

IBM® Distributed Computing Environment Versão 3.2 para
AIX®



Iniciação Rápida

IBM® Distributed Computing Environment Versão 3.2 para
AIX®



Iniciação Rápida

Nota

Antes de usar este documento, leia as informações gerais em “Apêndice D. Avisos” na página 145.

Primeira Edição (Julho de 2001)

Esta edição se aplica à Versão 3.2 do *IBM Distributed Computing Environment para AIX* e a todos os releases e alterações subsequentes até indicação contrária em novas edições ou em novas notícias técnicas.

Solicite as publicações através de seu representante IBM ou da filial IBM que serve a sua localidade. As publicações não estão armazenadas no endereço abaixo.

Seus comentários são bem-vindos à IBM. Envie seus comentários para o seguinte endereço:

Centro Industrial IBM Brasil
Centro de Traduções
Caixa Postal 71
13001-970 Campinas - SP
Brasil

Ao enviar informações para a IBM, você concede à IBM um direito não exclusivo para usar ou distribuir a informação da maneira que a mesma achar apropriada sem incorrer em quaisquer obrigações para com você.

© Copyright International Business Machines Corporation 2001. Todos os direitos reservados.

Índice

Tabelas.	v	Determinação dos Requisitos para Máquinas Clientes DCE	39
Bem-vindo ao DCE 3.2 para AIX	vii	Determinação dos Requisitos para Máquinas de Servidores DCE	43
Convenções Tipográficas e de Teclas	vii	Determinação dos Requisitos para Migração do DCE Anterior para um Servidor de Segurança LDAP	47
<hr/>		Utilitários de Administração DCE.	48
Parte 1. Entendendo o DCE 3.2 para AIX	1	Ambiente de Desenvolvimento de Aplicações	50
Capítulo 1. Visão geral do DCE 3.2 para AIX	3	Localização dos Arquivos Instalados de DCE	50
O que é DCE?	3	A Subárvore /opt/dcelocal	51
Comparação do Registro de Segurança DCE Anterior com o Registro de Segurança DCE Integrado LDAP	5	Diretórios Convencionais do UNIX	51
Conteúdo do Produto	5	Localizações de Arquivos	52
Programas Licenciados do DCE 3.2.	5	Capítulo 3. Instalação, Remoção da Instalação e Migração para o DCE 3.2 para AIX.	55
DCE Versão 3.2 Base Services para AIX	5	Pacotes Instaláveis	55
DCE Versão 3.2 para AIX	9	Software Necessário	58
Aperfeiçoamentos da IBM para o DCE	11	Instalação do DCE 3.2.	63
Adaptação aos Padrões	14	Processo de Software a Interromper	63
Compatibilidade DCE com AIX	14	Execução do Programa de Instalação Fácil	63
Recursos Não Suportados do OSF DCE	18	Instruções Especiais de Instalação	65
Limitações dos Serviços Suportados nas Contas Configuradas que utilizam a Autenticação de Chave Pública.	19	Migração de uma Célula DCE do AIX para o DCE 3.2 para AIX	65
Limitações de Serviços Suportados para Servidores de Segurança LDAP	19	Migração de uma Célula DCE Existente para Explorar a Integração do Registro de Segurança DCE com o LDAP	74
<hr/>		Remoção da instalação do DCE 3.2	75
Parte 2. Planejamento, Instalação, Remoção da Instalação e Migração do DCE 3.2 para AIX	23	Leitura Sugerida	75
Capítulo 2. Planejamento	25	Parte 3. Configuração, Início e Parada do DCE 3.2 para AIX	77
Requisitos do Sistema.	25	Capítulo 4. Configuração dos Servidores e Clientes do DCE 3.2 para AIX	79
Requisitos de Espaço em Disco.	26	Configuração do DCE.	79
Considerações Globais e de Célula	26	Visão Geral da Configuração	79
Questões de Planejamento a Considerar.	26	Comandos Fornecidos pelo Usuário	84
Criação de um Nome de Célula	29	Variáveis de Ambiente	86
O Espaço de Nomes da Célula	32	Configuração Inicial da Célula	87
Planejamento do Controle de Acesso	37	Configuração de Servidores	87
Considerações de Nomenclatura DCE para Internacionalização.	37	Configuração de Clientes.	92
Considerações sobre Cliente e Servidor	39	Configuração Adicional da Célula	102

Configuração de Servidores DTS	102	Uso do SMIT para Iniciar o DCE Imediatamente e no Reinício do Sistema	128
Configuração de um Cliente DTS	104	Alteração de Argumentos Passados para Daemons do DCE no Reinício.	128
Configuração de Servidores CDS Secundários.	105	Parada de Daemons do DCE	129
Configuração das Réplicas dos Servidores de Segurança	106	Capítulo 6. Obtenção de Informações	
Configuração do Global Directory Agent (GDA)	109	Adicionais	131
Configuração de Servidores EMS.	110	Manuais	131
Configuração de Servidores SNMP	111	Informações Online	131
Configuração da Integração de Segurança do DCE 3.2 para AIX.	111	Manuais Online	131
Configuração de Servidores de Auditoria	112	Arquivos de Ajuda	132
Configuração de Servidores de Senha Válida.	113	Impressão e Pedido de Manuais	132
Configuração do Name Service Interface Daemon (NSID)	115	Publicações do IBM DCE	132
Configuração de um Servidor de Mapeamento de Identidade	116	Outras Publicações	132
Configuração do DCE Web Secure para AIX	117	Uso da Documentação do DCE 3.2 para AIX	132
Configuração do DCE Web Secure Usando o SMIT	117	O programa start_dcedoc	132
Configuração do DCE Web Secure a partir de uma Linha de Comandos	118	Exibição de Arquivos de Texto Simples	133
Verificação da Configuração do DCE Web Secure.	119	Exibição da Documentação HTML usando um navegador da Web	134
Remoção de Configuração de Componentes do DCE	121	Impressão dos Manuais PDF	134
Considerações Antes de Remover a Configuração	121	Apêndice A. Documentação Online	135
Remoção de Configuração Dividida.	123	Apêndice B. Configuração Avançada do DCE Web Secure para AIX	139
Étapas para Remoção da Configuração do DCE	123	Configuração de Caminho Autenticado	139
Remoção de Configuração do DCE Web Secure	125	Configuração de Keyfile	139
Capítulo 5. Início e Parada do DCE 3.2 para AIX	127	Resumo da Sintaxe de Configuração Avançada	140
Início dos Daemons do DCE	127	Exemplos de Configuração Avançada	140
Uso da Linha de Comandos para Iniciar Daemons.	127	Apêndice C. Conjuntos de Arquivos Fictícios	143
		Apêndice D. Avisos	145
		Marcas	147
		Índice Remissivo	149

Tabelas

- | | | |
|----|---|----|
| 1. | Conjuntos de arquivos de instalação e software necessário | 59 |
| 2. | Pacotes de Software do DCE. | 64 |

Bem-vindo ao DCE 3.2 para AIX

Este manual descreve o produto IBM Distributed Computing Environment Versão 3.2 para AIX (DCE 3.2 para AIX). Ele inclui informações sobre os componentes do servidor e do cliente.

A “Parte 1. Entendendo o DCE 3.2 para AIX” na página 1 oferece uma visão geral do DCE 3.2 para AIX.

A “Parte 2. Planejamento, Instalação, Remoção da Instalação e Migração do DCE 3.2 para AIX” na página 23 explica como planejar, instalar, remover a instalação e migrar o DCE 3.2 para AIX.

A “Parte 3. Configuração, Início e Parada do DCE 3.2 para AIX” na página 77 explica como configurar e usar o DCE 3.2 para AIX.

Convenções Tipográficas e de Teclas

Este guia usa as seguintes convenções tipográficas:

Negrito

Palavras ou caracteres em **negrito** representam elementos do sistema que devem ser usados literalmente, como comandos, opções e nomes de caminhos.

Itálico Palavras ou caracteres em *itálico* representam valores variáveis que devem ser fornecidos. O tipo *itálico* pode também apresentar um novo termo do DCE.

Largura constante

Exemplos e informações que o sistema exibe aparecem como tipos de letras com largura constante.

[] Colchetes delimitam itens opcionais em descrições de sintaxe e de formato.

{ } Chaves delimitam uma lista na qual deve ser escolhido um item em descrições de sintaxe e de formato.

| Uma barra vertical separa itens em uma lista de opções.

< > Os sinais de menor que e maior que delimitam o nome de uma tecla. Eles também delimitam o nome descritivo de uma variável.

... Reticências indicam que se pode repetir o item precedente uma ou mais vezes.

Este guia usa as seguintes convenções de teclas:

<Ctrl- x> ou \hat{x}

A notação **<Ctrl- x>** ou \hat{x} seguida pelo nome de uma tecla indica uma seqüência de caracteres de controle. Por exemplo, **<Ctrl-C>** significa que se deve manter a tecla de controle pressionada enquanto se pressiona **<C>**.

<Return>

A notação **<Return>** se refere à tecla no terminal indicada pelas palavras Return ou Enter, ou pela seta à esquerda.

Parte 1. Entendendo o DCE 3.2 para AIX

Capítulo 1. Visão geral do DCE 3.2 para AIX

O IBM Distributed Computing Environment Versão 3.2 para AIX (DCE 3.2 para AIX) faz parte da família de produtos IBM Server Series. O DCE 3.2 para AIX é baseado na tecnologia DCE da Open Software Foundation (OSF) (Release 1.2.2).

O que é DCE?

O DCE oferece um ambiente padrão que suporta aplicações distribuídas. Ele representa as tecnologias que foram selecionadas pela OSF e que estão se tornando o padrão corporativo na área de serviços distribuídos.

Uma aplicação desenvolvida para usar o DCE pode ser executada em qualquer ambiente que suporte o padrão DCE da OSF. O DCE possibilita aos desenvolvedores de aplicações oferecer aos usuários acesso seguro a grande variedade de informações e serviços disponíveis em sua rede. O DCE realiza isso ocultando a complexidade do ambiente da rede.

Os serviços de computação distribuída, da forma como são implementados no DCE, compõem uma importante tecnologia de software de base para o desenvolvimento de aplicações distribuídas. O DCE torna a arquitetura de rede subjacente transparente para os desenvolvedores de aplicações. Ele consiste na camada de software entre o sistema operacional e a interface da rede e o programa da aplicação distribuída. O DCE fornece uma variedade de serviços comuns, os quais os usuários necessitam para desenvolver aplicações distribuídas. Estas aplicações incluem serviços de nomes e de horário, e uma interface padrão de chamada de procedimento remoto (remote procedure call - RPC). O DCE oferece um método para os desenvolvedores de aplicações planejarem, desenvolverem e disponibilizarem aplicações distribuídas.

Um grupo de máquinas DCE que opera em conjunto e que é administrado pelo DCE como uma unidade é chamado de *célula*. Por exemplo, imagine uma organização composta de vários departamentos, cada um em um edifício diferente e operando com o seu próprio orçamento. Cada departamento em uma organização como essa teria sua própria célula DCE.

Um ambiente DCE é um grupo de uma ou mais células DCE que podem comunicar-se entre si. Uma célula torna-se parte de um ambiente DCE quando ela obtém acesso a um ou mais serviços globais de diretório nos quais as outras células no ambiente estão registradas.

Se duas células para dois departamentos diferentes são parte de um ambiente DCE, um usuário na célula de um departamento pode acessar recursos na célula do outro departamento. Este acesso em geral é menos freqüente e mais restrito que o acesso aos recursos na célula do próprio usuário.

Um administrador pode configurar uma célula DCE de várias formas, dependendo das exigências dos usuários. Uma célula consiste na rede que conecta dois tipos de nós:

- **Máquinas de usuários DCE (clientes)** são máquinas DCE de uso geral. Elas contêm software que permite que atuem como clientes em todos os serviços DCE.
- **Máquinas de servidores DCE** incluem software especial que permite o fornecimento de um ou mais dos serviços DCE. Cada célula precisa ter no mínimo um dos seguintes servidores para poder funcionar:
 - Cell Directory Server
 - Servidor de Segurança (Security Server)

Outros servidores DCE podem estar presentes em uma determinada célula DCE para fornecer funcionalidade adicional. Por exemplo, um Global Directory Agent (GDA) pode permitir que o servidor de diretório da célula se comunique com servidores de diretório de outras células.

O DCE 3.2 para AIX é uma camada entre o sistema operacional AIX, os serviços de rede e uma aplicação distribuída. O DCE 3.2 para AIX fornece os serviços que permitem a uma aplicação distribuída interagir com vários computadores, sistemas operacionais e redes possivelmente heterogêneos como se fossem um só sistema. O DCE 3.2 para AIX inclui um conjunto de serviços, interfaces de software e ferramentas padrões que suportam a criação, uso e manutenção de aplicações distribuídas em um ambiente de computação diversificado.

O DCE 3.2 para AIX possui a mesma organização do DCE da OSF. A Parte 1 deste manual apresenta o conceito de uma célula DCE e dá um breve resumo de como as diferentes máquinas que participam em um Ambiente de computação Distribuída são organizadas.

O DCE 3.2 para AIX é baseado na base de código do OSF DCE Release 1.2.2 e é projetado para as funções suportadas do sistema operacional AIX. Consulte o *IBM DCE Version 3.2 para AIX: Notas do Release* para uma lista das versões suportadas do sistema operacional AIX.

Comparação do Registro de Segurança DCE Anterior com o Registro de Segurança DCE Integrado LDAP

Um recurso introduzido com o DCE 3.2 para AIX permite ao usuário integrar o Registro de Segurança existente com o LDAP de modo que todos os dados do registro possam ser armazenados em um diretório do LDAP.

Para os fins desta documentação, referências a *DCE anterior* indicam qualquer versão do DCE que não faça uso deste recurso, inclusive o DCE 3.2.

Conteúdo do Produto

O DCE 3.2 para AIX está disponível nos seguintes Programas Licenciados:

- **DCE Versão 3.2 Base Services para AIX**, que inclui os seguintes pacotes:
 - **Serviços de Cliente DCE, Versão 3.2**
 - **SMIT (System Management Interface Tool - ferramenta de interface de gerenciamento de sistemas) DCE, Versão 3.2**
 - **Gerenciamento de Sistema DCE, Versão 3.2**
 - **Biblioteca de APIs X.500 DCE, Versão 3.2**
 - **Ferramentas DCE para Desenvolvedores de Aplicações, Versão 3.2**
 - **Mensagens DCE, Versão 3.2**
 - **Documentação Online DCE, Versão 3.2**
 - **DCE Privacy Level Protection (antes conhecido como a Biblioteca DCE Data Encryption Standard (DES)), Versão 3.2**
- **DCE Versão 3.2 para AIX**, que inclui todos os pacotes encontrados no DCE Versão 3.2 Base Services para AIX, bem como os seguintes pacotes:
 - **DCE Cell Directory Server, Versão 3.2**
 - **DCE Security Server, Versão 3.2**

Programas Licenciados do DCE 3.2

Esta seção apresenta uma descrição dos Programas Licenciados e pacotes dos do DCE 3.2.

DCE Versão 3.2 Base Services para AIX

O Programa Licenciado DCE Versão 3.2 Base Services para AIX fornece suporte para chamadas de procedimento remoto, a funcionalidade de cliente para o serviço de diretório, segurança, hora, troca de mensagens e manutenção da célula. Este pacote também fornece suporte para a integração dos serviços de segurança do DCE à segurança básica do sistema operacional AIX. Como a arquitetura DCE é construída em um modelo baseado em threads, o DCE Base exige uma versão com várias entradas (threadsafe) da biblioteca C do AIX, `libc_r.a`. O sistema operacional AIX inclui a biblioteca

libc_r.a. A administração do DCE inclui ferramentas para configurar uma célula, incluir e excluir usuários em uma célula, incluir servidores e clientes em uma célula, e funções semelhantes.

Serviços de Clientes

Os seguintes serviços de clientes são fornecidos como parte do DCE Versão 3.2 Base Services para AIX:

- A chamada **Remote Procedure Call (RPC)** permite criar e executar aplicações do cliente e aplicações do servidor. O serviço de tempo de execução RPC implementa os protocolos de rede através dos quais o lado do cliente e o lado do servidor de uma aplicação se comunicam.
- A **Biblioteca de Compatibilidade de Threads DCE para AIX** fornece um modelo de programação para a construção de aplicações simultâneas que realizam várias operações ao mesmo tempo. Ela fornece suporte para aplicações multithread (baseadas no POSIX 1003.4a Draft 4) que usam o modelo de threads do DCE. O pacote para AIX inclui a Biblioteca de Compatibilidade de Threads DCE para AIX.
- O suporte a **Ambiente de Programação Multithread** permite que várias threads chamem funções padrões da biblioteca C sem interferirem umas com as outras.
- A função **Distributed Time Service (DTS)** fornece sincronização de horário no ambiente distribuído de rede nos computadores que participam em um Ambiente de Computação Distribuída (Distributed Computing Environment). O DTS sincroniza o horário de um host DCE com a UTC (Coordinated Universal Time - Hora Universal Coordenada), um padrão internacional de hora.
- O **cliente Cell Directory Service (CDS)** fornece a interface, **cdsclerk**, entre aplicações de clientes CDS e servidores CDS. O **cliente básico** também fornece a interface **cdsclerk** e a maior parte da funcionalidade do cliente regular, mas como o **dced** não está em execução em uma máquina de cliente básico, o processamento de nó de extremidade não pode ocorrer.
 - A **Preferência CDS** permite aos administradores especificar uma clearinghouse CDS preferencial da qual um cliente obterá informações do CDS. Este recurso é fornecido para melhorar o desempenho nos clientes CDS dando aos administradores de células a capacidade de especificar uma clearinghouse CDS preferencial da qual um cliente obterá informações do CDS. Isto é útil em situações onde, por exemplo, uma WAN de baixo desempenho conecta várias LANs de alto desempenho, e cada uma das LANs contém uma réplica da clearinghouse CDS. Com este recurso, os administradores podem especificar clearinghouses locais como preferenciais sobre clearinghouses distantes, e os clientes usarão as clearinghouses distantes somente quando as clearinghouses locais não puderem satisfazer aos pedidos.
- O **cliente de Segurança** fornece os seguintes serviços:

- A **Integração de Segurança AIX** coordena os serviços de segurança do sistema operacional base AIX com os serviços de segurança do DCE. Isto permite que um usuário efetue login no AIX e obtenha credenciais DCE ao mesmo tempo. Para obter maiores informações sobre a Integração de Segurança AIX, consulte *IBM DCE Version 3.2 for AIX and Solaris: Administration Guide—Core Components*.
- As **Extensões GSSAPI** são um conjunto de interfaces de programas aplicativos (application program interfaces - APIs) que fornecem para as aplicações não-RPC a capacidade de usar o protocolo de autenticação de segurança do DCE. O administrador do sistema pode usar GSSAPI para estabelecer credenciais ou extrair Extended Privilege Attribute Certificates (EPACs) para uma aplicação não-RPC.
- Os **Atributos de Registro Estendidos** (Extended Registry Attributes - ERAs) expandem os atributos estáticos de registro de Usuário Principal, Grupo e Conta para um conjunto dinâmico de atributos de registro que podem ser personalizados para uma célula.
- O **Serviço de Auditoria** realiza o registro em log dos registros de auditoria com base em critérios especificados. O Serviço de Auditoria tem três componentes básicos:
 - **Interfaces de Programação de Aplicações (Application Programming Interfaces - APIs)** fornecem as funções que são usadas para detectar e registrar eventos críticos quando o servidor atende a um cliente. Elas também são usadas para criar ferramentas que examinam e analisam os registros de eventos de auditoria.
 - O **Daemon de Auditoria** mantém os filtros e os logs de auditoria.
 - As **Interfaces de Gerenciamento de Auditoria** permitem especificar como o Daemon de Auditoria irá filtrar a gravação de Eventos de Auditoria. Estas interfaces estão disponíveis a partir do Programa de Controle DCE (**dcecp**).
- O **Servidor de Senha Válida Aprimorado** aumenta as capacidades do servidor de senha válida de releases anteriores do DCE. O servidor melhorado permite controlar as seguintes características das senhas de usuários:
 - Composição da senha
 - Tempo de uso da senha
 - Histórico e reutilização da senha
 - Dicionários de senhas e regras definidas pelo usuário
- O **DCE Web Secure** fornece credenciais DCE aos programas CGI. O DCE Web Secure deve ser instalado e configurado em uma estação de trabalho que tenha um cliente DCE e um servidor Web iPlanet FastTrack 4.1, iPlanet Enterprise 4.0 ou iPlanet Enterprise 4.1. O DCE Web Secure também suporta os servidores Web suportados pelo DCE 3.1. O DCE Web Secure para AIX pode ser configurado usando o SMIT.

DCE System Management Interface Tool (SMIT)

O SMIT para DCE permite realizar tarefas de gerenciamento de sistemas DCE usando o SMIT, **smitty** (uma versão TTY do SMIT) ou comandos DCE. É preciso instalar as opções de SMIT DCE antes que se possa acessar os menus do SMIT para DCE. O SMIT usa menus interativos para orientar os usuários em várias tarefas de gerenciamento do sistema.

DCE System Management

O DCE System Management fornece três ferramentas de gerenciamento: DCE Event Management Service (EMS), o Subagente DCE Simple Network Management Protocol (SNMP) e o DCE Web Administration.

- O **EMS** fornece suporte a eventos assíncronos para aplicações baseadas em DCE. O DCE EMS gerencia serviços de eventos em uma célula DCE. O EMS consiste em duas partes — o servidor **emspd** (daemon EMS) e APIs para acessar serviços de eventos através de uma interface aos fornecedores, consumidores, e administração do serviço de eventos para uso por clientes EMS. Para obter maiores informações sobre o EMS, consulte o *IBM DCE Version 3.2 for AIX and Solaris: Administration Guide—Core Components*.
- O **Subagente SNMP** fornece suporte o gerenciamento da rede no ambiente TCP/IP para monitorar recursos e serviços DCE. Os administradores do sistema e programadores de aplicações de gerenciamento do sistema podem usar o SNMP para monitorar o ambiente DCE. Isto permite que eles se concentrem em tornar seus recursos e serviços mais gerenciáveis. Para obter maiores informações sobre o SNMP, consulte o *IBM DCE Version 3.2 for AIX and Solaris: Application Development Guide—Core Components*.
- **DCE Web Administration** fornece um programa CGI que os administradores podem usar para gerenciar usuários, grupos, organizações e permissões do DCE. O programa DCE pode ser acessado por um navegador Web em:

```
http://<nome_do_servidor>/dceweb
```

onde <nome_do_servidor> é o nome do servidor onde o DCE Web Secure foi instalado e configurado. Este conjunto de arquivos exige a instalação e configuração do conjunto de arquivos do DCE Web Secure.

Biblioteca DCE X.500 API

A Biblioteca DCE X.500 API fornece interfaces de programação de aplicações para o espaço de nomes do CDS. Uma biblioteca de funções para acesso aos Serviços de Diretório está disponível.

Ferramentas DCE para Desenvolvedores de Aplicações

As Ferramentas DCE para Desenvolvedores de Aplicações (dce.tools) incluem as seguintes ferramentas para suporte ao desenvolvimento de aplicações e administração DCE:

- A ferramenta de Linguagem de Definição de Interface consiste em uma linguagem (e seu compilador) que suporta o desenvolvimento de aplicações distribuídas seguindo o modelo de cliente e servidor. Ela gera automaticamente código que transforma chamadas de procedimento em mensagens de rede.
- O compilador **sams** gera arquivos que podem ser usados para incluir suporte para troca de mensagens e manutenção a aplicações DCE.

Mensagens DCE

O pacote Mensagens inclui versões de menus e mensagens de erro traduzidas para idiomas diferentes do inglês.

Documentação Online

A Documentação Online para o DCE 3.2 para AIX fornece o conjunto da documentação IBM nos seguintes formatos:

- HTML
- PDF
- Texto simples

Para obter maiores informações sobre esta documentação, consulte “Capítulo 6. Obtenção de Informações Adicionais” na página 131.

DCE Privacy Level Protection

O DCE Privacy Level Protection (**dce.priv.rte**), antes conhecida como a Biblioteca Data Encryption Standard (DES), fornece uma interface de programação que permite a criptografia de dados de aplicações RPC. O recurso **dce.priv.rte** usa algoritmos do Data Encryption Standard (DES) que são parte do DCE Base Services para AIX. Este recurso inclui suporte a Criptografia de Mascaramento de Dados do Usuário, que antes era empacotado separadamente.

DCE Versão 3.2 para AIX

O Programa Licenciado DCE Versão 3.2 para AIX inclui todos os pacotes encontrados no DCE Versão 3.2 Base Services para AIX, bem como os seguintes pacotes:

DCE Cell Directory Server

O DCE Cell Directory Server é um repositório central para informações sobre recursos no sistema distribuído. Recursos típicos são usuários, máquinas e serviços baseados em RPC. As informações consistem no nome do recurso e seus atributos associados. Atributos típicos incluem o diretório pessoal de um usuário ou a localização de um servidor baseado em RPC.

- O Serviço de Diretório consiste no **Cell Directory Server (CDS)** e do **Global Directory Agent (GDA)**. O CDS gerencia um banco de dados de informações sobre os recursos em um grupo de máquinas denominado uma célula DCE. O CDS também fornece nomenclatura independente de

localização para servidores. O GDA permite comunicações entre células localizando células que foram registradas no ambiente global de nomes.

- A **Integração do GDA com o LDAP** é uma extensão do GDA que permite a resolução de nomes de células externas que não sejam do estilo Domain Name System (DNS). Com diretórios de X.500 e quaisquer diretórios que suportem o protocolo LDAP, o administrador pode estabelecer comunicação entre células. Para obter maiores informações sobre o LDAP, consulte o *IBM DCE Version 3.2 for AIX and Solaris: Administration Guide—Core Components*.

Servidor de Segurança DCE para AIX

O Servidor de Segurança DCE para AIX permite comunicações protegidas e acesso controlado a recursos. Ele fornece um conjunto das seguintes funções relacionadas a segurança:

- O **Serviço de Autenticação** permite a dois processos em máquinas diferentes certificarem-se das identidades um do outro.
- A **Comunicação Protegida** integra a DCE Remote Procedure Call (RPC) com o Serviço de Segurança para proteger a comunicação.
- A **Autorização** controla o acesso aos recursos comparando as credenciais conferidas a um usuário pelo Serviço de Privilégio com os direitos ao recurso. A Lista de Controle de Acesso do recurso especifica os direitos ao recurso.
- O **Servidor de Privilégio** faz as seguintes verificações uma vez que a identidade tenha sido estabelecida: O usuário está autorizado a acessar um recurso? Que permissões são exigidas? O usuário tem essas permissões? O uso de RPC Autenticada em geral envolve autenticação e autorização para o usuário.
- A **Funcionalidade de Lista de controle de Acesso (Access Control List - ACL)** lista os usuários que estão autorizados a acessar um dado recurso. Uma API de ACL permite aos programadores manipularem ACLs. Os comandos `dcecp acl` ou o comando `acl_edit` permite aos usuários modificarem ACLs associadas a recursos pertencentes a eles. Estes comandos também permitem aos usuários modificarem a quem (usuário ou grupo) o acesso é concedido e que permissões específicas são dadas.
- A **Funcionalidade de Login** inicializa o ambiente de segurança DCE de um usuário autenticando este ao Serviço de Segurança por meio da senha do usuário. A funcionalidade de Login em seguida retorna credenciais de segurança que autenticam o usuário para os serviços distribuídos necessários.
- O **login de autorização da Chave Pública** permite que um usuário obtenha credenciais DCE iniciais usando um certificado digital X.509v3 e seu par de chave pública associado para provar a identidade do usuário. Este recurso é uma extensão do protocolo de login de chave pública do OSF DCE 1.2.2 baseado no OSF RFC 68.4 (draft 7). Esta implementação exige a infraestrutura de chave pública (PKI) Entrust.

- A **Replicação de Segurança** permite que o Banco de Dados do Registro Principal seja replicado para um ou mais Bancos de Dados de Registro secundário. Os comandos `dcecp registry` ou o comando `sec_admin` são as interfaces usadas para exibir e manipular o estado das réplicas principais e secundárias.
- O **Serviço de Mapeamento de Identidade (Identity Mapping Server - IDMS)** é usado pelo Serviço de Autenticação para determinar a identidade de um usuário DCE quando este efetua login com o protocolo de autenticação de certificado de chave pública. O Serviço de Mapeamento de Identidade mapeia o nome de um usuário em um certificado de chave pública para um nome de usuário principal DCE.
- O **Registro de Segurança e a Integração LDAP** movem o Registro de Segurança anterior para um diretório do LDAP. Isto permite aos usuários que tenham LDAP em seus ambientes explorar de forma mais ampla o LDAP, permitindo que eles movam seus usuários DCE para um diretório do LDAP. Todas as interfaces existentes são suportadas.

Aperfeiçoamentos da IBM para o DCE

Os seguintes serviços e comandos incluídos nos Programas Licenciados do DCE 3.2 listados anteriormente são melhorias e extensões da IBM à implementação do DCE no AIX:

- **Serviços Adicionais:**
 - **Funcionalidade de Criptografia de Mascaramento de Dados de Usuário**
 - **Servidor de Senha Válida Aprimorado**
 - **Preferência CDS**
 - **DCE Web Secure**
 - **Simple Network Management Protocol (SNMP)**
 - **Event Management Service (EMS)**
 - **Integração de Segurança AIX**
 - **Login de Autorização da Chave Pública**
 - **Integração GDA com LDAP**
 - **Servidor de Mapeamento de Identidade (Identity Mapping Server - IDMS)**
 - **Cliente Básico**
 - **Integração do Registro de Segurança DCE com o LDAP**
 - **Melhorias GSSAPI**
 - **Confirmação da Certificação Entrust 5.0**
- **Comandos Adicionais:**
 - Comandos de Configuração:

Notas:

1. Os seguintes comandos usam um formato de comando diferente do formato do comando `config` usado no AIX DCE V2.1; entretanto, o DCE 3.2 ainda suporta o formato do comando `config` usado anteriormente.
2. Os seguintes comandos não são compatíveis com os comandos `dcecp` **host configure**, **host start**, **host stop** e **host unconfigure**.

chpsite

Atualiza o arquivo **pe_site**, que contém os endereços dos servidores de segurança utilizados.

clean_up.dce

Limpa arquivos do banco de dados que podem ser recriados, e arquivos de credenciais. Use este comando se surgirem problemas ao tentar iniciar o DCE.

config.dce

Configura e inicia componentes do DCE. Este comando permite uma configuração dividida de clientes. A configuração administrativa e a configuração local podem ser realizadas separadamente. Consulte "Configuração Adicional da Célula" na página 102 para obter maiores informações.

kerberos.dce

Cria os usuários principais do host, os usuários principais de FTP e entradas na tabela de chaves usadas para suportar os comandos de Segurança Remota.

migrate.dce

Migra dados da configuração do DCE de releases anteriores para uso com o release atual. Não há necessidade de configurar novamente quando se instala um novo release do DCE. Consulte "Migração de uma Célula DCE do AIX para o DCE 3.2 para AIX" na página 65 para obter maiores informações.

mkdceweb

Configura o DCE Web Secure e o DCE Web Administration em um servidor Web Netscape FastTrack ou Netscape Enterprise ou em um servidor Web iPlanet FastTrack ou iPlanet Enterprise.

mkreg.dce

Inclui informações sobre uma célula DCE no espaço de nomes DOMAIN.

rmkceweb

Remove a configuração do DCE Web Secure e do DCE Web

Administration de um servidor Web Netscape FastTrack ou Netscape Enterprise ou em um servidor Web iPlanet FastTrack ou iPlanet Enterprise.

rmreg.dce

Remove informações sobre uma célula DCE do espaço de nomes DOMAIN.

show.cfg

Exibe a configuração DCE ou DFS do host local ou ambas as configurações. As opções **dce** e **dfs** permitem a exibição de informações do DCE.

start.dce

Inicia os componentes do DCE configurados. Este comando certifica-se de que todos os componentes iniciem na ordem correta.

stop.dce

Pára os componentes do DCE configurados. Este comando certifica-se de que todos os componentes parem na ordem correta.

unconfig.dce

Remove a configuração de componentes do DCE. Este comando prevê a remoção de uma configuração dividida, portanto a remoção da configuração administrativa e a da configuração local podem ser realizadas separadamente. Consulte "Configuração Adicional da Célula" na página 102 para obter maiores informações.

– Comandos CDS:

cdsdel Exclui recursivamente o espaço de nomes de uma célula.

cdsli Lista recursivamente o espaço de nomes de uma célula.

– Comandos RPC:

rpcprotseqs

Determina o protocolo suportado em um dado host.

rpcresolve

Resolve recursivamente os elementos de uma entrada do espaço de nomes.

– Comandos de Segurança:

rmxcred

Elimina tickets expirados do diretório de credenciais.

Adaptação aos Padrões

- O DCE 3.2 para AIX suporta os padrões relacionados abaixo, mas não pode afirmar a adaptação a tais padrões porque alguns deles não estão em seu formato definitivo ou porque não existem testes de adaptação.

Threads

- POSIX 1003.4a, draft 4
- AES/Distributed Computing - Threads

RPC AES/Distributed Computing - Remote Procedure Call

Segurança

- Autenticação
 - Kerberos Versão 5, draft 4
- Autorização
 - POSIX 1003.6, draft 12 (acls)
- AES/Distributed Computing - Security
- GSSAPI, incluindo Internet RFC 1964

Diretório

- AES/Distributed Computing - Directory Services
- X/OPEN-X.400 API Association XDS API Draft 6

União de Transporte

- RFC 1006, TPO-to-TCP

Horário

- RFC 1129, NTP
- AES/Distributed Computing - Directory Services

Compatibilidade DCE com AIX

Esta seção descreve a compatibilidade do DCE para AIX com as versões suportadas do AIX para o RISC System/6000.

- O comando do AIX **man** não é suportado para exibir a documentação de referência atual do DCE. Entretanto, **dceman**, o qual exibe uma única página de manual para comandos e sub-rotinas do DCE, será fornecido e poderá simular o comando AIX **man**. Quando o pacote de documentação é instalado, **dceman** é ligado ao diretório **/usr/bin**, juntamente com **asciiview** e **start_dcedoc**. Para solicitar o comando **dceman**, digite:

```
dceman -lang locale comando_dce
```

onde *comando_dce* pode ser qualquer comando ou sub-rotina documentados no *IBM DCE Version 3.2 for AIX and Solaris: Administration Commands Reference* ou *IBM DCE Version 3.2 for AIX and Solaris: Application Development Reference*. O parâmetro `-lang` permite que o usuário exiba comandos ou sub-rotinas do DCE em qualquer idioma. O *locale* pode ser substituído por um dos seguintes nomes de locale:

Notas:

1. Nem todos os manuais são traduzidos para todos os idiomas. Os comandos e sub-rotinas documentados em manuais não traduzidos serão exibidos em inglês.
2. Qualquer valor especificado para a opção `-lang` que não seja um locale válido fará com que a documentação seja exibida em inglês para o `comando_dce`.

en_US locale Inglês

ja_JP locale Japonês (EUC)

Ja_JP locale Japonês (PC Kanji)

JA_JP locale Japonês (UTF-8)

ko_KR
locale Coreano

KO_KR
locale Coreano (UTF-8)

pt_BR locale Português do Brasil

PT_BR
locale Português do Brasil (UTF-8)

zh_TW
locale Chinês Simplificado (EUC)

Zh_TW
locale Chinês Simplificado (GBK)

ZH_TW
locale Chinês Simplificado (UTF-8)

- O AIX Network Computing System (NCS) versão 1.5.1 e o DCE Base Services para AIX podem coexistir no mesmo sistema porque o processo **dced** do DCE fornece a funcionalidade que as aplicações do NCS esperam do comando **llbd**.
- Os serviços de segurança de operação básica do AIX foram integrados com os **Serviços de Segurança do DCE**. Esta integração apresenta ao usuário final típico uma imagem de um sistema único em lugar de imagens separadas de um sistema UNIX local e de um sistema DCE remoto. Há algumas limitações à integração, explicadas totalmente no *IBM DCE Version 3.2 for AIX and Solaris: Administration Guide—Core Components*; entretanto, a maioria dos usuários será capaz de adquirir credenciais DCE através de comandos do AIX (como **login** e **su**), de alterar suas senhas DCE através do comando do AIX **passwd**, e de recuperar informações de tipo Unix do registro do DCE através das rotinas padrões do AIX **libc.a**, **getpwnam()**,

getpwuid(), **getgrnam()** e **getgrgid()**. As rotinas mais gerais, **getpwent()** e **getgrent()**, não têm conhecimento do DCE atualmente.

- **Nota Importante sobre Alteração de Senhas:** as operações de senha do AIX são dirigidas para o registro definido pelo atributo de usuário **registry** ou, na ausência de uma definição do atributo **registry**, para o registro definido pela variável de ambiente **AUTHSTATE**.

As operações de senha não são dirigidas para ambos os registros, o local e o do DCE.

A alteração de senhas para um cliente somente DCE é feita através de **dcecp**. A alteração de senhas (do DCE e local) para um usuário sincronizado (um que está definido tanto localmente quanto no DCE) pode ser feita com o comando do AIX **passwd** em um procedimento de duas etapas:

```
$ AUTHSTATE=senha DCE
$ AUTHSTATE=senha de compat
```

As senhas devem ser mantidas sincronizadas para usuários sincronizados, caso contrário uma das autenticações do DCE ou local, falhará. Além disso, se um usuário existir localmente em mais de uma máquina, a senha local precisa ser sincronizada em todas as máquinas.

Os comandos de segurança DCE não integrados tais como **dce_login** (para efetuar login no DCE) e **dcecp** para alteração de senhas e consultas ao registro do DCE ainda estão disponíveis. É claro que o acesso local é pré-requisito para o uso destes comandos.

O administrador local deve definir o sistema para habilitar o DCE para integração de segurança do AIX; instruções completas de configuração são encontradas no *IBM DCE Version 3.2 for AIX and Solaris: Administration Guide*.

