HP-UX
Basis	ibmlb.base
Verwaltung und Nachrichten	ibmlb.admin ibmlb.nlv- <i>Sprache</i>
Load-Balancer-Lizenz	ibmlb.lic
Load-Balancer-Komponenten	ibmlb. <i>Komponente</i>
Dokumentation	ibmlb.doc
Metric Server	ibmlb.ms
Anmerkungen: <ol style="list-style-type: none">1. Die Variable <i>Sprache</i> muss durch einen der folgenden sprachspezifischen Codes ersetzt werden: de_DE, es_ES, fr_FR, it_IT, ja_JP, ko_KR, zh_CN, zh_TW.2. Die Variable <i>Komponente</i> muss durch einen der folgenden Werte ersetzt werden: disp (Dispatcher), cbr (CBR), ss (Site Selector), cco (Cisco CSS Controller) oder nal (Nortel Alteon Controller).3. Das Dokumentationspaket (ibmlb.doc) enthält nur englische Dateien. Die übersetzten Versionen der Dokumentation zu Edge Components finden Sie auf der folgenden Website: www.ibm.com/software/webservers/appserv/ecinfocenter.html.	

HP-UX bietet keine Unterstützung für die Locale Brasilianisches Portugiesisch (pt_BR). Die folgenden Locales werden unter HP-UX unterstützt:

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

Anweisungen für die Installation der Pakete

Im Folgenden sind die Schritte, die Sie zum Installieren des Produkts ausführen müssen, ausführlich beschrieben.

1. Melden Sie sich als lokaler Superuser "root" an:

```
su - root
Password: Kennwort
```

2. Führen Sie den Installationsbefehl zum Installieren der Pakete aus.

Setzen Sie den folgenden Installationsbefehl ab:

```
swinstall -s /Quelle Paketname
```

Quelle steht hier für den absoluten Verzeichnispfad zum Paket und *Paketname* für den Namen des Pakets.

Der folgende Befehl installiert beispielsweise das Basispaket für Load Balancer (ibmlb.base), wenn Sie die Installation aus dem Stammverzeichnis der CD heraus durchführen:

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

Setzen Sie zum Installieren aller Pakete für Load Balancer den folgenden Befehl ab, wenn Sie die Installation aus dem Stammverzeichnis der CD heraus ausführen:

```
swinstall -s /Quelle ibmlb
```

3. Überprüfen Sie die Installation der Load-Balancer-Pakete.

Führen Sie den Befehl **swlist** aus, um alle Pakete aufzulisten, die Sie installiert haben. Beispiel:

```
swlist -l fileset ibmlb
```

Anweisungen für die Deinstallation der Pakete

Verwenden Sie den Befehl **swremove**, um die Pakete zu deinstallieren. Die Pakete müssen in umgekehrter Installationsreihenfolge deinstalliert werden. Beispiel:

- Setzen Sie den folgenden Befehl ab, um alle Pakete für Load Balancer zu deinstallieren:

```
swremove ibmlb
```

Setzen Sie den folgenden Befehl ab, um ein einzelnes Paket (z. B. den Cisco CSS Controller) zu deinstallieren:

```
swremove ibmlb.cco
```

Load Balancer verwendet folgende Installationspfade:

- Verwaltung: /opt/ibm/edge/lb/admin
- Load-Balancer-Komponenten: /opt/ibm/edge/lb/servers
- Metric Server: /opt/ibm/edge/lb/ms
- Dokumentation (*Administratorhandbuch*): /opt/ibm/edge/lb/documentation

Installation unter Linux

In diesem Abschnitt wird erläutert, wie Load Balancer von der Edge-Components-CD unter Linux installiert wird.

Installationsvorbereitung

Vergewissern Sie sich vor der Installation von Load Balancer, dass folgende Voraussetzungen erfüllt sind:

- Sie sind als Benutzer root angemeldet.
- Sie haben alle früheren Versionen des Produkts deinstalliert. Stellen Sie vor der Deinstallation sicher, dass alle Steuerprogramme (Executor) und Server gestoppt wurden. Geben Sie dann den folgenden Befehl ein, um das gesamte Produkt zu deinstallieren:

```
rpm -e Paketname
```

Bei der Deinstallation müssen Sie die Reihenfolge, in der die Pakete installiert wurden, umkehren und auf diese Weise sicherstellen, dass die Verwaltungspakete zuletzt deinstalliert werden.

Installationsschritte

1. Legen Sie die Edge-Components-CD in das CD-ROM-Laufwerk ein oder laden Sie das Produkt von der Website herunter und installieren Sie das Installations-Image mit RPM (Red Hat Packaging Manager).

Das Installations-Image ist eine Datei im Format *lblinux-Version.tar*.

