NetIQ® eDirectory™ 8.8 SP8

Guia de novidades

Setembro de 2013

Informações legais

Índice

Sobre este livro e a biblioteca

O *Guia de Novidades* apresenta os novos recursos do NetIQ eDirectory.

Para obter a versão mais recente do *Guia de Novidades do NetIQ eDirectory 8.8 SP8*, consulte o site de documentação online do NetIQ eDirectory 8.8.

Público-alvo

Ele é dirigido aos administradores de rede.

Outras informações na biblioteca

A biblioteca fornece os seguintes recursos informativos:

Guia de Administração do XDASv2

Descreve como configurar e usar o XDASv2 para auditar o eDirectory e o NetIQ Identity Manager.

Installation Guide (Guia de Instalação)

Descreve como instalar o eDirectory. Destina-se a administradores de rede.

Guia de administração

Descreve como gerenciar e configurar o eDirectory.

Troubleshooting Guide (Guia de Solução de Problemas)

Descreve como resolver problemas do eDirectory.

Guia de Ajuste para plataformas Linux

Este documento descreve como analisar e ajustar o eDirectory em plataformas Linux para proporcionar um desempenho superior em todas as suas implementações.

Estes guias estão disponíveis no site de documentação do NetIQ eDirectory 8.8 (https://www.netiq.com/documentation/edir88/).

Para obter informações sobre o utilitário de gerenciamento do eDirectory, consulte o *Guia de Administração do NetIQ iManager 2.7* (https://www.netiq.com/documentation/imanager/).

Sobre a NetIQ Corporation

Nós somos uma empresa global de software corporativo com foco nos três desafios persistentes do seu ambiente: mudança, complexidade e risco, bem como de maneira podemos ajudá-lo e controlá-los.

Nosso ponto de vista

Adaptar-se a mudanças e gerenciar complexidades e riscos não são novidades

De fato, dentre todos os desafios que você enfrenta, estas são provavelmente as variáveis mais proeminentes, que impedem que você obtenha o controle de que precisa para gerenciar, monitorar e medir de forma segura seus ambientes de computação físicos, virtuais e em nuvem.

Habilitando serviços essenciais para empresas de forma mais rápida e eficiente

Nós acreditamos que fornecer o máximo possível de controle para organizações de TI é a única maneira de possibilitar uma entrega de serviços mais oportuna e econômica. Pressões persistentes como mudanças e complexidade só continuarão a aumentar conforme as organizações continuarem a mudar e as tecnologias necessárias para gerenciá-las se tornarem inerentemente mais complexas.

Nossa filosofia

Vender soluções inteligentes, não somente software

Visando providenciar um controle seguro, primeiro nos certificamos de que entendemos os cenários do mundo real, nos quais organizações de TI como a sua operam todos os dias. Somente dessa maneira podemos desenvolver soluções de TI práticas e inteligentes, que geram com sucesso resultados comprovados e mensuráveis. E isso é muito mais recompensador do que simplesmente vender software.

Promover seu sucesso é nossa paixão

O seu sucesso encontra-se no âmago de como fazemos negócios. Desde os primeiros esboços até a implantação de um produto, nós compreendemos que você precisa de soluções de TI que funcionem bem e se integrem perfeitamente com seus investimentos existentes, suporte contínuo e treinamento pós-implantação, bem como alguém com quem trabalhar seja verdadeiramente fácil, o que sabemos que não é muito comum. Em última análise, quando você é bem-sucedido, todos nós somos bem-sucedidos.

Nossas soluções

- Governança de acesso e identidade
- Gerenciamento de acesso
- Gerenciamento de segurança
- Gerenciamento de aplicativos e sistemas

- Gerenciamento de carga de trabalho
- Gerenciamento de serviços

Entrando em contato com o Suporte a vendas

Para esclarecer dúvidas sobre produtos, preços e recursos, entre em contato com seu parceiro local. Se não for possível entrar em contato com seu parceiro, entre em contato com nossa equipe de Suporte a vendas.

Mundial:	www.netiq.com/about_netiq/officelocations.asp
Estados Unidos e Canadá:	1-888-323-6768
E-mail:	info@netiq.com
Site na Web:	www.netiq.com

Entrando em contato com o Suporte técnico

Para questões sobre produtos específicos, entre em contato com nossa equipe de Suporte técnico.