- As **ACLs do DCE** diferem das ACLs do AIX. O DCE tem seus próprios comandos, **acl_edit** e **dcecp**, para manipular ACLS de DCE em objetos no espaço de nomes do DCE. Os comandos do AIX (**acledit**, **aclget** e **aclput**), não funcionam em objetos no espaço de nomes do DCE, incluindo arquivos e diretórios no espaço de arquivos DFS do DCE. Comandos do AIX que fazem backup e restauração de dados não mantêm ACLs do DCE em diretórios e arquivos LFS do DCE. Use a funcionalidade de backup de DFS do DCE para fazer backup e restauração de conjuntos de arquivos LFS do DCE.
- O comando de depuração do AIX **dbx** tem a capacidade de reconhecer e depurar threads múltiplas. Para obter maiores informações sobre o depurador, consulte o *IBM DCE Version 3.2 for AIX and Solaris: Application Development Guide—Core Components*.
- O texto a seguir discute a compatibilidade entre o C++ e o DCE.

- O uso do C++ com o DCE exige algumas considerações, mas em geral nada além do que se exige para usar uma biblioteca baseada em C com o C++. O fator principal é usar a versão correta de **xlC**. O DCE exige no mínimo o **xlC** versão 3.1.3 para fazer a ligação com as bibliotecas do DCE.

Quando o DCE é instalado, ele cria uma ligação de **xlC_r4** para **xlC**. Isto deve ser usado ao compilar e ligar aplicações DCE. Este nome determina a estância no arquivo **/etc/xlC.cfg** que é usada para controlar a configuração do compilador. O uso da versão incorreta ou do nome ligado incorreto do compilador pode levar a problemas na compilação, ligação e tempo de execução.

- As exceções do DCE são separadas das exceções fornecidas pela especificação da linguagem C++. A principal limitação ao uso de exceções DCE em programas C++ é que quando uma exceção de DCE é indicada, os destruidores não serão chamados quando a pilha for desmontada. O programador deve certificar-se de que os objetos sejam liberados explicitamente quando exceções DCE forem manipuladas. Isto pode eliminar o uso de objetos alocados automaticamente em segmentos do código de aplicação.
- Assim como para quaisquer funções de C chamadas do C++, certifique-se de incluir arquivos de cabeçalho DCE em declarações C externas. Isto assegura que a ligação C++ examine os nomes C não misturados, e não os nomes C++.

Em C, a memória em geral é alocada usando **malloc**. Em C++, a memória é alocada usando novo *tipo_de_objeto*. O DCE inclui **rpc_ss_allocate** para dados voláteis que precisam ser liberados pelo sistema após uma rpc retornar. É preciso ter cuidado para certificar-se de que a memória alocada por um método seja sempre liberada usando a rotina correspondente.

Assim como com qualquer biblioteca C usada no C++, pode ser difícil manter uma arquitetura orientada ao objeto *puro*. Em muitos casos, os componentes no DCE são corretamente baseados em objetos no projeto. Entretanto, como a maioria das partes do DCE são projetadas para trabalharem em conjunto, elas muitas vezes passam estruturas de dados entre funções muitas vezes não relacionadas. Por exemplo, um manipulador de login é um tipo de dados obscuro, que possui um núcleo com muitas funções bastante relacionadas para gerenciar e manter o contexto de login. Enquanto por um lado isto é, adequado para agrupar os dados e funções como um objeto, por outro o manipulador deverá ser transmitido, implicitamente ou explicitamente, para a maioria dos objetos que possam ser criados. Como não é correto expor o valor de um dado dentro de um objeto, um design sofisticado deve ser estudado (possivelmente um manipulador ou objeto substituto).

- O AIX 4.3.x não suporta o Cset 3.1.4. Se estiver compilando uma aplicação C++ no AIX 4.3.x, será preciso usar o compilador C e C++ do IBM para o AIX v3.6, o qual suporta o AIX 4.1.4, 4.2.x e 4.3.x.
- Aplicações construídas usando o compilador VACPP 5.0 do AIX são suportadas pelo DCE 3.2 em execução no kernel de 32 bits do AIX 5.1.

Recursos Não Suportados do OSF DCE

As diferenças estão agrupadas em seções por tipo. Cada seção é subdividida em categorias funcionais, que correspondem a serviços específicos do DCE (tais como configuração, segurança e CDS).

Serviços Não Suportados:

- Segurança:
 - Confiança Transitiva em uma hierarquia de células
 - A API de Gerenciamento de Certificado de Chave Pública.
 - O servidor de Armazenamento de Chave Privada.
 - Login de chave pública usando o protocolo do OSF DCE 1.2.2 foi substituído pelo protocolo de login de autorização da chave pública. Entretanto, o servidor de segurança ainda pode processar pedidos de login de outros clientes DCE que suportam o protocolo de login de chave pública do OSF DCE 1.2.2.
- Diretório:
 - Células Hierárquicas.
 - cdsalias create, cdsalias connect.
 - Serviços Globais de Relatório (Global Directory Services - GDS) não é fornecido neste release. Entretanto, o GDS pode existir na mesma célula e ser usado para comunicações entre células, se for fornecido por outro fornecedor ou produto.
- dcecp:
 - **host configure**—Configura um host na célula como um cliente ou servidor.
 - **host unconfigure**—Remove o host dos bancos de dados de nome e de segurança.
 - **host start**—Inicia o DCE no host especificado.
 - **host stop**—Pára o DCE no host especificado.

Comandos Não Suportados:

- CDS:
 - catraverse
 - cds_dbdump

- cdsd_diag
- cdsbrowser
- Configuração:

O script **dce_config** foi substituído por outros comandos de configuração e por uma interface do SMIT. Consulte o *IBM DCE Version 3.2 for AIX and Solaris: Administration Commands Reference* para obter maiores informações.
- Segurança:

Os comandos **sec_salvage_db**, **rlogin**, **rlogind**, **rsh** e **rshd** fornecidos pela OSF.
- Serviço de Horário Distribuído:

O comando **dtss-graph** , o qual converte o rastreamento de sincronismo para PostScript.

Limitações dos Serviços Suportados nas Contas Configuradas que utilizam a Autenticação de Chave Pública

Há várias limitações para contas configuradas para usar autenticação de chave pública. Elas incluem:

- Contas de Chave Pública não podem usar o Servidor de Senha Válida.
- A API de gerenciamento de chave somente deve ser usada por aplicações que usam o protocolo de autenticação de chave de segredo compartilhado. Aplicações que usam contas de chave pública devem usar o protocolo usuário a usuário.
- Quando usar GSSAPI, o administrador DCE deve configurar uma conta no banco de dados do registro DCE para o iniciador e o aceitador. As seguintes restrições se aplicam à conta para o aceitador:
 - A conta para o aceitador deve ser configurada para usar uma chave em um arquivo keytab como a senha da conta.
 - A conta para o aceitador não pode ser configurada para usar o protocolo usuário a usuário.
 - A conta para o aceitador não pode ser configurada para usar o protocolo de autenticação de chave pública.

Nenhuma restrição se aplica à conta para o iniciador.

Limitações de Serviços Suportados para Servidores de Segurança LDAP

Com a exceção de armazenar o registro de segurança em uma segurança do LDAP, os servidores de segurança LDAP operam de modo semelhante aos servidores de segurança anteriores. Portanto, a maioria dos mesmos comandos são usados para administrar servidores de segurança LDAP. Entretanto, há

umas poucas funções de segurança anteriores que não são suportadas pelos servidores de segurança LDAP. A lista a seguir relaciona esses recursos não suportados e limitações:

- Quando se emite o comando **sec_admin -s** em um servidor de segurança anterior, pode-se fornecer o nome da réplica como ele aparece na lista de réplicas. Os servidores de segurança LDAP não suportam este recurso. Entretanto, pode-se continuar a fornecer o nome da célula, o nome global ou o endereço de rede do host. Para obter maiores informações sobre o comando **sec_admin**, consulte o *IBM DCE Version 3.2 for AIX and Solaris: Administration Commands Reference*.
- Ao contrário dos servidores de segurança anteriores, os servidores de segurança LDAP não suportam ACLs de contêiner a menos que o objeto contêiner seja criado pelo DCE. ACLs de contêiner são significativas somente quando o DCE cria diretórios. Se atributos de DCE forem conectados a objetos LDAP existentes, as ACLs do pai serão ignorados. Para obter maiores informações sobre ACLs de contêiner em servidores de segurança anteriores, consulte o *IBM DCE Version 3.2 for AIX and Solaris: Administration Guide—Core Components*.
- O LDAP não suporta aliases DCE. Um alias é um nome alternativo para um nome principal.
- O DCE anterior permite que usuários principais, grupos e orgs sejam renomeados usando **dcecp** ou **rgy_edit**, ou usando a API **sec_rgy_pgo_rename**. Esta funcionalidade não é suportada após os dados de segurança serem migrados para o LDAP.

Se o servidor de segurança principal estiver executando o DCE 3.2 e detectar um servidor de migração LDAP configurado na célula, estes comandos serão rejeitados.

Se o servidor de segurança principal não estiver executando o DCE 3.2 e um comando for emitido para renomear um usuário principal, grupo ou org, as réplicas LDAP indicarão que realizaram a função, embora não o tenham feito. Isto evita que o servidor de segurança principal fique tentando continuamente realizar a atualização. Entretanto, o banco de dados anterior e o banco de dados LDAP terão dados inconsistentes.

- Se objetos DCE estiverem localizados em várias subárvores, comandos de catálogo **dcecp** pesquisarão somente a subárvore padrão do DCE nessa região. Se os objetos DCE estiverem em subárvores diferentes, use pesquisas LDAP para funções de catálogo.
- É altamente recomendável usar somente nomes que ignorem maiúsculas e minúsculas para regiões DCE, usuários principais, grupos e organizações. O motivo é que alguns servidores LDAP (tais como o SecureWay LDAP) convertem qualquer nome para caixa única ao processar o nome em um DN ou em uma ACL. A conversão de nomes para caixa única pode causar resultados incorretos com algumas operações de LDAP. Por exemplo, não se pode ter um nome principal armazenado como **joe_programmer** e outro

armazenado como JOE_PROGRAMMER porque o LDAP lerá ambos como joe_programmer e os tratará como o mesmo nome principal.

Parte 2. Planejamento, Instalação, Remoção da Instalação e Migração do DCE 3.2 para AIX

Capítulo 2. Planejamento

Requisitos do Sistema

Todo o conteúdo no produto DCE 3.2 para AIX exige o release de varejo do IBM AIX Versão 4.3.3 ou o modo do kernel de 32 bits do IBM AIX Versão 5.1. Consulte o **README** para atualizações da listagem de versões suportadas do AIX. Consulte o *IBM DCE Version 3.2 para AIX: Notas do Release* para instruções sobre acesso ao **README**.

Além dos requisitos do sistema operacional, atualizações adicionais do AIX podem ser necessárias. O texto a seguir descreve as atualizações de software do AIX exigidas pelos seguintes conjuntos de arquivos do DCE:

- **dce.client.rte.threads** exige:
 - Em sistemas AIX 4.3.3:
 - bos.adt.libpthread 4.3.3.0**
 - bos.rte 4.3.3.0**
 - bos.rte.libc 4.3.3.0**
 - Em sistemas AIX 5.1:
 - bos.adt.libpthread 5.1.0.0**
 - bos.rte 5.1.0.0**
 - bos.rte.libc 5.1.0.0**
- **dce.client.rte** exige:
 - Em sistemas AIX 4.3.3:
 - xlC.rte 4.0.2.0**
 - bos.net.tcp.client 4.3.3.0**
 - bos.adt.lib 4.3.3.0**
 - Em sistemas AIX 5.1:
 - xlC.rte 5.0.2.0**
 - bos.net.tcp.client 5.1.0.0**
 - bos.adt.lib 5.1.0.0**
- **dce.tools.appdev.adt** exige:
 - Em sistemas AIX 4.3.3:
 - bos.adt.syscalls 4.3.3.0**
 - bos.adt.include 4.3.3.0**
 - Em sistemas AIX 5.1:
 - bos.adt.syscalls 5.1.0.0**

bos.adt.include 5.1.0.0

Notas:

1. Somente o modo de kernel de 32 bits do sistema operacional AIX 5.1 é suportado pelo DCE 3.2.
2. Após instalar qualquer das atualizações, é preciso reinicializar o sistema. Esta reinicialização deve ocorrer antes de se configurar ou reiniciar o DFS.

Requisitos de Espaço em Disco

Consulte o arquivo **README** para os requisitos de espaço em disco dos Programas Licenciados. Note que os tamanhos listados são aproximados.

Considerações Globais e de Célula

O propósito desta seção é auxiliar no planejamento para a instalação e configuração do DCE. O DCE fornece o SMIT e utilitários de configuração para auxiliá-lo. “Capítulo 3. Instalação, Remoção da Instalação e Migração para o DCE 3.2 para AIX” na página 55 e “Configuração do DCE” na página 79 descrevem o processo de configuração, incluindo a instalação de arquivos executáveis, definição de uma célula DCE e configuração de servidores e clientes.

Esta seção discute os seguintes tópicos:

- “Questões de Planejamento a Considerar”
- “Criação de um Nome de Célula” na página 29
- “O Espaço de Nomes da Célula” na página 32
- “Planejamento do Controle de Acesso” na página 37
- “Considerações de Nomenclatura DCE para Internacionalização” na página 37

Questões de Planejamento a Considerar

Nota: As informações nesta seção são pertinentes ao DCE anterior ou a um ambiente onde o recurso de Integração do Registro de Segurança DCE com o LDAP está sendo considerado. Para considerações ampliadas sobre o recurso de Integração do Registro de Segurança DCE com o LDAP, consulte o *IBM DCE Version 3.2 for AIX and Solaris: DCE Security Registry and LDAP Integration Guide*.

É preciso considerar várias questões ao planejar um sistema distribuído.

Lembre-se das seguintes considerações globais ao planejar para o DCE:

- Quanto você acha que seu ambiente crescerá nos próximos anos? Você antecipa uma expansão rápida ou relativamente lenta de sua rede?

Se você acredita que seu ambiente crescerá rapidamente, considere a definição de várias células representando unidades menores de sua organização. Essas células menores podem ser gerenciadas conforme a rede se expanda. Conforme explicado anteriormente, os membros de cada célula compartilham um propósito comum, e a célula é uma unidade de administração e de segurança. Se você antecipar uma expansão lenta da rede, é possível estabelecer uma ou mais células com base na organização existente atualmente. Considere quantos administradores será preciso para manter a célula DCE, com base no crescimento futuro antecipado.

- Quanta atualização das informações é necessária? Os usuários da rede principalmente examinam as informações, ou eles criam e alteram informações em suas estações de trabalhos?

Se as informações são alteradas com freqüência e os usuários na rede dependem da exatidão dessas informações, é preciso considerar quanto se pode confiar na replicação. É melhor acessar uma fonte central de informações para dados que mudam freqüentemente. Se os usuários examinam as informações, mas não precisam alterar as informações compartilhadas com outros usuários, pode-se confiar mais em dados replicados.

- Os dados mais importantes são os mais disponíveis? Você fez planos para replicar esses dados?

O CDS e o serviço de Segurança mantêm cópias principais de seus respectivos bancos de dados. Cada diretório do CDS pode ser replicado separadamente. O Serviço de Segurança suporta a replicação de todo o banco de dados do registro. Como outros componentes dependem das informações gerenciadas pelo Serviço de Segurança e partes do espaço de nomes CDS, esses dados precisam estar disponíveis durante todo o tempo. For exemplo, a cadeia especial de caracteres `/.` (o root da célula) é armazenada no CDS e deve estar sempre disponível.

Lembre-se que, se por um lado a replicação de dados melhora a disponibilidade, por outro há um custo em termos de desempenho e esforço de administração exigido.

- Se a rede tiver um gateway, os servidores estão localizados no mesmo lado do gateway que os clientes que dependem desses servidores?

Os servidores CDS transmitem mensagens a intervalos regulares para anunciar sua existência aos clientes CDS na rede. Os clientes adquirem mais informações sobre os servidores interceptando esses anúncios. A colocação dos servidores e clientes que deles dependem no mesmo lado do gateway facilita atualizações eficientes das informações e uma resposta rápida aos pedidos dos clientes. Administração adicional é necessária se houver dependência de servidores que não estejam disponíveis através do protocolo de anúncio, o qual é efetivo somente em uma rede local.

Em uma LAN que não tiver servidores CDS, o proxy dos anunciantes transmitirá os endereços de servidores CDS. Isto significa que os clientes

não precisam saber o endereço de um servidor CDS no momento da configuração. O proxy do anunciante transmitirá o endereço do servidor CDS com o qual foi configurado. Endereços de servidores CDS adicionais podem ser incluídos usando os comandos **cdscp define server** ou **dcecp cdscache create**.

Leve em consideração a velocidade e o custo das ligações se estiver administrando uma célula que inclua usuários em diferentes localizações geográficas. Pode ser interessante manter mais informações localmente para reduzir a dependência da transmissão de informações através de ligações.

- A comunicação é limitada a sua própria célula, ou é preciso comunicar-se com outras células?

Para que sua célula se comunique com outras, é preciso:

- Estabelecer um nome de DNS global exclusivo para sua célula.
- Definir sua célula no DNS.
- Ter no mínimo um GDA em sua célula ou ter realizado um **cdscp define server** ou um **dcecp cdscache create**.

Nota: O Serviço de Diretório Global (Global Directory Service - GDS) não é fornecido com este release do DCE 3.2 para AIX. Entretanto, este release pode usar o GDS se ele for fornecido por outro produto para localizar outras células.

Pode-se definir uma conta especial no registro de segurança de sua célula para uma célula externa, indicando que sua célula confia no Serviço de Autenticação da outra célula. Uma conta especial no registro de segurança da célula externa pode representar sua célula. (Para informações sobre a definição dessas contas especiais, consulte o *IBM DCE Version 3.2 for AIX and Solaris: Administration Guide*.) Mesmo que você não precise se comunicar com outras células agora, analise se isto será necessário no futuro. Certifique-se de estabelecer um nome de célula levando em conta estas futuras necessidades.

Suas respostas a estas perguntas determinam os requisitos básicos de seu ambiente de usuário. Use esses requisitos para ajudá-lo a decidir sobre o melhor uso das funções de DCE descritas nesta seção e nas seguintes.

- **Resolução de Diferenças entre Contas Padrões do DCE e do AIX:**

É altamente recomendável que quaisquer usuários e grupos definidos nos arquivos individuais do sistema **/etc/passwd** e **/etc/group** sejam sincronizados com os usuários e grupos no registro do DCE. A sincronização pode ser facilitada com os utilitários **passwd_export** e **passwd_import** após a configuração inicial da célula. Quaisquer usuários que não estejam sincronizados entre o registro da célula e os arquivos locais podem não extrair benefício total do recurso de integração. Por outro lado, este esquema de integração flexível suporta usuários errantes (aqueles que estão definidos no registro do DCE, mas não em um sistema local). Se uma

máquina estiver configurada para permiti-lo, esses usuários errantes poderão efetuar logon no sistema e obter credenciais DCE e acesso local com base em informações relevantes a UNIX no registro.

Quando o DCE cria o banco de dados de registro de segurança, ele inclui alguns usuários principais, grupos e contas padrões do UNIX. Estes não correspondem àqueles incluídos em um sistema AIX típico. Esta diferença pode levar a problemas caso você pretenda usar o comando **passwd_export** para manter **/etc/passwd** e **/etc/group** sincronizados com o registro do DCE.

Se somente máquinas AIX irão ser incluídas na célula, pode-se excluir os usuários principais, grupos e contas padrões do registro e incluir outros que correspondam aos usuários principais, grupos e contas do AIX.

Se a célula irá incluir mais tipos de máquinas além de AIX, pode-se converter as contas padrões conforme descrito no parágrafo anterior ou manter as contas criadas pelo DCE. Em seguida, pode-se usar os arquivos **/opt/dcelocal/etc/passwd_override** e **/opt/dcelocal/etc/group_override** em máquinas individuais para definir contas e grupos padrões que correspondam aos esperados pelo sistema operacional dessas máquinas. Para obter maiores informações sobre os arquivos de substituição, consulte o *IBM DCE Version 3.2 for AIX and Solaris: Administration Guide—Core Components*.

Se você planeja converter contas padrões UNIX no registro conforme descrito acima, deverá fazê-lo imediatamente após a configuração inicial da célula para reduzir a possibilidade de produzir órfãos (objetos de propriedade de UUIDs que foram excluídos).

- **Arquivos de Núcleo de Aplicação DCE:** Como as aplicações DCE são multithread, seus arquivos de núcleo se tornam grandes. Cada thread tem sua própria pilha e outras informações associadas que são salvas no arquivo de núcleo. Se desejar arquivos de núcleo adequados para uso de sua aplicação DCE enquanto estiver desenvolvendo e testando as aplicações, certifique-se de ter permissão para gravar grandes arquivos de núcleo. O comando **ulimit** pode ser usado para alterar temporariamente o tamanho máximo de arquivo de núcleo para o processo de shell atual, ou pode-se usar o comando **chuser** para alterar permanentemente o tamanho máximo de arquivo de núcleo para um usuário específico.

Criação de um Nome de Célula

Antes de poder configurar a célula DCE, é preciso criar um nome de célula. Esta seção descreve a sintaxe de nomenclatura DCE, convenções de nomenclatura e o procedimento para obter um nome de célula.

Nomes Globais

Todos os objetos DCE, incluindo aplicações, máquinas e usuários, têm um nome global. Um nome global é significativo e adequado para uso em qualquer parte do ambiente DCE. No DCE, nomes globais começam com a cadeia especial de caracteres **/...**, a qual indica o diretório root global.

Nomes Globais DNS: O DCE também suporta operações de diretório globais através do uso de DNS. O seguinte é um exemplo de um nome global que usa o formato DNS:

`/.../seattle.xyz.com/sec/principal/smith`

No formato DNS, `/.../seattle.xyz.com` é o nome da célula, seguido por uma entrada no espaço de nomes da célula.

Nomes Relativos à Célula

Nos dois exemplos anteriores, `sec/principal/smith` é a parte do nome global que reside na célula local. A parte `sec/principal/smith` do nome global pode ser usada para construir um nome relativo à célula. Nomes relativos à célula, também conhecidos como nomes locais, são significativos somente dentro da célula onde a entrada do nome existe. Nomes relativos à célula começam com a cadeia especial de caracteres `./.`, a qual substitui a parte global do nome (o nome da célula). Se você estiver na célula `seattle.xyz.com`, o seguinte nome relativo à célula será traduzido para o mesmo nome global mostrado nos exemplos anteriores:

`././sec/principal/smith`

Quando estiver digitando um nome CDS a partir da célula onde esse objeto está registrado, você poderá usar o nome relativo à célula. Entretanto, se estiver digitando um nome CDS a partir de outra célula, será preciso usar o nome global, começando com a cadeia de caracteres `/...` (o root global).

As convenções de nomenclatura de CDS e DNS são descritas em maiores detalhes no *IBM DCE Version 3.2 for AIX and Solaris: Administration Guide—Core Components*.

Escolha de um Nome de Célula DCE

Escolher um nome de célula DCE apropriado é importante pelas seguintes razões:

- Todas as células DCE que algum dia participarão no espaço de nomes global devem ter nomes exclusivos para diferenciá-las de células em outras organizações.
- Um nome de célula identificado com exclusividade é crítico para a operação da segurança DCE; este nome é a base para a autenticação na célula.
- O DNS espera que os nomes globais de células tenham um certo formato. Escolha um nome que respeite as convenções de nomenclatura de DNS.
- O DCE não suporta células registradas simultaneamente no GDS e no DNS.

Note que os nomes de células não diferenciam maiúsculas e minúsculas: ou seja, o nome **MyCell** é equivalente ao nome **MYCELL**. (Ao comparar nomes de células, as rotinas do DCE mudam os nomes para minúsculas antes de fazer a comparação.)

Nomes de células não podem conter um símbolo de arroba (@). Duas células na mesma LAN não devem ter o mesmo nome. Duas células com o mesmo nome serão percebidas como uma célula única. Dependendo da configuração, isto pode causar sérias perturbações ao funcionamento normal das células com o mesmo nome. Nomes de células também devem se restringir a caracteres no DCE Portable Character Set descrito em *IBM DCE Version 3.2 for AIX and Solaris: Administration Guide—Core Components*.

O nome de célula máximo que pode ser usado ao configurar uma célula DCE será calculado com base no tamanho máximo de nome de arquivo, que é 255. O maior nome de arquivo que é criado pelo DCE é **<nome_da_célula>#<nome_de_host_dce>.ch.checkpoint<número de 10 dígitos>**. Devido a esta limitação, o tamanho do nome da célula será calculado como **(229 - <comprimento nome_de_host_dce>)**. Este limite será obrigatório quando o servidor Principal de Segurança ou um Servidor CDS Inicial ou Adicional for configurado. O tamanho de célula máximo de 255 será obrigatório ao configurar um cliente ou qualquer outro servidor em uma célula existente.

Obtenção de um Nome de Célula DCE

Se você planeja criar uma célula privada e pretende que ela nunca se comunique com células fora de sua organização, não é obrigatório obter um nome de célula globalmente exclusivo. Entretanto, para que sua célula se comunique com outras fora de sua organização, é preciso ter uma definição para o ambiente entre as células e, antes de configurar sua célula, é preciso obter um nome de célula globalmente exclusivo das autoridades de nomenclatura global GDS ou DNS. O nome pode ser um que já exista e esteja em uso, ou você pode especificar que precisa de um novo nome. Este registro precisa estar concluído antes de começar a configurar o espaço de nomes da célula. Recomenda-se que se obtenha um nome global exclusivo para a célula mesmo que inicialmente não se use um serviço de diretório global para se comunicar com outras células, para que seja possível fazer isso no futuro.

Definição de uma Célula no DNS

O subcomando **show cell** de **cdscp** pode ser usado para obter dados necessários para criar ou modificar uma entrada de célula no DNS. Os dados obtidos do comando são o que o CDS usa para contactar servidores em células externas. Use o comando **mkreg.dce** para registrar informações da célula com o DNS. Para informações sobre a definição do ambiente entre as células, gerenciamento da nomenclatura entre as células e da administração de

um ambiente entre as células, consulte o *IBM DCE Version 3.2 for AIX and Solaris: Administration Guide—Core Components*.

O Espaço de Nomes da Célula

Uma parte integral do planejamento de uma célula DCE é compreender a organização do espaço de nomes da célula. Leve em consideração o seguinte ao planejar a organização de uma célula em sua rede:

- São mantidos requisitos de segurança?
- A organização da célula facilita o tráfego da rede onde as necessidades de compartilhamento de dados são maiores?
- Como serão gerenciadas as contas administrativas criadas para cada serviço DCE durante o processo de configuração?

Determinação dos Limites da Célula

No DCE, os limites de uma célula são equivalentes aos limites do espaço de nomes da célula. Uma organização pequena pode consistir em uma célula. Uma organização grande pode ter muitas células. Os fatores principais na determinação dos limites de uma célula são a finalidade e confiança comuns compartilhadas pelos usuários principais da célula. Os usuários principais em uma célula podem pertencer a grupos que compartilham os mesmos privilégios. Membros de um grupo compartilham o mesmo nível de confiança e são autorizados a realizar certas ações.

Como há um conjunto de tarefas administrativas associadas à definição e manutenção de cada célula, é de bom senso manter o número de células em sua organização o mínimo possível. Entretanto, o nível de confiança compartilhado por grupos de usuários principais é uma consideração mais importante que a carga administrativa.

Manutenção da Estabilidade das Células

Uma vez decidido o número de células desejado e onde os limites dessas células estarão, faça um esforço para manter a estrutura das células estável. Servidores não são mudados facilmente de uma célula para outra; portanto, certifique-se de planejar a estrutura do espaço de nomes cuidadosamente para minimizar reconfigurações. Se for necessário mover um host de uma célula para outra, será preciso:

- Mover do host os processos do servidor.
- Remover a configuração do host da célula antiga, usando o comando **unconfig.dce**.
- Usar o comando **config.dce** para reconfigurar o host na nova célula.

Tipos de Entradas do Espaço de Nomes da Célula

Esta seção descreve os diferentes tipos de entradas que compõem o espaço de nomes da célula. Estas entradas são criadas quando se segue o caminho de configuração padrão descrito em Configuração do DCE. O espaço de nomes da célula pode ser dividido nas seguintes partes:

- A parte de CDS do espaço de nomes
- A parte de segurança do espaço de nomes
- A parte de DFS do espaço de nomes (o espaço de arquivos)
- A parte **dced** (por host) do espaço de nomes

Cada serviço DCE mantém seu próprio espaço de nomes dentro do espaço de nomes da célula. O DFS mantém seu próprio espaço de nomes para assegurar a consistência entre muitos arquivos. O Serviço de Segurança mantém seu próprio espaço de nomes para assegurar que a célula DCE permaneça protegida. Os clientes deste serviço consultam o CDS para informações de ligação que permitem que eles encontrem o servidor de segurança. Os pontos onde as informações de ligação são armazenados servem como pontos de montagem no espaço de nomes CDS para os espaços de nomes que o DFS e o Serviço de Segurança gerenciam. Este ponto de transição entre dois espaços de nomes é chamado uma junção. O diretório `./:sec` é a junção da parte de CDS com a parte de segurança do espaço de nomes da célula, e o diretório `./:fs` é a junção da parte de CDS com a parte de DFS do espaço de nomes da célula.

A junção `./:hosts/nome_do_host/config` é a junção do CDS com a parte **dced** (por host) do espaço de nomes.

A Figura 1 mostra o nível superior do espaço de nomes da célula. Em alguns casos, os nomes no espaço de nomes da célula são fixados (ou bem conhecidos) e não podem ser alterados. Em outros casos, pode-se escolher um nome diferente do que é listado. Na Figura 1, `./:` e **cell-profile** são nomes bem conhecidos.

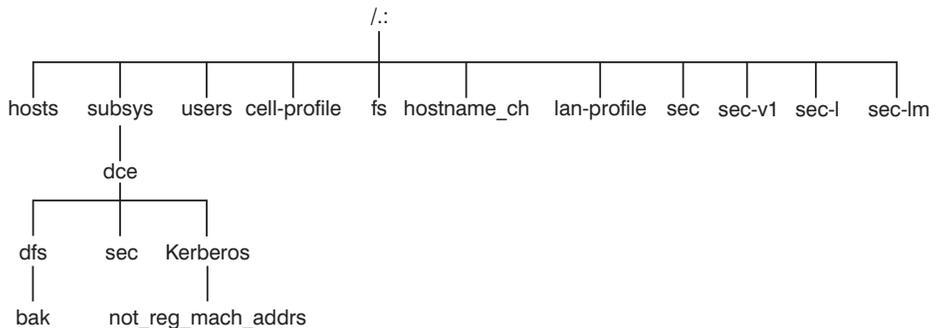


Figura 1. Nível Superior do Espaço de Nomes da Célula

Os comandos **dcecp**, **rpccp**, **cdscp** ou **cdsli** podem ser usados para exibir o espaço de nomes CDS, incluindo as junções **sec** e **fs**. Pode-se usar comandos como **ls** para ver o conteúdo da parte de DFS do espaço de nomes da célula, e **dcecp** para ver o conteúdo da parte de segurança do espaço de nomes CDS.

Entradas do Espaço de Nomes CDS: O Serviço de Diretório de Célula (Cell Directory Service - CDS) do DCE é um serviço de banco de dados distribuído e replicado que é usado para armazenar nomes e atributos de recursos localizados em uma célula DCE. Este banco de dados consiste no conjunto hierárquico de nomes denominado espaço de nomes. Cada servidor CDS mantém uma parte do espaço de nomes em um banco de dados local denominado uma *clearinghouse*, o qual é otimizado para acesso local. Uma clearinghouse é projetada para relativamente poucas operações de **gravação** (tais como criar ou excluir diretórios e objetos ou exportar informações de ligação), mas muitas operações de **leitura** (tais como importar informações de ligação). Note que uma clearinghouse é criada automaticamente durante o processo de configuração para um servidor CDS. Consulte “Configuração do Servidor CDS Inicial” na página 90 para obter maiores informações.

Um banco de dados CDS, que é distribuído e replicado entre vários servidores CDS e várias clearinghouses, deve ser mantido consistente. O grande número de operações de **gravação** usado para repicar e manter a consistência pode causar falhas de CDS induzidas pelo esforço. O uso de um grande número de diretórios CDS replicados também pode resultar em esforço excessivo porque as atualizações precisam ser propagadas para todas as réplicas somente para leitura. Use o comando **cdscp show server** para exibir o número de operações de **leitura** e **gravação** manipuladas por um servidor desde que o serviço foi iniciado. Este comando permite monitorar o nível de atividade e ajustar a configuração caso necessário.

Assim como um serviço de diretório, o CDS é projetado para gerenciar informações que não mudam com frequência. Por exemplo, informações de ligação armazenadas no CDS não incluem nós de extremidade já que estes mudam frequentemente. Quando se projetam aplicações, deve-se evitar a necessidade de armazenar dados altamente dinâmicos no espaço de nomes CDS.

O espaço de nomes CDS contém entradas para servidores, hosts, clearinghouses CDS, (coleções de réplicas de diretórios armazenadas em um servidor particular), perfis RPC, grupos RPC e subsistemas. As entradas têm um tipo CDS de *diretório* ou *objeto*, indicando o tipo de objeto CDS ao qual o nome se refere. Um diretório CDS é um contêiner no qual objetos são armazenados. O CDS usa os diretórios para organizar grupos de entradas de objetos.

Os perfis catalogados no espaço de nomes CDS especificam um caminho de pesquisa através do Serviço de Diretório. O perfil da célula (**./:cell-profile**) armazena a localização dos servidores que estão disponíveis na célula, independente da localização física. Em uma célula dispersa geograficamente, os servidores podem estar localizados em cidades diferentes ou mesmo em países diferentes. O perfil da LAN define servidores alternativos que podem

ser usados em situações onde a proximidade geográfica é importante. Por exemplo, **./lan-profile** é o perfil de LAN padrão usado pelo DTS. Este perfil contém entradas para o conjunto local do servidor DTS. Se uma célula abranger mais de uma LAN, um perfil pode ser criado para cada LAN abrangida pela célula. Por exemplo, em uma célula que envolva duas LANs, é possível direcionar os hosts em uma LAN para **./lanA-profile** e os hosts na outra LAN para **./lanB-profile**. Para informações sobre a definição de vários perfis de LAN, consulte “Configuração do DCE” na página 79.

Entradas do Espaço de Nomes de Segurança: Os tipos de entradas de segurança são os seguintes:

usuário principal

Este tipo de entrada contém um usuário principal individual

diretório de usuário principal

Este tipo de entrada contém usuários principais individuais ou um ou mais diretórios de usuários principais, ou ambos.

grupo Este tipo de entrada contém um grupo individual

diretório de grupo

Este tipo de entrada contém grupos individuais ou um ou mais diretórios de grupos, ou ambos.

org Este tipo de entrada contém uma organização individual

diretório de org

Este tipo de entrada contém organizações individuais ou um ou mais diretórios de organizações, ou ambos.

critério

Este tipo de entrada contém um critério de segurança.

Quando você (ou uma aplicação) estiver acessando uma entrada na parte de segurança do espaço de nomes, o nome da entrada por si só fornece informações suficientes para que o Serviço de Segurança trabalhe com elas. Por exemplo, o servidor de segurança sabe que o nome de login é um nome de usuário principal, registrado na parte de segurança do espaço de nomes; *./nome_do_usuario_principal*, *./nome_da_celula/nome_do_usuario_principal*, e *nome_do_usuario_principal* são todas formas válidas de representar o nome usado para efetuar login.

Quando se usa o comando **dcecp**, especifica-se o tipo de objeto no qual se irá operar. Por exemplo, para alterar informações de conta associadas ao usuário principal **smith**, você especifica que deseja operar em uma conta. Em seguida, digita o nome do usuário principal **smith**. O comando **dcecp** opera com os seguintes tipos de objetos relacionados a segurança:

- Usuários principais
- Grupos

- Organizações
- Contas
- Xattrschemas

O *IBM DCE Version 3.2 for AIX and Solaris: Administration Guide—Core Components* explica como usar o comando **dcecp** para exibir informações relacionadas a usuários principais, grupos, organizações, contas e xattrschemas.

O comando **dcecp** também suporta operações realizadas por **acl_edit**. O objeto **acl** de **dcecp** é usado para este propósito. O comando **dcecp** exige o nome de caminho completamente qualificado do objeto ao modificar ACLs, conforme mostra o seguinte exemplo:

```
././sec/principal/smith
```

e não simplesmente o seguinte:

```
smith
```

As seguintes partes do espaço de nomes compõem o espaço de nomes de segurança:

```
././sec/principal
././sec/group
././sec/org
././sec/policy
././sec/xattrschema
```

Considerações sobre Replicação do Espaço de Nomes CDS

A replicação de diretório é a maneira mais confiável de fazer backup das informações no espaço de nomes CDS. Como os dados de CDS são replicados por diretório, quando se replica um diretório todas as entradas de objeto nele são automaticamente replicadas. Use o programa de controle **dcecp** para criar réplicas de diretórios em uma clearinghouse CDS. Se você criar uma clearinghouse além das que são automaticamente criadas em um Servidor CDS no momento da configuração, essa clearinghouse deve ser criada no diretório root (**./.**) do espaço de nomes da célula.

Siga estas diretrizes para replicar partes do espaço de nomes da célula:

- O diretório root (**./.**) é automaticamente replicado (sem diretórios filhos) quando se cria uma clearinghouse.
- Deve-se ter no mínimo duas réplicas de cada diretório CDS para assegurar que todo o espaço de nomes esteja disponível durante todo o tempo. Para mais informações sobre backup de informações CDS, consulte o *IBM DCE Version 3.2 for AIX and Solaris: Administration Guide—Core Components*.

Planejamento do Controle de Acesso

Ao planejar o controle de acesso, é importante manter o nível de controle de acesso na célula restritivo o suficiente para assegurar que a segurança seja mantida. Um conjunto especial de indivíduos ou um grupo especial podem receber permissão para criar contas e grupos no diretório root do espaço de nomes de segurança. O grupo **acct-admin** é criado ao configurar o DCE. **acct-admin** é o único grupo que pode criar contas e grupos no diretório root do espaço de segurança.