2. Entpacken Sie die tar-Datei mit dem folgenden Befehl in einem temporären Verzeichnis:

```
tar -xf lblinux-Version.tar
```

Folgende Gruppe von Dateien mit der Erweiterung .rpm wird entpackt:

- *ibmlb-base-Release-Version.Hardware.rpm* (Basisprodukt)
- *ibmlb-admin-Release-Version.Hardware.rpm* (Verwaltung)
- *ibmlb-lic-Release-Version.Hardware.rpm* (Lizenz)
- *ibmlb-Komponente-Release-Version.Hardware.rpm* (LB-Komponente)
- *ibmlb-doc-Release-Version.Hardware.rpm* (Dokumentation)
- *ibmlb-ms-Release-Version.Hardware.rpm* (Metric Server)

Die Parameter sind im Folgenden erläutert:

- *Release-Version* steht für das aktuelle Release, z. B. 6.1.0-0.
- *Hardware* steht für einen der folgenden Werte: i386, ppc64, ppc, s390, s390x, x86_64.
- *Komponente* steht für einen der folgenden Werte: disp (Komponente Dispatcher), cbr (Komponente CBR), ss (Komponente Site Selector), cco (Cisco CSS Controller), nal (Nortel Alteon Controller).

Das Dokumentationspaket enthält nur englische Dateien. Die übersetzten Versionen der Dokumentation zu Edge Components finden Sie auf der folgenden Website: www.ibm.com/software/webervers/appserv/ecinfocenter.html.

3. Führen Sie im Verzeichnis mit den RPM-Dateien folgenden Befehl aus, um die einzelnen Pakete zu installieren. Beispiel:

```
rpm -i Paket.rpm
```

Systeme mit Red Hat Linux: Aufgrund eines bekannten Problems in Red Hat Linux müssen Sie außerdem die RPM-Dateien `_db*` löschen. Andernfalls tritt ein Fehler auf.

Die Pakete müssen in der folgenden Reihenfolge installiert werden:

- Basis (base)
- Verwaltung (admin)
- Lizenz (lic)
- Load-Balancer-Komponenten (ds, cbr, ss, cco, nal)
- Metric Server (ms)
- Dokumentation (doc)

Anmerkung: Mindestens eine RPM-Datei erfordert, dass Java installiert und in der RPM-Datenbank registriert ist. Ist Java installiert, aber nicht in der RPM-Datenbank registriert, verwenden Sie den Installationsbefehl mit der Option "nodeps" (no dependencies, keine Abhängigkeiten) wie folgt:

```
rpm -i --nodeps Paket.rpm
```

4. Überprüfen Sie, ob das Produkt installiert ist. Geben Sie dazu folgenden Befehl ein:

```
rpm -qa | grep ibmlb
```

Wenn Sie das vollständige Produkt installiert haben, wird folgende Ausgabe angezeigt:

- *ibmlb-base-Release-Version*
- *ibmlb-admin-Release-Version*
- *ibmlb-lic-Release-Version*
- *ibmlb-dsp-Release-Version*
- *ibmlb-cbr-Release-Version*
- *ibmlb-ss-Release-Version*
- *ibmlb-cco-Release-Version*
- *ibmlb-nal-Release-Version*
- *ibmlb-doc-Release-Version*
- *ibmlb-ms-Release-Version*

Load Balancer verwendet folgende Installationspfade:

- Verwaltung: `/opt/ibm/edge/lb/admin`
- Load-Balancer-Komponenten: `/opt/ibm/edge/lb/servers`
- Metric Server: `/opt/ibm/edge/lb/ms`
- Dokumentation: `/opt/ibm/edge/lb/documentation`

Bei der Deinstallation müssen Sie die Reihenfolge, in der die Pakete installiert wurden, umkehren und auf diese Weise sicherstellen, dass die Verwaltungspakete zuletzt deinstalliert werden.

Installation unter Solaris

In diesem Abschnitt wird erläutert, wie Load Balancer von der Edge-Components-CD unter Solaris installiert wird.

Installationsvorbereitung

Vergewissern Sie sich vor Beginn der Installation, dass Sie als "root" angemeldet sind und dass alle früheren Versionen des Produkts deinstalliert wurden.

Stellen Sie vor der Deinstallation sicher, dass alle Steuerprogramme (Executor) und Server gestoppt wurden. Geben Sie anschließend folgenden Befehl ein:

```
pkgrm Paketname
```

Installationsschritte

1. Legen Sie die CD-ROM mit der Load-Balancer-Software in das CD-ROM-Laufwerk ein.
2. Geben Sie an der Eingabeaufforderung folgenden Befehl ein:

```
pkgadd -d Pfadname
```

-d *Pfadname* steht für den Einheitennamen des CD-ROM-Laufwerks oder das Verzeichnis auf dem Festplattenlaufwerk, in dem sich das Paket befindet. Beispiel: -d /cdrom/cdrom0/.