Mundial:	www.netiq.com/support/contactinfo.asp
América do Norte e do Sul:	1-713-418-5555
Europa, Oriente Médio e África:	+353 (0) 91-782 677
E-mail:	support@netiq.com
Site na Web:	www.netiq.com/support

Entrando em contato com o Suporte de documentação

Nosso objetivo é fornecer uma documentação que atenda às suas necessidades. Se você tem sugestões de melhorias, clique em **Adicionar comentário** na parte inferior de qualquer página nas versões em HTML da documentação publicada em www.netiq.com/documentation. Você também pode enviar um e-mail para Documentation-Feedback@netiq.com. Nós valorizamos sua opinião e aguardamos seu contato.

Entrando em contato com a comunidade online de usuários

A Qmunity, a comunidade online da NetIQ, é um rede colaborativa que conecta você, seus colegas e os especialistas da NetIQ. Fornecendo mais informações imediatas, links para recursos úteis e acesso aos especialistas da NetIQ, a Qmunity ajuda a garantir que você domine os conhecimentos de que precisa para utilizar todo o potencial dos investimentos de TI dos quais depende. Para obter mais informações, visite http://community.netiq.com.

1 Recursos e Melhorias do Service Pack 8

Este capítulo fornece uma visão geral dos recursos e melhorias incluídas no eDirectory 8.8 SP8.

1.1 Melhorias de escalabilidade

As melhorias de escalabilidade mencionadas a seguir foram incluídas no eDirectory 8.8 SP8 para garantir uma sincronização de dados, processamento de obituário mais rápidos, bem como um espaço de memória reduzido ao processar eventos de diário.

Nesta versão, alguns processos em segundo plano foram reprojetados para atender a ambientes dinâmicos maiores. Isto inclui otimização dos processos em segundo plano existentes e fornecimento de opções de configuração para ajustar o sistema de acordo com o ambiente adequado.

1.1.1 Controle de processo em segundo plano

Os administradores podem controlar processos em segundo plano ao configurar as Políticas de Atraso de Processo em Segundo Plano a seguir na janela Configurações de Processo em Segundo Plano no NetIQ iMonitor.

- **CPU** - Especifica o percentual máximo de recursos do computador e a duração de hibernação máxima do mesmo processo (skulker, purgador ou obituário).
- **Limite físico** - Especifica uma configuração de atraso estática para cada processo skulker, purgador e obituário individual.

Para obter mais informações sobre como configurar processos em segundo plano, consulte "Configurando processos em segundo plano" no *Guia de Administração do NetIQ eDirectory 8.8 SP8*.

1.1.2 Processo Skulker

Para aumentar as threads criadas para replicar ainda mais servidores simultaneamente, você pode usar o processo skulker para definir manualmente o número máximo de threads criadas. Esta configuração aplica-se a todas as partições de um servidor.

Para obter informações sobre como configurar o processo skulker, consulte "Configuração manual de threads de sincronização" no *Guia de Administração do NetIQ eDirectory 8.8 SP8*.

1.1.3 Replicação assíncrona

Para reduzir o tempo exigido para replicação, as operações a seguir agora são executadas em paralelo.

- Processamento de cache de alteração
- Envio de pacotes para um servidor remoto

A nova opção **Configurações de sincronização de saída assíncrona (milissegundos)** permite evitar a sobrecarga do servidor receptor. Por padrão, essa opção é desativada. A configuração depende do seu ambiente. Ao habilitar esta opção, defina-a para `100` e ajuste-a para cima ou para baixo conforme necessário.

Para obter mais informações sobre configuração de sincronização de saída assíncrona, consulte "Configuração de sincronização de saída assíncrona" no *Guia de Administração do NetIQ eDirectory 8.8 SP8*.

1.1.4 Replicação baseada em política

Os administradores agora podem criar uma política (arquivo XML) para especificar como replicar alterações. Por exemplo, isto pode ser útil com um anel de réplica distribuído em diversos locais. Se a política contiver um erro de digitação ou sintaxe incorreta, a replicação será revertida para o método padrão.

Para obter mais informações, consulte "Replicação com base em política" no *Guia de Administração do NetIQ eDirectory 8.8 SP8*.