Ao mesmo tempo que mantém um nível adequado de segurança na célula, você também precisa levar em conta as exigências dos administradores que estão mantendo os serviços DCE quando definir os níveis de controle de acesso.

A seguir estão alguns dos grupos criados quando se configura o DCE usando o SMIT, **smitty** ou o comando **config.dce**:

sec-admin

Este grupo administra os servidores de segurança, funções de registro da célula e outras funções de segurança.

audit-admin

Este grupo administra servidores de Auditoria e funções de auditoria relacionadas.

cds-admin

Este grupo administra servidores CDS, replicação CDS e outras funções CDS.

dced-admin

Este grupo administra servidores de hosts DCE e ACLs.

dts-admin

Este grupo administra servidores DTS e funções DTS relacionadas.

dfs-admin

Este grupo administra Servidores de Arquivos DFS e funções DFS relacionadas.

Além dos grupos administrativos, os usuários individuais precisam de permissão para controlar algumas informações mantidas no banco de dados de registro. Por exemplo, um usuário precisa ser capaz de alterar sua senha, diretório pessoal ou shell de login.

Considerações de Nomenclatura DCE para Internacionalização

O DCE padrão (OSF) restringe as entradas no espaço de nomes de segurança, tais como nomes de usuários principais, aos caracteres no DCE Portable Character Set. Consulte a Visão Geral da Arquitetura do DCE no *IBM DCE Version 3.2 for AIX and Solaris: Introduction to DCE* para a definição do DCE

Portable Character Set. O DCE da IBM fornece uma capacidade de substituição que habilita o uso de caracteres não portáteis.

Esta capacidade deve ser usada somente em ambientes que sejam homogêneos com respeito ao conjunto de códigos e nos quais todas as instalações de DCE suportem esta extensão. Entradas no espaço de nomes de segurança que usam caracteres não portáteis são garantidas quanto ao funcionamento correto somente quando o conjunto de códigos de toda a empresa é o mesmo que o do processo sob o qual os nomes foram criados. Para ativar o uso de nomes de segurança não portáteis, a variável de ambiente `DCE_USE_NONPORTABLE_NAMES` deve ser definida como 1 antes de iniciar o DCE, em todos os processos de cliente e de servidor nos quais a segurança DCE executará.

Certos nomes, tais como nomes de diretório CDS, também podem ser compostos de caracteres de fora do DCE Portable Character Set. Como o DCE não realiza conversão de conjunto de códigos em nomes, os caracteres não portáteis devem ser usados somente em ambientes que são, e irão permanecer, homogêneos com respeito ao conjunto de códigos. Em ambientes que não são homogêneos com respeito ao conjunto de códigos, todos os nomes DCE devem ser restritos ao DCE Portable Code Set.

Sujeitos à restrições mencionadas anteriormente e às regras adicionais de nomenclatura documentadas no *IBM DCE Version 3.2 for AIX and Solaris: Introduction to DCE* e no *IBM DCE Version 3.2 for AIX and Solaris: Application Development Guide—Core Components*, os seguintes nomes podem conter caracteres fora do Portable Characters Set:

- Objeto CDS
- Diretório CDS
- Atributo CDSe
- Link CDS
- Dados RPC `idl_byte`
- Nome completo RPC
- Usuário principal
- Grupo
- Organização
- ERA
- Nome de arquivo DFS

Considerações sobre Cliente e Servidor

Esta seção descreve configurações para máquinas clientes DCE, os diferentes tipos de máquinas de servidores DCE e máquinas do ambiente de Desenvolvimento de Aplicações DCE. Uma máquina cliente DCE pode executar código de cliente de todos os serviços DCE. Máquinas de servidores DCE são configuradas para executar um certo conjunto de software. Este software é composto de no mínimo um daemon e, em alguns casos, um ou mais programas adicionais que compõem o lado do servidor de um componente do DCE. As máquinas de servidores DCE também executam o software que compõe a configuração de cliente DCE.

Os seguintes tópicos são apresentados:

- “Determinação dos Requisitos para Máquinas Clientes DCE”
- “Determinação dos Requisitos para Máquinas de Servidores DCE” na página 43
- “Determinação dos Requisitos para Migração do DCE Anterior para um Servidor de Segurança LDAP” na página 47
- “Utilitários de Administração DCE” na página 48.

Determinação dos Requisitos para Máquinas Clientes DCE

Esta seção descreve as considerações de planejamento envolvidas na definição de máquinas clientes DCE. Todas as máquinas DCE, inclusive as máquinas de servidores DCE, são também clientes DCE.

As seguintes subseções descrevem os executáveis que executam em uma máquina cliente DCE.

Programas de Cliente RPC

Um cliente DCE contém os seguintes programas de RPC:

- O daemon **dced** deve executar em qualquer máquina que tenha um processo servidor RPC que exporte uma interface com ligações dinâmicas. O daemon **dced** é usado para registrar informações de ligação.

O daemon **dced** precisa estar em execução antes de configurar quaisquer outros serviços DCE que registrem seus nós de extremidade. Os serviços DCE precisam registrar seus nós de extremidade com **dced**. Somente um daemon **dced** pode executar em uma máquina por vez, porque **dced** usa uma porta bem conhecida.

As interfaces de rede, serviços de roteamento e outros serviços de rede devem estar disponíveis antes que o RPC inicie. O daemon **dced** é iniciado pelo comando **start.dce**. O comando **start.dce** pode ser solicitado a partir de **/etc/inittab** especificando-se a opção **-autostart yes** no comando **config.dce** ou incluindo **/opt/dcelocal/etc/rc.dce** neste arquivo. Isto permitirá que os serviços DCE sejam ativados sempre que a máquina reinicializar. Consulte

“Uso do SMIT para Iniciar o DCE Imediatamente e no Reinício do Sistema” na página 128 para informações sobre o menu do SMIT para iniciar o DCE 3.2 para AIX na reinicialização.

- O programa de controle DCE (**dcecp**) é um utilitário que permite que você examine, atualize, inclua e exclua os atributos de entradas RPC armazenados no espaço de nomes CDS e os nós de extremidade que são gerenciados por daemons **dced** locais e remotos.

Programas de Cliente do Serviço de Segurança

O daemon **dced** mantém a identidade do usuário principal da máquina local atualizando periodicamente o ticket que concede tickets para o usuário principal da máquina. Isto assegura que o usuário root local ou qualquer daemon que herde a identidade da máquina tenha credenciais DCE válidas. O daemon **dced** também exporta e implementa uma variedade de interfaces, incluindo suporte a substituição de senha e de grupo, certificação do servidor de segurança e suporte a pré-autenticação.

Para obter maiores informações sobre tickets que concedem tickets, consulte *IBM DCE Version 3.2 for AIX and Solaris: Administration Guide—Core Components*.

Programas de Cliente CDS

O cliente DCE executa os seguintes processos CDS:

- O anunciante CDS, o processo **cdsadv**, permite que as aplicações acessem e se comuniquem com o **cdsd**. Ele inicia quaisquer clerks CDS (**cdsclerk**) necessários e cria o cache compartilhado pelos clerks CDS locais. Ele recebe e coloca em cache de transmissões do servidor.
- O **cdsclerk** é uma interface entre aplicações de clientes CDS e servidores CDS. Um clerk precisa existir em cada máquina que executa uma aplicação de cliente CDS. Um processo **cdsclerk** executa para cada usuário principal do AIX em uma máquina que acesse o CDS. O clerk CDS manuseia pedidos de aplicações de clientes para um servidor e coloca os resultados retornados pelo servidor em cache. Como os resultados do pedido do servidor são colocados em cache, o clerk não precisa ir repetidamente ao servidor para obter as mesmas informações. Todos os clerks CDS em uma máquina compartilham um cache. Um clerk pode atender a muitas aplicações de clientes.
- O programa de controle DCE (**dcecp**) pode ser usado para examinar, atualizar e excluir entradas de CDS, e gerenciar o espaço de nomes. Para obter maiores informações, consulte o *IBM DCE Version 3.2 for AIX and Solaris: Administration Guide—Core Components*.
- O programa de controle CDS, **cdsnp**, é uma interface de comando usada para controlar servidores e clerks CDS e gerenciar o espaço de nomes e seu conteúdo. A interface de comando **cdsnp** estava disponível com versões anteriores do DCE e é fornecida para facilitar a migração para o uso do

utilitário **dcecp**. Para obter maiores informações sobre o programa de controle CDS, consulte o *IBM DCE Version 3.2 for AIX and Solaris: Administration Guide—Core Components*.

Programas de Cliente DTS

O cliente DCE executa os seguintes processos DTS:

- O daemon **dttd** é definido como um cliente ou um servidor. Em uma máquina cliente, **dttd** sincroniza o relógio local.
- O programa **dtscp** permite administrar o DTS, incluindo configurar o daemon **dttd** como um cliente ou com um servidor.

Programas do Cliente Básico

Em geral, sistemas clientes têm menos memória disponível que sistemas de servidores. Se um cliente não oferecer serviços DCE para outros sistemas na célula, ele pode não precisar de todas as funções fornecidas pelos daemons iniciados pela configuração do software DCE no sistema cliente. O cliente básico oferece a capacidade de ser tal cliente "reduzido" na célula.

Como nenhuma informação sobre o cliente básico é mantida na célula, a intervenção do administrador, ou seja, **cell_admin** não é exigida para configurá-lo. Em vez disso, use o comando **config.dce** para configurar o cliente básico. Use os comandos **start.dce** e **stop.dce**, respectivamente, para iniciar e parar o cliente básico. Para remover a configuração do cliente básico, use o comando **unconfig.dce**.

A opção de cliente básico reduz o consumo de memória do DCE em sistemas clientes por meio da execução de uma só instância do clerk CDS sem nenhum outro daemon de DCE. A execução de uma única instância do clerk CDS é feita iniciando o clerk com a opção **-n**. Isto inicia um clerk sem o anunciante CDS. Se existem tantos outros serviços e funções DCE que podem ser executados, como pode um só clerk CDS ser suficiente? A resposta é que a maioria dos cliente DCE precisam somente das seguintes funções DCE:

- chamadas RPC (tanto autenticadas quanto não autenticadas)
- login DCE
- pesquisas de nomes CDS

Para chamadas RPC e a maioria dos logins, nenhum daemon DCE é necessário. Estas funções simplesmente usam rotinas de tempo de execução de RPC e de segurança.

Para pesquisas de nomes CDS, somente um clerk CDS é necessário. Com o DCE completo, os clerks CDS são iniciados pelo anunciante CDS, exigindo que este esteja presente. Entretanto, no DCE 3.2 para AIX, a opção **-n** no comando **cdsclerk** inicia uma instância única do clerk CDS sem precisar do anunciante. Este clerk não terminará após estar ocioso por 20 minutos, como é

o caso no DCE completo. Além disso, quando o clerk é iniciado desta maneira, ele assume a função do anunciante CDS no gerenciamento do cache do cliente CDS. O clerk não receberá ou colocará no cache de transmissões dos servidores CDS, uma função do anunciante.

Sem um anunciante, o **cdsclerk** não pode ser gerenciado por **dcecp** ou **cdscp**. Os seguintes comandos falharão:

```
cdscp show clerk
cdscp disable clerk
cdscp show cached clearinghouse
cdscp define cached server
cdscp show cached server
cdscp clear cached server
dcecp -c cdscache create
dcecp -c cdscache delete
dcecp -c cdscache show -server
dcecp -c cdscache show -clearinghouse
```

Os seguintes serviços de **dced** não executarão em um cliente básico DCE:

- O **Serviço Mapeador de Nó de Extremidade do dced** deve ser executado em qualquer sistema que forneça um serviço que possa ser acessado através de RPCs. Tal servidor é denominado um servidor RPC. Quando um sistema emite uma RPC para um serviço RPC, ele usa as rotinas de tempo de execução RPC para enviar o pedido ao endereço de uma máquina específica e pede o serviço RPC desejado pelo seu nome. Após a RPC atingir a máquina onde o serviço reside, o Serviço Mapeador de Nó de Extremidade mapeia o nome do serviço RPC para o nó de extremidade, ou número da porta, do programa específico que fornece o serviço. Após o nó de extremidade ser conhecido, o cliente está ligado ao serviço RPC específico, e RPCs podem ser emitidas diretamente a esse serviço.

Embora todo sistema cliente emita RPCs, a maioria não precisa do Serviço Mapeador de Nó de Extremidade, porque provavelmente não são servidores RPC. Portanto, a limitação relativa a RPC de não executar **dced** em um sistema cliente é que ele não pode ser um servidor RPC.

- O **Serviço de Validação de Segurança** fornece as funções listadas abaixo. Se um sistema cliente não precisar dessas funções, ele não precisa do Serviço de Validação de Segurança do **dced**. Note que um **dce_login** e RPCs autenticadas ainda podem ser emitidos em um sistema que não tenha esse serviço em execução.
 - **Certificação do Servidor de Segurança.**
 - **Pré-autenticação de terceiros durante dce_login.**
 - **Manutenção do contexto da máquina atualizado.**
 - **Substituições de senha e de grupo.**
- A **Réplica de Segurança Preferencial** não é suportada pelo cliente básico.
- **Serviços de Gerenciamento do Sistema:**

As funções de gerenciamento do sistema fornecidas pelo DCE são listadas abaixo. Sem o **dced**, um sistema cliente não pode ser gerenciado remotamente por meio dessas funções.

- O **Gerenciamento de Dados de Host** mantém arquivos locais de dados do host (que incluem o nome do host, nome da célula e aliases da célula) e um arquivo pós-processador. O arquivo pós-processador contém nomes de programas que são correspondentes a outros itens de dados do host. O **dced** executa o programa se o item de dados do host correspondente for alterado.
- O **Controle do Servidor** mantém dados que descrevem a configuração de inicialização e o estado de execução para cada servidor. Ele também pode iniciar ou parar servidores específicos, e ativar ou desativar serviços específicos de servidores. Este serviço não é necessário em um cliente que não esteja executando nenhum servidor RPC.
- O **Gerenciamento de Tabela de Chaves** permite a manutenção remota das tabelas de chaves de um servidor. Este serviço não é necessário em um cliente que não esteja executando nenhum servidor RPC.

A **Integração de Segurança, dceunixd**, pode executar em um cliente básico. Lembre-se que, como o serviço de certificação não está disponível, quando um usuário efetuar login sua identidade não poderá ser certificada quanto a ter sido emitida por um servidor de segurança legítimo, e que a integração de segurança em um cliente básico não pode usar substituições de senha e de grupo. Como o contexto da máquina não está disponível, a integração de segurança em um cliente básico usa acesso não autenticado ao registro. Além disso, usuários root locais executarão não autenticados porque não há contexto de máquina para ser herdado por eles.

Determinação dos Requisitos para Máquinas de Servidores DCE

Esta seção fornece informações sobre os requisitos para os diferentes tipos de máquinas de servidores DCE.

Arquivos Instalados em Máquinas de Servidores DCE

As subseções seguintes discutem os arquivos que precisam ser instalados em cada uma das diferentes máquinas de servidores DCE e o espaço necessário aproximado. Note que como todos os servidores DCE também são clientes DCE, os arquivos descritos em “Determinação dos Requisitos para Máquinas Clientes DCE” na página 39 também precisam ser instalados em máquinas de servidores. Portanto, inclua os requisitos apropriados de espaço no servidor aos requisitos de espaço da máquina cliente DCE para chegar ao requisito de espaço total aproximado para a configuração que estiver planejando.

Processos do Servidor de Segurança e DCE Anterior

Nota: A discussão a seguir é baseada no DCE anterior e pode ser estendida para se aplicar ao recurso de Integração do Registro de Segurança DCE e LDAP.

Toda célula tem uma máquina principal do DCE Security Service e também pode ter a réplica de máquinas do DCE Security Service. Os seguintes processos executam em uma máquina principal ou em uma réplica do DCE Security Service:

- O processo do servidor de segurança, ou **secd**, implementa o serviço de Autenticação, o serviço de Privilégio e o registro de Registro.
- O programa **sec_create_db** inicializa o banco de dados de segurança. O comando **config.dce** passa um parâmetro indicando se deve ser criado um servidor de segurança principal ou réplica na máquina.
- O programa de controle DCE (**dcecp**) é usado para o registro, gerenciamento e manutenção do servidor de segurança. Opcionalmente, pode-se usar o programa **sec_admin**. Consulte "Utilitários de Administração DCE" na página 48 para descrições destes programas.

Tenha em mente as seguintes considerações ao planejar servidores de segurança:

- O nó que executa o servidor de segurança principal deve ter alta disponibilidade e estar fisicamente protegido. Veja a possibilidade de colocar a máquina do servidor de segurança principal em uma sala fechada e de manter um registro de quem acessa essa máquina.
- Certifique-se de mover o servidor de segurança principal antes de remover o nó da rede ou de desligar o nó por muito tempo. As modificações são feitas no servidor de segurança principal e transmitidas para as réplicas através da célula. Se o servidor de segurança principal não estiver disponível, nenhuma atualização poderá ser feita. Para obter maiores informações consulte "Manipulando Reconfigurações da Rede" no *IBM DCE Version 3.2 for AIX and Solaris: Administration Guide—Core Components*.
- Uma célula pode possuir somente um servidor de segurança principal. Se você planeja criar uma célula a partir de várias células existentes com servidores de segurança principais independentes, é preciso antes combinar seus registros.
- Tenha em mente as seguintes considerações ao planejar servidores de servidores de Mapeamento de Identidade:
 - O servidor de segurança DCE usa o servidor de Mapeamento de Identidade quando um usuário DCE efetua login usando o recurso de login com certificado de chave pública. É preciso configurar ao menos um servidor de Mapeamento de Identidade para usar login com certificado de chave pública.

- Devido à interação entre o servidor de Mapeamento de Identidade e o servidor de segurança DCE, nós que executam servidores de Mapeamento de Identidade devem ter alta disponibilidade e estar fisicamente protegidos. Recomenda-se que um servidor de Mapeamento de Identidade seja executado em cada nó que execute um servidor de segurança DCE.

Para mais informações sobre planejamento para o serviço de Segurança DCE, consulte o *IBM DCE Version 3.2 for AIX and Solaris: Administration Guide—Core Components*.

Como o registro de segurança é replicado por inteiro em todas as réplicas de segurança, se o host que contém o servidor de segurança principal não estiver ativo, os hosts que possuem réplicas dos Servidores de Segurança ainda podem fornecer informações do registro; portanto, examine a possibilidade de ter várias réplicas em sua rede. Use fatores tais como o número de máquinas na célula, a confiabilidade das máquinas que executam servidores de segurança e os recursos disponíveis na célula para determinar quantas réplicas dos servidores de segurança é preciso ter.

Processos do Servidor de Segurança e Registro de Segurança LDAP

Todas as considerações delineadas em “Processos do Servidor de Segurança e DCE Anterior” na página 44 devem ser analisadas em um ambiente onde o DCE anterior está sendo ou foi migrado para usar o diretório LDAP para armazenar dados de usuários.

Para mais informações sobre planejamento para o Servidor de Segurança DCE usando o diretório LDAP para dados de usuários, consulte o *IBM DCE Version 3.2 for AIX and Solaris: DCE Security Registry and LDAP Integration Guide*.

Processos de Servidor CDS e GDA

Um servidor CDS armazena e mantém nomes de objetos em uma célula e manipula pedidos para criar, modificar e examinar dados. Um servidor GDA habilita a célula na qual está executando a se comunicar com outras células.

Os seguintes processos executam em uma máquina de servidor CDS:

- O daemon CDS, **cdsd**, é o processo do servidor CDS.
- O **cdsadv**, além de receber difusões de servidores para descobrir quais servidores estão disponíveis para a máquina do cliente local, também envia anúncios do servidor.
- O programa de controle DCE (**dcecp**) é usado para o gerenciamento e manutenção do software de CDS. Além disso, o programa **cdscp** é usado para controlar e exibir informações sobre clerks e servidores CDS. Consulte “Utilitários de Administração DCE” na página 48 para descrições destes programas.

em preparação para o CDS, é preciso selecionar os nós de servidores que armazenam e mantêm as clearinghouses (bancos de dados CDS) na célula.

Tenha em mente as seguintes diretrizes para obter confiabilidade, o melhor desempenho e disponibilidade dos dados:

- Escolha nós confiáveis. Um servidor CDS precisa do menor tempo de inatividade possível e deve reiniciar rapidamente. O servidor CDS precisa ser um dos primeiros sistemas disponíveis na rede porque as aplicações clientes e outros servidores DCE dependem dele para informações atualizadas. O servidor CDS inicializa o espaço de nomes CDS quando se configura o DCE.
- Use conexões de rede confiáveis. Isto ajuda a assegurar que todos os servidores que mantêm réplicas de diretórios podem ser alcançados quando o CDS realiza uma espreita. Espreitas são atualizações periódicas que verificam a consistência em todas as réplicas.
- Considere o tamanho de sua célula e o quanto ela está geograficamente dispersa para decidir quantos servidores CDS são necessários. Deve-se ter no mínimo duas cópias (um principal e uma réplica somente leitura) de cada diretório CDS para assegurar acesso aos dados se um dos servidores não estiver disponível.
- Cada servidor CDS mantém no mínimo uma clearinghouse. Todas as clearinghouses contêm uma cópia do diretório root, além de outros diretórios nela replicados.
- Você deve tomar decisões de replicação com base em onde o conteúdo dos diretórios é referenciado. Ponha as réplicas onde o conteúdo é lido e os principais onde o conteúdo é gravado.

O daemon **gdad** é o servidor GDA, o qual envia pedidos de pesquisa para nomes de células ao DNS e retorna os resultados ao clerk CDS na célula que iniciou o pedido.

O GDA pode estar na mesma máquina de um servidor CDS ou pode existir independentemente em outra máquina. Pode-se ter dois ou mais daemons **gdad** em execução em uma célula para assegurar a disponibilidade do GDA.

Programas do Servidor DTS

A configuração do cliente DCE já contém todos os arquivos necessários para uma máquina de servidor DTS, com exceção do provedor de horário original.

- O daemon **dttd** (que pode ser instalado em uma máquina cliente DCE) é configurado para executar como um servidor. Como um processo de servidor, **dttd** sincroniza-se com outros servidores DTS, além de sincronizar o relógio local, como faz em uma máquina cliente.
- O **dtc_nome_do_dispositivo_provedor** especifica as comunicações entre o processo do servidor DTS e o processo do provedor de horário. Para

nome_do_dispositivo, substitua o dispositivo que está sendo usado, que pode ser um rádio, relógio ou modem, ou outra origem de horário UTC para o DTS. Um provedor de horário é opcional. Se for usado um provedor de horário, ele deve se conectar a um processo do servidor.

Considere as seguintes diretrizes ao planejar sua implementação de DTS:

- Cada célula deve ter no mínimo três servidores DTS. Ao menos três servidores DTS são necessários para detectar se um deles está defeituoso quando são consultados sobre o horário. É preferível ter quatro ou mais servidores DTS para fornecer redundância. Os servidores adicionais aumentam a exatidão da sincronização de horário. Entretanto, aumentar o número de servidores consultados sobre o horário também aumenta a atividade na rede. O administrador deve balancear o nível de exatidão com a quantidade de atividade na rede.
- Um provedor de horário é opcional no DTS; entretanto, células que devem ser precisamente sincronizadas com um padrão de hora precisam ter no mínimo um provedor de horário.
- Os servidores devem estar localizados nos locais com o maior número de diferentes conexões de rede.
- Se houver menos de três servidores de horário configurados na célula, use um dos seguintes comandos:

```
dtscp set servers required n  
(onde n é o número de servidores de horário na célula)  
dcecp -c dts modify -minservers n  
(onde n é o número de servidores de horário na célula)
```

Isto evitará que uma mensagem de aviso seja registrada sempre que o servidor tentar sincronizar.

Há muitas decisões de configuração da rede que afetam o planejamento de DTS. O *IBM DCE Version 3.2 for AIX and Solaris: Administration Guide—Core Components* contém detalhes sobre o processo total de planejamento de DTS, incluindo planejamento da configuração para Redes Locais (Local Area Networks - LANs), LANs estendidas e Redes Amplas (Wide Area Networks - WANs), bem como uma explicação dos critérios que devem ser usados ao selecionar uma origem de horário para uso da rede.

Determinação dos Requisitos para Migração do DCE Anterior para um Servidor de Segurança LDAP

Para informações sobre planejamento para que o Servidor de Segurança DCE use o diretório LDAP para dados de registro, consulte o *IBM DCE Version 3.2 for AIX and Solaris: DCE Security Registry and LDAP Integration Guide*.

Utilitários de Administração DCE

Esta seção descreve os utilitários de administração do sistema que podem ajudá-lo a desempenhar tarefas administrativas do DCE.

Programa de Controle DCE

O programa de controle DCE **dcecp** cria, mantém e gerencia objetos de RPC, CDS, segurança, DTS, EMS e DCED. Para obter maiores informações sobre **dcecp**, consulte o *IBM DCE Version 3.2 for AIX and Solaris: Administration Guide—Core Components* e o *IBM DCE Version 3.2 for AIX and Solaris: Administration Commands Reference*.

Programas de Administração RPC

O Serviço do DCE Remote Procedure Call fornece os seguintes utilitários de administração:

- O daemon **dced** é usado para registrar informações de ligação.
- O programa de controle DCE (**dcecp**) permite que você examine, atualize, inclua e exclua os atributos de entradas RPC armazenadas no espaço de nomes CDS e os nós de extremidade que são gerenciados por daemons **dced** locais e remotos.

Consulte o *IBM DCE Version 3.2 for AIX and Solaris: Administration Guide—Core Components* e o *IBM DCE Version 3.2 for AIX and Solaris: Administration Commands Reference* para obter informações mais detalhadas sobre estes programas.

Programas de Administração do DCE Security Service

O DCE Security Service fornece os seguintes utilitários de administração:

- O comando **dcecp acl** exibe, inclui, modifica e exclui entradas de ACL para um objeto específico. O *IBM DCE Version 3.2 for AIX and Solaris: Administration Commands Reference* contém informações detalhadas sobre o uso do comando **dcecp acl**.
- Os comandos **dcecp account**, **group**, **organization**, **principal**, **registry**, **user** e **xattrschema** permitem editar o banco de dados do registro ou o registro local. Quase toda a edição do banco de dados do registro deve ser feita com estes comandos. O *IBM DCE Version 3.2 for AIX and Solaris: Administration Commands Reference* explica o uso dos comandos.
- O comando **passwd_import** permite criar entradas no registro com base nos arquivos de grupo e de senha de máquinas que não implementam a Segurança DCE.
- O comando **passwd_export** permite atualizar os arquivos UNIX **/etc/passwd** e **/etc/group** com informações atuais de usuários obtidas do registro.
- Os arquivos **passwd_override** e **group_override** permitem estabelecer substituições às informações contidas no registro.
- O comando **rmxcred** elimina tickets expirados do diretório de credenciais.

- O comando **dcecp registry** ajuda a gerenciar réplicas do registro no servidor, a alterar o local do servidor principal, a migrar servidores para LDAP e a reinicializar um servidor secundário. Este comando também ajuda a gerenciar o servidor de segurança e seu banco de dados. Pode-se desempenhar tarefas tais como gerar uma nova senha principal para o banco de dados e interromper o servidor de segurança.

Nota: Para obter mais informações neste tópico relacionadas aos recursos Registro de Segurança DCE e Integração LDAP, consulte o *IBM DCE Version 3.2 for AIX and Solaris: DCE Security Registry and LDAP Integration Guide*.

Programas de Administração CDS

O CDS fornece os seguintes utilitários de administração:

- O programa **cdscp** está descrito em “Programas de Cliente CDS” na página 40.
- O **cdsli** dá a um usuário DCE a capacidade de listar recursivamente o espaço de nomes de células.
- O **cdsdel** exclui recursivamente o espaço de nomes de células. O programa de controle DCE (**dcecp**) pode ser usado para examinar, atualizar e excluir entradas de CDS, e para gerenciar o espaço de nomes. Ele pode ser usado em lugar de **cdscp**.
- O comando **mkreg.dce** insere informações sobre a célula DCE no banco de dados mantido pelo servidor de nomes do domínio (o daemon **named**).
- O comando **rmreg.dce** remove informações do banco de dados mantido pelo servidor de nomes do domínio (o daemon **named**) que foram incluídas pelo comando **mkreg.dce**.

Programas de Administração SVC

O programa **svcdumplog** imprime o conteúdo de um arquivo de log binário de manutenção como texto legível. Para obter maiores informações sobre **svcdumplog**, consulte o *IBM DCE Version 3.2 for AIX and Solaris: Administration Commands Reference*. O programa **dce_err** exibe o texto associado a um ID de mensagem do DCE.

Programas de Administração DTS

- O comando **dtscp** controla a interface que pode ser usada para configurar e gerenciar o DTS. Ele já está incluído no software do cliente DCE.
- O programa **dtscp** permite administrar o DTS, incluindo configurar o daemon **dtstd** como um cliente ou com um servidor.

DCE Web Secure

O produto DCE Web Secure estende os servidores Web Netscape FastTrack ou Netscape Enterprise ou os servidores Web iPlanet FastTrack ou iPlanet Enterprise para fornecer autenticação DCE a suas transações na Web,

permitindo usar um navegador da Web para executar programas Common Gateway Interface (CGI) que exijam credenciais DCE, tais como a DCE Web Administration.

Com o DCE Web Secure você pode fornecer credenciais DCE a um programa CGI. Por exemplo com um programa rcl chamado changeusers.tcl que faz alterações em lote em um grupo de contas DCE, os administradores colocariam o programa changeusers.tcl em um diretório que tivesse sido configurado para acesso CGI nos arquivos de configuração do servidor Web. Quando um usuário executar o programa CGI através do navegador da Web, ele obterá as credenciais DCE sob o id de usuário DCE com o qual o usuário do navegador da Web efetuou login.

DCE Web Administration

Com os programas CGI do DCE Web Administration, os administradores podem obter toda a funcionalidade de gerenciar usuários, grupos e organizações DCE, bem como de gerenciar permissões.

Ambiente de Desenvolvimento de Aplicações

Você pode configurar uma máquina DCE para o desenvolvimento de aplicações DCE. Esta configuração exige a inclusão à configuração básica de cliente DCE de vários arquivos de inclusão (.h) e de especificação de interface (.idl) files, juntamente com o compilador idl. Os arquivos e o compilador estão incluídos no pacote **dce.tools.appdev.adt** disponível no programa produto licenciado Desenvolvedores de Aplicações DCE. Você também pode usar o utilitário **sams** para incluir suporte a troca de mensagens e manutenção em suas aplicações. O utilitário **sams** está incluído no pacote **dce.tools.appdev.adt**.

Localização dos Arquivos Instalados de DCE

Os arquivos usados pelo DCE estão agrupados nas seguintes localizações:

- Os subdiretórios de **/opt/dcelocal**
- Subdiretórios convencionais do UNIX

Algumas informações precisam ser mantidas localmente em uma máquina para confiabilidade e para garantir que a segurança seja mantida. Por exemplo, ao configurar o DCE, o arquivo que contém o nome da célula precisa estar na máquina que está sendo configurada. Este arquivo é armazenado na subárvore **/opt/dcelocal**.

A subárvore **/opt/dcelocal** é criada quando se instalam componentes do DCE.

Em alguns casos, os arquivos são instalados em diretórios tais como `/usr/lib`, `/usr/bin` ou `/bin` por motivos de desempenho. Em outros casos, links simbólicos podem ser usados a partir dos subdiretórios convencionais do UNIX para `/opt/dcelocal`.

Esta seção contém os seguintes tópicos:

- “A Subárvore `/opt/dcelocal`”
- “Diretórios Convencionais do UNIX”
- “Localizações de Arquivos” na página 52
- “Sistemas de Arquivos a Serem Criados e Montados” na página 53

A Subárvore `/opt/dcelocal`

Para poder inicializar um servidor pela primeira vez e configurar a célula, os arquivos apropriados para os servidores obrigatórios (CDS e segurança) precisam estar disponíveis nessa máquina de servidor (na subárvore `/opt/dcelocal`).

Nota: É altamente recomendado que cópias do conjunto mínimo de programas e arquivos de dados instalados durante o procedimento de instalação padrão do DCE sejam mantidas localmente em máquinas de servidores para operação independente e manutenção de emergência.

O conteúdo da subárvore `/opt/dcelocal` pode variar de máquina para máquina em uma célula DCE para acomodar e atender a configurações específicas. Além disso, toda máquina deve ter acesso local a certos arquivos de modo que possa executar como um sistema independente se a máquina for desconectada ou particionada da célula. Os arquivos apropriados em servidores DCE que devem ser locais à máquina do servidor devem ser armazenados sob `/opt/dcelocal`. Arquivos de dados relacionados a cliente são armazenados sob `/opt/dcelocal/etc` (dados de configuração estáticos) e `/opt/dcelocal/var/adm`. Todos os arquivos de dados específicos do servidor são localizados no diretório `/opt/dcelocal/var/nome-do-componente-dce`.

A subárvore `/opt/dcelocal` é povoada e inicializada durante a instalação e configuração do DCE.

Diretórios Convencionais do UNIX

Alguns arquivos e diretórios usados pelo DCE são acessíveis em diretórios convencionais do UNIX. Estes arquivos e diretórios do DCE precisam estar acessíveis em localizações convencionais para que os usuários possam acessar de forma conveniente utilitários e dados usados com frequência, tais como `idl` do diretório `/usr/bin` e `localtime` do diretório `/etc/zoneinfo`. Os arquivos de cabeçalho estão acessíveis em `/usr/include` ou em seu subdiretório, `/usr/include/dce`, e as bibliotecas, tais como `libdce.a`, são mantidas em `/usr/lib`.

Localizações de Arquivos

O processo de instalação para o DCE 3.2 para AIX coloca arquivos nas seguintes localizações:

/usr/lpp/dce

Todos os arquivos DCE exceto aqueles listados mais adiante nesta lista.

/usr/lpp/dcedoc

Todo os arquivos de documentação para o DCE para AIX e as ferramentas relacionadas a eles.

/etc/dce

Os seguintes arquivos:

- **rc.dce**
- **dce.clean**
- **rpc.clean**

/etc/dce/rspfiles

Arquivos de resposta de configuração.

/etc/zoneinfo

Regras de fusos horários para DTS.

/tmp/dce

Localização temporária para processamento da configuração.

/usr/lib/nls/msg/<linguagem>

Catálogos de mensagens, onde <linguagem> é um dos seguintes locais: **en_US, es_ES, Es_ES, ES_ES, ja_JP, Ja_JP, JA_JP, ko_KR, KO_KR, pt_BR, PT_BR, zh_TW, Zh_TW** ou **ZH_TW**.

/usr/include

Arquivos de inclusão (a maioria sob **/usr/include/dce**).

/usr/lib

libdce.a, libcfgdce.a, libdcelibc_r.a, libdcephthreads.a, libidlctx.a, libcfgdfs.stubs.a, libdceweb.a, libdceweb4.a, libxdsxom.a e libsnmp.a.

/usr/lib/security

O módulo de carregamento **DCE** para operações de segurança integrada AIX/DCE.

Os seguintes links simbólicos são estabelecidos:

o subdiretório	é um link simbólico para
/opt/dcelocal/	/usr/lpp/dce
/opt/dcelocal/var	/var/dce
/opt/dcelocal/etc	/etc/dce
/opt/dcelocal/tmp	/tmp/dce

Um link para cada um dos comandos DCE é colocado em **/usr/bin**.

Além disso, os objetos do SMIT são carregados no banco de dados do Object Data Manager (ODM).

Sistemas de Arquivos a Serem Criados e Montados

Você provavelmente desejará criar novos sistemas de arquivos JFS do AIX para usar o DCE eficientemente:

/var/dce

Todos os componentes do DCE armazenam informações no diretório **/var/dce**. Se o sistema de arquivos **/var** estiver completamente preenchido, DCE e outros subsistemas que dependem de **/var** (tais como os subsistemas de correio e spooler) não poderão operar corretamente.

Você deve criar um novo sistema de arquivos montado sobre **/var/dce** antes de instalar o DCE. Você deve destinar cerca de 30 megabytes para **/var/dce** para a configuração inicial do DCE.

/var/dce/directory

O servidor CDS armazena os arquivos de clearinghouse, os quais contêm a parte deste servidor no espaço de nomes, e dados locais neste diretório.

Se esta máquina estiver configurada como um servidor CDS, recomenda-se a criação de um novo sistema de arquivos montado sobre **/var/dce/directory** antes de instalar o DCE.

Reserve cerca de 30 megabytes para uso do servidor.

Se não planejar criar um sistema de arquivos separado para o servidor CDS, inclua os 30 megabytes adicionais em **/var/dce**.

/var/dce/security

Aqui é onde o servidor de segurança armazena o registro, credenciais e dados locais. Se esta máquina vai ser um servidor de segurança, deve-se incluir 10 megabytes adicionais em **/var/dce** para uso do servidor.

Os arquivos armazenados em **/var/dce** são quaisquer arquivos particulares à máquina individual. Deve-se monitorar o uso do espaço em **/var/dce** (e quaisquer sistemas de arquivos associados separados) para certificar-se de que ele não fique cheio. Para limpar arquivos de credenciais expiradas em **/var/dce**, use o comando **/usr/lpp/dce/bin/rmxcred**. Os recursos de Auditoria e Manutenção do DCE também usam espaço em **/var/dce**. Consulte o *IBM DCE Version 3.2 for AIX and Solaris: Administration Commands Reference* para obter maiores informações sobre **rmxcred** e Auditoria DCE. Consulte o *IBM DCE*

Version 3.2 for AIX and Solaris: Problem Determination Guide para obter maiores informações sobre logs de manutenção DCE.

Capítulo 3. Instalação, Remoção da Instalação e Migração para o DCE 3.2 para AIX

Use as seguintes seções para a instalação:

- “Pacotes Instaláveis”
- “Instalação do DCE 3.2” na página 63
- “Migração de uma Célula DCE do AIX para o DCE 3.2 para AIX” na página 65

Pacotes Instaláveis

A seguir, um resumo dos conjuntos de arquivos instaláveis para os pacotes do DCE 3.2 para AIX. Para obter descrições mais detalhadas, consulte o “Capítulo 1. Visão geral do DCE 3.2 para AIX” na página 3.