Die folgende Liste enthält die angezeigten Pakete und die empfohlene Reihenfolge für ihre Installation.

- ibmlbbase (Basis)
- ibmlbadm (Verwaltung)
- ibmlblic (Lizenz)
- ibmlbdisp (Komponente Dispatcher)
- ibmlbcbr (Komponente CBR)
- ibmlbss (Komponente Site Selector)
- ibmlbcc (Komponente Cisco CSS Controller)
- ibmlbna (Komponente Nortel Alteon Controller)
- ibmlbdoc (Dokumentation)
- ibmlbms (Metric Server)

Das Dokumentationspaket (ibmlbdoc) enthält nur englische Dateien. Die übersetzten Versionen der Dokumentation zu Edge Components finden Sie auf der folgenden Website: www.ibm.com/software/webservers/appserv/ecinfocenter.html.

Wenn Sie alle Pakete installieren möchten, geben Sie einfach `all` ein und drücken Sie die Eingabetaste. Möchten Sie nur bestimmte Komponenten installieren, geben Sie die Namen der zu installierenden Pakete, durch ein Leerzeichen oder Komma getrennt, ein und drücken Sie die Eingabetaste. Möglicherweise werden Sie dazu aufgefordert, Berechtigungen für vorhandene Verzeichnisse oder Dateien zu ändern. Drücken Sie die Eingabetaste oder bestätigen Sie die Aufforderung mit Ja. Sie müssen die erforderlichen Pakete selbst installieren (weil die Installation der Pakete in alphabetischer Reihenfolge erfolgt und nicht in der vorausgesetzten Reihenfolge). Bei Eingabe von `all` können Sie alle Aufforderungen mit Ja beantworten, und die Installation wird erfolgreich ausgeführt.

Wenn Sie nur die Komponente Dispatcher mit der Dokumentation und Metric Server installieren möchten, müssen Sie die folgenden Pakete installieren: `ibmlbbase`, `ibmlbadm`, `ibmlblic`, `ibmdisp`, `ibmlbdoc` und `ibmlbms`.

3. Überprüfen Sie, ob das Produkt installiert wurde. Geben Sie dazu folgenden Befehl ein:

```
pkginfo | grep ibm
```

Load Balancer verwendet folgende Installationspfade:

- Verwaltung: `/opt/ibm/edge/lb/admin`
- Load-Balancer-Komponenten: `/opt/ibm/edge/lb/servers`
- Metric Server: `/opt/ibm/edge/lb/ms`
- Dokumentation: `/opt/ibm/edge/lb/documentation`

Teil 5. Aufbau von Netzen mit Edge Components

Dieser Teil beschreibt, wie Sie grundlegende Beispielnetze mit Edge Components aufbauen können. Diese Netze sind nicht für den Einsatz in Produktionsumgebungen bestimmt. Die Erstkonfiguration eines Netzes kann einem Administrator, der mit dem Produkt noch nicht vertraut ist, zahlreiche Konzepte der Edge-Technologie im Netz verdeutlichen. Eine umfassende Beschreibung aller Komponentenfunktionen und ausführliche Informationen zur Konfiguration finden Sie im *Caching Proxy Administratorhandbuch* und im *Load Balancer Administratorhandbuch*.

Mit Hilfe dieser Prozeduren kann jedes von der Komponente unterstützte Computersystem auf jedem Knoten verwendet werden.

Dieser Teil enthält folgende Kapitel:

Kapitel 15, „Aufbau eines Caching-Proxy-Netzes“, auf Seite 75.

Kapitel 16, „Aufbau eines Load-Balancer-Netzes“, auf Seite 79.

Kapitel 15. Aufbau eines Caching-Proxy-Netzes

Abb. 19 zeigt ein grundlegendes Proxyservernetz, in dem drei Computersysteme auf drei Netzknoten verwendet werden. Dieses Netz bindet den Proxyserver an einen dedizierten Inhaltshost (IBM HTTP Server), der sich auf Server 2 befindet. Der Proxyserver bedient den Host. In der Abbildung wird diese Zuordnung durch das zwischen der Workstation und dem Server 1 liegende Internet veranschaulicht.

Wichtig: Caching Proxy ist mit folgender Ausnahme in allen Edge-Components-Installationen verfügbar:

- Caching Proxy ist nicht verfügbar in Edge-Components-Installationen auf 64-Bit-Plattformen mit Itanium-2- oder AMD-Opteron-Prozessoren.
- Caching Proxy ist nicht verfügbar in Edge-Components-Installationen von Load Balancer for IPv4 and IPv6.