- `dce.bundles` — Pacotes do DCE

`dce.bundles.Bnd`

Pacotes do DCE

- `dce.cds` — Pacote do Servidor de Diretório de Célula (Cell Directory Server - CDS)

`dce.cds.rte`

Serviços de Diretório de Célula

`dce.cds.smit`

Serviços de Diretório de Célula SMIT

- `dce.client` — Pacote de Serviços de Base

`dce.client.rte`

Serviços de Cliente

`dce.client.core.rte`

Serviços de Cliente-PARA ATUALIZAÇÕES

`dce.client.core.rte.rpc`

Ferramentas RPC de Cliente-PARA ATUALIZAÇÕES

`dce.client.rte.admin`

Ferramentas Administrativas de Cliente

`dce.client.rte.cds`

Ferramentas CDS de Cliente

`dce.client.rte.config`

Ferramentas de Configuração de Cliente

dce.client.rte.threads

Biblioteca de Compatibilidade de Threads

dce.client.rte.rpc

Ferramentas RPC de Cliente

dce.client.rte.security

Ferramentas de Segurança de Cliente

dce.client.rte.time

Ferramentas de Horário de Cliente

dce.client.rte.web

DCE Web Secure

dce.client.rte.zones

Fusos Horários de Cliente

dce.client.smit

Ferramentas SMIT de Cliente

- dce.compat—pacote de atualização DCE

dce.compat.cds.smit

Serviços de Diretório de Célula DCE SMIT-PARA ATUALIZAÇÕES

dce.compat.client.core.smit

Ferramentas de Cliente DCE SMIT-PARA ATUALIZAÇÕES

dce.compat.sysmgmt.ems.smit

Serviços de Gerenciamento de Eventos DCE SMIT-PARA ATUALIZAÇÕES

dce.compat.sysmgmt.snmpagt.smit

Subagente SNMP DCE SMIT-PARA ATUALIZAÇÕES

dce.compat.security.smit

Serviços de Segurança DCE SMIT-PARA ATUALIZAÇÕES

dce.compat.web.admin.smit

Administração do DCE SMIT Web Secure-PARA ATUALIZAÇÕES

- dce.doc — Documentação Online do DCE

Nota: Substitua *<linguagem>* pelo nome de locale apropriado. O DCE 3.2 para AIX suporta os seguintes locales: **en_US, ja_JP, Ja_JP, JA_JP, ko_KR, KO_KR, pt_BR, PT_BR, zh_TW, Zh_TW** ou **ZH_TW**.

dce.doc.rte.asciiNavegador ASCII DCE e **dceman****dce.doc.<linguagem>.ascii**

Arquivos do Navegador ASCII DCE

dce.doc.<linguagem>.html
Arquivos de Documentação HTML

dce.doc.<linguagem>.pdf
Arquivos de Documentação PDF

- dce.msg.en_US — Pacote de Mensagens

Nota: Substitua <linguagem> pelo nome de locale apropriado. O DCE 3.2 para AIX suporta os seguintes locales: **en_US, es_ES, Es_ES, ES_ES, ja_JP, Ja_JP, JA_JP, ko_KR, KO_KR, pt_BR, PT_BR, zh_TW, Zh_TW, ou ZH_TW.**

dce.msg.<linguagem>.client.rte
Mensagens de Cliente Básicas

dce.msg.<linguagem>.cds.smit
Mensagens do Servidor de Diretório de Célula (Cell Directory Server - CDS) SMIT

dce.msg.<linguagem>.client.smit
Mensagens Básicas SMIT

dce.msg.<linguagem>.security.smit
Mensagens do Servidor de Segurança SMIT

dce.msg.<linguagem>.sysmgmt.ems.smit
Mensagens de Gerenciamento de Eventos DCE SMIT

dce.msg.<linguagem>.sysmgmt.snmpagt.smit
Mensagens de Subagente SNMP DCE SMIT

dce.msg.<linguagem>.sysmgmt.ems.rte
Mensagens de Serviços de Gerenciamento de Eventos DCE

dce.msg.<linguagem>.sysmgmt.snmpagt.rte
Mensagens de Subagente SNMP DCE

dce.msg.<linguagem>.sysmgmt.webadmin.rte
Mensagens do DCE Web Administration

- dce.priv — Pacote do Recurso de Proteção de Nível de Privacidade (Privacy Level Protection)

dce.priv.rte
Recurso de Proteção de Nível de Privacidade (Privacy Level Protection)

dce.pthreads.rte
Biblioteca de Compatibilidade de Threads- PARA ATUALIZAÇÕES

- dce.security — Pacote do Servidor de Segurança

dce.security.rte
Serviços de Segurança

- dce.security.smit**
Serviços de Segurança SMIT
- **dce.sysmgmt** — Pacote de Gerenciamento do Sistema DCE
 - dce.sysmgmt.ems.rte**
Serviços de Gerenciamento de Eventos DCE
 - dce.sysmgmt.ems.smit**
Serviços de Gerenciamento de Eventos DCE SMIT
 - dce.sysmgmt.snmpagt.rte**
Subagente SNMP DCE
 - dce.sysmgmt.snmpagt.smit**
Subagente SNMP DCE SMIT
 - dce.sysmgmt.webadmin.rte**
GUI de Administração do DCE Web Secure
- **dce.tools** — Ferramentas DCE para Desenvolvedores de Aplicações
 - dce.tools.admin.rte**
Ferramentas de Administração
 - dce.tools.appdev.adt**
Ferramentas de Desenvolvimento de Aplicações
- **dce.web**—Atualizações do DCE Web Secure
 - dce.web.admin.rte**
GUI do DCE Web Secure para atualizações
 - dce.web.secure.rte**
DCE Web Secure para atualizações
- **dce.xdsxom** — Pacote da Biblioteca de APIs X.500
 - dce.xdsxom.rte**
Biblioteca de APIs X.500

Software Necessário

A Tabela 1 na página 59 lista os conjuntos de arquivos do DCE 3.2 para AIX na ordem na qual eles são instalados. Consulte o *IBM DCE Version 3.2 para AIX: Notas do Release* para os níveis mais recentes de software necessário.

Nota: Os nomes de software que começam com "dce" estão no mesmo nível de release do produto DCE enviado.

Tabela 1. Conjuntos de arquivos de instalação e software necessário

Conjunto de Arquivos que está sendo instalado	Nomes de Software Pré-requisito ¹ , Co-requisito ² , e Instreq ³	Descrição de Software Pré-requisito, Co-requisito ou Instreq
dce.bundles — Pacotes do DCE		
dce.bundles	N/A	N/A
dce.client — Pacote de Serviços de Base		
dce.client.rte.pthreads	bos.rte ¹	Tempo de Execução do Sistema Operacional de Base (BOS) AIX
dce.client.rte.pthreads	bos.rte.libpthreads ¹	Biblioteca libpthreads
dce.client.rte.pthreads	bos.rte.libc ¹	Biblioteca libc
dce.client.rte	bos.net.tcp.client ¹	Suporte a Cliente TCP/IP
dce.client.rte	xlC.rte ¹	Conjunto C ++ para o Tempo de Execução da Aplicação AIX
dce.client.rte	bos.adt.lib ¹	Bibliotecas de Base de Desenvolvimento de Aplicações
dce.client.rte	dce.client.rte.pthreads ¹	Biblioteca de Compatibilidade de Threads DCE para AIX
dce.client.rte	dce.client.rte.config ²	Ferramentas de Configuração de Cliente DCE
dce.client.rte	dce.client.rte.security ²	Ferramentas de Segurança de Cliente DCE
dce.client.rte	dce.client.rte.cds ²	Ferramentas CDS de Cliente DCE
dce.client.rte	dce.client.rte.time ²	Ferramentas de Horário de Cliente DCE
dce.client.rte	dce.client.rte.zones ²	Fusos Horários de Cliente DCE
dce.client.rte	dce.client.rte.admin ²	Ferramentas Administrativas de Cliente DCE
dce.client.rte	dce.client.rte.rpc ²	Ferramentas RPC de Cliente DCE
dce.client.rte.admin	dce.client.rte ¹	Serviços de Cliente DCE
dce.client.rte.cds	dce.client.rte ¹	Serviços de Cliente DCE

Tabela 1. Conjuntos de arquivos de instalação e software necessário (continuação)

Conjunto de Arquivos que está sendo instalado	Nomes de Software Pré-requisito ¹ , Co-requisito ² , e Instreq ³	Descrição de Software Pré-requisito, Co-requisito ou Instreq
dce.client.rte.config	dce.client.rte ¹	Serviços de Cliente DCE
dce.client.rte.rpc	dce.client.rte ¹	Serviços de Cliente DCE
dce.client.rte.security	dce.client.rte ¹	Serviços de Cliente DCE
dce.client.rte.time	dce.client.rte ¹	Serviços de Cliente DCE
dce.client.rte.zones	dce.client.rte ¹	Serviços de Cliente DCE
dce.client.smit	dce.client.rte ¹	Serviços de Cliente DCE
dce.client.rte.web	dce.client.rte ¹	Serviços de Cliente DCE
dce.priv — Pacote de Proteção de Nível de Privacidade (Privacy Level Protection)		
dce.priv.rte	dce.client.rte ¹	Serviços de Cliente DCE
dce.security — Pacote do Servidor de Segurança		
dce.security.rte	dce.client.rte ¹	Serviços de Cliente DCE
dce.security.smit	dce.security.rte ¹	Servidor de Segurança DCE
dce.security.smit	dce.client.smit ¹	Ferramentas de Cliente DCE SMIT
dce.cds — Pacote do Servidor do Diretório de Célula		
dce.cds.rte	dce.client.rte ¹	Serviços de Cliente DCE
dce.cds.smit	dce.cds.rte ¹	DCE Cell Directory Server
dce.cds.smit	dce.client.smit ¹	Ferramentas do Cliente DCE SMIT
dce.doc — Documentação Online do DCE		
dce.doc.rte.ascii	dce.client.rte.pthreads ¹	Biblioteca de Compatibilidade de Threads DCE para AIX
dce.doc.en_US.ascii	dce.doc.rte.ascii ¹	Navegador ASCII DCE e dceman
dce.doc.en_US.html	N/A	Navegador da Web
dce.doc.en_US.pdf	N/A	Arquivos PDF
dce.tools — Ferramentas DCE para Desenvolvedores de Aplicações		

Tabela 1. Conjuntos de arquivos de instalação e software necessário (continuação)

Conjunto de Arquivos que está sendo instalado	Nomes de Software Pré-requisito ¹ , Co-requisito ² , e Instreq ³	Descrição de Software Pré-requisito, Co-requisito ou Instreq
dce.tools.admin.rte	dce.client.rte ¹	Serviços de Cliente DCE
dce.tools.appdev.adt	dce.client.rte ¹	Serviços de Cliente DCE
	bos.adt.syscalls ¹	Kit de Ferramentas de Desenvolvimento de aplicações de Chamadas do Sistema
	bos.adt.include ¹	Arquivos de Inclusão de Desenvolvimento de Aplicações de Base
dce.xdsxom — X.500 Pacote da Biblioteca de APIs		
dce.xdsxom.rte	dce.client.rte.pthreads ¹	Biblioteca de Compatibilidade de Threads DCE para AIX
dce.sysmgmt — Pacote de Gerenciamento do Sistema DCE		
dce.sysmgmt.ems.smit	dce.sysmgmt.ems.rte ¹	Serviços de Gerenciamento de Eventos DCE
dce.sysmgmt.ems.smit	dce.client.smit ¹	Ferramentas de Cliente DCE SMIT
dce.sysmgmt.ems.rte	dce.client.rte ¹	Serviços de Cliente DCE
dce.sysmgmt.snmpagt.rte	dce.client.rte ¹	Serviços de Cliente DCE
dce.sysmgmt.snmpagt.smit	dce.sysmgmt.ems.rte ¹	Serviços de Gerenciamento de Eventos DCE
dce.sysmgmt.snmpagt.smit	dce.client.smit ¹	Serviços de Cliente DCE SMIT
dce.sysmgmt.webadmin.rte	dce.client.rte.web ¹	DCE Web Secure
dce.msg.en_US — Pacote de Mensagens		
dce.msg.en_US.client.rte	dce.client.rte ³	Serviços de Cliente DCE
dce.msg.en_US.cds.smit	dce.cds.smit ³	DCE SMIT Cell Directory Server
dce.msg.en_US.client.smit	dce.client.smit ³	Ferramentas de Cliente DCE SMIT
dce.msg.en_US.security.smit	dce.security.smit ³	Servidor de Segurança DCE SMIT

Tabela 1. Conjuntos de arquivos de instalação e software necessário (continuação)

Conjunto de Arquivos que está sendo instalado	Nomes de Software Pré-requisito ¹ , Co-requisito ² , e Instreq ³	Descrição de Software Pré-requisito, Co-requisito ou Instreq
dce.msg.en_US.sysmgmt.ems.smit	dce.sysmgmt.ems.smit ³	Gerenciamento de Eventos DCE SMIT
dce.msg.en_US.sysmgmt.snmpagt.smit	dce.sysmgmt.snmpagt.smit ³	Subagente SNMP DCE SMIT
dce.msg.en_US.sysmgmt.ems.rte	dce.sysmgmt.ems.rte ³	DCE Event Management Services
dce.msg.en_US.sysmgmt.snmpagt.rte	dce.sysmgmt.snmpagt.rte ³	Subagente DCE SNMP
dce.msg.en_US.sysmgmt.webadmin.rte	dce.sysmgmt.webadmin.rte ³	DCE Web Administration

Notas:

Para o Pacote de Mensagens, os seguintes conjuntos de arquivos de idiomas podem substituir o conjunto de arquivos **en_US**: **es_ES, Es_ES, ES_ES, ja_JP, Ja_JP, JA_JP, ko_KR, KO_KR, pt_BR, PT_BR, zh_TW, Zh_TW** ou **ZH_TW**.

Para a Documentação Online do DCE, os seguintes conjuntos de arquivos de idiomas podem substituir o conjunto de arquivos **en_US**: **ja_JP, Ja_JP, JA_JP, ko_KR, KO_KR, pt_BR, PT_BR, zh_TW, Zh_TW** ou **ZH_TW**.

¹Os conjuntos de arquivos de pré-requisito devem ser instalados antes do conjunto de arquivos que se deseja instalar. (O conjunto de arquivos não pode ser instalado antes do conjunto de arquivos pré-requisito.)

²Os conjuntos de arquivos de co-requisito (Coreq) devem estar disponíveis para serem instalados quando da instalação do conjunto de arquivos desejado. (A ordem de instalação dos conjuntos de arquivos não é importante). Não se pode remover a instalação de um conjunto de arquivos sem remover seus co-requisitos, e vice-versa.

³Conjuntos de arquivos que apontam outros como instreq somente serão instalados se o conjunto de arquivos apontado como instreq estiver instalado ou disponível para instalação. O conjunto de arquivos que é instreq de outro não tem dependência do conjunto de arquivos que o apontou como instreq. (A ordem de instalação dos conjuntos de arquivos não é importante). O conjunto de arquivos que apontou outro como instreq pode ser removido. O conjunto de arquivos que foi apontado como instreq não pode ser removido sem que o conjunto de arquivos que o apontou como instreq também seja removido.

Nota: Para usar e configurar o LDAP com os servidores de segurança, é preciso instalar o conjunto de arquivos **ldap.client.rte 3.2.1.0** ou posterior.

Instalação do DCE 3.2

Esta seção discute a instalação do DCE 3.2.

Processo de Software a Interromper

Se estiver atualizando uma instalação existente, encerre manualmente todas as aplicações em execução no DCE, e execute **dce.clean all** para interromper todos os processos do DCE em execução.

Execução do Programa de Instalação Fácil

Com o sistema operacional AIX, pode-se instalar software mais facilmente usando pacotes de software. Um pacote de software contém uma lista de produtos de software adequados a um uso específico. O procedimento a seguir mostra como instalar o DCE para AIX usando este recurso. Ele pode ser executado no console do sistema ou remotamente e executa sob X Windows ou em um terminal ASCII.

1. Efetue login como root.
2. Digite:
smitty easy_install_bundle
3. Especifique o dispositivo de instalação ou diretório para a mídia de instalação pressionando <F4> para exibir uma lista. Selecione o dispositivo de entrada desejado.
4. Pressione <Enter>.
5. Selecione **Definido pela Mídia** e pressione <Enter>.
6. Pressione <Enter> novamente para aceitar as seleções de Instalação Fácil.
7. No prompt **Tem Certeza**, pressione <Enter> novamente. Os Pacotes de DCE são instalados em **/usr/sys/inst.data/sys_bundles**.
8. Pressione <F3> para cancelar.
9. Pressione <F4> para obter a nova lista de pacotes de software a instalar.
Des-Apl
Cliente
DCE-CDS
DCE-Cliente
DCE-Gerenciamento
DCE-Segurança
DCE-Inicial
DCE-Ferramentas
Definido-pela-Mídia
Prod-Pess
Servidor

Consulte Tabela 2 na página 64 para o conteúdo de cada seleção de pacote do DCE.

10. Para cada pacote que deseja instalar:

- a. Selecione o nome do pacote.
- b. Pressione <Enter>.
- c. Pressione <Enter> novamente.
- d. Pressione <F3> para cancelar.
- e. Pressione <F4> para retornar à lista de pacotes, se ainda desejar instalar pacotes adicionais.

Tabela 2. Pacotes de Software do DCE

Pacote de Software	Nome do Pacote	Nome e Conjuntos de Arquivos
DCE-CDS	DCE-CDS.bnd	Pacote do CDS dce.cds.smit dce.cds.rte
DCE-Cliente	DCE-Client.bnd	Pacote do Cliente DCE dce.client.rte dce.xdsxom.rte dce.client.smit
DCE-Gerenciamento	DCE-Management.bnd	Pacote de Gerenciamento DCE dce.sysmgmt.ems.rte dce.sysmgmt.snmpagt.rte dce.sysmgmt.ems.smit dce.sysmgmt.snmpagt.smit dce.client.rte.web
DCE-Segurança	DCE-Security.bnd	Pacote de Segurança do DCE dce.security.rte dce.security.smit dce.client.rte.security

Tabela 2. Pacotes de Software do DCE (continuação)

Pacote de Software	Nome do Pacote	Nome e Conjuntos de Arquivos
DCE-Inicial	DCE-Starter.bnd	Pacote Inicial do DCE dce.client.rte dce.xdsxom.rte dce.client.smit dce.security.rte dce.cds.rte dce.security.smit dce.cds.smit
DCE-Ferramentas	DCE-Tools.bnd	Pacote de Ferramentas do DCE dce.tools.admin.rte dce.tools.appdev.adt

Instruções Especiais de Instalação

Para informações sobre procedimentos de instalação, consulte o *RISC System/6000 Installation Guide* enviado com o Sistema Operacional AIX. Este manual contém informações sobre o comando **installp**.

Migração de uma Célula DCE do AIX para o DCE 3.2 para AIX

Como o DCE 3.2 para AIX depende do AIX 4.3.3 ou AIX 5.1, uma destas versões deve estar instalada nas máquinas para migrar do DCE 1.3, 2.1, 2.2 ou 3.1 (qualquer destas versões com ou sem PTFs) para AIX para o DCE 3.2 para AIX. Esta migração pode ser feita sem uma reconfiguração da célula DCE existente usando os seguintes procedimentos. Não é necessário migrar as máquinas em uma ordem específica, mas preste muita atenção às limitações à funcionalidade do Servidor de Segurança DCE conforme descrito em “Migração de Réplicas de Segurança DCE (somente o DCE Anterior)” na página 66. Leia toda esta seção antes de começar o procedimento de migração.

Antes de Migrar

1. No DCE 3.2 para AIX, cada estação de trabalho em uma célula DCE mantém informações de configuração sobre os clientes e servidores DCE em execução na máquina local.
2. No caso de ser necessário recuperar a configuração do DCE anterior à migração, faça backup de todos os dados nos seguintes diretórios e subdiretórios:

`/opt/dcelocal/var`
`/opt/dcelocal/krb5`
`/opt/dcelocal/etc`

ou execute o comando **dceback** que se encontra no CD-ROM do DCE. O comando **dceback** está documentado no *IBM DCE Version 3.2 for AIX and Solaris: Administration Commands Reference*.

3. Instale o AIX 4.3.3 ou o AIX 5.1, incluindo os PTFs que são pré-requisitos para o DCE. Os pré-requisitos estão listados no *IBM DCE Version 3.2 para AIX: Notas do Release*. Use a versão de **Migração** da Instalação do AIX.

Migração de Clientes DCE

1. Pare o DCE. Consulte “Parada de Daemons do DCE” na página 129 para obter informações sobre como parar o DCE.
2. Instale o DCE 3.2 para AIX. Escolha os mesmos pacotes de servidor e de cliente que estavam instalados para o nível anterior do DCE para AIX nesta máquina.
3. Inicie o DCE executando **start.dce**. **start.dce** chamará **migrate.dce** para migrar todos os dados de configuração do DCE para o formato do DCE 3.2 para AIX. Como a Integração de Segurança AIX (**dceunixd**) não era suportada pelas ferramentas de configuração antes do DCE 2.2, ela será migrada somente se puder ser detectada no arquivo `/etc/inittab`. Se o DFS estava configurado anteriormente e **start.dce** for especificado, **migrate.dfs** migrará os dados do DFS.

Migração de Réplicas de Segurança DCE (somente DCE Anterior)

As Réplicas dos Servidores de Segurança DCE podem ser migrados usando as etapas documentadas em “Migração de Clientes DCE”. Recomenda-se que todas as réplicas de segurança na célula sejam migradas antes de ativar a função do DCE 3.2 para AIX no servidor de segurança principal. Ao planejar a migração, lembre-se das seguintes limitações:

1. Se as réplicas de segurança forem migradas antes da migração do servidor de segurança principal, elas executarão somente com a função do nível anterior do DCE para AIX ativada. Quando a função do DCE 3.2 para AIX for ativada no principal de segurança usando o comando **dcecp** (dado na Etapa 3 na página 67 sob “Migração do DCE Security Master (somente DCE Anterior)” na página 67), estas réplicas dos servidores de segurança também ativarão a função do DCE 3.2 para AIX.
2. Se a função do DCE 3.2 para AIX for ativada no servidor de segurança principal antes da migração de todas as réplicas de segurança, quaisquer réplicas que estejam executando o nível

anterior do DCE serão encerradas. Estas réplicas de segurança não podem suportar a função do DCE 3.2 para AIX.

Migração de Servidores CDS do DCE

1. Assegure-se de que todas as réplicas do diretório principal do CDS localizadas nesta máquina estejam replicadas em no mínimo uma outra máquina de servidor na célula. Se desejar suportar atualizações a estes diretórios do CDS durante o processo de migração, mova estas réplicas do diretório principal para outro servidor CDS.
2. Realize as tarefas descritas em “Migração de Clientes DCE” na página 66.

Migração do DCE Security Master (somente DCE Anterior)

1. Para minimizar o impacto em operações em andamento na célula, assegure que no mínimo uma réplica do servidor de segurança esteja em execução antes de começar. Isto suportará a continuidade das operações de **consulta** do servidor de segurança, embora operações de **atualização** não sejam suportadas durante o tempo em que o servidor de segurança principal estiver inoperante.

Se a máquina que é o servidor de segurança principal também for um servidor CDS, assegure-se de que todas as réplicas do diretório principal do CDS localizadas nesta máquina estejam replicadas em no mínimo uma outra máquina de servidor CDS na célula. Se desejar suportar atualizações a estes diretórios do CDS durante o processo de migração, mova estas réplicas do diretório principal para outro servidor CDS.

2. Realize as tarefas descritas em “Migração de Clientes DCE” na página 66.

Neste ponto do processo de migração, todas as funções do nível anterior do DCE para AIX permanecem operacionais, mas as funções do DCE 3.2 para AIX ainda não estão ativadas.

Nota: Se pretender ativar o recurso de Integração do Registro de Segurança com o LDAP, consulte o *IBM DCE Version 3.2 for AIX and Solaris: DCE Security Registry and LDAP Integration Guide* para obter informações sobre como definir o nível do registro de segurança.

3. Com login efetuado como administrador da célula, ative a função do DCE 3.2 para AIX executando as seguintes etapas:
 - a. Verifique a versão do registro emitindo o seguinte comando:
`dcecp -c registry show`
 - b. Se a versão da não for `secd.dce.1.2.2`, emita o seguinte comando:

```
dcecp -c registry modify -version {secd.dce.1.2.2}
```

- c. Se a célula suportará login com certificado de Chave Pública, emita o seguinte comando:

```
dcecp -c registry modify -version {secd.dce.1.2.2a}
```

- d. Se for ativar o LDAP, consulte o *IBM DCE Version 3.2 for AIX and Solaris: DCE Security Registry and LDAP Integration Guide*. Se a célula do DCE 3.2 for migrada para explorar o recurso de Integração do Registro de Segurança com o LDAP, o número da versão do Registro mudará para secd.dce.1.3.

Recomenda-se que estas etapas sejam executadas somente após todos os servidores de segurança de réplica na célula terem sido migrados para o DCE 3.2 para AIX. Para mais informações, consulte o *IBM DCE Version 3.2 for AIX and Solaris: Administration Guide—Core Components*.

Nota: Quando a versão do registro de Segurança é alterada, quaisquer réplicas dos servidores de segurança na célula que não puderem ser executados nessa nova versão do registro de Segurança serão encerrados. As versões do registro de Segurança do OSF DCE secd.1.2.2 e secd.1.2.2a são suportadas pelo DCE 2.2 para AIX, DCE 3.1 para AIX e Solaris, DCE 3.2 para AIX e Solaris e DCE para Windows NT V2.2. A versão do registro de Segurança do OSF DCE secd.1.3 somente é suportada pelo DCE 3.2 para AIX e Solaris.

4. Após haver migrado o servidor de segurança principal, é preciso validar quaisquer contas entre as células que existam no registro do DCE. Isto pode ser feito usando o seguinte comando, estando com login efetuado como administrador da célula:

```
/usr/bin/dcecp -c account modify krbtgt/nome_da_célula  
-change {acctvalid yes}
```

onde *nome_da_célula* é o nome da célula externa. Se essas contas não forem validadas, o acesso entre as células de clientes não-AIX OSF 1.2.2 à célula externa falhará.

Migração de Servidores DTS

Para migrar corretamente servidores DTS, siga as tarefas descritas em “Migração de Clientes DCE” na página 66. Note que quaisquer provedores de horário em uso no sistema não serão reconhecidos pela ferramenta de migração. Para continuar a usar um provedor de horário, pode ser necessário reconfigurá-lo manualmente após concluir a migração.

Migração de Servidores de Senha Válida

As informações a seguir serão úteis ao migrar uma máquina com um servidor de Senha Válida configurado.

O servidor de Senha Válida enviado com o DCE 3.1 é um servidor de Senha Válida melhorado. Este novo servidor de Senha Válida sobreporá o `pwd_strengthd` em `/opt/dcelocal/bin`. A versão anterior de `pwd_strengthd` que estava em `/opt/dcelocal/bin` será salva como `/usr/lpp/save.config/usr/lpp/dce/bin/pwd_strengthd`.

- **Servidor de Senha Válida fornecido pelo DCE**

Se você estava usando o servidor de Senha Válida enviado com uma versão anterior do DCE (`pwd_strengthd`), a menos que etapas manuais adicionais de migração forem realizadas, o novo servidor de Senha Válida suportará somente o nível de função enviado no release anterior. Para operar no modo melhorado, o novo servidor de Senha Válida exige etapas adicionais de configuração que não foram realizadas em releases anteriores do DCE. Estas etapas adicionais não podem ser realizadas pelo processo de migração porque é exigida autoridade de administrador de célula para executar as etapas. Para ativar os novos recursos, siga um dos seguintes procedimentos:

- Atualize a configuração do servidor de Senha Válida existente.

1. Efetue login como administrador da célula.

2. Execute

```
/opt/dcelocal/bin/migrate_pwd_strengthd
```

- Reconfigure o servidor de Senha Válida.

Na máquina do servidor de Senha Válida:

1. Execute

```
unconfig.dce pw_strength_svr
```

2. Execute

```
config.dce pw_strength_svr
```

Consulte *IBM DCE Version 3.2 for AIX and Solaris: Administration Guide—Core Components* para obter informações sobre como ativar as regras do servidor de Senha Válida para senhas de usuários DCE.

- **Servidores de Senha Válida Personalizados**

Se você criou seu próprio servidor de Senha Válida usando um nome de executável diferente de `/opt/dcelocal/bin/pwd_strengthd`, nenhuma etapa especial de migração é necessária.

Se você estava usando uma versão personalizada de `pwd_strengthd` em `/opt/dcelocal/bin`, encontrará seu programa personalizado na localização salva indicada anteriormente. Se desejar continuar a usar sua versão personalizada de `pwd_strengthd`, recomenda-se que

o `pwd_strengthd` seja movido para uma nova localização e em seguida reconfigurado. Se isto for feito, a instalação de futuras versões do DCE não sobreporão o `pwd_strengthd` personalizado. Como alternativa, pode-se substituir o `pwd_strengthd` instalado pelo `pwd_strengthd` que foi salvo. Note que as regras que foram definidas não serão obrigadas a menos que se reinicie o DCE após substituir o servidor de Senha Válida instalado.

Se desejar reconfigurar o servidor de Senha Válida personalizado, execute as seguintes etapas na máquina do servidor de Senha Válida:

1. Copie o servidor de senha válida personalizado de `/usr/lpp/save.config/usr/lpp/dce/bin/pwd_strengthd` para uma localização diferente de `/opt/dcelocal/bin`.
2. Remova a configuração do servidor de senha válida usando o seguinte comando:

```
unconfig.dce -pwdstr_principal pwd_strengthd pw_strength_svr
```

3. Reconfigure o servidor de senha válida usando o seguinte comando:

```
config.dce -pwdstr_principal <nome do usuário principal \
-pwdstr_cmd <exe completamente qualificado> \
-pwdstr_arg <argumentos da linha de comandos> \
pw_strength_svr
```

onde *<nome do usuário principal>* é o nome do usuário principal usado pelo servidor de Senha Válida. O padrão para o release anterior era `pwd_strengthd`.

Notas:

- a. Se mais de um argumento da linha de comandos for aplicado à opção `-pwdstr_arg`, os argumentos precisam estar delimitados por aspas duplas (""). Por exemplo:

```
-pwdstr_arg "-v -d"
```

- b. Se desejar especificar um nome de usuário principal de senha válida diferente de `pwd_strengthd`, especifique as duas opções, `-pwdstr_principal` e `-pwdstr_arg -server_princ`. Por exemplo:

```
-pwdstr_principal pwd_server
-pwdstr_arg "-server_princ pwd_server"
```

Migração de Servidores de Mapeamento de Identidade

1. Para migrar corretamente um Servidor de Mapeamento de Identidade, siga as duas primeiras etapas de "Migração de Clientes DCE" na página 66.

2. Se, e somente se, você substituiu `/opt/dcelocal/bin/idmsd` por seu próprio daemon `idmsd`, copie seu `idmsd` de backup de `/usr/lpp/save.config/usr/lpp/dce/bin`.
3. Inicie o DCE executando `start.dce`.

Migração de Servidores CDS em Cache

Ao migrar uma versão anterior do DCE de um sistema DCE AIX que tenha uma conexão entre as células estabelecida pelo uso do comando `cdscp define cached server`, o comando `config.dce` precisa ser usado após instalar o novo nível do DCE e antes de usar `start.dce` para preservar o conhecimento do servidor em cache. Use a opção `-cds_replica_list` para especificar os servidores `cds`. Esta é uma lista delimitada que pode ter vários servidores separados por espaços. Ou o nome do host ou o endereço IP pode ser usado nesta lista. Por exemplo:

```
config.dce -cds_replica_list "server1 server2"
```

Executando este comando, a lista de servidores `cds` será preservada fora do cache `cds`. Esta informação será usada para atualizar o cache `cds` toda vez que o DCE for reiniciado. A opção `-cds_replica_list` pode ser usada a qualquer momento para atualizar a lista de servidores `cds`. O comando `config.dce` realizará um `define cached server` para cada novo servidor `cds`. Quando servidores forem removidos, o cache não será atualizado até que seja limpo.

Se a etapa anterior não for realizada, a conexão entre as células pode ser retomada repetindo o comando `cdscp define cached server` original ou o comando `dcecp cdscache create` correspondente.

Nota: A opção `-cds_replica_list` era suportada no DCE 3.1. Se as informações deste servidor CDS foram salvas antes desta migração, não é preciso salvá-las novamente. As informações sobre o servidor CDS podem ser atualizadas executando novamente o comando anterior.

Migração do DCE Web Secure para a versão atual do DCE para AIX

Se o DCE Web Secure estava configurado para um release anterior ao DCE 3.1, é preciso migrar o servidor Web para o release atual antes que ele possa estar funcional. Será feita uma tentativa de migrar as informações de configuração de `dceweb` quando algum dos seguintes comandos for executado:

- `migrate.dceweb`
- `start.dce`
- `stop.dce`
- `config.dce`

- **unconfig.dce**

Além disso, se o servidor dceweb específico que se está tentando configurar ou desconfigurar não tiver sido migrado com êxito, será feita uma tentativa de migrar as informações de configuração de dceweb quando algum dos seguintes comandos for executado:

- **mkdceweb**
- **rmdceweb**

Para que um servidor Netscape do DCE Web Secure/Admin específico configurado anteriormente seja funcional, as seguintes condições devem ser satisfeitas:

- O servidor Netscape em questão deve estar em execução.
- O DCE deve estar em execução.
- Os dados de configuração da configuração do DCE WebSecure/Admin para o servidor devem ter sido migrados.
- O servidor Netscape em questão deve ter sido parado e reiniciado após os dados de configuração terem sido migrados.

O processo **migrate.dceweb** parará e reiniciará o servidor Netscape do DCE Web Secure/Admin que ele tiver conseguido migrar com êxito.

Recomenda-se que se execute **migrate.dceweb** e se resolvam quaisquer problemas encontrados antes de tentar iniciar o DCE.

Migração do DCE Web Secure/Admin do IBM DCE V2.1 para AIX para o IBM DCE V3.2 para AIX

Há uma situação onde um servidor DCE Web Secure/Admin pode estar configurado e trabalhando, mas todas as informações pertinentes a ele não foram armazenadas no arquivo **/opt/dcelocal/web/etc/servers**. Devido a isto, alguns servidores do DCE WebSecure/Admin configurados anteriormente podem não ter sido migrados até o nível do IBM DCE V3.2 para AIX.

Verifique o arquivo **/opt/dcelocal/web/etc/servers** para ver se todos os servidores configurados estão listados. Uma entrada no arquivo dos servidores deve ser semelhante a:

```
my_server admin Enterprise 3.62 /netscape/suitespot
```

O primeiro campo é o nome do servidor. O segundo nome é o tipo de DCE WebSecure/Admin (secure para somente secure, admin para admin/secure). O terceiro campo é o tipo de servidor Netscape (Enterprise ou FastTrack). O quarto campo é o número da versão do Netscape. O último campo é o diretório pessoal Netscape do servidor.

Se estiver examinando este arquivo antes de realizar a migração, algumas destas linhas podem estar divididas. **Não tente consertar essas linhas divididas.** O arquivo dos servidores deve ser modificado somente por programas do DCE (a menos que a documentação do DCE dê instruções em contrário).

Se algum dos servidores do DCE WebSecure/Admin configurados anteriormente não estiver listado, faça o seguinte:

1. Para cada servidor do dceweb ausente, execute o seguinte como root:

```
add_dceweb_entry <nome_do_servidor> <dceweb_type> <ns_home>
```

Por exemplo:

```
add_dceweb_entry my_server admin /netscape/suitespot
```

2. Após todas as entradas terem sido incluídas com êxito no arquivo servidores, execute o programa de migração do DCE Web Secure/Admin, **migrate.dceweb**.

O programa **add_dceweb_entry** fará o seguinte:

- Se a entrada do servidor já existir no arquivo **/opt/dcelocal/web/etc/servers**, ela será exibida.
- Se a entrada do servidor foi incluída com êxito no arquivo servidores, a nova entrada será exibida.
- Se ocorreu um erro, o programa exibirá os dados que estão causando o problema juntamente com três pontos de interrogação (???)

O programa **add_dceweb_entry** é planejado somente para incluir entradas no arquivo servidores. Ele não atualizará entradas que já existam nesse arquivo.

Conjuntos de Arquivos Duplicados e Obsoletos Listados nos Menus de Instalação do SMIT (System Management Interface Tool)

Vários conjuntos de arquivos do DCE foram renomeados no release IBM DCE V3.1 para AIX. Quando uma instalação de atualização é feita, os conjuntos de arquivos são instalados com base no que já está instalado. Como os conjuntos de arquivos foram renomeados, os novos nomes não são encontrados no sistema. Para permitir atualizações, conjuntos de arquivos "fictícios" com os nomes antigos foram criados. Estes conjuntos de arquivos são co-requisitos daqueles com os novos nomes. Eles não instalam nenhum arquivo.

Quando instalar através do SMIT usando os menus instalar o mais recente ou instalar tudo, você verá o mesmo conjunto de arquivos listado duas vezes. Um destes é o conjunto de arquivos real com um

novo nome, e o outro é o conjunto de arquivos "fictício". O conjunto de arquivos "fictício" terá **PARA ATUALIZAÇÕES** em sua descrição. Por exemplo, **dce.client.core.rte** foi renomeado para **dce.client.rte**. Há um conjunto de arquivos "fictício" denominado **dce.client.core.rte**. A descrição que você verá para o pacote dce.client será:

```
dce client
+ 3.2.0.0 DCE Client Administrative Tools
+ 3.2.0.0 DCE Client CDS Tools
+ 3.2.0.0 DCE Client Configuration Tools
+ 3.2.0.0 DCE Client RPC Tools
+ 3.2.0.0 DCE Client RPC Tools - FOR UPGRADES
+ 3.2.0.0 DCE Client Security Tools
+ 3.2.0.0 DCE Client Services
+ 3.2.0.0 DCE Client Services - FOR UPGRADES
+ 3.2.0.0 DCE Client Time Tools
+ 3.2.0.0 DCE Client Time Zones
+ 3.2.0.0 DCE SMIT Client Tools
+ 3.2.0.0 DCE Threads Compatibility Library
+ 3.2.0.0 DCE Web Secure
```

Note que há duas entradas para "Serviços do Cliente DCE" e "Ferramentas RPC do Cliente DCE". Uma entrada contém "- PARA ATUALIZAÇÕES". Este é o conjunto de arquivos "fictício".

As opções de conjuntos de arquivos "fictício" não precisam ser selecionadas. Elas estão presentes para uso pelo menu Atualizar_tudo.

Uma vez que o DCE esteja instalado, os conjuntos de arquivos "fictícios" não precisam estar no sistema. A maioria deles será removida por outros conjuntos de arquivos. Às vezes, uns poucos podem ser deixados no sistema. A ordem na qual são instalados pode fazer com que alguns sejam deixados. Eles podem ser deixados no sistema ou removidos.

Consulte "Apêndice C. Conjuntos de Arquivos Fictícios" na página 143 para uma lista de conjuntos de arquivos "fictícios".

Migração de uma Célula DCE Existente para Explorar a Integração do Registro de Segurança DCE com o LDAP

A Integração do Registro de Segurança do DCE com o LDAP é um recurso novo no IBM DCE 3.2 para AIX. Este recurso aperfeiçoa o IBM DCE removendo as informações de segurança armazenadas no banco de dados específico do DCE conhecido como registro de segurança e armazenando essas informações em um diretório do LDAP.

Consulte o *IBM DCE Version 3.2 for AIX and Solaris: DCE Security Registry and LDAP Integration Guide* para obter informações sobre a migração de uma célula DCE existente para explorar este novo recurso.

Remoção da instalação do DCE 3.2

Antes de remover a instalação do DCE para AIX, Versão 3.2, é preciso remover a configuração de sua máquina. Consulte “Remoção de Configuração de Componentes do DCE” na página 121 para obter informações sobre a remoção da configuração.

No painel **Software Installation and Maintenance** do SMIT:

1. Selecione **Software Maintenance and Utilities**.
2. Selecione **Remove Software Products**.
3. Selecione **The Software to Remove**.

Digite o nome do software do qual deseja remover a instalação. Pressione <F4> para exibir uma lista de todo o software instalado.

4. Selecione **OK** ou **Do**.

Leitura Sugerida

Para informações sobre os procedimentos de instalação AIX, consulte o *RISC System/6000 Installation Guide*, enviado com o Sistema Operacional AIX.

Para informações sobre a configuração de uma célula DCE, consulte os comandos “Configuração do DCE” na página 79 e **config.dce** no *IBM DCE Version 3.2 for AIX and Solaris: Administration Commands Reference*.

Para informações sobre a remoção da configuração de componentes individuais do DCE, consulte o comando **unconfig.dce** no *IBM DCE Version 3.2 for AIX and Solaris: Administration Commands Reference*.

Para informações sobre a configuração e remoção da configuração do DCE Web Secure, consulte os comandos **mkdceweb** e **rmdceweb** no *IBM DCE Version 3.2 for AIX and Solaris: Administration Commands Reference*.

Parte 3. Configuração, Início e Parada do DCE 3.2 para AIX

Capítulo 4. Configuração dos Servidores e Clientes do DCE 3.2 para AIX

Configuração do DCE

As seções a seguir descrevem a criação e configuração de uma célula DCE:

- “Visão Geral da Configuração”
- “Configuração Inicial da Célula” na página 87
- “Configuração Adicional da Célula” na página 102
- “Remoção de Configuração de Componentes do DCE” na página 121

Estas seções incluem componentes de servidor e de cliente para os seguintes serviços do DCE: Security Service, Cell Directory Service (CDS), Distributed Time Service (DTS), Remote Procedure Call (RPC) e Global Directory Agent (GDA).

Para acessar os menus do SMIT para o DCE, selecione **Aplicações e Serviços de Comunicações** a partir do menu principal do SMIT. Em seguida, selecione **Distributed Computing Environment (DCE)** a partir do submenu Aplicações e Serviços de Comunicações.

Para obter informações sobre a definição do ambiente entre as células, o gerenciamento dos nomes entre as células e a administração de um ambiente nesse contexto, consulte o *IBM DCE Version 3.2 for AIX and Solaris: Administration Guide—Core Components*.

Visão Geral da Configuração

A configuração de uma célula DCE ocorre em duas fases. Durante a primeira fase, ou *configuração inicial da célula*, certas tarefas devem ser realizadas para Inicializar a célula. Durante a segunda fase, tarefas genéricas podem ser realizadas para configurar (ou reconfigurar) recursos adicionais na célula.

Uma célula DCE exige os seguintes componentes:

- Um servidor de segurança
- Um servidor CDS

Recomenda-se que também haja ao menos um servidor DTS (embora três ou mais servidores DTS sejam preferíveis para exatidão da sincronização de horário).

Os servidores de Segurança e CDS devem ser configurados para inicializar qualquer célula. Após a célula estar operacional e em execução, geralmente não é preciso repetir nenhuma destas tarefas de configuração.

Os componentes adicionais que podem ser configurados em uma célula são os seguintes:

- Clientes DCE (**dced**, **cdsadv**, **cdsclerk**, **dttd**)
- Servidores CDS secundários (**cdsd**)
- Réplicas dos Servidores de Segurança (**secd**)
- Serviços de Auditoria (**auditd**)
- Global Directory Agents (**gdad**)
- Serviços DTS (**dttd**)
- Simple Network Management Protocol (**dceagtd**)
- Event Management Service (**emsd**)
- Servidor de Senha Válida (**pwd_strengthd**)
- Integração de Segurança (**dceunixd**)
- Serviço de Mapeamento de Identidade (**idmsd**)
- Daemon da Interface do Serviço de Nomes (**nsid**)
- DCE Web Secure

A configuração destes componentes adicionais é uma tarefa que pode ser realizada a qualquer momento durante o tempo de operação da célula após a inicialização.

Lembre-se dos seguintes itens quando configurar uma célula:

- Para melhor desempenho e confiabilidade instale o servidor de segurança principal e o servidor CDS inicial em máquinas diferentes.
- Os clientes podem ser configurados de três maneiras:

Configuração Dividida

Este tipo de configuração é usado quando o administrador da célula DCE provavelmente não terá acesso root a todas as máquinas na célula. Ele é composto de dois conjuntos distintos de operações:

administração

Este tipo de configuração atualiza o espaço de nomes e o registro de segurança com informações sobre o novo cliente. O administrador da célula precisa executar o comando **config.dce** a partir de uma máquina na célula existente. Ele não pode ser executado a partir da máquina do novo cliente. O administrador da célula não precisa autoridade de usuário root para executar a parte de administração da configuração.

local

Este tipo de configuração cria os arquivos necessários na máquina local e inicia os daemons para o novo cliente. A parte de administração de **config.dce** deve ter sido

executada antes, caso contrário a configuração local falhará ao tentar contactar a célula. O usuário deve ter autoridade root na máquina, mas não precisa ter nenhuma autoridade na célula DCE. Os seguintes componentes não exigem que a parte de administração de **config.dce** seja executada antes: cliente básico, auditoria, login integrado e RPC.

Configuração Completa

Este tipo de configuração é o padrão. A configuração completa inclui as etapas de configuração de administração e local. O administrador da célula DCE deve ter autoridade root na máquina local que está sendo configurada na célula.

- Antes de configurar uma máquina em uma célula, certifique-se de que o relógio da máquina esteja dentro de cinco minutos do relógio do servidor de segurança principal da célula. Se o relógio da máquina estiver defasado mais de cinco minutos, erros de autenticação podem resultar, e a configuração pode falhar. Se já houver no mínimo um servidor DTS configurado na célula, o sinalizador **-sync_clocks** pode ser usado para realizar a sincronização automaticamente.
- Se desejar reconfigurar um componente particular (ou toda uma máquina) com novos parâmetros, é preciso remover a configuração existente dela antes de definir a nova configuração.
- Para ativar a comunicação entre as células usando o GDA, é preciso também registrar o nome da célula em um diretório global, tal como o Domain Name System (DNS). Para informações sobre o ambiente entre as células, consulte o *IBM DCE Version 3.2 for AIX and Solaris: Administration Guide—Core Components*.
- É possível realizar as tarefas iniciais e adicionais de configuração usando o SMIT (System Management Interface Tool). O SMIT usa menus interativos (em lugar de uma interface de linha de comandos) para guiar os usuários ao longo da configuração e de outras tarefas de gerenciamento do sistema. As seções a seguir fornecem procedimentos passo a passo para a configuração da célula usando o SMIT.

O DCE 3.2 para AIX também fornece os seguintes comandos para realizar essas mesmas tarefas de configuração na linha de comandos:

chpsite

Atualiza o arquivo **pe_site**, o qual contém os endereços dos servidores de segurança utilizados.

clean_up.dce

Limpa os arquivos do banco de dados que podem ser recriados, os arquivos de cache e os arquivos de credenciais. Este comando é planejado para ser usado quando surgirem problemas ao tentar iniciar o DCE.

config.dce

Configura e inicia componentes do DCE. Este comando permite uma *configuração dividida de clientes*. A configuração administrativa e a configuração local podem ser realizadas separadamente. Consulte “Configuração Adicional da Célula” na página 102 para obter maiores informações.

kerberos.dce

Cria os usuários principais do host, os usuários principais de FTP e entradas na tabela de chaves usadas para suportar os comandos de Segurança Remota.

migrate.dce

Migra dados da configuração do DCE de releases anteriores para uso com o release atual. Não há necessidade de configurar novamente quando se instala um novo release do DCE.

mkdcweb

Configura o DCE Web Secure e a DCE Web Administration em um servidor Web Netscape FastTrack ou Netscape Enterprise ou em um servidor Web iPlanet FastTrack ou iPlanet Enterprise.

mkreg.dce

Inclui informações sobre uma célula DCE no espaço de nomes DOMAIN.

rmdcweb

Remove a configuração do DCE Web Secure e a DCE Web Administration de um servidor Web Netscape FastTrack ou Netscape Enterprise ou em um servidor Web iPlanet FastTrack ou iPlanet Enterprise.

rmreg.dce

Remove informações sobre uma célula DCE do espaço de nomes DOMAIN (DNS).

show.cfg

Exibe a configuração DCE ou DFS do host local. As opções **dce** e **dfs** permitem exibir somente informações de DCE ou de DFS.

start.dce

Inicia os componentes do DCE configurados. Este comando certifica-se de que todos os componentes sejam iniciados na ordem correta.

stop.dce

Pára os componentes do DCE configurados. Este comando certifica-se de que todos os componentes sejam interrompidos na ordem correta.

unconfig.dce

Remove a configuração de componentes do DCE. Este comando prevê a *remoção de configuração dividida*, o que significa que a configuração

administrativa e a configuração local podem ser realizadas separadamente. Consulte “Configuração Adicional da Célula” na página 102 para obter maiores informações.

Nota: No IBM DCE V2.2 para AIX e acima, o comando **rm**dce é mapeado para **unconfig.dce**. Há várias alterações no comportamento do IBM DCE V2.1 para AIX e abaixo para o IBM DCE V2.2 para AIX e acima para o comando **rm**dce -o. Devido à verificação adicional de dependência de componentes que foi incluída em **unconfig.dce**, o sinalizador -F deve ser especificado quando se usar **rm**dce para realizar a remoção da configuração administrativa de um cliente DCE. O comando correto é:

```
rm
```

dce -o admin -h <nome_do_host_dce> -F all_cl

Além disso, há casos em que **rm**dce falhará com a seguinte mensagem:

```
0x11315417: Nem o nome do host IP nem o endereço IP da máquina
            foram especificados.
0x11315463: A tentativa de determinar o nome e endereço
            IP do host não obteve êxito.
            Emita novamente o comando unconfig.dce
            especificando a opção -host_id.
```

Para resolver isto, a opção -i foi adicionada a **rm**dce.

identificador -i

Identifica o host cuja configuração deve ser removida usando a opção de administração -o. Pode ser o nome do host ou o endereço TCP/IP de uma máquina.

Para informações detalhadas sobre estes comandos, consulte o *IBM DCE Version 3.2 for AIX and Solaris: Administration Commands Reference*.

Nota: O comando **ls**dce agora chama o comando **show.cfg**. O formato da saída do comando **ls**dce foi alterado. A saída agora é semelhante ao seguinte:

```
Reunindo informações sobre o estado do componente...
```

```
Resumo dos Componentes para o Host: witsend.austin.ibm.com
```

```
Componente Estado da Configuração
Servidor de Segurança Principal Configurado
Cliente de Segurança Configurado
RPC Configurado
Servidor de Diretório inicial Configurado
Cliente de diretório Configurado
```

```
0 resumo de componentes está concluído.
```

O comando **lsdce** passa um sinalizador para **show.cfg** para contornar as verificações do estado do daemon. O comando **show.cfg** executa mais lentamente que o antigo comando **lsdce** porque ele precisa determinar o estado de execução do daemon. Consulte a documentação em *IBM DCE Versão 3.2 for AIX e Solaris: Administration Commands Reference* sobre **show.cfg** para obter maiores informações.

Comandos Fornecidos pelo Usuário

O código de `config/unconfig/start/stop` do DCE 3.2 para AIX agora fornece suporte para comandos fornecidos pelo usuário. Os comandos fornecidos pelo usuário podem ser executados antes, depois, ou antes e depois da configuração, remoção da configuração, início e parada do DCE. A intenção deste suporte é permitir que o usuário execute seus próprios comandos sem ter que modificar os scripts enviados com o produto DCE. Quando um release futuro deste produto for instalado, os comandos fornecidos pelo usuário serão executados automaticamente com o novo release.

Nota: Os comandos do usuário são scripts, executáveis, etc, fornecidos pelo usuário, que os comandos de **config/unconfig/start/stop** do DCE chamam. Os comandos do DCE são scripts TCL e somente podem chamar comandos em um novo shell. Devido a isto, não é possível definir variáveis de ambiente nos scripts do usuário e esperar que elas estejam disponíveis ao comando DCE responsável pela chamada. Se for preciso definir variáveis de ambiente, coloque-as em **/etc/environment**, ou defina-as antes de executar os comandos de configuração do DCE. Se os métodos anteriores de definição de variáveis de ambiente não forem aceitáveis, as variáveis de ambiente podem ser incluídas diretamente no script **user_cmd.tcl**. As variáveis de ambiente definidas desta forma estão disponíveis a todos os scripts **config/unconfig/start/stop** do DCE. Use a seguinte sintaxe TCL:

```
set env(SUA_VAR_AMBIENTE) "valor-de-sua_var_ambiente"
```

onde `SUA_VAR_AMBIENTE` é a variável de ambiente que você deseja definir.

Faça o seguinte:

Escreva o comando para fazer o que desejar. Quando executados, os comandos de configuração (**config.dce**, **unconfig.dce**, **start.dce** e **stop.dce**) definem a variável de ambiente, **"callers_cmd_line"** (incluindo todos os parâmetros com exceção da senha do administrador da célula), para a linha de comandos. Por exemplo, ao configurar o DCE, se o comando executado for:

```
"config.dce -cell_name mycellname -admin_pwd -dce-sec_srv cds_srv"
```

A variável de ambiente **callers_cmd_line** é definida para:

```
"-cell_name mycellname -admin_pwd <****>  
sec_srv cds_srv"
```

Esta variável de ambiente pode ser útil para seu script de comando.

Crie o arquivo **/opt/dcelocal/tcl/user_cmd.tcl**. Este arquivo deve conter o subconjunto apropriado das seguintes entradas:

Para o DCE:

- **set pre_config_dce** — O caminho completo para o comando de pré-configuração DCE e quaisquer argumentos.
- **set pre_config_dce_fail_on_error** — **\$TRUE** ou **\$FALSE** para indicar se **config.dce** deve falhar (ou não) se seu comando falhar.
- **set post_config_dce** — o caminho completo para o comando de pós-configuração DCE e quaisquer argumentos.
- **set post_config_dce_fail_on_error** — **\$TRUE** ou **\$FALSE** para indicar se **config.dce** deve falhar (ou não) se seu comando falhar.
- **set pre_unconfig_dce** — O caminho completo para o comando de pré-remoção de configuração DCE e quaisquer argumentos.
- **set pre_unconfig_dce_fail_on_error** — **\$TRUE** ou **\$FALSE** para indicar se **unconfig.dce** deve falhar (ou não) se seu comando falhar.
- **set post_unconfig_dce** — O caminho completo para o comando de pós-remoção de configuração DCE e quaisquer argumentos.
- **set post_unconfig_dce_fail_on_error** — **\$TRUE** ou **\$FALSE** para indicar se **unconfig.dce** deve falhar (ou não) se seu comando falhar.
- **set pre_start_dce** — O caminho completo para o comando de pré-início de DCE e quaisquer argumentos.
- **set pre_start_dce_fail_on_error** — **\$TRUE** ou **\$FALSE** para indicar se **start.dce** deve falhar (ou não) se seu comando falhar.
- **set post_start_dce** — O caminho completo para o comando de pós-início de DCE e quaisquer argumentos.
- **set post_start_dce_fail_on_error** — **\$TRUE** ou **\$FALSE** para indicar se **start.dce** deve falhar (ou não) se seu comando falhar.
- **set pre_stop_dce** — O caminho completo para o comando de pré-interrupção do DCE e quaisquer argumentos.
- **set pre_stop_dce_fail_on_error** — **\$TRUE** ou **\$FALSE** para indicar se **stop.dce** deve falhar (ou não) se seu comando falhar.
- **set post_stop_dce** — O caminho completo para o comando de pós-parada de DCE e quaisquer argumentos.

- **set post_stop_dce_fail_on_error** — **\$TRUE** ou **\$FALSE** para indicar se **stop.dce** deve falhar (ou não) se seu comando falhar.

Nota: Use # para incluir um comentário em uma linha por si só. Use ;# para incluir um comentário em uma linha de código.

Os códigos de configuração, remoção de configuração, início e parada procuram o arquivo **/opt/dcelocal/tcl/user_cmd.tcl** e os seguintes nomes de variáveis:

pre_config_dce	pre_config_dce_fail_on_error
post_config_dce	post_config_dce_fail_on_error
pre_unconfig_dce	pre_unconfig_dce_fail_on_error
post_unconfig_dce	post_unconfig_dce_fail_on_error
pre_start_dce	pre_start_dce_fail_on_error
post_start_dce	post_start_dce_fail_on_error
pre_stop_dce	pre_stop_dce_fail_on_error
post_stop_dce	post_stop_dce_fail_on_error

Exemplos:

```
#Certifique-se de que App XYZ ainda não esteja configurada
#config.dce deve falhar se /usr/bin/APP_XYZ_config_check falhar
set pre_config_dce "/usr/bin/APP_XYZ_config_check"
set pre_config_dce_fail_on_error $TRUE
```

```
#O comando a seguir executa o comando de configuração App XYZ
#App XYZ deve ser configurada após o DCE
#config.dce NÃO falhará se /usr/bin/APP_XYZ_config falhar
set post_config_dce "/usr/bin/APP_XYZ_config -arg1valor_arg1 -arg2 valor_arg2"
```

```
#O comando a seguir executa o comando App XYZ start
#App XYZ deve iniciar após o DCE
#start.dce NÃO falhará se /usr/bin/APP_XYZ_start falhar
set post_start_dce "/usr/bin/APP_XYZ_start"
set post_start_dce_fail_on_error $FALSE
```

```
#Parar App ABC antes de parar o DCE
set pre_stop_dce "/usr/bin/APP_ABC_stop"
#stop.dce falhará se /usr/bin/APP_ABC_stop falhar
set pre_stop_dce_fail_on_error $TRUE
```

Variáveis de Ambiente

As variáveis de ambiente são variáveis usadas pelo DCE que podem ser definidas pelos próprios clientes. Consulte *IBM DCE Version 3.2 for AIX and Solaris: Administration Guide—Introduction* para obter maiores informações sobre as variáveis de ambiente do DCE.

Configuração Inicial da Célula

Para inicializar uma célula, é preciso realizar três tarefas básicas em ordem:

1. Configurar a máquina do servidor de segurança principal. Consulte “Configuração do Servidor de Segurança Principal”.
2. Configurar a máquina do servidor CDS inicial. Consulte “Configuração do Servidor CDS Inicial” na página 90.
3. Configurar um cliente CDS no servidor de segurança principal. Consulte “Configuração de um Cliente CDS no Servidor de Segurança Principal” na página 100.

Nos procedimentos a seguir, assegure-se de que o *dce_nome do host* de cada máquina seja exclusivo na célula. O *dce_nome do host* é o nome listado no diretório hosts (**hosts/dce_nome do host**) no espaço de nomes. O comando **config.dce** permite atribuir um *dce_nome de host* independente do nome de host de uma máquina na rede. Por padrão o nome de host da máquina é usado.

Atenção: Se você tentar configurar duas máquinas que têm o mesmo *dce_hostname*, precisará remover a configuração do DCE e reconfigurá-lo em ambas as máquinas. Se uma dessas máquinas for o servidor de Segurança ou o servidor CDS inicial, será preciso remover a configuração do DCE e reconfigurá-lo em *todas* as máquinas na célula.

As seções a seguir fornecem procedimentos detalhados para realizar estas tarefas de configuração inicial usando o **smitty**. Consulte o *IBM DCE Version 3.2 for AIX and Solaris: Administration Commands Reference* para informações sobre os comandos que podem ser usados para realizar estas mesmas tarefas de configuração na linha de comandos.

Configuração de Servidores

Esta seção discute o seguinte:

- “Configuração do Servidor de Segurança Principal”
- “Configuração do Servidor CDS Inicial” na página 90

Configuração do Servidor de Segurança Principal

Para configurar o servidor de segurança principal para uma célula, realize as seguintes etapas na máquina designada como o servidor de segurança principal:

Nota: O servidor de segurança pode ser iniciado com até 512 threads de executor. Por padrão, o servidor de segurança é iniciado com 10 threads de executor. O aumento do número de threads de executor pode aumentar o rendimento do servidor de segurança. Entretanto, se o servidor de segurança estiver executando no AIX 4.3.3 ou no AIX 5.1, o

número máximo de threads do executor não deve exceder 200. Consulte “Alteração de Argumentos Passados para Daemons do DCE no Reinício” na página 128 e as informações sobre o servidor de segurança **secd** no *IBM DCE Version 3.2 for AIX and Solaris: Administration Commands Reference*.

Para configurar o servidor de segurança principal usando o **smitty**:

1. Como root, inicie o **smitty** com o atalho **mkdcesrv**:

```
smitty mkdcesrv
```

ou execute a seguinte seqüência de opções de menu do **smitty**:

1. **Aplicações e Serviços de Comunicações**
 2. **DCE (Distributed Computing Environment)**
 3. **Configurar DCE/DFS**
 4. **Configurar Servidores DCE/DFS**
2. Selecione a opção **Servidor de SEGURANÇA** e pressione <Enter>.
 3. Selecione a opção **primário** e pressione <Enter>.
 4. No prompt **nome da CÉLULA**, digite o nome da célula. Para cada célula, na primeira vez que este menu for executado e um nome for digitado neste prompt, será estabelecido o nome da célula. Você usará o nome da célula mais tarde em outros menus de configuração.

Nota: O nome da célula não pode ser alterado durante o tempo de operação da célula.

5. Se não desejar usar o *admin_célula* padrão, digite o nome da conta do administrador da célula no prompt **Conta do ADMINISTRADOR da célula**.
6. Se não desejar usar o ID UNIX padrão do administrador da célula, digite o ID UNIX do administrador da célula no prompt **ID UNIX da conta do ADMINISTRADOR da célula**. O padrão é 100.
7. Digite o *dce_nome do host* para esta máquina no campo **DCE NOME DO HOST da máquina**. Se não for selecionado um nome, será usado o nome do host TCP/IP, incluindo o domínio.
8. Tabule para selecionar **sim** ou **não** no campo **Iniciar os componentes no reinício do Sistema** para indicar se os componentes do DCE devem ou não ser iniciados automaticamente na reinicialização do sistema;
9. Tabule para selecionar **sim** ou **não** no campo **Limpar DCE no reinício do Sistema** para indicar se **clean_up.dce** deve ser executado na reinicialização do sistema. **clean_up.dce** remove todos os arquivos DCE que podem ser recriados (ou seja, arquivos cred, arquivos cdscache, etc). Isto será feito antes de reiniciar o DCE.

10. No campo **Protocolo**, pressione <F4> para listar os protocolos. Selecione os protocolos nos quais o DCE será configurado e pressione <Enter>. Uma vez selecionados, os mesmos protocolos devem ser usados para configurações subseqüentes.
11. O **dced** atualizará automaticamente o arquivo **pe_site** com as informações do servidor de segurança. Digite um tempo a aguardar entre atualizações de **pe_site** no campo **Minutos a aguardar entre atualizações do arquivo pe_site**.

0	(zero) desligar a atualização automática do arquivo pe_site
10 - 1440	10 a 1440 minutos

O padrão é 1440 minutos (24 horas).
12. Digite o nome do servidor de segurança para esta máquina no campo **Nome do Servidor de Segurança**. Se não for selecionado um nome, o nome do host DCE será usado.
13. Tabule para selecionar **sim** ou **não** no campo **Usar login baseado em CERTIFICADO** para indicar se a autenticação de certificado PK deve ser ativada.
14. Se a autenticação de certificado PK deverá ser usada, digite o caminho completamente qualificado do arquivo que contém o **PERFIL ENTRUST para o servidor de segurança**.
15. Se a autenticação de certificado PK deverá ser usada, digite o caminho completamente qualificado do **arquivo de INICIALIZAÇÃO ENTRUST**.
16. Se a autenticação de certificado PK deverá ser usada, digite a **senha do PERFIL ENTRUST** para o servidor de segurança DCE.
17. Se desejar combinar os arquivos **/etc/passwd** e **/etc/group** atuais no novo registro DCE, você poderá encontrar conflitos de ID UNIX. Para evitar tais conflitos, digite novos valores (se necessário) nos campos apropriados para o ponto inicial e o valor máximo para IDs UNIX atribuídas a usuários principais, grupos e organizações. Os padrões são os valores exibidos. Como os IDs UNIX não podem ser alterados uma vez que o serviço de segurança haja criado contas, você deve definir já os valores para o ponto inicial e o valor máximo para IDs UNIX, quando o registro é criado pela primeira vez.
18. Pressione <Enter> para selecionar **Fazer**.
19. quando consultado, digite a senha a ser atribuída à conta inicial criada no banco de dados do registro. Anote a senha para a conta do administrador da célula, pois ela é necessária para realizar outras tarefas de configuração. Esta senha também é atribuída à conta DCE para root à qual é concedida autoridade privilegiada pelo DFS.

Para configurar o servidor de segurança principal a partir de uma linha de comandos, no prompt de comandos digite:

```

config.dce -cell_name <nome_da_célula>
[-sec_server_name <servidor_de_segurança>]
[-cell_admin <id de admin_célula>] [-admin_pwd <senha_de_admin>]
[-min_princ_id <id_mín_de_usuario_principal>]
[-min_group_id <id_mín_de_grupo>]
[-min_org_id <id_mín_de_org>] [-max_unix_id <id_UNIX_máx>]
[-no_pesite_update] [-pesite_update_time <tempo_de_atualização>]
[-autostart yes | no] [-clean_autostart yes | no] [-protocol tcp udp]
[-certificate_based_login yes | no ] [-kdc_profile <perfil_kdc>]
[-kdc_ini_file <arquivo_ini_kdc> ] [-kdc_passphrase <kdc_passphrase>]
[-group_rsp_path <nome_do_arquivo>] [-rsp_file <nome_do_arquivo>]
sec_srv

```

Neste ponto, **dced** (RPC e um cliente de segurança) e o servidor de segurança principal são configurados na máquina. Você poderá retornar a esta máquina mais tarde para configurar o CDS e o DTS.

Configuração do Servidor CDS Inicial

Só pode existir um servidor CDS *inicial* para cada célula. Para configurar o servidor CDS inicial para uma célula, realize as seguintes etapas na máquina designada como o servidor CDS inicial:

Para configurar o servidor CDS inicial usando o **smitty**:

1. Como root, inicie o **smitty** com o atalho **mkdcesrv**:

```
smitty mkdcesrv
```

ou execute a seguinte seqüência de opções de menu do **smitty**:

1. **Aplicações e Serviços de Comunicações**
 2. **DCE (Distributed Computing Environment)**
 3. **Configurar DCE/DFS**
 4. **Configurar Servidores DCE/DFS**
2. Selecione a opção **Servidor CDS (Cell Directory Service)** e pressione **<Enter>**.
 3. Selecione a opção **inicial** e pressione **<Enter>**.
 4. Se esta máquina não for o servidor de segurança principal, execute as seguintes etapas. Se esta máquina for o servidor de segurança principal, estes campos estarão preenchidos automaticamente com os valores apropriados.
 - a. No prompt **nome da CÉLULA**, digite o nome da célula.
 - b. Se não estiver usando o *admin_célula* padrão, digite o nome da conta do administrador da célula no prompt **Conta do ADMINISTRADOR da célula**.
 - c. Digite o *dce_nome do host* para esta máquina no campo **DCE NOME DO HOST da máquina**. Se não for selecionado um nome, será usado o nome do host TCP/IP, incluindo o domínio.

- d. Tabule para selecionar **sim** ou **não** no campo **Iniciar os componentes no reinício do Sistema** para indicar se os componentes do DCE devem ou não ser iniciados automaticamente na reinicialização do sistema;
- e. Tabule para selecionar **sim** ou **não** no campo **Limpar DCE no reinício do Sistema** para indicar se **clean_up.dce** deve ser executado na reinicialização do sistema. Isto será feito antes de reiniciar o DCE.
- f. No campo **Protocolo**, pressione <F4> para listar os protocolos. Selecione os protocolos nos quais o DCE será configurado e pressione <Enter>. Uma vez selecionados, os mesmos protocolos devem ser usados para configurações subseqüentes.
- g. No prompt **Servidor de SEGURANÇA PRINCIPAL**, digite o nome do host TCP/IP ou endereço IP da máquina que é o servidor de segurança principal. (o nome do host TCP/IP ou endereço IP não é necessariamente o mesmo que o *dce_hostname*.)
- h. O **dced** atualizará automaticamente o arquivo **pe_site** com as informações do servidor de segurança. Digite um tempo a aguardar entre atualizações de **pe_site** no campo **Minutos a aguardar entre atualizações do arquivo pe_site**.

0	(zero) desligar a atualização automática do arquivo <i>pe_site</i>
10 - 1440	10 a 1440 minutos

O padrão é 1440 minutos (24 horas).

5. Tabule para selecionar **sim** ou **não** no campo **Relógios Sincronizados** para indicar se o relógio da máquina local deve ou não ser sincronizado com um servidor DTS.
6. Digite o nome do servidor de horário que deseja usar para sincronização no prompt **Servidor de Horário com o qual Sincronizar Relógios**. O servidor de horário pode ser qualquer servidor DTS.
7. Se a célula irá conter várias LANs e requer o uso de servidores DTS globais, ou se o suporte a réplica de segurança preferencial será ativado, digite o nome do perfil de LAN que esta máquina deve usar no campo **PERFIL DE LAN**. Entretanto, se esta for a mesma máquina do servidor de segurança, o campo já estará preenchido.
8. Pressione <Enter> para selecionar **Fazer**.
9. Quando consultado, digite a senha do administrador da célula.

Para configurar o servidor CDS inicial a partir de uma linha de comandos, no prompt de comandos digite:

```
config.dce [-cell_name <nome_da_célula>] [-cell_admin <id_do_admin_da_célula>]
[-admin_pwd <senha_de_admin>] [-sec_master <servidor_de_segurança_principal>]
[-autostart yes | no] [-clean_autostart yes | no] [-protocol tcp udp]
[-group_rsp_path <nome_do_arquivo>] [-rsp_file <nome_do_arquivo>]
[-wrap_audit_trail yes | no]
cds_srv
```

Neste ponto, **dced** (RPC e um cliente de segurança), o servidor CDS inicial e um clerk CDS são configurados na máquina. (Se esta máquina for o servidor de segurança principal, somente o servidor CDS inicial e um clerk CDS são realmente configurados nesta seção.) Você poderá retornar a esta máquina mais tarde para configurar o DTS.

Note que uma clearinghouse é criada automaticamente quando se configura um servidor CDS. Embora seja possível definir várias clearinghouses para um servidor CDS, deve-se ter somente uma por servidor CDS durante a operação normal. Se estiver movendo uma clearinghouse de um servidor CDS para outro, no entanto, você poderá definir temporariamente uma segunda clearinghouse no servidor original. Consulte o *IBM DCE Version 3.2 for AIX and Solaris: Administration Guide—Core Components* para obter maiores informações sobre como mover uma clearinghouse.

Configuração de Clientes

Esta seção discute o seguinte:

- “Configuração de Clientes DCE”
- “Configuração Administrativa do Cliente” na página 93
- “Configuração Local do Cliente” na página 94
- “Configuração Completa do Cliente” na página 96
- “Configuração do Cliente Básico” na página 98
- “Configuração de um Cliente CDS no Servidor de Segurança Principal” na página 100

Em geral, é preciso configurar muitos clientes em uma célula DCE. A configuração de clientes envolve dois conjuntos distintos de operações:

- Tarefas que exigem autoridade de *administrador de célula* na célula DCE
- Tarefas que exigem autoridade de *usuário root* na máquina que deve ser configurada como um cliente DCE.

Estas tarefas são separadas em uma *configuração dividida de clientes* porque é provável que um administrador de célula DCE não tenha acesso de usuário root a todas as máquinas em uma célula.

Configuração de Clientes DCE

Os clientes DCE podem ser configurados de três maneiras: completa, administrativa ou local.

A configuração dividida do cliente para clientes de segurança **sec_cl** e clientes CDS (**cds_cl**) é um processo de duas partes. (O administrador da célula pode não ter acesso de root às máquinas clientes, ou o usuário root pode não ter acesso de administrador de célula.) As duas partes são as seguintes:

- O administrador da célula executa a parte **administrativa** a partir de qualquer máquina na célula para atualizar o espaço de nomes CDS e o registro de segurança.
- O usuário root da máquina cliente executa a parte **local** para criar os arquivos necessários e para iniciar os daemons do cliente para todos os componentes do cliente.

Configuração Administrativa do Cliente

Para fazer a parte **administrativa** da configuração de um cliente DCE, o administrador da célula realiza as seguintes etapas a partir de qualquer máquina na célula:

Para fazer a parte **administrativa** da configuração de um cliente DCE usando o **smitty**:

1. Inicie o **smitty** com o atalho **mkdceclient**:

```
smitty mkdceclient
```

ou execute a seguinte seqüência de opções de menu do **smitty**:

1. **Aplicações e Serviços de Comunicações**
 2. **DCE (Distributed Computing Environment)**
 3. **Configurar DCE/DFS**
 4. **Configurar Clientes DCE/DFS**
2. Selecione **somente configuração administrativa para outra máquina** e pressione **<Enter>**.
 3. Pressione **<F4>** para obter uma lista de clientes DCE. Para a configuração **administrativa**, as únicas seleções são **all_cl**, **sec_cl**, **cds_cl**, **dts_cl** e **nsid**. Todo o restante da configuração do cliente é feita na máquina cliente e não exige autoridade de administrador de célula. Selecione o nome do cliente DCE que deseja configurar e pressione **<Enter>**.
 4. Se não estiver usando o *admin_célula* padrão, digite o nome da conta do administrador da célula no prompt **Conta do ADMINISTRADOR da célula**.
 5. Digite o *dce_nome do host* para a máquina cliente no campo **DCE NOME DO HOST da máquina**. Se não for selecionado um nome, o nome de host TCP/IP, incluindo o domínio da Etapa 6, será usado.
 6. Identifique qual máquina está sendo configurada como um cliente digitando seu nome de host TCP/IP ou endereço IP no campo **Nome ou endereço TCP/IP da máquina**.
 7. Se a célula irá conter várias LANs e requer o uso de servidores DTS globais, digite o nome do perfil de LAN que a máquina cliente deve usar no prompt **PERFIL DE LAN**.
 8. Pressione **<Enter>** para selecionar **Fazer**.

Para fazer a parte **administrativa** da configuração de um cliente DCE a partir de uma linha de comandos, no prompt de comandos digite:

```
config.dce -config_type admin -host_id <identificador da máquina>
[dce_hostname <dce_nome do host> [-cell_admin <id_do_admin_da_célula>
[-admin_pwd <senha_do_admin>] [-lan_profile <perfil>]
[-protocol tcp udp] [-group_rsp_path <nome_do_arquivo>]
[-rsp_file <nome_do_arquivo>]
sec_cl | cds_cl | dts_cl
```

Neste ponto, as entradas do espaço de nomes e do banco de dados do registro de segurança foram atualizadas. Agora é necessário executar a parte **local** da configuração para concluir o processo.

Configuração Local do Cliente

Para fazer a parte **local** da configuração de um cliente DCE (após a parte **administrativa** ter sido concluída, quando apropriado), realize as seguintes etapas como root na máquina do cliente:

Para fazer a parte **local** da configuração de um cliente DCE usando o **smitty**:

1. Inicie o **smitty** com o atalho **mkdceclient**:

```
smitty mkdceclient
```

ou execute a seguinte seqüência de opções de menu do **smitty**:

1. **Aplicações e Serviços de Comunicações**
2. **DCE (Distributed Computing Environment)**
3. **Configurar DCE/DFS**
4. **Configurar Clientes DCE/DFS**
2. Selecione **somente configuração local para esta máquina** e pressione **<Enter>**.
3. Pressione **<F4>** para obter uma lista de clientes DCE. Para a configuração **local**, as seleções são **all_cl**, **rpc**, **sec_cl**, **cds_cl**, **dts_cl**, **slim_cl** e **dce_unixd**. Selecione o nome do cliente DCE que deseja configurar e pressione **<Enter>**.
4. Assegure que o campo **nome da CÉLULA** está preenchido com os valores apropriados.
5. Digite o **DCE_nome do host** para esta máquina no prompt **DCE NOME DO HOST da máquina**. Se não for selecionado um nome, será usado o nome do host TCP/IP, incluindo o domínio.
6. Tabule para selecionar **sim** ou **não** no campo **Iniciar os componentes no reinício do Sistema** para indicar se os componentes do DCE devem ou não ser iniciados automaticamente na reinicialização do sistema;
7. Tabule para selecionar **sim** ou **não** no campo **Limpar DCE no reinício do Sistema** para indicar se **clean_up.dce** deve ser executado na reinicialização do sistema. Isto será feito antes de reiniciar o DCE.