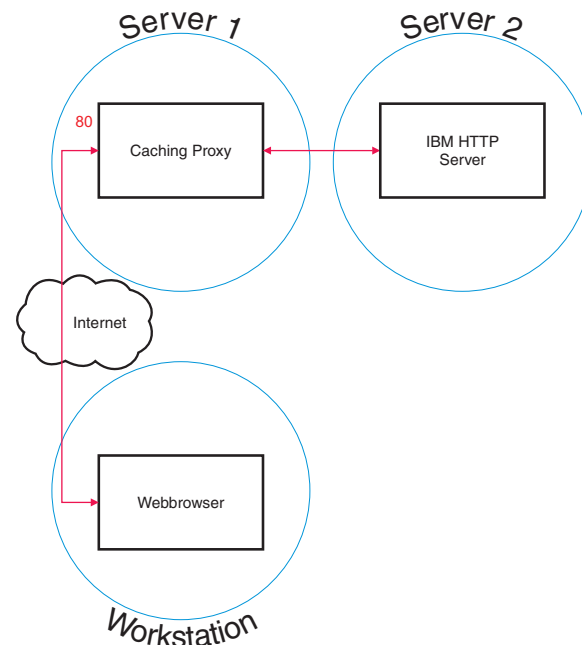


Abbildung 19. Beispiel für ein Caching-Proxy-Netz

Arbeitsablauf

Zum Erstellen eines Caching-Proxy-Netzes führen Sie nacheinander folgende Arbeitsschritte aus:

1. Erforderliche Computersysteme und Software überprüfen.
2. Server 1 erstellen (Linux- und UNIX-Systeme) oder Server 1 erstellen (Windows-System).
3. Server 1 konfigurieren.
4. Das Caching-Proxy-Netz testen.

Erforderliche Computersysteme und Software überprüfen

Folgende Computersysteme und Zusatzsoftware werden benötigt:

- Ein Computersystem, das als Server 1 dient. Dieses System muss einen Internet-Zugang haben.
- Ein Computersystem, das als Server 2 dient. Auf dem Inhaltshost muss ein HTTP-Server installiert sein.
- Ein Computersystem, das als Workstation dient. Auf diesem System muss ein Webbrowser installiert sein.

Server 1 erstellen (Linux- und UNIX-Systeme)

Installieren und konfigurieren Sie Caching Proxy wie folgt:

1. Vergewissern Sie sich, dass der Server alle Hardware- und Softwarevoraussetzungen erfüllt.
2. Melden Sie sich als lokaler Superuser (normalerweise "root") an.
3. Installieren Sie die Komponente Caching Proxy.
4. Geben Sie zum Erstellen einer Administrator-ID und eines Kennworts für den Zugriff auf die Konfigurations- und Verwaltungsformulare folgenden Befehl ein:

```
# htadm -adduser /opt/ibm/edge/cp/server_root/protect/webadmin.passwd
```

Geben Sie auf Anforderung den Benutzernamen, das Kennwort und den echten Namen des Administrators für das Programm **htadm** ein.

5. Fahren Sie mit dem Abschnitt „Server 1 konfigurieren“ fort.

Server 1 erstellen (Windows-System)

Installieren und konfigurieren Sie Caching Proxy wie folgt:

1. Vergewissern Sie sich, dass die Betriebssysteme Windows 2000 und Windows 2003 alle Hardware- und Softwarevoraussetzungen erfüllen.
2. Melden Sie sich als Benutzer mit Administratorrechten an.
3. Installieren Sie die Komponente Caching Proxy.
4. Geben Sie zum Erstellen einer Administrator-ID und eines Kennworts für den Zugriff auf die Konfigurations- und Verwaltungsformulare folgenden Befehl ein:

```
cd "Programme\IBM\edge\cp\server_root\protect"  
htadm -adduser webadmin.passwd"
```

Geben Sie auf Anforderung den Benutzernamen, das Kennwort und den echten Namen des Administrators für das Programm **htadm** ein.

5. Fahren Sie mit dem Abschnitt „Server 1 konfigurieren“ fort.

Server 1 konfigurieren

Führen Sie auf der Workstation folgende Aktionen aus:

1. Starten Sie einen Webbrowser.
2. Geben Sie in Ihrem Browser im Feld **Adresse** den Befehl `http://Server_1` ein, wobei *Server_1* für den Hostnamen oder die IP-Adresse der als Server 1 bestimmten Maschine steht.
3. Klicken Sie auf **Konfigurations- und Verwaltungsformulare**.

4. Geben Sie Administratornamen und Kennwort ein. Die Konfigurations- und Verwaltungsformulare werden im Browser geöffnet.
5. Klicken Sie auf **Serverkonfiguration—>Anforderungsverarbeitung—>Anforderungs-Routing**.
6. Fügen Sie vor der vorhandenen Ausweichzuordnungsregel eine neue ein, indem Sie den Radioknopf **Einfügen vor** und den Indexwert der vorhandenen Ausweichzuordnungsregel auswählen.
7. Wählen Sie in der Dropdown-Liste **Aktion** die Option **Proxy** aus.
8. Geben Sie im Feld **URL-Anforderungsschablone** die Zeichen `/*` ein.
9. Geben Sie im Feld **IP-Adresse oder Hostname des Servers** den Hostnamen der Site ein, an die HTTP-Anforderungen weitergeleitet werden sollen. Stellen Sie diesem Wert die Angabe `http://` voran.
10. Klicken Sie auf **Übergeben**.
11. Fügen Sie eine Zuordnungsregel ein, die den Zugriff auf die Konfigurations- und Verwaltungsformulare ermöglicht. Wählen Sie dazu den Radioknopf **Einfügen vor** und den Indexwert der Zuordnungsregel von Schritt 6 aus.
12. Wählen Sie in der Dropdown-Liste **Aktion** die Option **Pass** aus.
13. Geben Sie im Feld **URL-Anforderungsschablone** den Wert `/pub/*` ein.
14. Geben Sie das Verzeichnis der Konfigurations- und Verwaltungsformulare an:
 - Befindet sich Caching Proxy auf einer Linux- oder UNIX-Maschine, geben Sie im Feld **IP-Adresse oder Hostname des Servers** den Pfad `/opt/ibm/edge/cp/server_root/pub/de_DE/*` ein.
 - Befindet sich Caching Proxy auf einer Windows-Maschine, geben Sie im Feld **IP-Adresse oder Hostname des Servers** den Pfad `"C:\Programme\IBM\edge\cp\server_root\pub\de_DE*"` ein.
15. Klicken Sie auf **Übergeben**.
16. Klicken Sie oben im Konfigurationsformular auf das Symbol **Server erneut starten**.
17. Fahren Sie mit dem Abschnitt „Das Caching-Proxy-Netz testen“ fort.

Das Caching-Proxy-Netz testen

Führen Sie auf der Workstation folgende Aktionen aus:

1. Starten Sie einen Webbrowser.
2. Geben Sie im Browser im Feld **Adresse** den Befehl `http://Server_1` ein. HTML-Seiten von Server 2 werden über Server 1 als Proxyserver an den Webbrowser übermittelt.
3. Geben Sie für den Zugriff auf die Konfigurations- und Verwaltungsformulare im Browser im Feld **Adresse** den Befehl `http://Server_1/pub/` ein. Daraufhin wird die Homepage der Konfigurations- und Verwaltungsformulare angezeigt.

Kapitel 16. Aufbau eines Load-Balancer-Netzes

Abb. 20 zeigt ein grundlegendes Load-Balancer-Netz mit drei lokal angeschlossenen Workstations, die die MAC-gestützte Weiterleitung der Komponente Dispatcher verwenden, um die Last des Webdatenverkehrs auf zwei Webserver zu verteilen. Wird ein Lastausgleich für eine TCP-Anwendung oder eine Anwendung mit UDP ohne Statusverfolgung (stateless) ausgeführt, sieht die Konfiguration ähnlich aus.

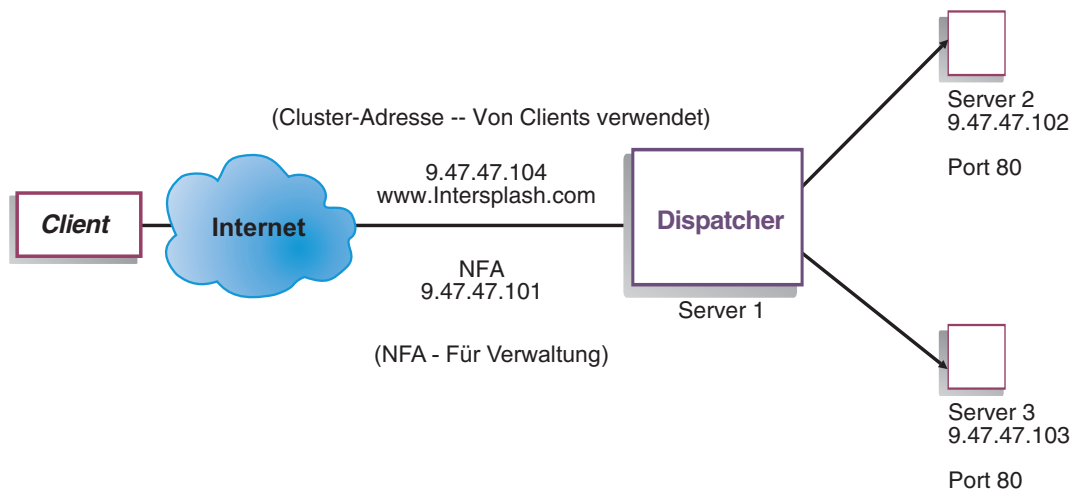


Abbildung 20. Beispiel für ein Load-Balancer-Netz

Anmerkung: Für diese Konfiguration würden zwei Workstations reichen. Der Dispatcher würde sich dabei auf einer der Webserver-Workstations befinden. Dies wäre dann eine Konfiguration, in der Server und Dispatcher zusammengelegt wurden.