8. No campo **Protocolos**, pressione <F4> para listar os protocolos. Selecione os protocolos nos quais o DCE será configurado e pressione <Enter>. Uma vez selecionados, os mesmos protocolos devem ser usados para configurações subseqüentes. Se você for configurar quaisquer componentes do DFS nesta máquina, é preciso usar os protocolos **udp**.
9. Se a máquina estiver em uma LAN separada de qualquer servidor CDS e não puder enviar pacotes de difusão a um servidor CDS ou se você não tiver certeza sobre se a máquina está em uma LAN separada, digite o nome de host TCP/IP ou endereço IP do servidor de segurança principal no prompt **Servidor de SEGURANÇA PRINCIPAL**.
10. O **dced** atualizará automaticamente o arquivo **pe_site** com as informações do servidor de segurança. Digite um tempo a aguardar entre atualizações de **pe_site** no campo **Minutos a aguardar entre atualizações do arquivo pe_site**.

0 (zero) desligar a atualização automática do arquivo **pe_site**
 10 - 1440 10 a 1440 minutos

O padrão é 1440 minutos (24 horas).

11. Se a máquina estiver em uma LAN separada de qualquer servidor CDS e não puder enviar pacotes de difusão a um servidor CDS ou se você não tiver certeza sobre se a máquina está em uma LAN separada, digite o nome de host TCP/IP ou endereço IP do servidor CDS no prompt **Servidor CDS (Se em uma rede separada)**.
12. Se desejar definir outros servidores CDS no cache CDS, digite os nomes de host TCP/IP ou endereços IP desses servidores CDS no campo **Lista de Servidores CDS Adicionais**.
13. Tabule para selecionar **sim** ou **não** no campo **Relógios Sincronizados** para indicar se o relógio da máquina local deve ou não ser sincronizado com um servidor DTS.
14. Digite o nome do servidor de horário que deseja usar para sincronização no prompt **Servidor de Horário com o qual Sincronizar Relógios**. O servidor de horário pode ser qualquer servidor DTS.
15. Se a máquina estiver em uma LAN separada e você desejar que o cliente CDS propague a difusão da localização do servidor CDS, no prompt **Redifundir a Localização do Servidor CDS** tabule para selecionar **sim**. O padrão é **não**.
16. Pressione <Enter> para selecionar **Fazer**.

Para fazer a parte **local** da configuração de um cliente DCE a partir de uma linha de comandos, no prompt de comandos digite:

```
config.dce -config_type local
[-cell_name <nome_da_célula>] [-dce_hostname <dce_nome do host>]
[-sec_master <servidor_de_segurança_principal>] [-cds_server <servidor_cds>]
[-no_pesite_update] [-pesite_update_time <tempo_de_atualização>]
```

```
[-time_server <id do servidor>] [-sync_clocks yes | no] [-autostart yes | no]
[-clean_autostart yes | no] [-protocol tcp udp] [-proxy]
[-group_rsp_path <nome_do_arquivo>] [-rsp_file <nome_do_arquivo>]
[-num_dce_unixd <número>] [cache_lifetime <minutos>]
[-cds_replica_list <lista_de_servidores_cds>] [-wrap_audit_trail yes | no]
client_components
```

Neste ponto, os clientes selecionados são configurados na máquina.

Configuração Completa do Cliente

Se você é tanto o *administrador da célula* quanto o *usuário root* de uma máquina que está sendo configurada atualmente como um cliente, pode realizar uma configuração **completa de cliente**, a qual incorpora as partes **administrativa e local** da configuração.

Para realizar a configuração **completa** de um cliente DCE, execute as seguintes etapas como root na máquina do cliente:

Para realizar a configuração **completa** de um cliente DCE usando o **smitty**:

1. Inicie o **smitty** com o atalho **mkdceclient**:

```
smitty mkdceclient
```

ou execute a seguinte seqüência de opções de menu do **smitty**:

1. **Aplicações e Serviços de Comunicações**
2. **DCE (Distributed Computing Environment)**
3. **Configurar DCE/DFS**
4. **Configurar Clientes DCE/DFS**
2. Selecione **configuração completa para esta máquina** e pressione <Enter>.
3. Pressione <F4> para obter uma lista de clientes DCE. Para a configuração **completa**, todos os clientes estão disponíveis para seleção. Selecione o nome do cliente DCE que deseja configurar e pressione <Enter>.
4. Assegure que o campo **nome da CÉLULA** está preenchido com os valores apropriados.
5. Se não estiver usando o *admin_célula* padrão, digite o nome da célula
6. Digite o **DCE_nome do host** para esta máquina no prompt **DCE NOME DO HOST da máquina**. Se não for selecionado um nome, será usado o nome do host TCP/IP, incluindo o domínio.
7. Tabule para selecionar **sim** ou **não** no campo **Iniciar os componentes no reinício do Sistema** para indicar se os componentes do DCE devem ou não ser iniciados automaticamente na reinicialização do sistema;
8. Tabule para selecionar **sim** ou **não** no campo **Limpar DCE no reinício do Sistema** para indicar se **clean_up.dce** deve ser executado na reinicialização do sistema. Isto será feito antes de reiniciar o DCE.

9. No campo **Protocolos**, pressione <F4> para listar os protocolos. Selecione os protocolos nos quais o DCE será configurado e pressione <Enter>. Uma vez selecionados, os mesmos protocolos devem ser usados para configurações subseqüentes. Se você for configurar quaisquer componentes do DFS nesta máquina, é preciso usar os protocolos **udp**.
10. Se a máquina estiver em uma LAN separada de qualquer servidor CDS e não puder enviar pacotes de difusão a um servidor CDS ou se você não tiver certeza sobre se a máquina está em uma LAN separada, digite o nome de host TCP/IP ou endereço IP do servidor de segurança principal no prompt **Servidor de SEGURANÇA PRINCIPAL**.
11. O **dced** atualizará automaticamente o arquivo **pe_site** com as informações do servidor de segurança. Digite um tempo a aguardar entre atualizações de **pe_site** no campo **Minutos a aguardar entre atualizações do arquivo pe_site**.

0	(zero) desligar a atualização automática do arquivo pe_site
10 - 1440	10 a 1440 minutos

O padrão é 1440 minutos (24 horas).

12. Se a máquina estiver em uma LAN separada de qualquer servidor CDS e não puder enviar pacotes de difusão a um servidor CDS ou se você não tiver certeza sobre se a máquina está em uma LAN separada, digite o nome de host TCP/IP ou endereço IP do servidor CDS no prompt **Servidor CDS (Se em uma rede separada)**.
13. Se desejar definir outros servidores CDS no cache CDS, digite os nomes de host TCP/IP ou endereços IP desses servidores CDS no campo **Lista de Servidores CDS Adicionais**.
14. Tabule para selecionar **sim** ou **não** no campo **Relógios Sincronizados** para indicar se o relógio da máquina local deve ou não ser sincronizado com um servidor DTS.
15. Digite o nome do servidor de horário que deseja usar para sincronização no prompt **Servidor de Horário com o qual Sincronizar Relógios**. O servidor de horário pode ser qualquer servidor DTS.
16. Se a célula irá conter várias LANs e requer o uso de servidores DTS globais, ou se o suporte a réplica de segurança preferencial será ativado, digite o nome do perfil de LAN que esta máquina deve usar no campo **PERFIL DE LAN**.
17. Se a máquina estiver em uma LAN separada e você desejar que o cliente CDS propague a difusão da localização do servidor CDS, no prompt **Redifundir a Localização do Servidor CDS** tabule para selecionar **sim**. O padrão é **não**.
18. Pressione <Enter> para selecionar **Fazer**.

Para realizar a configuração **completa** de um cliente DCE a partir de uma linha de comandos, no prompt de comandos digite:

```

config.dce -config_type full
[-cell_name <nome_da_célula>] [-dce hostname <dce_nome do host>]
[-admin_pwd <senha_do_admin>] [-cell_admin <id_do_admin_da_célula>]
[-sec_master <servidor_de_segurança_principal>] [-cds_server <servidor_cds>]
[-lan_profile <perfil>] [-pesite_update time <tempo de atualização>]
[-no_pesite_update] [-time_server <id do servidor>] [-sync_clocks yes | no]
[-autostart yes | no] [-clean_autostart yes | no] [-protocol tcp udp]
[-proxy] [-group_rsp_path <nome_do_arquivo>] [-rsp_file <nome_do_arquivo>]
[-num_dce_unixd <número>] [cache_lifetime <minutos>]
[-cds_replica_list <lista_de_servidores_cds>] [-wrap_audit_trail yes | no]
client_components

```

Configuração do Cliente Básico

Notas:

1. A senha do administrador da célula não é necessária ao configurar um cliente básico.
2. Somente um cliente DFS e a Integração de Segurança podem ser configurados com um cliente básico.
3. Não há etapas de configuração **administrativa** a realizar antes ou depois de configurar um cliente básico.

Para configurar um cliente básico DCE, execute as seguintes etapas como root na máquina do cliente:

Para configurar um cliente básico DCE usando o **smitty**:

1. Inicie o **smitty** com o atalho **mkdceclient**:

```
smitty mkdceclient
```

ou execute a seguinte seqüência de opções de menu do **smitty**:

1. **Aplicações e Serviços de Comunicações**
2. **DCE (Distributed Computing Environment)**
3. **Configurar DCE/DFS**
4. **Configurar Clientes DCE/DFS**
2. Selecione **somente configuração local para esta máquina** e pressione **<Enter>**.
3. Selecione **slim_cl** na lista de **CLIENTES a configurar** e pressione **<Enter>**.
4. Assegure que o campo **nome da CÉLULA** está preenchido com os valores apropriados.
5. Digite o **DCE_nome do host** para esta máquina no prompt **DCE NOME DO HOST da máquina**. Se não for selecionado um nome, será usado o nome do host TCP/IP, incluindo o domínio.

6. Tabule para selecionar **sim** ou **não** no campo **Iniciar os componentes no reinício do Sistema** para indicar se os componentes do DCE devem ou não ser iniciados automaticamente na reinicialização do sistema;
7. Tabule para selecionar **sim** ou **não** no campo **Limpar DCE no reinício do Sistema** para indicar se **clean_up.dce** deve ser executado na reinicialização do sistema. Isto será feito antes de reiniciar o DCE.
8. No campo **Protocolos**, pressione <F4> para listar os protocolos. Selecione os protocolos nos quais o DCE será configurado e pressione <Enter>. Uma vez selecionados, os mesmos protocolos devem ser usados para configurações subseqüentes. Se você for configurar quaisquer componentes do DFS nesta máquina, é preciso usar os protocolos **udp**.
9. Se a máquina estiver em uma LAN separada de qualquer servidor CDS e não puder enviar pacotes de difusão a um servidor CDS ou se você não tiver certeza sobre se a máquina está em uma LAN separada, digite o nome de host TCP/IP ou endereço IP do servidor de segurança principal no prompt **Servidor de SEGURANÇA PRINCIPAL**.
10. O **dced** atualizará automaticamente o arquivo **pe_site** com as informações do servidor de segurança. Digite um tempo a aguardar entre atualizações de **pe_site** no campo **Minutos a aguardar entre atualizações do arquivo pe_site**.

0	(zero) desligar a atualização automática do arquivo pe_site
10 - 1440	10 a 1440 minutos

O padrão é 1440 minutos (24 horas).

11. Se a máquina estiver em uma LAN separada de qualquer servidor CDS e não puder enviar pacotes de difusão a um servidor CDS ou se você não tiver certeza sobre se a máquina está em uma LAN separada, digite o nome de host TCP/IP ou endereço IP do servidor CDS no prompt **Servidor CDS (Se em uma rede separada)**.
12. Se desejar definir outros servidores CDS no cache CDS, digite os nomes de host TCP/IP ou endereços IP desses servidores CDS no campo **Lista de Servidores CDS Adicionais**.
13. Tabule para selecionar **sim** ou **não** no campo **Relógios Sincronizados** para indicar se o relógio da máquina local deve ou não ser sincronizado com um servidor DTS.
14. Digite o nome do servidor de horário que deseja usar para sincronização no prompt **Servidor de Horário com o qual Sincronizar Relógios**. O servidor de horário pode ser qualquer servidor DTS.
15. Se a máquina estiver em uma LAN separada e você desejar que o cliente CDS propague a difusão da localização do servidor CDS, no prompt **Redifundir a Localização do Servidor CDS** tabule para selecionar **sim**. O padrão é **não**.
16. Pressione <Enter> para selecionar **Fazer**.

Para configurar um cliente básico DCE a partir da linha de comandos, no prompt de comandos digite:

```
config.dce -cell_name <nome_da_célula>
[-dce_hostname <dce_nome do host>]
[-sec_master <servidor_de_segurança_principal>]
[-cds_server <servidor_cds>] [-time_server <id do servidor>]
[-sync_clocks yes | no] [-autostart yes | no]
[-clean_autostart yes | no] [-protocol tcp udp]
[-lan_profile <perfil>] [-group_rsp_path <nome_do_arquivo>]
[-rsp_file <nome_do_arquivo>]
[-wrap_audit_trail yes | no]
slim_cl
```

Neste ponto, os clientes selecionados são configurados na máquina.

Configuração de um Cliente CDS no Servidor de Segurança Principal

Se você configurou o servidor de segurança principal e o servidor CDS inicial na mesma máquina, você pode pular esta seção pois um cliente CDS foi configurado quando da configuração do servidor CDS inicial.

Caso contrário, para configurar um cliente CDS no servidor de segurança principal, execute as seguintes etapas na máquina que é o servidor de segurança principal:

Para configurar um cliente CDS no servidor de segurança principal usando o **smitty**:

1. Como root, inicie o **smitty** com o atalho **mkdceclient**:

```
smitty mkdceclient
```

ou execute a seguinte seqüência de opções de menu do **smitty**:

1. **Aplicações e Serviços de Comunicações**
2. **DCE (Distributed Computing Environment)**
3. **Configurar DCE/DFS**
4. **Configurar Clientes DCE/DFS**
2. Selecione **configuração completa para esta máquina** e pressione <Enter>.
3. No prompt **CLIENTES a configurar**, pressione <F4> para listar. Selecione **cds_cl**, e pressione <Enter>.
4. Assegure que os campos **nome da CÉLULA** e **Servidor de SEGURANÇA** estão preenchidos com os valores apropriados.
5. Se não estiver usando o *admin_célula* padrão, digite o nome da conta do administrador da célula no prompt **Conta do ADMINISTRADOR da célula**.
6. Assegure que o campo **DCE NOME DO HOST** da máquina está preenchido com o nome apropriado.

7. Tabule para selecionar **sim** ou **não** no campo **Iniciar os componentes no reinício do Sistema** para indicar se os componentes do DCE devem ou não ser iniciados automaticamente na reinicialização do sistema;
8. Tabule para selecionar **sim** ou **não** no campo **Limpar DCE no reinício do Sistema** para indicar se **clean_up.dce** deve ser executado na reinicialização do sistema. Isto será feito antes de reiniciar o DCE.
9. Se o servidor de segurança principal estiver em uma LAN separada do servidor CDS inicial e não puder enviar pacotes de difusão para este, digite o nome de host TCP/IP ou endereço IP do servidor CDS inicial no prompt **Servidor CDS (se em uma rede separada)**. (O nome do host TCP/IP ou endereço IP não é necessariamente o mesmo que o *dce_hostname*.) Se não tiver certeza sobre se ele está em uma LAN separada, digite o nome de host TCP/IP ou endereço IP do servidor CDS inicial no prompt **Servidor CDS (se em uma rede separada)**.
10. Tabule para selecionar **sim** ou **não** no campo **Relógios Sincronizados** para indicar se o relógio da máquina local deve ou não ser sincronizado com um servidor DTS.
11. Digite o nome do servidor de horário que deseja usar para sincronização no prompt **Servidor de Horário com o qual Sincronizar Relógios**. O servidor de horário pode ser qualquer servidor DTS.
12. Se a célula irá conter várias LANs e requer o uso de servidores DTS globais, ou se o suporte a réplica de segurança preferencial será ativado, digite o nome do perfil de LAN que esta máquina deve usar no campo **PERFIL DE LAN**.
13. Se este cliente CDS estiver em uma LAN separada e você desejar que ele propague a difusão da localização do servidor CDS, no prompt **Redifundir a Localização do Servidor CDS** tabule para selecionar **sim**.
14. Todos os outros campos devem estar preenchidos porque a máquina já está configurada.
15. Pressione <Enter> para selecionar **Fazer**.
16. Quando consultado, digite a senha do administrador da célula.

Para configurar um cliente CDS no servidor de segurança principal a partir de uma linha de comandos, no prompt de comandos digite:

```
config.dce [-cell_admin <admin_da_célula>][-cds_server <servidor_cds>]
cds_c1
```

Neste ponto, um cliente CDS é configurado na máquina.

Configuração Adicional da Célula

Após concluir a inicialização da célula, pode ser preciso realizar tarefas adicionais de configuração durante a operação, conforme sejam feitas alterações na célula. Por exemplo, você pode querer incluir uma nova máquina na célula como um cliente. Ou pode decidir configurar um servidor CDS secundário para fornecer acesso mais rápido ou mais confiável ao espaço de nomes.

As seções a seguir fornecem procedimentos detalhados para a realização de tarefas adicionais de configuração.

Configuração de Servidores DTS

Para configurar servidores DTS locais ou globais, execute as seguintes etapas em cada máquina designada como um servidor DTS:

Para configurar servidores DTS locais ou globais usando o **smitty**:

1. Como root, inicie o **smitty** com o atalho **mkdcesrv**:

```
smitty mkdcesrv
```

ou execute a seguinte seqüência de opções de menu do **smitty**:

1. **Aplicações e Serviços de Comunicações**
2. **DCE (Distributed Computing Environment)**
3. **Configurar DCE/DFS**
4. **Configurar Servidores DCE/DFS**
2. Selecione a opção **Servidor DTS (Serviço de Horário Distribuído)**. Pressione <Enter>.
3. Assegure que o campo **nome da CÉLULA** está preenchido com os valores apropriados.
4. Se não estiver usando o *admin_célula* padrão, digite o nome da conta do administrador da célula no prompt **Conta do ADMINISTRADOR da célula**.
5. Digite o *dce_nome do host* para esta máquina no campo **DCE NOME DO HOST da máquina**. Se não for selecionado um nome, será usado o nome do host TCP/IP, incluindo o domínio.
6. Tabule para selecionar **sim** ou **não** no campo **Iniciar os componentes no reinício do Sistema** para indicar se os componentes do DCE devem ou não ser iniciados automaticamente na reinicialização do sistema;
7. Tabule para selecionar **sim** ou **não** no campo **Limpar DCE no reinício do Sistema** para indicar se **clean_up.dce** deve ser executado na reinicialização do sistema. Isto será feito antes de reiniciar o DCE.

8. No campo **Protocolo**, pressione <F4> para listar os protocolos. Selecione os protocolos com os quais o DCE será configurado e pressione <Enter>. Uma vez selecionados, os mesmos protocolos devem ser usados para configurações subseqüentes.
9. Se a máquina estiver em uma LAN separada de qualquer servidor CDS e não puder enviar pacotes de difusão para ele, digite o nome de host TCP/IP ou endereço IP do servidor de segurança principal no prompt **Servidor de SEGURANÇA PRINCIPAL**. Se não tiver certeza sobre se ele está em uma LAN separada, digite o nome de host TCP/IP ou endereço IP do servidor de segurança principal no prompt **Servidor de SEGURANÇA PRINCIPAL**.
10. O **dced** atualizará automaticamente o arquivo **pe_site** com as informações do servidor de segurança. Digite um tempo a aguardar entre atualizações de **pe_site** no campo **Minutos a aguardar entre atualizações do arquivo pe_site**.

0	(zero) desligar a atualização automática do arquivo pe_site
10 - 1440	10 a 1440 minutos

O padrão é 1440 minutos (24 horas).
11. Se a máquina estiver em uma LAN separada de qualquer servidor CDS e não puder enviar pacotes de difusão para ele, digite o nome de host TCP/IP ou endereço IP do servidor CDS inicial no prompt **Servidor CDS (se em uma rede separada)**. Se não tiver certeza sobre se a máquina está em uma LAN separada, digite o nome de host TCP/IP ou endereço IP do servidor CDS inicial no prompt **Servidor CDS (se em uma rede separada)**.
12. Se desejar definir outros servidores CDS no cache CDS, digite os nomes de host TCP/IP ou endereços IP desses servidores CDS no campo **Lista de Servidores CDS Adicionais**.
13. Se a célula irá conter várias LANs e requer o uso de servidores DTS globais, ou se o suporte a réplica de segurança preferencial será ativado, digite o nome do perfil de LAN que esta máquina deve usar no campo **PERFIL DE LAN**.
14. Se a máquina estiver em uma LAN separada e você desejar que o cliente CDS propague a difusão da localização do servidor CDS, no prompt **Redifundir a Localização do Servidor CDS** tabule para selecionar **sim**.
15. No prompt **Tipo de SERVIDOR**, pressione <F4> para listar. Selecione o tipo apropriado de servidor e pressione <Enter>. Note que um servidor DTS não pode ser configurado na mesma máquina que outro servidor DTS ou cliente DTS.
16. No prompt **Tipo de COURIER**, pressione <F4> para listar. Selecione o tipo apropriado de courier e pressione <Enter>.
17. Pressione <Enter> para selecionar **Fazer**.

18. Quando consultado, digite a senha do administrador da célula.

Para configurar servidores DTS locais ou globais a partir de uma linha de comandos, no prompt de comandos digite:

```
config.dce [-courier_role (courier | noncourier | backup)]
[-cell_name <nome_da_célula>] [-cell_admin <id_do_admin_da_célula>]
[-admin_pwd <senha_de_admin>] [-sec_master <servidor_de_segurança_principal>]
[-cds_server <servidor_cds>] [-lan_profile <perfil>]
[-time_server <id_do_servidor>] [-sync_clocks yes | no]
[-autostart yes | no] [-clean_autostart yes | no] [-protocol tcp udp]
[-group_rsp_path <nome_do_arquivo>] [-rsp_file <nome_do_arquivo>]
[-wrap_audit_trail yes | no]
dts_local | dts_global
```

Se houver menos de três servidores de horário configurados na célula, use o seguinte comando:

```
dcecp -c dts modify -minservers n
```

onde *n* é o número de servidores de horário na célula. Isto evita que uma mensagem de aviso seja registrada sempre que o servidor tentar sincronizar.

Neste ponto, um servidor DTS é configurado na máquina, juntamente com **dced** (RPC e um cliente de segurança) e um cliente CDS os quais foram configurados como parte da configuração do cliente DCE.

Configuração de um Cliente DTS

Para configurar um cliente DTS:

1. Como root, inicie o **smitty** com o atalho **mkdceclient**:

```
smitty mkdceclient
```

ou execute a seguinte seqüência de opções de menu do **smitty**:

1. **Aplicações e Serviços de Comunicações**
 2. **DCE (Distributed Computing Environment)**
 3. **Configurar DCE/DFS**
 4. **Configurar Clientes DCE/DFS**
2. Selecione **configuração completa para esta máquina** e pressione **<Enter>**.
 3. No prompt **CLIENTES a configurar**, pressione **<F4>** para listar. Selecione **dts_cl**, e pressione **Enter**.
 4. Se não estiver usando o *admin_célula* padrão, digite o nome da conta do administrador da célula no prompt **Conta do ADMINISTRADOR da célula**.
 5. Todos os outros campos devem estar preenchidos automaticamente com os valores apropriados devido a uma configuração anterior na máquina.

6. Pressione <Enter> para selecionar **Fazer**.
7. Quando consultado, digite a senha do administrador da célula.
neste ponto, um cliente DTS é configurado nas máquinas do servidor de segurança principal e do servidor CDS inicial, concluindo a inicialização da célula.

Para configurar um cliente DTS a partir de uma linha de comandos, no prompt de comandos digite:

```
config.dce [-cell_admin <id_do_admin_da_célula>] dts_cl
```

Configuração de Servidores CDS Secundários

Após haver configurado um servidor CDS inicial, você pode desejar configurar um ou mais servidores CDS *secundários* para fornecer acesso mais rápido ou mais confiável ao espaço de nomes.

Um Servidor CDS Secundário permite aos administradores criar réplicas de Diretórios CDS para fins de backup e disponibilidade. Quando se configura um Servidor CDS Secundário, uma réplica do diretório root e seu conteúdo é criada automaticamente.

O único diretório filho sob o root que é replicado automaticamente no novo Servidor CDS Secundário é o diretório `./:subsyst/dce/sec`. Este diretório é replicado porque contém as informações de ligação para localizar o servidor de segurança principal. Esta ação fornece acessibilidade ao servidor de segurança mesmo quando o Servidor CDS inicial não está disponível. Consulte o *IBM DCE Version 3.2 for AIX and Solaris: Administration Guide—Core Components* para obter informações sobre réplicas de CDS e como criá-las.

Para configurar um servidor CDS secundário, execute as seguintes etapas em cada máquina designada como um servidor CDS secundário.

Nota: Se a máquina ainda não é um cliente DCE, siga as etapas delineadas em “Configuração de Clientes DCE” na página 92 para configurá-la como um cliente DCE.

Para configurar um servidor CDS secundário em uma máquina já configurada como um cliente usando o **smitty**:

1. Como root, inicie o **smitty** com o atalho **mkdcesrv**:

```
smitty mkdcesrv
```

ou execute a seguinte seqüência de opções de menu do **smitty**:

1. **Aplicações e Serviços de Comunicações**
 2. **DCE (Distributed Computing Environment)**
 3. **Configurar DCE/DFS**
 4. **Configurar Servidores DCE/DFS**
2. Selecione a opção **Servidor CDS (Cell Directory Service)** e pressione **<Enter>**.
 3. Selecione a opção **adicional** e pressione **<Enter>**.
 4. Se não estiver usando o *admin_célula* padrão, digite o nome da conta do administrador da célula no prompt **Conta do ADMINISTRADOR da célula**.
 5. Como a máquina já está configurada como um cliente DCE, todos os outros campos devem estar preenchidos automaticamente com os valores apropriados. Pressione **<Enter>** para selecionar **Fazer**.
 6. Quando consultado, digite a senha do administrador da célula.

Para configurar um servidor CDS secundário a partir de uma linha de comandos, no prompt de comandos digite:

```
config.dce [-cell_name <nome_da_célula>] [-cell_admin <id_do_admin_da_célula>]
[-admin_pwd <senha_de_admin>] [-sec_master <servidor_de_segurança_principal>]
[-cds_server <servidor-cds>] [-lan_profile <perfil>]
[clr_house <id_do_servidor>] [-autostart yes | no] [-clean_autostart yes | no]
[-protocol tcp udp] [-time_server <id do servidor>] [-sync_clocks yes | no]
[-group_rsp_path <nome_do_arquivo>] [-rsp_file <nome_do_arquivo>]
[-wrap_audit_trail yes | no]
cds_second
```

Neste ponto, **dced** (RPC e um cliente de segurança), um servidor CDS secundário, um cliente CDS e um cliente DTS são configurados na máquina. Quando se configura um servidor CDS secundário, somente os diretórios **root** e **./:subsys/dce/sec** são replicados automaticamente. Quaisquer outros diretórios devem ser replicados manualmente nos servidores CDS secundários. Consulte o *IBM DCE Version 3.2 for AIX and Solaris: Administration Guide* para informações sobre como replicar outros diretórios.

Configuração das Réplicas dos Servidores de Segurança

Uma réplica do servidor de segurança é uma cópia somente para leitura do servidor de segurança principal. As vantagens de usar uma réplica do servidor de segurança incluem aliviar a carga do servidor de segurança principal e preservar a célula no caso desse servidor de segurança ficar desativado.

Para configurar uma réplica servidor de segurança, execute as seguintes etapas em cada máquina designada como uma réplica do servidor de segurança.

Nota: Se a máquina ainda não é um cliente DCE, siga as etapas delineadas em “Configuração de Clientes DCE” na página 92 para configurá-la como um cliente DCE.

Para configurar uma réplica do servidor de segurança usando o **smitty**:

1. Como root, inicie o **smitty** com o atalho **mkdcesrv**:

```
smitty mkdcesrv
```

ou execute a seguinte seqüência de opções de menu do **smitty**:

1. **Aplicações e Serviços de Comunicações**
 2. **DCE (Distributed Computing Environment)**
 3. **Configurar DCE/DFS**
 4. **Configurar Servidores DCE/DFS**
2. Selecione a opção **Servidor de SEGURANÇA** e pressione <Enter>.
 3. Selecione a opção **secundário** e pressione <Enter>.
 4. Se não estiver usando o *admin_célula* padrão, digite o nome da conta do administrador da célula no prompt **Conta do ADMINISTRADOR da célula**.
 5. Se desejar dar um nome à réplica de segurança, digite sua escolha no campo **Nome do Servidor de Segurança**. Se não for especificado um nome, o padrão é o *dce_hostname* da máquina. Use o padrão, a menos que tenha certeza absoluta de que o nome que você especificar seja exclusivo em toda a rede.
 6. Tabule para selecionar **sim** ou **não** no campo **Usar LDAP para armazenar informações de segurança** para indicar se o Registro do DCE deve ser armazenado no LDAP.
 7. Se o LDAP deve ser usado para armazenar informações do Registro DCE, digite os nomes dos Servidores LDAP ou dos Servidores LDAP e portas a serem usados no campo **Lista de Informações de SERVIDORES LDAP**.
 8. Se o LDAP deve ser usado para armazenar informações do Registro DCE, digite o nome distinto usado para autenticar no LDAP no campo **NOME DISTINTO DO LDAP**.
 9. Se o LDAP deve ser usado para armazenar informações do Registro DCE, digite a senha para o nome distinto do LDAP no campo **Senha do NOME DISTINTO DO LDAP**.
 10. Se o LDAP deve ser usado para armazenar informações do Registro DCE, tabule para selecionar o Método de Autenticação do LDAP no campo **Método de AUTENTICAÇÃO DO LDAP**. Os valores válidos são nenhum, ssl, gssapi ou cram-md5. O padrão é **nenhum**.
 11. Se o LDAP deve ser usado para armazenar informações do Registro DCE, tabule para selecionar **sim** ou **não** no campo **Usar Comunicação SSL** para indicar se deve ser usada comunicação SSL entre o DCE e o LDAP.

12. Se o LDAP deve ser usado para armazenar informações do Registro DCE, digite o caminho completamente qualificado para o arquivo de **ANEL DE CHAVES DO LDAP**.
13. Digite a senha do anel de chaves no campo **Senha do ANEL DE CHAVES DO LDAP** se estiver usando comunicação SSL. Se não for digitado um valor, o SSL usará a senha que está criptografada no arquivo stash de senha apropriado.
14. Se o LDAP deve ser usado para armazenar informações do Registro DCE, tabule para selecionar **sim** ou **não** no campo **Armazenar Senha Mestra do DCE no LDAP** para indicar se a Senha Mestra do DCE deve ser armazenada no LDAP. O padrão é **não**.
15. Se o LDAP deve ser usado para armazenar informações do Registro DCE, digite o caminho completamente qualificado para o arquivo da **Senha Mestra do DCE** se esta **NÃO** deve ser armazenada no LDAP. A localização padrão é **/opt/dcelocal/var/security/.mkey**.
16. Tabule para selecionar **sim** ou **não** no campo **Usar login baseado em CERTIFICADO** para indicar se a autenticação de certificado PK deve ser ativada.
17. Se a autenticação de certificado PK deverá ser usada, digite o caminho completamente qualificado do arquivo que contém o **PERFIL ENTRUST para o servidor de segurança**.
18. Se a autenticação de certificado PK deverá ser usada, digite o caminho completamente qualificado do **arquivo de INICIALIZAÇÃO ENTRUST**.
19. Se a autenticação de certificado PK deverá ser usada, digite a **senha do PERFIL ENTRUST** para o servidor de segurança DCE.
20. Se a máquina já estiver configurada como um cliente, todos os outros campos estarão preenchidos. Se a máquina ainda não está configurada como um cliente, especifique os nomes de host TCP/IP do Servidor de Segurança Principal e do Servidor CDS.
21. Pressione **<Enter>** para selecionar **Fazer**.
22. Quando consultado, digite a senha do administrador da célula.

Para configurar uma réplica do servidor de segurança a partir de uma linha de comandos, no prompt de comandos digite:

```
config.dce [-sec_server_name <servidor_de_segurança>]
[-cell_name <nome_da_célula>]
[-cell_admin <id_do_admin_da_célula>] [-admin_pwd <senha>]
[-sec_master <servidor_de_segurança_principal>] [-cds_server <servidor_cds>]
[-autostart yes | no] [-clean_autostart yes | no] [-protocol <tcp udp>]
[-time_server <id_do_servidor>] [-sync_clocks yes | no]
[-certificate_based_login yes | no] [-kdc_profile <perfil_kdc>]
[-kdc_ini_file <arquivo_ini_kdc> ] [-kdc_passphrase <kdc_passphrase>]
[-group_rsp_path <nome_do_arquivo>] [-rsp_file <nome_do_arquivo>]
[ldap_auth <none | ssl | cram-md5>] [-ldap_dn <ldap_dn>]
[-ldap_dn_pw <ldap_dn_pw>] [-ldap_keyring <arq_anel_chaves_ldap>]
```

```
[-ldap_keyring_pw <senha_arq_chaves_ldap>] [-ldap_ssl yes | no]
[-ldap_registry] [-ldap_master_key_in_ldap yes | no]
[-ldap_dce_master_key <arq_chave_mestra_dce>]
[-ldap_server <servidor_ldap | ldap_server:número_da_porta>]
sec_rsp
```

Neste ponto, **dced** (RPC e um cliente de segurança), uma réplica de segurança e um cliente CDS são configurados na máquina.

Configuração do Global Directory Agent (GDA)

O Global Directory Agent (GDA) permite a comunicação entre as células localizando uma célula externa que tenha sido registrada no serviço de diretório global do Domain Naming System (DNS). Somente um GDA precisa ser configurado na célula para permitir a comunicação entre as células, mas podem ser configurados mais para aumentar a disponibilidade.

Para configurar o GDA em uma máquina, execute as seguintes etapas na máquina.

Nota: Se a máquina ainda não é um cliente DCE, siga as etapas delineadas em “Configuração de Clientes DCE” na página 92.

Para configurar o GDA usando o **smitty**:

1. Como root, inicie o **smitty** com o atalho **mkdcesrv**:

```
smitty mkdcesrv
```

ou execute a seguinte seqüência de opções de menu do **smitty**:

1. **Aplicações e Serviços de Comunicações**
2. **DCE (Distributed Computing Environment)**
3. **Configurar DCE/DFS**
4. **Configurar Servidores DCE/DFS**
2. Selecione a opção **GDA (Global Directory Agent)** e pressione <Enter>.
3. Se não estiver usando o *admin_célula* padrão, digite o nome da conta do administrador da célula no prompt **Conta do ADMINISTRADOR da célula**.
4. digite os nomes dos Servidores LDAP ou dos Servidores LDAP e portas a serem usados no campo **O id do host do servidor LDAP com 'número_da_porta' opcional..**
5. Como a máquina já está configurada como um cliente DCE, todos os outros campos devem estar preenchidos automaticamente com os valores apropriados. Pressione <Enter> para selecionar **Fazer**.
6. Quando consultado, digite a senha do administrador da célula.

Para configurar o GDA a partir de um prompt de comandos, na linha de comandos digite:

```
config.dce [-cell_name <nome_da_célula>] [-admin_pwd<senha_do_admin>]
[-cell_admin <id_do_admin_da_célula>]
[-sec_master <servidor_segurança_principal>]
[-cds_server <servidor-cds>] [-lan_profile <perfil>]
[-ldap_server <servidor_ldap | ldap_server:número_da_porta>]
[-time_server <id_do_servidor>] [-sync_clocks yes | no]
[-autostart yes | no] [-clean_autostart yes | no] [-protocol tcp udp]
[-group_rsp_path <nome_do_arquivo>] [-rsp_file <nome_do_arquivo>]
[-wrap_audit_trail yes | no]
gda_srv
```

Neste ponto, o GDA é configurado na máquina. Para ativar a comunicação entre as células, consulte as informações sobre o ambiente entre as células no *IBM DCE Version 3.2 for AIX and Solaris: Administration Guide—Core Components*. Além disso, consulte o *IBM DCE Version 3.2 for AIX and Solaris: Administration Guide—Core Components* para obter informações sobre como registrar uma célula globalmente.

Configuração de Servidores EMS

Para configurar um servidor EMS execute as seguinte etapas.

Nota: Se a máquina ainda não é um cliente DCE, siga as etapas delineadas em “Configuração de Clientes DCE” na página 92.

Para configurar um servidor EMS usando o **smitty**:

1. Como root, inicie o **smitty** com o atalho **mkdcesrv**:

```
smitty mkdcesrv
```

ou execute a seguinte seqüência de opções de menu do **smitty**:

1. **Aplicações e Serviços de Comunicações**
 2. **DCE (Distributed Computing Environment)**
 3. **Configurar DCE/DFS**
 4. **Configurar Servidores DCE/DFS**
2. Selecione a opção **Servidor EMS** e pressione <Enter>.
 3. Como a máquina já está configurada como um cliente DCE, todos os outros campos devem estar preenchidos automaticamente com os valores apropriados. Você não será consultado quanto à senha do administrador da célula quando o cliente DCE já estiver configurado. Pressione <Enter> para selecionar **Fazer**.

Para configurar um servidor EMS a partir de uma linha de comandos, no prompt de comandos digite:

```

config.dce [-cell_name <nome_da_célula>] [-admin_pwd<senha_do_admin>]
[-cell_admin <id_do_admin_da_célula>]
[-sec_master <servidor_segurança_principal>]
[-cds_server <servidor-cds>] [-lan_profile <perfil>]
[-time_server <id do servidor>] [-sync_clocks yes | no]
[-autostart yes | no] [-clean_autostart yes | no] [-protocol tcp udp]
[-group_rsp_path <nome_do_arquivo>] [-rsp_file <nome_do_arquivo>]
[-wrap_audit_trail yes | no]
ems_srv

```

Neste ponto, um servidor EMS é configurado na máquina, juntamente com **dced** (RPC e um cliente de segurança) e um cliente CDS os quais foram configurados como parte da configuração do cliente DCE.