Arbeitsablauf

Zum Aufbau eines Load-Balancer-Netzes führen Sie nacheinander die folgenden Arbeitsschritte aus:

1. Erforderliche Computersysteme und Software überprüfen.
2. Das Netz konfigurieren.
3. Den Dispatcher konfigurieren.
4. Das Load-Balancer-Netz testen.

Erforderliche Computersysteme und Software überprüfen

Folgende Computersysteme und Zusatzsoftware werden benötigt:

- Ein Computersystem, das als Dispatcher fungiert. Für dieses System wird eine eigene IP-Adresse und eine Adresse für den Lastausgleich benötigt.
- Zwei Computersysteme, die als Webserver fungieren. Jeder Webserver benötigt eine IP-Adresse.

Das Netz konfigurieren

1. Konfigurieren Sie Ihre Workstations so, dass sie sich innerhalb eines LAN-Segments befinden. Stellen Sie sicher, dass der Datenaustausch im Netz zwischen den drei Maschinen nicht über Router oder Bridges erfolgen muss.
2. Konfigurieren Sie die Netzwerkadapter der drei Workstations. In diesem Beispiel wird die folgende Netzkonfiguration angenommen:

Workstation	Name	IP-Adresse
1	server1.unternehmen.com	9.67.67.101
2	server2.unternehmen.com	9.67.67.102
3	server3.unternehmen.com	9.67.67.103
Netzmaske = 255.255.255.0		

Jede Workstation enthält nur eine Standard-Ethernet-Netzschnittstellenkarte.

3. Stellen Sie sicher, dass server1.unternehmen.com ping-Aufrufe sowohl an server2.unternehmen.com als auch an server3.unternehmen.com senden kann.
4. Stellen Sie sicher, dass server2.unternehmen.com und server3.unternehmen.com ping-Aufrufe an server1.unternehmen.com senden können.
5. Stellen Sie sicher, dass der Inhalt auf den beiden Webservern (Server 2 und 3) identisch ist. Dazu können die Daten auf den beiden Workstations repliziert werden, indem ein gemeinsames Dateisystem wie AFS oder DFS oder eine andere für Ihre Site geeignete Methode verwendet wird.
6. Stellen Sie sicher, dass die Webserver auf server2.unternehmen.com und server3.unternehmen.com betriebsbereit sind. Rufen Sie die Seiten in einem Webbrowser direkt von `http://server2.unternehmen.com` und `http://server3.unternehmen.com` ab.
7. Definieren Sie eine andere gültige IP-Adresse für dieses LAN-Segment. Dies ist die Adresse, die Sie den Clients mitteilen, die auf Ihre Site zugreifen möchten. In diesem Beispiel handelt es sich um folgende Angabe:

Name= `www.unternehmen.com`
IP=`9.67.67.104`

8. Konfigurieren Sie die beiden Webserver-Workstations in der Weise, dass sie Datenübertragungen für `www.unternehmen.com` akzeptieren.
Fügen Sie zur **Loopback**-Schnittstelle auf server2.unternehmen.com und server3.unternehmen.com einen Aliasnamen für `www.unternehmen.com` hinzu.
 - Für AIX:
ifconfig lo0 alias `www.unternehmen.com` netmask 255.255.255.0
 - Für Solaris 7:
ifconfig lo0:1 `www.unternehmen.com` 127.0.0.1 up
9. Löschen Sie alle zusätzlichen Routes, die eventuell infolge der Zuweisung eines Aliasnamens für die Loopback-Schnittstelle erstellt wurde.
Sie haben jetzt alle für die beiden Webserver-Workstations erforderlichen Konfigurationsschritte ausgeführt.

Den Dispatcher konfigurieren

Die Konfiguration des Dispatcher können Sie über die Befehlszeile, den Konfigurationsassistenten oder die grafische Benutzerschnittstelle (GUI) erstellen.

Anmerkung: Die Parameterwerte müssen mit Ausnahme der Parameterwerte für Hostnamen und Dateinamen aus dem englischen Zeichensatz stammen.

Konfiguration über die Befehlszeile

Gehen Sie zum Konfigurieren des Dispatcher über die Befehlszeile wie folgt vor:

1. Starten Sie dsserver auf dem Dispatcher:
 - Führen Sie unter AIX, HP-UX, Linux oder Solaris den folgenden Befehl als root aus: `dsserver`
 - Auf Windows-Plattformen ist dsserver ein Dienst, der automatisch gestartet wird.
2. Starten Sie wie folgt die Executor-Funktion des Dispatcher:
`dscontrol executor start`
3. Fügen Sie wie folgt die Cluster-Adresse zur Dispatcher-Konfiguration hinzu:
`dscontrol cluster add www.unternehmen.com`
4. Fügen Sie wie folgt den Port für das Protokoll HTTP zur Dispatcher-Konfiguration hinzu:
`dscontrol port add www.unternehmen.com:80`
5. Fügen Sie wie folgt alle Webserver zur Dispatcher-Konfiguration hinzu:
`dscontrol server add www.unternehmen.com:80:server2.unternehmen.com`
`dscontrol server add www.unternehmen.com:80:server3.unternehmen.com`
6. Konfigurieren Sie wie folgt die Workstation, so dass sie den Datenverkehr für die Cluster-Adresse akzeptiert:
`dscontrol executor configure www.unternehmen.com`
7. Starten Sie wie folgt die Manager-Funktion des Dispatcher:
`dscontrol manager start`
Der Dispatcher führt den Lastausgleich jetzt basierend auf der Serverleistung durch.
8. Starten Sie wie folgt die Advisor-Funktion des Dispatcher:
`dscontrol advisor start http 80`
Der Dispatcher stellt jetzt sicher, dass keine Clientanforderungen an einen ausgefallenen Webserver gesendet werden.

Die Basiskonfiguration mit lokal angeschlossenen Servern ist damit abgeschlossen.

Wichtig: Bei der Installation von **Load Balancer for IPv4 and IPv6** ist die Syntax für den Dispatcher-Befehl (`dscontrol`) mit einer wichtigen Ausnahme identisch. Der Begrenzer für `dscontrol`-Befehle ist das kommerzielle A (@) und nicht der Doppelpunkt (:). (Es muss ein anderer Begrenzer als der Doppelpunkt definiert werden, weil das Format IPv6 den Doppelpunkt im Adressierungsschema verwendet.)

Erläuterung am Beispiel der vorherigen Dispatcher-Konfiguration

- Verwenden Sie in einer Installation von Load Balancer for IPv4 and IPv6 den folgenden Befehl, um den HTTP-Protokoll-Port der Dispatcher-Konfiguration hinzuzufügen:

```
dscontrol port add www.unternehmen.com@80
```

- Verwenden Sie in einer Installation von Load Balancer for IPv4 and IPv6 den folgenden Befehl, um jeden einzelnen der Webserver der Dispatcher-Konfiguration hinzuzufügen:

```
dscontrol server add www.unternehmen.com@80@server2.unternehmen.com
```

```
dscontrol server add www.unternehmen.com@80@server3.5unternehmen.com
```

Nähere Informationen zur Installation von Load Balancer for IPv4 and IPv6 finden Sie im Kapitel zur Implementierung von Dispatcher in Load Balancer for IPv4 and IPv6 im *WebSphere Application Server Load Balancer Administratorhandbuch*, das die Einschränkungen und Konfigurationsunterschiede beschreibt.

Konfiguration mit dem Konfigurationsassistenten

Gehen Sie zum Konfigurieren des Dispatcher mit dem Konfigurationsassistenten wie folgt vor:

1. Starten Sie dsserver auf dem Dispatcher wie folgt:
 - Führen Sie unter AIX, HP-UX, Linux oder Solaris den folgenden Befehl als root aus:
dsserver
 - Auf Windows-Systemen ist dsserver ein Dienst, der automatisch gestartet wird.
2. Starten Sie den Assistenten des Dispatcher, dswizard.

Der Assistent führt Sie schrittweise durch das Erstellen einer Basiskonfiguration für die Komponente Dispatcher. Der Assistent stellt Ihnen Fragen bezüglich Ihres Netzes und führt Sie durch die Konfiguration eines Cluster, in dem der Dispatcher den Datenverkehr auf eine Gruppe von Servern verteilt.