Configuração de Servidores SNMP

Para configurar um servidor SNMP execute as seguinte etapas.

Para configurar um servidor SNMP usando o **smitty**:

1. Como root, inicie o **smitty** com o atalho **mkdcesrv**:

```
smitty mkdcesrv
```

ou execute a seguinte seqüência de opções de menu do **smitty**:

1. **Aplicações e Serviços de Comunicações**
2. **DCE (Distributed Computing Environment)**
3. **Configurar DCE/DFS**
4. **Configurar Servidores DCE/DFS**
2. Selecione a opção **Servidor SNMP** e pressione <Enter>.
3. Tabule para selecionar **sim** ou **não** no campo **Iniciar os componentes no reinício do Sistema** para indicar se os componentes do DCE devem ou não ser iniciados automaticamente na reinicialização do sistema;
4. Tabule para selecionar **sim** ou **não** no campo **Limpar DCE no reinício do Sistema** para indicar se **clean_up.dce** deve ser executado na reinicialização do sistema. Isto será feito antes de reiniciar o DCE.
5. Pressione <Enter> para selecionar **Fazer**.

Para configurar um servidor SNMP a partir de uma linha de comandos, no prompt de comandos digite:

```

config.dce
[-autostart yes | no] [-clean_autostart yes | no]
snmp_srv

```

Configuração da Integração de Segurança do DCE 3.2 para AIX

Use as seguintes etapas para configurar o daemon dceunixd.

Nota: Se a máquina ainda não é um cliente DCE, siga as etapas delineadas em “Configuração de Clientes DCE” na página 92.

Para configurar um sistema para integração de segurança usando o **smitty**:

1. Como root, inicie o **smitty** com o atalho **mkdcesrv**:

```
smitty mkdcesrv
```

ou execute a seguinte seqüência de opções de menu do **smitty**:

1. **Aplicações e Serviços de Comunicações**
 2. **DCE (Distributed Computing Environment)**
 3. **Configurar DCE/DFS**
 4. **Configurar Servidores DCE/DFS**
2. Selecione a opção **Servidor UNIXD DCE** e pressione <Enter>.
 3. Se não estiver usando o **cell_admin** padrão, digite o nome da conta do administrador da célula no prompt **Conta do ADMINISTRADOR da célula**.
 4. Digite o número de processos **dceunixd** que deseja executar no campo **Número de instâncias de processos dce unixd**.
 5. Digite o número de minutos que o cache **dceunixd** deve ser mantido no campo **Tempo de operação do cache em minutos**.
 6. Como a máquina já está configurada como um cliente DCE, todos os outros campos devem estar preenchidos automaticamente com os valores apropriados. Pressione <Enter> para selecionar **Fazer**.

Para configurar um sistema para operações de integração de segurança a partir de uma linha de comandos, no prompt de comandos digite:

```
config.dce [-cache_lifetime <minutos>][-num_dce_unixd <núm>]  
dce_unixd
```

Neste ponto, um servidor **dceunixd** é configurado na máquina, juntamente com **dced** (RPC e um cliente de segurança) e um cliente CDS os quais foram configurados como parte da configuração do cliente DCE. Para configurar a máquina para usar o login integrado de segurança DCE, consulte o *IBM DCE Version 3.2 for AIX and Solaris: Administration Guide—Core Components* para detalhes completos.

Configuração de Servidores de Auditoria

Para configurar um servidor de Auditoria execute as seguinte etapas.

Notas:

1. Se a máquina ainda não é um cliente DCE, siga as etapas delineadas em “Configuração de Clientes DCE” na página 92.

2. Para permitir que o servidor use auditoria, é preciso definir a variável de ambiente DCEAUDITON=1. A forma mais fácil de fazer isto é configurar a auditoria e em seguida parar e reiniciar os servidores, certificando-se de que a variável de ambiente DCEAUDITON esteja definida antes de iniciar.

Para configurar um servidor de Auditoria usando o **smitty**:

1. Como root, inicie o **smitty** com o atalho **mkdcesrv**:

```
smitty mkdcesrv
```

ou execute a seguinte seqüência de opções de menu do **smitty**:

1. **Aplicações e Serviços de Comunicações**
 2. **DCE (Distributed Computing Environment)**
 3. **Configurar DCE/DFS**
 4. **Configurar Servidores DCE/DFS**
2. Selecione a opção **Daemon de Auditoria** e pressione **<Enter>**.
 3. Tabule para selecionar sim ou não no campo Reinício Cíclico da Trilha de Auditoria para indicar se a trilha de auditoria deve ter reinício cíclico.
 4. Como a máquina já está configurada como um cliente DCE, todos os outros campos devem estar preenchidos automaticamente com os valores apropriados. Você não será consultado quanto à senha do administrador da célula quando o cliente DCE já estiver configurado. Pressione **<Enter>** para selecionar **Fazer**.

Para configurar um servidor de Auditoria a partir de uma linha de comandos, no prompt de comandos digite:

```
config.dce [-cell_name <nome_da_célula>]
[-sec_master <servidor_de_segurança_principal>] [-cds_server <servidor_cds>]
[-lan_profile <perfil>][-autostart yes | no] [-clean_autostart yes | no]
[-protocol tcp udp][-time_server <id do servidor>] [-sync_clocks yes | no]
[-group_rsp_path <nome_do_arquivo>] [-rsp_file <nome_do_arquivo>]
[-wrap_audit_trail yes | no]
audit
```

Neste ponto, um servidor de Auditoria é configurado na máquina, juntamente com **dcad** (RPC e um cliente de segurança) e um cliente CDS os quais foram configurados como parte da configuração do cliente DCE.

Configuração de Servidores de Senha Válida

Para configurar um servidor de Senha Válida em uma máquina, execute as seguintes etapas na máquina.

Nota: Se a máquina ainda não é um cliente DCE, siga as etapas delineadas em “Configuração de Clientes DCE” na página 92.

Para configurar um servidor de Senha Válida usando o **smitty**:

1. Como root, inicie o **smitty** com o atalho **mkdcesrv**:

```
smitty mkdcesrv
```

ou execute a seguinte seqüência de opções de menu do **smitty**:

1. **Aplicações e Serviços de Comunicações**
 2. **DCE (Distributed Computing Environment)**
 3. **Configurar DCE/DFS**
 4. **Configurar Servidores DCE/DFS**
2. Selecione a opção **Servidor de Senha Válida** e pressione <Enter>.
 3. Selecione a opção **Servidor Básico** ou a opção **Servidor IBM Melhorado** e pressione <Enter>.
 4. Se não estiver usando o **cell_admin** padrão, digite o nome da conta do administrador da célula no prompt **Conta do ADMINISTRADOR da célula**.
 5. Se não estiver usando os argumentos padrões do servidor de senha válida, digite os argumentos no prompt **Argumento do servidor de senha válida**.
 6. Se não estiver usando o nome padrão do servidor de senha válida, digite o comando do servidor de senha válida, incluindo o caminho completo, no prompt **Daemon do servidor de senha válida**.
 7. Se não estiver usando o usuário principal padrão do servidor de senha válida, digite o usuário principal do servidor de senha válida no prompt **ID do usuário principal para o Servidor de senha válida**.
 8. Tabule para selecionar **sim** ou **não** no campo **Permitir bibliotecas definidas pelo usuário** para indicar se este servidor deve ou não poder acessar bibliotecas definidas pelo usuário para obrigatoriedade de regras adicionais. (Esta opção somente estará disponível se o Servidor IBM Melhorado tiver sido selecionado na etapa 3.
 9. Como a máquina já está configurada como um cliente DCE, todos os outros campos devem estar preenchidos automaticamente com os valores apropriados. Pressione <Enter> para selecionar **Fazer**.
 10. Quando consultado, digite a senha do administrador da célula.

Para configurar um servidor de Senha Válida a partir de uma linha de comandos, no prompt de comandos digite:

```
config.dce [-cell_name <nome_da_célula>] [-cell_admin <id_do_admin_da_célula>]  
[-admin_pwd <senha_de_admin>] [-sec_master <servidor_de_segurança_principal>]  
[-cds_server <servidor_cds>] [-lan_profile <perfil>]  
[-pwdstr_arg <args da linha de comandos>] [-pwdstr_cmd <nome_do_servidor>]  
[-pwdstr_principal <id do usuário principal de senha válida>]  
[-autostart yes | no] [-clean_autostart yes | no] [-protocol tcp udp]
```

```
[-time_server <id_do_servidor>] [-sync_clocks yes | no]
[-group_rsp_path <nome_do_arquivo>] [-rsp_file <nome_do_arquivo>]
[-wrap_audit_trail yes | no]
pw_strength_srv
```

Notas:

1. Se mais de um argumento da linha de comandos for aplicado à opção **-pwdstr_arg**, os argumentos precisam estar delimitados por aspas duplas ("). Por exemplo:
`-pwdstr_arg "-v -d"`
2. Se desejar especificar um nome de usuário principal de senha válida diferente de `pwd_strengthd`, especifique as duas opções, **-pwdstr_principal** e **-pwdstr_arg -server_princ**. Por exemplo:
`-pwdstr_principal pwd_server`
`-pwdstr_arg "-server_princ pwd_server"`

Neste ponto, um servidor de Senha Válida é configurado na máquina, juntamente com **dced** (RPC e um cliente de segurança) e um cliente CDS os quais foram configurados como parte da configuração do cliente DCE.

Configuração do Name Service Interface Daemon (NSID)

Para configurar o NSID em uma máquina, execute as seguintes etapas na máquina.

Nota: Se a máquina ainda não é um cliente DCE, siga as etapas delineadas em “Configuração de Clientes DCE” na página 92.

Para configurar o NSID usando o **smitty**:

1. Como root, inicie o **smitty** com o atalho **mkdcesrv**:

```
smitty mkdcesrv
```

ou execute a seguinte seqüência de opções de menu do **smitty**:

1. **Aplicações e Serviços de Comunicações**
 2. **DCE (Distributed Computing Environment)**
 3. **Configurar DCE/DFS**
 4. **Configurar Servidores DCE/DFS**
2. Selecione a opção **NSI (Interface do Serviço de Nomes)** e pressione **<Enter>**.
 3. Se não estiver usando o **cell_admin** padrão, digite o nome da conta do administrador da célula no prompt **Conta do ADMINISTRADOR da célula**.
 4. Como a máquina já está configurada como um cliente DCE, todos os outros campos devem estar preenchidos automaticamente com os valores apropriados. Pressione **<Enter>** para selecionar **Fazer**.

5. Quando consultado, digite a senha do administrador da célula.

Para configurar o NSID a partir de uma linha de comandos, no prompt de comandos digite:

```
config.dce [-cell_name <nome_da_célula>] [-cell_admin <id de cell_admin>]
[-admin_pwd <senha_do_admin>] [-sec_master <servidor_de_segurança_principal>]
[-cds_server <servidor_cds>] [-lan_profile <perfil>]
[-time_server <id do servidor>] [-sync_clocks yes | no]
[-autostart yes | no] [-clean_autostart yes | no] [protocol tcp udp]
[-group_rsp_path <nome_do_arquivo>] [-rsp_file <nome_do_arquivo>]
[-nsid_pwd <senha_nsid>] [-wrap_audit_trail yes | no]
nsid
```

Neste ponto, o NSID é configurado na máquina, com **dced** (RPC e um cliente de segurança) e um cliente CDS os quais foram configurados como parte da configuração do cliente DCE.

Configuração de um Servidor de Mapeamento de Identidade

Para configurar um servidor de Mapeamento de Identidade, execute as seguintes etapas na máquina usando o **smitty**:

Nota: Se a máquina ainda não está configurada como um servidor de segurança, siga as etapas delinadas em “Configuração do Servidor de Segurança Principal” na página 87 ou “Configuração das Réplicas dos Servidores de Segurança” na página 106.

1. Como root, inicie o **smitty** com o atalho **mkdcesrv**:

```
smitty mkdcesrv
```

ou execute a seguinte seqüência de opções de menu do **smitty**:

1. **Aplicações e Serviços de Comunicações**
2. **DCE (Distributed Computing Environment)**
3. **Configurar DCE/DFS**
4. **Configurar Servidores DCE/DFS**
2. Selecione a opção **Servidor de Mapeamento de Identidade** e pressione **<Enter>**.
3. Se não desejar usar o *admin_célula* padrão, digite o nome da conta do administrador da célula no prompt **Conta do ADMINISTRADOR da célula**.
4. Tabule para selecionar **sim** ou **não** no campo **Iniciar os componentes no reinício do Sistema** para indicar se os componentes do DCE devem ou não ser iniciados automaticamente na reinicialização do sistema;
5. Tabule para selecionar **sim** ou **não** no campo **Limpar DCE no reinício do Sistema** para indicar se *clean_up.dce* deve ser executado na reinicialização do sistema. Isto será feito antes de reiniciar o DCE.

6. No prompt **PERFIL ENTRUST para o servidor de Segurança**, digite o nome do perfil Entrust, incluindo o nome do caminho completo.
7. No prompt **Arquivo de INICIALIZAÇÃO ENTRUST**, digite o nome do arquivo de Inicialização Entrust, incluindo o caminho completo.
8. No prompt **Senha do PERFIL ENTRUST**, digite a senha associada ao perfil Entrust para o Servidor de Segurança DCE.
9. Pressione <Enter> para selecionar **Fazer**.
10. Quando consultado, digite a senha do administrador da célula.

Para configurar um Servidor de Mapeamento de Identidade: a partir de uma linha de comandos, o servidor de Mapeamento de Identidade deve estar configurado na mesma máquina do servidor de segurança principal ou de uma réplica do servidor de principal. No prompt digite:

```
config.dce [-autostart yes | no] [-clean_autostart yes | no] [kdc_profile
<arquivo de perfil>] [-kdc_ini_file <arquivo de inicialização Entrust>]
[-kdc_passphrase <senha do perfil Entrust>]
idms_srv
```

Quando consultado, digite a senha do administrador da célula.

Neste ponto, um servidor de Mapeamento de Identidade, servidor de segurança (principal ou réplica), **dced** (RPC e um cliente de segurança) e um cliente CDS são configurados na máquina.

Nota: Modifique a versão do registro emitindo o seguinte comando a partir de uma linha de comandos:

```
dcecp -c registry modify -version {secd.dce.1.2.2a}
```

Configuração do DCE Web Secure para AIX

O DCE Web Secure deve ser instalado e configurado em uma estação de trabalho que tenha um cliente DCE e um servidor Web iPlanet FastTrack 4.1, iPlanet Enterprise 4.0 ou iPlanet Enterprise 4.1. O DCE Web Secure também suporta os servidores Web suportados pelo DCE 3.1. O DCE Web Secure para AIX pode ser configurado usando o SMIT.

Configuração do DCE Web Secure Usando o SMIT

A partir do painel principal do SMIT:

1. Selecione **Aplicações e Serviços de Comunicação**.
2. Selecione **DCE (Distributed Computing Environment)**.
3. Selecione **Configurar / Remover Configuração de DCE Web**.
4. Selecione **Configurar DCE Web**.
5. Digite o diretório root onde o servidor Netscape está instalado no campo **Diretório Netscape** e pressione <Enter>.

6. No painel **Configurar DCE Web**:

- Digite o ID do servidor Netscape no campo **ID do servidor Netscape**.
- Digite um *id de usuário* no campo **ID de Usuário**.
- Selecione **Tudo** no campo **Componentes a configurar**. **Tudo** é o padrão para configurar o DCE Web Secure e o DCE Web Administration.

7. Selecione **OK** e pressione <Enter> para iniciar a configuração.

O *diretório root do servidor netscape* é o diretório root onde o servidor Netscape está instalado.

O *ID do Servidor Netscape* identifica o nome do computador da máquina onde o servidor Web Netscape foi instalado. Este é o campo *nome do host* na janela View Server Settings na GUI do Servidor de Administração do iPlanet Web Server. Ele é também o *ServerName* identificado no arquivo **magnus.conf**. Se não tiver certeza quanto a valor a fornecer, pressione F4 para uma lista de opções.

O *id de usuário* é o nome da conta do usuário do sistema operacional sob a qual o servidor Netscape deve executar. O *id de usuário* não pode ser *ninguém*.

O componente pode ser **secure**, **admin** ou **tudo**. **secure** configura o DCE Web Secure. **admin** e **tudo** configuram o DCE Web Secure e o DCE Web Administration. Para obter maiores informações, consulte o *IBM DCE Version 3.2 for AIX and Solaris: Administration Commands Reference*.

Configuração do DCE Web Secure a partir de uma Linha de Comandos

Para configurar o DCE Web Secure para AIX ou o DCE Web Secure e o DCE Web Administration para AIX a partir da linha de comandos, digite:

```
mkdcweb -n <dir_netscape> -s <id_netscape> -i <id_de_usuario>
-t <componente>
```

- A <dir_netscape> é o diretório root onde o produto servidor Netscape está instalado.
- O <id_netscape> identifica o nome do servidor Web. Este valor vem do campo **Identificador do Servidor** especificado pelo administrador através do Servidor de Administração Netscape quando o servidor foi instalado.
- O <id_de_usuario> é o nome da conta do usuário do sistema operacional sob a qual o servidor Netscape deve executar. O <id_de_usuario> não pode ser *nobody*, e recomenda-se que o servidor Web não execute como *root*.
- O <componente> indica quais componentes configurar:
 - **secure** configura somente o DCE Web Secure.
 - **admin** configura o DCE Web Administration e o DCE Web Secure, já que o DCE Web Secure é um pré-requisito do DCE Web Administration.
 - **tudo** configura o DCE Web Secure e o DCE Web Administration.

Nota: Para alguns locais asiáticos, não é possível iniciar um servidor Web Netscape, como o DCE Web Secure, a partir da linha de comandos em um aixterm. Se planejar configurar ou iniciar o DCE Web Secure a partir da linha de comandos, use um dterm, não um aixterm. Como alternativa, use a página da Administração do Servidor Netscape em lugar da linha de comandos para gerenciar o DCE Web Secure.

Verificação da Configuração do DCE Web Secure

A melhor maneira de verificar se a configuração obteve êxito ou não, além da ausência de mensagens de erro durante a configuração, é usar os recursos do DCE Web Secure através de um navegador da Web. Para fazer isto, digite o seguinte endereço da Web no navegador da Web:

```
http://id_netscape[:porta]/dcweb
```

id_netscape é o nome do servidor Web especificado quando o DCE Web Secure foi configurado. A porta é opcional se a porta padrão, 80, estiver sendo usada.

Acesso a uma CGI usando Credenciais DCE

Com o DCE Web Secure instalado e configurado, podem-se fornecer credenciais DCE a programas CGI (Common Gateway Interface). Esta funcionalidade pode ser especialmente útil se desejar executar um script de shell ou script tcl que precise de credenciais DCE a partir do navegador da Web.

Como um exemplo, coloque o seguinte script de shell em um arquivo chamado testcgi.sh em /opt/dcelocal/web/admin/cgi-bin. Assegure que o script de shell tenha permissão de execução para o id de usuário do sistema operacional sob o qual o servidor Web está executando.

Pode ser preciso alterar a Fonte do Navegador da Web para a página de códigos 850. Para fazer isto:

1. Clique em **Editar**→**Preferências**→**Aparência**→**Fontes**. Selecione **Definida pelo Usuário** para Codificação e **ibm-850** para as fontes.
2. Clique em **Exibir**→**Conjunto de Caracteres**. Selecione **Definido pelo Usuário**.

```
#!/bin/sh
# testcgi.sh Programa CGI de teste para mostrar credenciais DCE.
echo "Content-type: text/html"
echo ""
echo "<html>"
echo "<head>"
echo "<title>Programa CGI de teste para mostrar credenciais DCE</title>"
echo "</head>"
echo "<body>"
echo "<h1>Programa CGI de teste para mostrar credenciais DCE</h1>"
echo "<p><h3>CGI está executando sob as seguintes credenciais DCE:</h3>"
```

```
echo "<pre>"
klist | grep "Global Principal"
echo "</pre>"
echo "</body>"
echo "</html>"
```

Quando executado, o CGI mostrará quais credenciais estão sendo usadas. Por exemplo, se você armazenou o arquivo em **/opt/dcelocal/web/admin/cgi-bin/testcgi.sh** e definiu o servidor web para permitir que programas CGI sejam executados a partir de **/opt/dcelocal/web/admin/cgi-bin**, poderá executar este CGI a partir do seguinte endereço da Web:

```
http://<nome-do-servidor>/dcweb/cgi-bin/testcgi.sh
```

Para garantir que o CGI execute com credenciais DCE, verifique que o acesso não autenticado não esteja ligado para o caminho **/opt/dcelocal/web/admin/cgi-bin** na configuração do servidor Web.

Execução de um Programa CGI no Caminho Padrão

A Configuração do Web Secure define o caminho padrão de CGI no arquivo **obj.conf**. O caminho padrão é **/opt/dcelocal/web/admin/cgi-bin** (mapeia para **/dcweb/cgi-bin**), portanto scripts e aplicações CGI poderiam ser copiados para esse diretório.

Para executar um URL de aplicação CGI:

```
http://nome_do_servidor:porta/dcweb/cgi-bin/nome_do_script_cgi
```

nome_do_servidor

O nome do host para o Servidor Web.

porta O número da porta na qual o servidor Web está. Esta parâmetro é opcional se o número da porta for *80*.

nome_do_script_cgi

é o nome do arquivo do script ou aplicação CGI

O usuário pode especificar um caminho diferente para armazenar os scripts e aplicações CGI, mas terá que alterar o arquivo **obj.conf** manualmente ou através da GUI do Servidor de Administração do iPlanet Web Server.

Alteração do Locale Ativo para o DCE Web Administration

Primeiro pare o Web Secure, altere seu locale, e reinicie-o.

Por exemplo, a partir da linha de comandos, você pode usar comandos como estes:

```
>/usr/netscape/suitespot/httpd-<nome_do_servidor>/stop
>export LC_ALL=<locale>
>/usr/netscape/suitespot/httpd-<nome_do_servidor>/start
```

Em seguida, pare e inicie o Navegador Netscape e acesse o DCE Web Administration.

Remoção de Configuração de Componentes do DCE

Ocasionalmente, certas situações exigem que se remova a configuração (ou os arquivos de configuração e do banco de dados) de um componente específico do DCE de uma máquina. Por exemplo, se você deseja reconfigurar um componente específico com novos parâmetros, é preciso desconfigurá-lo ou remover a configuração existente antes de definir a nova configuração. Ou, se a configuração de um componente falhou, deixando-o parcialmente configurado, é preciso remover essa configuração parcial antes de tentar novamente a configuração.

Outras situações exigem que se remova a configuração de toda a máquina (ou seja, de todos os componentes DCE da máquina). Por exemplo, se você deseja transferir uma máquina de uma célula para outra, é preciso remover da máquina as configurações da antiga célula antes de definir as configurações para a nova célula.

Em casos raros, pode-se desejar remover a configuração de toda uma célula. Se desconfigurar uma célula, será preciso remover o registro de seu nome do espaço de nomes global.

Atenção: Após remover a configuração de um servidor CDS secundário (`unconfig.dce cds_second`), é preciso aguardar duas horas antes de reconfigurar um servidor CDS secundário com o mesmo nome. O servidor CDS principal atualiza sua identidade a intervalos de duas horas.

A seção a seguir fornece mais informações sobre a remoção de configuração de componentes do DCE.

Considerações Antes de Remover a Configuração

Nota: As informações nesta seção se referem ao DCE anterior. Para informações neste tópico relacionadas aos recursos Registro de Segurança DCE e Integração LDAP, consulte o *IBM DCE Version 3.2 for AIX and Solaris: DCE Security Registry and LDAP Integration Guide*.

Deve-se ter cuidado ao remover a configuração de componentes do DCE, especialmente se for remover os componentes que desempenham os serviços exigidos por outros componentes. A remoção da configuração de um componente desativará parcial ou totalmente outros componentes que dependem dele.

Atenção: No caso de ser preciso reconfigurar uma célula e se o DFS estiver em execução no ambiente, consulte a documentação do DFS que suporta o IBM DCE 3.2 quanto a considerações antes de reconfigurar uma célula.

Há casos especiais que devem ser levados em consideração ao remover a configuração de componentes do DCE:

- O servidor de segurança principal e o servidor CDS que contém a réplica principal do diretório */:* são a base de qualquer célula. Se um destes servidores, ou ambos, forem desconfigurados, será preciso desconfigurar e reconstruir toda a célula.
- Para remover a configuração do Servidor de Segurança Principal, é preciso usar a opção **local**.
- Para remover a configuração de um servidor CDS que tenha uma réplica principal de qualquer diretório, é preciso usar a opção **local**.

Nota: Consulte o *IBM DCE Version 3.2 for AIX and Solaris: Administration Guide—Core Components* para obter maiores informações sobre como alterar a localização da réplica principal de um diretório.

Quando se remove a configuração de componentes do DCE em uma máquina, dois tipos de operações são realizadas:

- Operações locais (atualização de arquivos de configuração e parada de daemons)
- Operações administrativas (atualização do registro de segurança, do espaço de nomes CDS)

Assim como a configuração é separada nas partes **administrativa** e **local**, o mesmo acontece com a maior parte da remoção de configuração. As exceções são o servidor de segurança principal (**sec_srv**) e qualquer servidor CDS (**cds_srv** ou **cds_second**) que contenha uma réplica principal de um diretório em uma de suas clearinghouses.

Quando se remove a configuração de componentes do DCE em uma máquina, se todas as operações locais podem ser desfeitas, a própria máquina é considerada desconfigurada. Entretanto, se as tentativas de desfazer as operações administrativas falharem, a máquina não será totalmente desconfigurada da célula; ainda podem existir entradas para a máquina no espaço de nomes CDS ou nos bancos de dados de registro. Em uma remoção de configuração total, se as tentativas de desfazer operações administrativas falharem, uma lista das operações que falharam é impressa em **/opt/dcelocal/etc/cfgdce.log** para que se possa executar manualmente essas operações e remover referências à máquina do espaço de nomes e dos bancos de dados de registro. A partir de outra máquina configurada na célula,

pode-se executar a remoção de configuração **administrativa** para as operações que falharam de modo que se pode limpar o banco de dados do registro DCE e o espaço de nomes.

Consulte o *IBM DCE Version 3.2 for AIX and Solaris: Administration Commands Reference* para obter informações completas sobre os comandos DCE referenciados acima.

Remoção de Configuração Dividida

Algumas vezes é benéfico usar um recurso conhecido como a *remoção de configuração dividida de clientes*, o qual permite ao usuário root realizar as etapas da remoção da configuração na máquina local enquanto o administrador da célula limpa o resto da célula. Uma remoção de configuração local é útil nas seguintes situações:

- Se a célula para a qual uma máquina está configurada está inacessível ou você não tem a senha para a conta do administrador para essa célula, é preciso somente remover os arquivos de configuração locais da máquina para reconfigurá-la para uma nova célula.
- Se a configuração de uma máquina estiver tão danificada que ela não pode alcançar o servidor de segurança para ser autenticada para realizar operações remotas, você pode limitar a remoção da configuração a itens locais.
- Se estiver removendo a configuração do servidor de segurança principal, é preciso limitar a remoção da configuração a itens locais.
- Se estiver removendo a configuração de um servidor CDS que contém a réplica principal de um diretório, é preciso limitar a remoção da configuração a itens locais.
- Se estiver removendo a configuração de um cliente básico, somente as etapas de remoção de configuração local são necessárias.

O administrador da célula deve executar a parte **administrativa** da remoção de configuração a partir de uma máquina na célula para concluir o processo de remoção da configuração. Um cliente completo que tiver sido desconfigurado localmente não pode ser configurado de volta na célula até que a parte administrativa da remoção da configuração tenha sido feita.

Etapas para Remoção da Configuração do DCE

Para remover a configuração de um ou mais componentes do DCE de uma máquina, execute as seguintes etapas:

- Para remover a configuração de um ou mais componentes do DCE usando o SMIT
 1. Como root, inicie o SMIT com o atalho **unconfig.dce**:

```
smitty rmdce
```

ou execute a seguinte seqüência de opções de menu do SMIT:

1. **Aplicações e Serviços de Comunicações**
 2. **DCE (Distributed Computing Environment)**
 3. **Remover Configuração do DCE/DFS**
2. Na caixa de seleção **Tipo de Remoção de Configuração**, selecione um dos seguintes:
- **remoção de configuração completa para esta máquina**
 - **remoção de configuração somente local para esta máquina**
 - **remoção de configuração somente administrativa para outra máquina**
3. No painel **COMPONENTES a Remover** digite ou selecione na lista sobreposta os componentes que deseja remover.
- Para a **remoção de configuração somente administrativa**, digite o *dce_nome do host* da máquina para a qual você está desconfigurando componentes no campo **NOME DE HOST DCE da Máquina Cliente**.
- Para a **remoção de configuração completa e remoção de configuração local**, o campo **Remover componentes DEPENDENTES?** tem como padrão **Não**. Este campo deve ser alterado para **Sim** somente se você tiver selecionado um componente e estiver *certo* de que deseja remover a configuração de todos os componentes que dependem da presença do componente selecionado. Por exemplo, todos os componentes dependem da presença de **dced**. Portanto, se você selecionar **dced** como o único cliente a ser desconfigurado e alterar **Remover componentes DEPENDENTES?** para **Sim**, o resultado será o mesmo que se você tivesse selecionado **Tudo** para **COMPONENTES a Remover**.
- Nota:** Se você estiver removendo a configuração de um servidor de Senha Válida, deve digitar seu ID no campo **ID do Usuário Principal para o Servidor de Senha Válida**.
4. Se não estiver usando o *admin_célula* padrão, digite o nome da conta do administrador da célula no prompt **Conta do ADMINISTRADOR da célula**.
5. Para a **remoção de configuração completa** e a **remoção de configuração somente local**, o campo **IGNORAR Verificação de Dependência?** tem o padrão de **Não**. Ele deve ser alterado para **Sim** somente se você estiver *certo* de que deseja remover a configuração de um componente sem remover a configuração de outros componentes que dependem dele. Por exemplo, se você desconfigurar o RPC mas deixar **sec_cl** e **cds_cl** configurados, estes dois não poderão funcionar corretamente.
6. Selecione **Fazer**.
7. Se consultado, digite a senha do administrador da célula para a **remoção de configuração completa** e a **remoção de configuração administrativa**.

- Para remover a configuração de um ou mais componentes do DCE a partir de uma linha de comandos, no prompt de comandos digite:

```
unconfig.dce -config_type full
[-cell_admin <id de cell_admin>] [-dependents]
[-force] [-pwdstr_principal <id do usuário_principal_de_senha_válida>]
componentes
```

Remoção de Configuração do DCE Web Secure

É **preciso** remover a configuração do DCE Web Secure antes de remover a instalação dele.

O DCE Web Secure pode ser desconfigurado usando o SMIT ou a partir de uma linha de comandos.

Para remover a configuração do DCE Web Secure usando o SMIT:

A partir do painel principal do SMIT:

1. Selecione **Aplicações e Serviços de Comunicação**.
2. Selecione **DCE (Distributed Computing Environment)**.
3. Selecione **Configurar / Remover Configuração de DCE Web**.
4. Selecione **Remover Configuração de DCE Web**.
5. No painel **Diretório do Netscape**:
 - Digite o diretório root onde o servidor Netscape está instalado no campo **Diretório Netscape** e pressione <Enter>.
6. No painel **Remover Configuração de DCE Web**:
 - Digite o ID do servidor Netscape no campo **ID do servidor Netscape**.
 - Digite um id de usuário no campo **ID do Usuário**.
 - Selecione **Tudo** no campo **Componentes a desconfigurar**. **Tudo** é o padrão para desconfigurar o DCE Web Secure e o DCE Web Administration.
 - Selecione **Sim** ou **Não** no campo **Remover arquivos de Configuração Arquivada**. **Não** é o padrão.
7. Selecione **OK** e pressione <Enter> para iniciar a remoção da configuração.

Para obter maiores informações, consulte o *IBM DCE Version 3.2 for AIX and Solaris: Administration Commands Reference*.

Remoção da Configuração do DCE Web Secure a partir de uma Linha de Comandos

Para remover a configuração do DCE Web Secure para AIX a partir da linha de comandos, digite:

```
rmdceweb -n <dir_netscape> -s <id_netscape> -t <componente>
```

- A <dir_netscape> é o diretório root onde o produto servidor Netscape está instalado.

- O <id_netscape> identifica o nome do servidor Web. Este valor vem do campo **Identificador do Servidor** especificado pelo administrador através do Servidor de Administração Netscape quando o servidor foi instalado.
- O <componente> indica quais componentes desconfigurar:
 - **secure** remove a configuração do DCE Web Secure e do DCE Web Administration, já que o DCE Web Secure é um pré-requisito do DCE Web Administration.
 - **admin** remove a configuração do DCE Web Administration.
 - **tudo** remove a configuração do DCE Web Secure e do DCE Web Administration.

Capítulo 5. Início e Parada do DCE 3.2 para AIX

Início dos Daemons do DCE

Você pode usar a linha de comandos ou a interface do SMIT para iniciar os daemons do DCE.

Uso da Linha de Comandos para Iniciar Daemons

O comando **start.dce** inicia os daemons do DCE para os componentes configurados do DCE. Antes de iniciar os daemons do DCE, é preciso efetuar login como root.

Para iniciar todos os daemons para os componentes configurados do DCE, digite o seguinte na linha de comandos:

```
start.dce all
```

Para iniciar todos os daemons para os componentes configurados do DCE, digite um dos seguintes comandos na linha de comandos:

```
start.dce core  
start.dce
```

Para iniciar componentes configurados específicos, inclua o nome do componente, tal como **cds_srv**, no comando:

```
start.dce cds_srv
```

Nota: Se o servidor de segurança principal e o servidor CDS Inicial estiverem em máquinas diferentes e ambos tiverem sido interrompidos, use as seguintes etapas para reiniciar o DCE:

Máquina 1

(rpc, sec_cl, sec_srv, cds_cl, e quaisquer outros componentes do dce)

Máquina 2

(rpc, sec_cl, cds_srv, cds_cl, e quaisquer outros componentes do dce)

1. Máquina 1: **start.dce rpc sec_cl sec_srv**
2. Máquina 2: **start.dce rpc sec_cl cds_cl cds_srv**
3. Máquina 1: **start.dce all**
4. Máquina 2: **start.dce all**

Uso do SMIT para Iniciar o DCE Imediatamente e no Reinício do Sistema

Você pode executar **start.dce** agora para iniciar todos os daemons de componentes configurados do DCE e DFS. Você também pode executar **start.dce** no reinício do sistema se as entradas apropriadas estiverem em **/etc/inittab**.

Nota: Para compatibilidade e para ser consistente com outros comandos do AIX os comandos **rc.()** são postos em **/etc/inittab**. **rc.dce** invocará **start.dce**. Use o SMIT para incluir ou excluir estas entradas.

1. Como root, inicie o SMIT:

```
smitty mkdceitab
```

2. Tabule para selecionar **sim** ou **não** no campo **Iniciar DCE agora**. A seleção de **sim** fará com que **start.dce** seja executado imediatamente. O padrão é **sim**.
3. Tabule para selecionar **sim** ou **não** no campo **Iniciar DCE no reinício do sistema**. A seleção de **sim** fará com que **rc.dce** seja posto em **/etc/inittab**, a seleção de **não** removerá **rc.dce** de **/etc/inittab**. O padrão é **não**.
4. Tabule para selecionar **sim** ou **não** no campo **Limpar arquivos DCE files na reinicialização do sistema**. A seleção de **sim** fará com que **clean_up.dce** seja posto em **/etc/inittab**, a seleção de **não** removerá **clean_up.dce** de **/etc/inittab**. O padrão é **não**.
5. Clique em **Fazer**.

Nota: Opções no comando **config.dce** permitem ligar ou desligar o início automático.

Alteração de Argumentos Passados para Daemons do DCE no Reinício

Os argumentos que são passados aos daemons do DCE durante a inicialização podem ser alterados pelo usuário.

Os parâmetros da linha de comandos podem ser alterados editando o arquivo **/opt/dcelocal/etc/cfgarg.dat**. Faça backup do arquivo antes de editá-lo.

Cada daemon que está configurado no sistema terá uma entrada em **cfgarg.dat**. Cada entrada terá o seguinte formato:

```
nome_do_daemon: opções da linha de comandos
```

Por exemplo, a entrada para o daemon **dced** no arquivo **cfgarg.dat** pode ser semelhante ao seguinte:

```
dced: -b -t 1440
```

Se um daemon específico inicia sem argumentos, nada estará listado após os dois pontos.

O seguinte é um exemplo do arquivo **cfgarg.dat** para uma máquina que está configurada como um servidor de Segurança Principal, Servidor CDS Inicial, cliente de Segurança e cliente CDS:

```
dced: -b -t 1440
secd:
cdsadv:
cdsd:
```

Se os argumentos forem alterados no arquivo **cfgarg.dat** enquanto o DCE estiver em execução, o DCE precisa ser parado e reiniciado para que os novos argumentos sejam efetivados.

Nota: Consulte o *IBM DCE Version 3.2 for AIX and Solaris: Administration Commands Reference* para uma lista completa de argumentos para cada daemon do DCE.

Parada de Daemons do DCE

O comando **stop.dce** pára os daemons do DCE para componentes configurados do DCE. Para parar os daemons do DCE, é preciso efetuar login como root.

Para parar todos os daemons para componentes configurados do DCE e DFS, digite um dos seguintes na linha de comandos:

```
stop.dce core
stop.dce
stop.dce all
```

Para parar daemons específicos para componentes configurados do DCE, inclua o nome do daemon no comando **stop.dce** e digite o seguinte na linha de comandos:

```
stop.dce dts_cl
```

Capítulo 6. Obtenção de Informações Adicionais

Esta capítulo descreve as fontes de informação que podem ser úteis quando se usa o DCE 3.2 para AIX.