Der Konfigurationsassistent enthält folgende Anzeigen:

- Einführung in den Assistenten
- Erwartungen
- Konfiguration vorbereiten
- Zu konfigurierenden Host auswählen (sofern erforderlich)
- Cluster definieren
- Port hinzufügen
- Server hinzufügen
- Advisor starten
- Servermaschine konfigurieren

Konfiguration über die grafische Benutzerschnittstelle (GUI)

Gehen Sie zum Starten der GUI wie folgt vor:

1. Stellen Sie sicher, dass der dsserver-Prozess aktiv ist:
 - Führen Sie unter AIX, HP-UX, Linux oder Solaris den folgenden Befehl als root aus:
dsserver
 - Auf Windows-Systemen ist dsserver ein Dienst, der automatisch gestartet wird.
2. Führen Sie anschließend einen der folgenden Schritte aus:
 - Geben Sie unter AIX, HP-UX, Linux oder Solaris lbadmin ein.
 - Klicken Sie auf Windows-Systemen auf **Start > Programme > IBM WebSphere > Edge Components > IBM Load Balancer > Load Balancer**.

Das Load-Balancer-Netz testen

1. Rufen Sie in einem Webbrowser die Adresse `http://www.unternehmen.com` auf, um zu überprüfen, ob eine Seite angezeigt wird.
2. Laden Sie die Seite erneut in den Webbrowser.
3. Geben Sie folgenden Befehl ein: `dscontrol server report www.unternehmen.com:80:`. Überprüfen Sie, ob die Summe der Spalten "Summe Verbindungen" der beiden Server 2 ergibt.

Bemerkungen

Erste Ausgabe (Mail 2006)

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden.

Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Dienstleistungen von IBM verwendet werden können. Anstelle der Produkte, Programme oder Dienstleistungen können auch andere ihnen äquivalente Produkte, Programme oder Dienstleistungen verwendet werden, solange diese keine gewerblichen oder andere Schutzrechte verletzen. Die Verantwortung für den Betrieb von Fremdprodukten, Fremdprogrammen und Fremdservices liegt beim Kunden.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich und in englischer Sprache zu richten an:

IBM Director of Licensing
IBM Europe, Middle East & Africa
Tour Descartes
2, avenue Gambetta
92066 Paris La Defense
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die Angaben in diesem Handbuch werden in regelmäßigen Zeitabständen aktualisiert. Die Änderungen werden in Überarbeitungen oder in Technical News Letters (TNLs) bekannt gegeben. IBM kann jederzeit ohne Vorankündigung Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter dienen lediglich als Benutzerinformationen und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängigen, erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

IBM Corporation
ATTN: Software Licensing
11 Stanwix Street
Pittsburgh, PA 15222-9183
U.S.A.

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des im Handbuch aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt im Rahmen der Internationalen Nutzungsbedingungen der IBM für Programmpakete oder einer äquivalenten Vereinbarung.

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer gesteuerten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Garantie, dass diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können abweichen. Benutzer dieses Dokuments sollten die entsprechenden Daten in ihrer spezifischen Umgebung prüfen. Diese Daten stellen deshalb keine Leistungsgarantie dar.

Informationen über Produkte anderer Hersteller als IBM wurden von den Herstellern dieser Produkte zur Verfügung gestellt, bzw. aus von ihnen veröffentlichten Ankündigungen oder anderen öffentlich zugänglichen Quellen entnommen. IBM hat diese Produkte nicht getestet und übernimmt im Hinblick auf Produkte anderer Hersteller keine Verantwortung für einwandfreie Funktion, Kompatibilität oder andere Ansprüche. Bei Fragen zur Leistungsfähigkeit von Produkten anderer Hersteller als IBM wenden Sie sich an die Hersteller dieser Produkte.

Die oben genannten Erklärungen bezüglich der Produktstrategien und Absichtserklärungen von IBM stellen die gegenwärtige Absicht der IBM dar, unterliegen Änderungen oder können zurückgenommen werden und repräsentieren nur die Ziele der IBM.

Diese Veröffentlichung enthält Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufes. Diese Beispiele enthalten Namen von Personen, Firmen, Marken oder Produkten. Alle diese Namen sind frei erfunden; Ähnlichkeiten mit tatsächlichen Namen und Adressen sind rein zufällig.

Marken

Die folgenden Namen sind in gewissen Ländern Marken der IBM Corporation:

- AFS
- AIX
- DFS
- IBM
- iSeries
- RS/6000
- SecureWay
- Tivoli
- ViaVoice
- WebSphere

Java und alle Java-basierten Marken sind in gewissen Ländern Marken von Sun Microsystems, Inc.

Microsoft, Windows, Windows NT und das Windows-Logo sind in gewissen Ländern Marken der Microsoft Corporation.

Intel, Intel Inside (Logos), MMX und Pentium sind in gewissen Ländern Marken der Intel Corporation.

UNIX ist in gewissen Ländern eine eingetragene Marke von The Open Group.

Linux ist in gewissen Ländern eine Marke von Linus Torvalds.

Andere Namen von Unternehmen, Produkten und Dienstleistungen können Marken anderer Unternehmen sein.



GC12-3678-00