Manuais

A biblioteca do DCE 3.2 para AIX contém uma cópia impressa e uma versão online do *IBM DCE Versão 3.2 para AIX: Iniciação Rápida* e uma cópia impressa do *IBM DCE Version 3.2 para AIX: Notas do Release*. Toda a demais documentação de suporte do produto é fornecida somente no formato online.

Informações Online

Extensa documentação online é fornecida como parte do produto DCE para AIX. A documentação online do IBM DCE 3.2 para AIX é fornecida em três formatos de arquivos:

- Arquivos HTML que podem ser exibidos em qualquer navegador da Web ativado para frames, como o Netscape Navigator.
- Arquivos PDF que podem ser exibidos por um visualizador de PDF, como o Adobe Acrobat Reader.
- Arquivos de texto corrido que podem ser exibidos com qualquer editor de texto, como o vi.

Manuais Online

Os seguintes manuais do IBM DCE estão disponíveis online:

- *IBM DCE Versão 3.2 para AIX: Iniciação Rápida*
- *IBM DCE Version 3.2 for AIX and Solaris: Introduction to DCE*
- *IBM DCE Version 3.2 for AIX and Solaris: Problem Determination Guide*
- *IBM DCE Version 3.2 for AIX and Solaris: Administration Guide—Introduction*
- *IBM DCE Version 3.2 for AIX and Solaris: Administration Guide—Core Components*
- *IBM DCE Version 3.2 for AIX and Solaris: Administration Commands Reference*
- *IBM DCE Versão 3.2 for AIX: High Availability Cluster Multi-Processing Guide para DCE e DFS*
- *IBM DCE Version 3.2 for AIX and Solaris: DCE Security Registry and LDAP Integration Guide*
- *IBM DCE Version 3.2 for AIX and Solaris: Application Development Guide—Introduction and Style Guide*

- *IBM DCE Version 3.2 for AIX and Solaris: Application Development Guide—Core Components*
- *IBM DCE Version 3.2 for AIX and Solaris: Application Development Guide—Directory Services*
- *IBM DCE Version 3.2 for AIX and Solaris: Application Development Reference*

Arquivos de Ajuda

O DCE 3.2 para AIX fornece assistência para tarefas de gerenciamento do sistema na forma de ajuda do SMIT. Ele também fornece ajuda HTML para a Interface Gráfica com o Usuário (GUI) da Administração do DCE).

Impressão e Pedido de Manuais

Publicações do IBM DCE

Além das edições impressas do *IBM DCE Versão 3.2 para AIX: Iniciação Rápida* e do *IBM DCE Version 3.2 para AIX: Notas do Release*, a IBM fornece arquivos PDF no CD-ROM para todos os documentos online do DCE 3.2 para os clientes que desejem a opção de ter documentação impressa.

Outras Publicações

Embora não escritos especificamente para produtos AIX, os seguintes livros da O'Reilly podem ser úteis:

- Hu, Wei. *DCE Security Programming*, 1st. ed. Sebastopol, CA: O'Reilly & Associates, 1994.
- Rosenberry, Ward. *Understanding DCE*, 2nd. ed. Sebastopol, CA: O'Reilly & Associates, 1993.
- Shirley, John. *Guide to Writing DCE Applications*, 2nd. ed. Sebastopol, CA: O'Reilly & Associates, 1994.

Uso da Documentação do DCE 3.2 para AIX

O produto DCE 3.2 para AIX inclui documentação de usuário, administração e desenvolvimento de aplicações que é acessível online.

Consulte “Apêndice A. Documentação Online” na página 135 para obter informações sobre os conjuntos de arquivos que precisam ser instalados para acessar a documentação online do DCE para AIX.

Nota: Nem todos os manuais estão traduzidos para todos os idiomas. Os manuais não traduzidos serão exibidos em inglês.

O programa `start_dcedoc`

Você pode usar o programa `start_dcedoc` para exibir a documentação online do DCE. O programa `start_dcedoc` assume como padrão o visualizador apropriado para sua interface com base na variável de ambiente `$DISPLAY`.

Você também pode usar sinalizadores para especificar qual visualizador deseja que **start_dcedoc** inicie. Os sinalizadores são **-a** para uma interface ASCII e **-g** para uma interface gráfica. O sinalizador **-a** permite exibir documentação somente em inglês no formato de texto corrido. Para exibir a documentação no formato HTML para qualquer idioma, use os sinalizadores **-g** e **-lang** da seguinte forma:

```
start_dcedoc -g -lang locale
```

onde *locale* pode ser substituído por um dos seguintes nomes de locale:

en_US locale Inglês

ja_JP locale Japonês (EUC)

Ja_JP locale Japonês (PC Kanji)

JA_JP locale Japonês (UTF-8)

ko_KR
locale Coreano

KO_KR
locale Coreano (UTF-8)

pt_BR locale Português do Brasil

PT_BR
locale Português do Brasil (UTF-8)

zh_TW
locale Chinês Tradicional (EUC)

Zh_TW
locale Chinês Tradicional (Big5)

ZH_TW
locale Chinês Tradicional (UTF-8)

Nota: O sinalizador **-g** inicia o navegador Netscape Navigator. Se o Netscape Navigator não estiver instalado, **start_dcedoc** falhará. Para mais informações, consulte “Exibição da Documentação HTML usando um navegador da Web” na página 134.

Exibição de Arquivos de Texto Simples

Para exibir a documentação online do DCE em formato de texto simples:

1. Mude para o diretório apropriado `/usr/lpp/dcedoc/3270/en_US`
2. Examine a lista de manuais para identificar o documento correto
3. Exiba o documento selecionado usando qualquer editor de texto simples, como o `vi`

Nota: `en_US` pode ser substituído por um dos nomes de locais citados anteriormente.

Exibição da Documentação HTML usando um navegador da Web

Usuários com interfaces gráficas podem usar um navegador da Web tal como o Netscape Navigator, o qual é incluído com o sistema operacional AIX, para ler os arquivos HTML da documentação do DCE. O navegador Netscape Navigator fornece links de hipertexto, utilitários de navegação, um índice de hipertexto, exibição gráfica de ilustrações, utilitários de pesquisa e de impressão, uma função de marcador e um utilitário de ajuda online ativado para NLS. Consulte a documentação do AIX para informações sobre como instalar o navegador Netscape Navigator.

Se você tiver instalado os arquivos de documentação localmente, use seu navegador da Web para exibir a documentação HTML do DCE abrindo o arquivo:

```
/usr/lpp/dcedoc/html/en_US/index.html
```

Nota: `en_US` pode ser substituído por um dos nomes de locale citados anteriormente.

Se você tiver instalado os arquivos de documentação e o DCE Web Secure estiver instalado e configurado, use seu navegador da Web remotamente para exibir a documentação HTML do DCE no seguinte endereço da Web:

```
http://<nome_do_servidor>/dcedoc/en_US
```

onde `<nome_do_servidor>` é o nome do servidor onde o DCE Web Secure está instalado e configurado.

Nota: `en_US` pode ser substituído por um dos nomes de locais citados anteriormente.

Impressão dos Manuais PDF

Se você preferir documentação impressa, um conjunto de arquivos PDF está incluído no CD-ROM do produto. Estes manuais podem ser impresso diretamente do CD-ROM. Vá para a localização `/usr/lpp/dcedoc/pdf/en_US/` e selecione o arquivo PDF que deseja enviar para a impressora. Consulte “Apêndice A. Documentação Online” na página 135 para uma lista das publicações e seus prefixos de arquivos.

Nota: `en_US` pode ser substituído por um dos nomes de locais citados anteriormente.

Apêndice A. Documentação Online

A tabela a seguir identifica os documentos pelo prefixo do arquivo:

Prefixo	Título
admingd	<i>IBM DCE Version 3.2 for AIX and Solaris: Administration Guide—Core Components</i>
adminintro	<i>IBM DCE Version 3.2 for AIX and Solaris: Administration Guide—Introduction</i>
aixquick	<i>IBM DCE Versão 3.2 para AIX: Iniciação Rápida</i>
apgstyle	<i>IBM DCE Version 3.2 for AIX and Solaris: Application Development Guide—Introduction and Style Guide</i>
appdev	<i>IBM DCE Version 3.2 for AIX and Solaris: Application Development Guide—Core Components</i>
appref	<i>IBM DCE Version 3.2 for AIX and Solaris: Application Development Reference</i>
comref	<i>IBM DCE Version 3.2 for AIX and Solaris: Administration Commands Reference</i>
dceintro	<i>IBM DCE Version 3.2 for AIX and Solaris: Introduction to DCE</i>
dirsrv	<i>IBM DCE Version 3.2 for AIX and Solaris: Application Development Guide—Directory Services</i>
hacmp	<i>IBM DCE Versão 3.2 for AIX: High Availability Cluster Multi-Processing Guide para DCE e DFS</i>
ldaprgy	<i>IBM DCE Version 3.2 for AIX and Solaris: DCE Security Registry and LDAP Integration Guide</i>
pdg	<i>IBM DCE Version 3.2 for AIX and Solaris: Problem Determination Guide</i>

Os seguintes arquivos estão contidos no pacote da Documentação Online:

Notas:

1. **en_US** pode ser substituído pelo nome de locale apropriado.
2. Nem todos os manuais estão traduzidos para todos os idiomas. Os manuais não traduzidos serão exibidos em inglês.
3. Os arquivos individuais são extraídos do arquivo tar no momento da instalação (somente HTML).

Conjunto de Arquivos:

dce.doc.en_US.ascii

/usr/lpp/dcedoc/3270/en_US/booklist

/usr/lpp/dcedoc/3270/en_US/admingd.list3270

/usr/lpp/dcedoc/3270/en_US/adminintro.list3270

/usr/lpp/dcedoc/3270/en_US/aixquick.list3270
/usr/lpp/dcedoc/3270/en_US/apgstyle.list3270
/usr/lpp/dcedoc/3270/en_US/appdev.list3270
/usr/lpp/dcedoc/3270/en_US/appref.list3270
/usr/lpp/dcedoc/3270/en_US/comref.list3270
/usr/lpp/dcedoc/3270/en_US/dceintro.list3270
/usr/lpp/dcedoc/3270/en_US/dirsrv.list3270
/usr/lpp/dcedoc/3270/en_US/hacmp.list3270
/usr/lpp/dcedoc/3270/en_US/ldaprgy.list3270
/usr/lpp/dcedoc/3270/en_US/pdg.list3270

Conjunto de Arquivos:

dce.doc.en_US.html

/usr/lpp/dcedoc/html/en_US/index.html
/usr/lpp/dcedoc/html/en_US/masthead.gif
/usr/lpp/dcedoc/html/en_US/backgr.jpg
/usr/lpp/dcedoc/html/en_US/ADMINGD/ADMINGD.tar.Z
/usr/lpp/dcedoc/html/en_US/ADMINTRO/ADMINTRO.tar.Z
/usr/lpp/dcedoc/html/en_US/AIXQUICK/AIXQUICK.tar.Z
/usr/lpp/dcedoc/html/en_US/APGSTYLE/APGSTYLE.tar.Z
/usr/lpp/dcedoc/html/en_US/APPDEV/APPDEV.tar.Z
/usr/lpp/dcedoc/html/en_US/APPREF/APPREF.tar.Z
/usr/lpp/dcedoc/html/en_US/COMREF/COMREF.tar.Z
/usr/lpp/dcedoc/html/en_US/DCEINTRO/DCEINTRO.tar.Z
/usr/lpp/dcedoc/html/en_US/DIRSRV/DIRSRV.tar.Z
/usr/lpp/dcedoc/html/en_US/HACMP/HACMP.tar.Z
/usr/lpp/dcedoc/html/en_US/LDAPRGY/LDAPRGY.tar.Z
/usr/lpp/dcedoc/html/en_US/PDG/PDG.tar.Z

Conjunto de Arquivos:

dce.doc.en_US.pdf

/usr/lpp/dcedoc/pdf/en_US/booklist
/usr/lpp/dcedoc/pdf/en_US/admingd.pdf
/usr/lpp/dcedoc/pdf/en_US/adminintro.pdf
/usr/lpp/dcedoc/pdf/en_US/aixquick.pdf
/usr/lpp/dcedoc/pdf/en_US/apgstyle.pdf
/usr/lpp/dcedoc/pdf/en_US/appdev.pdf
/usr/lpp/dcedoc/pdf/en_US/appref.pdf
/usr/lpp/dcedoc/pdf/en_US/comref.pdf
/usr/lpp/dcedoc/pdf/en_US/dceintro.pdf
/usr/lpp/dcedoc/pdf/en_US/dirsrv.pdf
/usr/lpp/dcedoc/pdf/en_US/hacmp.pdf
/usr/lpp/dcedoc/pdf/en_US/ldaprgy.pdf
/usr/lpp/dcedoc/pdf/en_US/pdg.pdf

Conjunto de Arquivos:

dce.doc.rte.ascii

```
/usr/lpp/dcedoc/bin/asciiview  
/usr/lpp/dcedoc/bin/dceman  
/usr/lpp/dcedoc/bin/start_dcedoc
```

Apêndice B. Configuração Avançada do DCE Web Secure para AIX

Estas instruções cobrem a configuração avançada do DCE Web Secure. Estas etapas supõem que a instalação e configuração básica foram bem-sucedidas.

A configuração avançada envolve a alteração manual dos arquivos **magnus.conf** e **obj.conf** para o navegador da Web Netscape. Você precisa ter conhecimento da sintaxe e do contexto destes arquivos antes de fazer qualquer alteração. Além disso, salve uma cópia de segurança dos arquivos caso suas alterações na configuração não atendam a suas expectativas. Consulte a documentação do Netscape ou o site da Netscape na Web para obter maiores informações sobre os arquivos de configuração do Netscape.

Para modificar o **obj.conf** com a GUI do Servidor de Administração do iPlanet Web Server após uma configuração do Web Secure, o usuário precisa sincronizar o arquivo **obj.conf** antes de fazer as alterações. Clique em Aplicar para carregar o Carregar Arquivos de Configuração que sincroniza o arquivo **obj.conf**. Esta sincronização assegura que o arquivo **obj.conf** permaneça consistente com a cópia mantida na GUI do Servidor de Administração do iPlanet Web Server.

Configuração de Caminho Autenticado

Você pode especificar os caminhos adicionais que precisam de credenciais DCE antes que o acesso seja concedido, usando o parâmetro **auth-path** na diretriz PathCheck. O caminho especificado é avaliado contra caminhos convertidos resultantes de diretrizes NameTrans no arquivo **obj.conf**.

Você pode especificar **auth-path** pelos seguintes motivos:

- O caminho contém programas CGI ativados para DCE.
- O caminho precisa de autenticação com um arquivo keytab do DCE em vez da autenticação básica, se usado em conjunto com o parâmetro **keyfile**.

Configuração de Keyfile

Quando um administrador do DCE deseja que os usuários acessem caminhos que exigem credenciais DCE, tais como um diretório que contenha CGIs ativados para DCE, e deseja que o usuário opere sob um id de usuário DCE específico, erl pode criar um arquivo keytab e especificar que este seja usado para um caminho específico.

O DCE Web Secure permite o uso de arquivos keytab incluindo os parâmetros **keyfile**="keytab-file-path" e **keyfile-user**="user-in-keytab-file" na diretriz **dce-restrict PathCheck** no arquivo **obj.conf** do servidor Web.

Resumo da Sintaxe de Configuração Avançada

```
PathCheck fn="dce-restrict" <auth-path="path">
  <keyfile="keytab-file-path"
  keyfile-user="user-in-keytab-file">
```

A diretriz **dce-restrict PathCheck** pode especificar combinações válidas dos seguintes argumentos opcionais:

auth-path

Especifica um prefixo de caminho que descreve objetos no sistema de arquivos que precisam de credenciais DCE antes que o acesso seja concedido.

keyfile

Indica que a autenticação em objetos que correspondam ao **auth-path** associado deve ser realizada através do arquivo keytab especificado. O **keyfile** deve ser um arquivo keytab de DCE existente e válido. O parâmetro **keyfile** deve ser usado sempre em conjunto com o parâmetro **keyfile-user**.

keyfile-user

Especifica um usuário principal DCE válido no arquivo keytab **keyfile**. O parâmetro **keyfile-user** deve ser usado sempre em conjunto com o parâmetro **keyfile**.

Exemplos de Configuração Avançada

O exemplo a seguir mostra várias diretrizes **dce-restrict PathCheck** que podem residir no arquivo **obj.conf** de um servidor Web.

```
PathCheck fn="dce-restrict" auth-path="/mycgidir"
PathCheck fn="dce-restrict" auth-path="/keytest/cgi"
  keyfile="/var/keyfile" keyfile-user="cgi_server_dceid"
```

A primeira instrução é um exemplo de como uma aplicação CGI pode ser configurada para que a autenticação DCE seja fornecida quando programas CGI em **/mycgidir** forem executados. A segunda instrução é um exemplo de como especificar um arquivo keytab para autenticação. Por exemplo, as instruções a seguir foram usadas para definir o arquivo keytab:

```
$ su (id-de-usuário-do-servidor-Netscape)
$ rgy_edit
rgy_edit> kta -p cgi_server_dceid -pw (senha-aleatória) -f /var/keyfile
rgy_edit> exit
```

Para testar se o keyfile está definido corretamente, estas instruções foram usadas:

```
$ su (id-de-usuário-do-servidor-Netscape)
$ dce_login cgi_server_dceid -k /var/keyfile
```

Apêndice C. Conjuntos de Arquivos Fictícios

A lista a seguir é uma lista de conjuntos de arquivos "fictícios". Estes conjuntos de arquivos existiam em releases anteriores do DCE. Eles foram renomeados ou combinados com outros conjuntos de arquivos no release IBM DCE V3.2 para AIX:

```
dce.client.core.rte
dce.client.core.rte.rpc
dce.pthreads.rte
dce.web.admin.rte
dce.web.secure.rte
dce.compat.cds.smit
dce.compat.client.core.smit
dce.compat.security.smit
dce.compat.sysmgmt.ems.smit
dce.compat.sysmgmt.snmpagt.smit
dce.compat.web.admin.smit
dce.msg.en_US.client.core.rte
dce.msg.en_US.compat.cds.smit
dce.msg.en_US.compat.client.core.smit
dce.msg.en_US.compat.security.smit
dce.msg.en_US.compat.sysmgmt.ems.smit
dce.msg.en_US.compat.sysmgmt.snmpagt.smit
dce.msg.en_US.pthreads.rte
dce.msg.en_US.web.admin.rte
dce.msg.en_US.web.secure.rte
dce.msg.es_ES.client.core.rte
dce.msg.es_ES.compat.cds.smit
dce.msg.es_ES.compat.client.core.smit
dce.msg.es_ES.compat.security.smit
dce.msg.es_ES.compat.sysmgmt.ems.smit
dce.msg.es_ES.compat.sysmgmt.snmpagt.smit
dce.msg.es_ES.pthreads.rte
dce.msg.es_ES.web.admin.rte
dce.msg.es_ES.web.secure.rte
dce.msg.Es_ES.client.core.rte
dce.msg.Es_ES.compat.dcs.smit
dce.msg.Es_ES.compat.client.core.smit
dce.msg.Es_ES.compat.security.smit
dce.msg.Es_ES.compat.sysmgmt.ems.smit
dce.msg.Es_ES.compat.sysmgmt.snmpagt.smit
dce.msg.Es_ES.pthreads.rte
dce.msg.Es_ES.web.admin.rte
dce.msg.Es_ES.web.secure.rte
dce.msg.ja_JP.client.core.rte
dce.msg.ja_JP.compat.cds.smit
dce.msg.ja_JP.compat.client.core.smit
dce.msg.ja_JP.compat.security.smit
dce.msg.ja_JP.compat.sysmgmt.ems.smit
dce.msg.ja_JP.compat.sysmgmt.snmpagt.smit
```

dce.msg.ja_JP.threads.rte
dce.msg.ja_JP.web.admin.rte
dce.msg.ja_JP.web.secure.rte
dce.msg.Ja_JP.client.core.rte
dce.msg.Ja_JP.compat.cds.smit
dce.msg.Ja_JP.compat.client.core.smit
dce.msg.Ja_JP.compat.security.smit
dce.msg.Ja_JP.compat.sysmgmt.ems.smit
dce.msg.Ja_JP.compat.sysmgmt.snmpagt.smit
dce.msg.Ja_JP.threads.rte
dce.msg.Ja_JP.web.admin.rte
dce.msg.Ja_JP.web.secure.rte
dce.msg.ko_KR.client.rte
dce.msg.ko_KR.compat.cds.smit
dce.msg.ko_KR.compat.client.core.smit
dce.msg.ko_KR.compat.security.smit
dce.msg.ko_KR.compat.sysmgmt.ems.smit
dce.msg.ko_KR.compat.sysmgmt.snmpagt.smit
dce.msg.ko_KR.threads.rte
dce.msg.ko_KR.web.admin.rte
dce.msg.ko_KR.web.secure.rte
dce.msg.zh_TW.client.core.rte
dce.msg.zh_TW.compat.cds.smit
dce.msg.zh_TW.compat.client.core.smit
dce.msg.zh_TW.compat.security.smit
dce.msg.zh_TW.compat.sysmgmt.ems.smit
dce.msg.zh_TW.compat.sysmgmt.snmpagt.smit
dce.msg.zh_TW.threads.rte
dce.msg.zh_TW.web.admin.rte
dce.msg.zh_TW.web.secure.rte
dce.msg.Zh_TW.client.core.rte
dce.msg.Zh_TW.compat.cds.smit
dce.msg.Zh_TW.compat.client.core.smit
dce.msg.Zh_TW.compat.securtity.smit
dce.msg.Zh_TW.compat.sysmgmt.ems.smit
dce.msg.Zh_TW.compat.sysmgmt.snmpagt.smit
dce.msg.Zh_TW.threads.rte
dce.msg.Zh_TW.web.admin.rte
dce.msg.Zh_TW.web.secure.rte

Apêndice D. Avisos

Essas informações foram desenvolvidas para produtos e serviços oferecidos nos Estados Unidos. A IBM pode não oferecer os produtos, serviços ou recursos tratados nesse documento em outros países. Consulte o seu representante local da IBM para obter mais informações sobre os produtos e serviços atualmente disponíveis em sua área. Qualquer referência a produtos, programas ou serviços da IBM, não tem a intenção de declarar ou significar que somente produtos, programas e serviços da IBM devem ser usados. Em vez disso, qualquer produto, programa ou serviço com funções equivalentes que não infrinja qualquer direito de propriedade intelectual da IBM pode ser usado. No entanto, é de responsabilidade do usuário avaliar e verificar a operação de qualquer produto, programa e serviço não pertencente à IBM.

A IBM pode ter patentes de aplicativos, ou solicitações de patentes pendentes, que abrangem o assunto descrito neste documento. O fornecimento deste documento não concede ao cliente nenhuma licença sobre essas patentes. Você pode pedir informações sobre a licença, por escrito, para o:

Gerente de Relações Industriais e Comerciais da IBM do Brasil
Av. Pasteur, 138/146 - Botafogo
Rio de Janeiro
CEP: 22290-240
Brasil.

O parágrafo seguinte não se aplica ao Reino Unido ou qualquer outro país onde tais fornecimentos sejam inconsistentes com as leis locais: A INTERNATIONAL BUSINESS MACHINES CORPORATION FORNECE ESTA PUBLICAÇÃO “COMO ESTÁ” SEM QUALQUER FORMA DE GARANTIA, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS NÃO SE LIMITANDO A, GARANTIAS IMPLÍCITAS DE NÃO-TRANSGRESSÃO, COMERCIALIZABILIDADE OU ADAPTAÇÃO A UM PROPÓSITO PARTICULAR. Alguns países não permitem a renúncia de garantias expressas ou implícitas em certas transações, por isso, essa cláusula pode não se aplicar ao seu caso.

Essas informações poderão incluir imprecisões técnicas ou erros tipográficos. As informações contidas nesta publicação estão sujeitas a alterações periódicas. A IBM pode melhorar e/ou modificar o(s) produto(s) e/ou programa(s) descritos nesta publicação a qualquer momento.

Quaisquer referências nessas informações a sites Web não pertencentes à IBM são fornecidos apenas por conveniência e não implicam, de nenhuma maneira,

em uma aprovação da IBM para esses sites Web. Os materiais nesses sites Web não fazem parte dos materiais da IBM para esse produto e o uso desses sites Web é de sua responsabilidade.

A IBM pode usar ou distribuir qualquer uma das informações que você enviar a ela, do modo que julgar apropriado, sem incorrer em qualquer obrigação para com você.

Os licenciados deste programa que desejarem ter informações sobre o mesmo com o propósito de possibilitar: (i) a troca de informações entre programas criados independentemente e outros programas (incluindo este) e (ii) o uso mútuo das informações que tenham sido trocadas, devem entrar em contato com:

Centro de Atendimento a Clientes da IBM
Av. Pasteur, 138/146, Botafogo
Rio de Janeiro
CEP: 22290-240
Brasil.

Tais informações podem estar disponíveis, sujeitas aos termos e condições apropriados que incluem, em alguns casos, o pagamento de uma taxa.

O programa licenciado descrito nesse documento e todo o material licenciado disponível são fornecidos pela IBM nos termos de Acordo do Cliente da IBM, do Acordo Internacional de Licença do Programa da IBM ou qualquer acordo equivalente entre as partes.

Alguns dados de desempenho aqui contidos foram determinados em um ambiente controlado. Conseqüentemente, os resultados obtidos em outros ambientes operacionais podem variar de maneira significativa. Algumas medidas podem ter sido determinadas em sistemas de nível de desenvolvimento e não existem garantias de que essas medidas sejam as mesmas nos sistemas disponíveis em geral. Além disso, algumas medidas podem ter sido estimadas por dedução. Os resultados atuais podem variar. Os usuários deste documento devem verificar os dados aplicáveis para o seu ambiente específico.

As informações a respeito dos produtos que não são da IBM foram obtidas através dos fornecedores deste produto, de seus anúncios públicos ou de outras fontes publicamente disponíveis. A IBM não testou estes produtos e não pode confirmar a precisão do desempenho, compatibilidade ou qualquer outra alegação relacionada a produtos que não são da IBM. Dúvidas sobre os recursos dos produtos que não são da IBM devem ser enviados aos fornecedores desses produtos.

Todas as declarações relacionadas aos objetivos e intenções futuras da IBM estão sujeitas a alterações e cancelamentos sem aviso, e representam apenas metas e objetivos.

Todos os valores IBM mostrados são preços de revenda sugeridos pela IBM, e atuais e estão sujeitos a alterações sem aviso. Os preços dos revendedores podem variar.

LICENÇA DE DIREITOS AUTORAIS:

Esta informação contém programas de amostra da aplicação em linguagem fonte, os quais ilustram as técnicas de programação em várias plataformas operacionais. Você pode copiar, modificar e distribuir esses programas de amostra, de qualquer forma e sem nenhum pagamento para a IBM, com propósitos de desenvolvimento, uso, comercialização ou distribuição dos programas aplicativos em conformidade com a Interface de Programação da Interface para plataforma operacional na qual os programas de amostra foram escritos.

Esses exemplos não foram completamente testados sob todas as condições. A IBM, assim sendo, não pode garantir ou implicar confiabilidade, utilidade ou funcionalidade desses programas. Você pode copiar, modificar e distribuir esses programas de qualquer forma sem qualquer pagamento para a IBM com propósitos de desenvolvimento, utilização, comercialização ou distribuição de programas aplicativos em conformidade com a interface de programação da aplicação (API) da IBM.

Cada cópia ou qualquer parte desses programas ou qualquer trabalho derivado deles, deve incluir a informação de direitos autorais a seguir:

© (nome da sua companhia) (ano). Partes deste código são derivados dos Programas de Amostra IBM Corp. © Copyright IBM Corp. 2001. Todos os direitos reservados.

Caso esteja vendo esta informação em cópia eletrônica, as ilustrações de fotografias e cores podem não aparecer.

Marcas

Os termos a seguir são marcas da International Business Machines Corporation nos Estados Unidos e/ou em outros países:

AIX
DFS

IBM
RISC System/6000
SecureWay

UNIX é uma marca de serviço da X/Open Company Limited.

Windows NT é uma marca de serviço da Microsoft Corporation.

Outros nomes de empresas, produtos e serviços podem ser marcas ou marcas de serviço de terceiros.

Índice Remissivo

Caracteres Especiais

/var/dce 53

A

ACLs, contêiner 20
ACLs de contêiner 20
ACLs do DCE
 diferenças entre DCE e AIX 16
adaptação aos padrões 14
AES/Distributed Computing -
 Directory Services 14
AES/Distributed Computing -
 Remote Procedure Call 14
AES/Distributed Computing -
 Security 14
AES/Distributed Computing -
 Threads 14
AES/Distributed Computing - Time
 Services 14
AIX, programas
 DCE Base Services para AIX 5
 DCE Cell Directory Server para
 AIX 9
 Privacy Level Protection 9
 Serviços de Segurança DCE para
 AIX 10
aliasas DCE 20
ambiente de programação
 multithread 6
aplicações com multithreads 16
arquivos
 a serem criados após a
 instalação 53
avisos
 duas máquinas com o mesmo
 dce_nome do host 87
 remoção da configuração de
 servidor CDS secundário 121

B

bibliografia 132
 arquivos de ajuda 132
 manuais online 131
 Publicações do DCE
 IBM 132
Biblioteca de Compatibilidade de
 Threads DCE para AIX 6

C

cdsadv 40, 45
cdsclerk 40
cdscp 41, 49
cdsd 45
cdsdel 49
cdsli 49
célula
 definição 3
 planejamento 26
chpesite 81
cleanup.dce 81
clerk CDS 40
cliente CDS
 configuração 100
 servidor de segurança
 principal 100
comando man não suportado 14
comandos adicionais
 CDS
 cdsdel 13
 cdsli 13
 configuração
 chpesite 12
 config.dce 12
 mkreg.dce 12
 rmreg.dce 13
 show.cfg 13
 unconfig.dce 13
 RPC
 rpcprotseqs 13
 rpcresolve 13
 segurança
 rmxcred 13
compatibilidade DCE com AIX
 arquivos de núcleo de
 aplicação 29
 comando man não suportado 14
 depuração 16
 segurança 15
compilador idl 50
componentes da tecnologia
 ambiente de programação
 multithread 6
 cliente de Segurança 6
 Distributed Time Service 6
 RPC 6
 XDS/XOM 8
componentes tecnológicos
 cliente de segurança
 atributos de registro
 estendidos 7
 extensões GSSAPI 7
 cliente de Segurança
 integração de segurança
 AIX 7
 Serviço de Diretório 9
config.dce 82
configuração 55
 chpesite 81
 cleanup.dce 81
 cliente CDS 100
 cliente DTS 104
 clientes DCE 92
 config.dce 82
 configuração adicional da
 célula 102
 configuração inicial da célula 79
 DCE Web Secure 117
 defasagem do relógio 81
 GDA 109
 inicial da célula 87
 integração de segurança do DCE
 3.2 para AIX 111
 kerberos.dce 12, 82
 migrate.dce 12, 82
 mkdceweb 12, 82
 mkreg.dce 82
 Name Service Interface Daemon
 (NSID) 115
 réplicas dos servidores de
 segurança 106
 requisitos mínimos 80
 rmdceweb 12, 82
 rmreg.dce 82
 servidor CDS inicial 90
 Servidor de Mapeamento de
 Identidade 116
 servidor de segurança
 principal 87, 100
 servidor EMS do DCE 3.2 para
 AIX 110
 servidor SNMP do DCE 3.2 para
 AIX 111
 servidores CDS secundários 105
 servidores de auditoria 112

- configuração 55 (*continuação*)
 - servidores de segurança
 - secundários 106
 - Servidores de Senha Válida 113
 - servidores DTS 102
 - show.cfg 82
 - start.dce 82
 - stop.dce 82
 - unconfig.dce 82
 - uso do SMIT 81
 - visão geral 79
 - configuração administrativa do cliente 93
 - configuração completa de cliente 96
 - configuração da célula
 - configuração das réplicas dos servidores de segurança 106
 - configuração de clientes DCE 92
 - configuração de servidores de segurança secundários 106
 - configuração do GDA 109
 - integração de segurança do DCE 3.2 para AIX 111
 - introdução 102
 - Name Service Interface Daemon (NSID) 115
 - Servidor de Mapeamento de Identidade 116
 - servidor EMS do DCE 3.2 para AIX 110
 - servidor SNMP do DCE 3.2 para AIX 111
 - servidores CDS secundários 105
 - servidores de auditoria 112
 - Servidores de Senha Válida 113
 - configuração dividida de clientes
 - administrativa 93
 - completa 96
 - local 94
 - configuração inicial da célula 87
 - servidor CDS 90
 - servidor de segurança
 - principal 87, 100
 - servidores DTS 102
 - configuração local do cliente 94
 - contas padrões do AIX 28
 - controle de acesso 37
 - criar, sistemas de arquivos 53
- D**
- daemons
 - cdsd 45
 - dtstd 41, 46
 - gdad 45, 46
 - secd 44
 - DCE
 - descrição 3
 - dce_nome do host 87
 - DCE para Desenvolvedores de Aplicações (dctools) 8
 - DCE system management 8
 - DCE Web Administration 8
 - Event Management Service (EMS) 8
 - Simple Network Management Protocol (SNMP) 8
 - DCE Web Administration 50
 - DCE Web Secure 49
 - dcecp 48, 49
 - desenvolvimento de aplicações 50
 - diretórios UNIX 51
 - Documentação Online 9
 - Documentação Online DCE 9
 - DTS
 - configuração de servidores 102
 - planejamento 47
 - dtstd 41, 46
- E**
- espaço de nomes
 - célula 36
 - clearinghouse 34
 - definição 34
 - introdução 32
 - planejamento 26
 - replicação 36
 - segurança 35
 - tipos de entradas 34
 - espaço de nomes da célula
 - entradas 33
 - estabilidade 32
 - limites 32
 - espaço em disco necessário (MB) 26
- G**
- GDA
 - planejamento 46
 - processos 46
 - gda_child 46
 - gdad 46
 - group_override 48
 - grupo cds-admin 37
 - grupo dfs-admin 37
 - grupo dts-admin 37
 - grupo sec-admin 37
 - grupos 37
- I**
- informações
 - pedido de publicações 132
 - início do DCE
 - uso da linha de comandos 127
 - início do DCE (*continuação*)
 - uso do SMIT 128
 - instalação 55
 - espaço em disco necessário (MB) 26
 - parada de processos 63
 - programa, fácil 63
 - software necessário 58
 - installp 65
- K**
- Kerberos 14
 - kerberos.dce 12, 82
- L**
- limitações 19
 - ACLs de contêiner 20
 - aliases DCE 20
 - nomes principais 20
 - renomeação de usuários
 - principais, grupos e orgs 20
 - sec_admin -s 20
 - uso de comandos de catálogo
 - dcecp para pesquisar várias subárvores 20
 - livros da O'Reilly & Associates 132
 - localização de arquivos
 - /opt/dcelocal 51
 - subdiretórios UNIX 51
- M**
- migração
 - antes 65
 - permissões 65
 - migrate.dce 12, 82
 - mkdceweb 12, 82
 - mkreg.dce 82
- N**
- nomes
 - célula 29, 32
 - relativos à célula 30
 - nomes globais
 - nome de célula DCE 30
 - obtendo 31
 - nomes globais DNS 30
 - nomes principais, armazenamento
 - no LDAP 20
 - nomes relativos à célula 30
 - NTP 14
- P**
- pacote
 - AIX, programas 6
 - Biblioteca de Compatibilidade de Threads DCE para AIX 6
 - programas AIX 6

- parada de processos para instalação 63
- parada do DCE 129
- passwd_export 48
- passwd_import 48
- passwd_override 48
- perfis, espaço de nomes CDS 34
- pesquisa de várias subárvores 20
- planejamento global 26
- POSIX 14
- Preferência CDS 6
- Privacy Level Protection 9
- processos de servidor
 - CDS 45
 - DTS 46
 - segurança 44
- programa de controle 48
- programa de instalação fácil 63
- programas AIX
 - DCE Base Services para AIX 5
 - DCE Cell Directory Server para AIX 9
 - Privacy Level Protection 9
 - Serviços de Segurança DCE para AIX 10
- programas clientes
 - CDS 40
 - DTS 41
 - RPC 39
- programas de administração 48
 - cdscp 49
 - cdsdel 49
 - cdsli 49
 - dcecp 48, 49
 - DTS 49
 - group_override 48
 - passwd_export 48
 - passwd_import 48
 - passwd_override 48
 - registry 49
 - rmxcred 48
 - rpc 48
- publicações 131

Q

- questões para planejamento 26

R

- recursos OSF não suportados
 - comandos
 - comandos do usuário 19
 - configuração 19
 - dce_config 19
 - dtss-graph 19
 - sec_salvage_db 19
 - segurança 19

- registry 49
- remoção de configuração
 - antes 121
 - etapas 123
 - introdução 121
 - remoção de configuração
 - dividida de clientes 123
- renomeação de usuários principais, grupos e orgs 20
- RFC 1006 14
- RFC 1129 14
- rmdcweb 12, 82
- rmreg.dce 82
- rmxcred 48
- rpcprotseqs 13
- rpcresolve 13

S

- secd 44
- segurança 37
- serviço de auditoria
 - AIX, programas 7
 - daemon de auditoria 7
 - interfaces de gerenciamento de auditoria 7
 - interfaces de programação de aplicações para auditoria 7
 - programas AIX 7
 - sobre 7
- serviço de segurança
 - servidor de senha válida 7
- serviços adicionais
 - documentação 132
- Serviços de Auditoria DCE para AIX 7
- Serviços de Segurança DCE para AIX 10
- servidor CDS inicial
 - configuração 90
- servidor de segurança principal
 - cliente CDS 100
 - configuração 87
- servidor de senha válida 7
- show.cfg 82
- sistemas de arquivos adicionais a serem criados 53
- SMIT 8
- smitty 8
- software necessário 59
- start.dce 82
- start.dce all 127
- start.dce core 127
- stop.dce 82, 129
- stop.dce all 129
- stop.dce core 129
- subárvore /opt/dcelocal 51

T

- TPO-to-TCP 14

U

- unconfig.dce 82



Número da Peça: CT6AHBP

Impresso em Brazil

(1P) P/N: CT6AHBP