1.1.5 Obituário

Um obituário gerado devido à exclusão, renomeação ou mudança de objetos é processado mais rapidamente do que nas versões anteriores do eDirectory. Por exemplo, uma atualização que exigia cinco ciclos nas versões anteriores agora exigirá apenas dois ciclos.

Além disso, o processo de obituário pode agora ser executado em paralelo com o processo skulker.

1.1.6 Monitorando a contagem do obituário e do cache de alterações pelo iMonitor

O iMonitor exibe o número de objetos com obituários em cada estado. Além disso, ele exibe o número de objetos no cache de alteração de uma partição ao visualizar um objeto da partição pelo iMonitor em um servidor específico. Isto ajuda a monitorar ainda mais o estado da sincronização e o processamento do obituário.

1.1.7 Links de referência distribuídos (DRL)

Para otimizar o processamento do obituário, o eDirectory não usa mais os seguintes atributos de DRL:

- `UsedBy`
- `ObitUsedBy`

1.1.8 Armazenamento em cache de evento de diário

O sistema de Evento de diário é modificado para permitir o uso de uma combinação da memória e do disco para manter os eventos na fila. Isto reduz drasticamente o crescimento da memória do processo ndsd.

Melhorias nos eventos de diário incluem:

- **Armazenamento em cache**

Quando uma fila de evento de diário ultrapassa um ponto na memória (32 MB = máx. de 8 blocos x 4 MB), o eDirectory começa a usar um cache no disco rígido.

- **Variáveis**

  Os eventos de diário incluem as seguintes variáveis que podem ser configuradas pelos usuários:

  - NDSD_EVENT_DISK_CACHE
  - NDSD_EVENT_DISK_CACHE_DIR

- **Compactação**

  A compressão aprimorada minimiza o tamanho dos dados no disco rígido. A razão de compressão é aproximadamente 20:1.

1.1.9 Suporte a Solid State Disks (SSD)

Esta versão suporta SSD empresarial para uma melhor operação de IO.

1.1.10 Custo de referência avançada (ARC)

Nesta versão, o ARC é habilitado por padrão.

Para obter mais informações, consulte "Custo de referência avançada" no *Guia de Administração do NetIQ eDirectory 8.8 SP8*.

1.1.11 Intervalo de atualização de login

A nova opção de Intervalo para desabilitar a atualização de login permite aos administradores especificarem um intervalo (em segundos) durante o qual o eDirectory não atualiza os atributos de login.

Observação: Esta opção aplica-se apenas a logins de Serviços de Diretório NetIQ (NDS).

Para obter mais informações, consulte "Controlando e configurando o Agente DS" no *Guia de Administração do NetIQ eDirectory 8.8 SP8*.

1.2 Melhorias de LDAP

Esta versão inclui as seguintes melhorias de LDAP:

1.2.1 Controle de modificação permissivo

Você pode estender a operação de modificação de LDAP atual ao usar esta opção. Ao tentar excluir um atributo que não existe ou adicionar qualquer valor a um atributo existente, a operação ocorre sem exibir qualquer mensagem de erro.

Para obter mais informações, consulte "Configurando o controle de modificação permissivo" no *Guia de Administração do NetIQ eDirectory 8.8 SP8*.

1.2.2 Suporte a horário genérico

A opção suporte a horário genérico permite exibir o tempo no formato `AAAAMMDDHHmmSS.0Z`.

Observe que `0Z` significa suporte a frações de segundos conforme suportado pelo Active Directory. Como o eDirectory não suporta a exibição de frações de segundos, esta opção exibe *0* para evitar romper a funcionalidade em um ambiente coexistente.

Para obter mais informações, consulte "Configurando o suporte a horário genérico" no *Guia de Administração do NetIQ eDirectory 8.8 SP8*.

1.2.3 Controle de exclusão de subárvore

Esta versão suporta o controle de exclusão de subárvore, permitindo apagar qualquer objeto de contêiner. Anteriormente, apenas objetos de folha podiam ser apagados. Contudo, o controle de exclusão de subárvore não suporta a exclusão de contêineres de partições.

1.3 Suporte ao IPv6

Esta versão suporta ambas as redes IPv4 e IPv6. Por padrão, a IPv6 é automaticamente habilitada ao instalar o eDirectory. Se você estiver atualizando a partir de uma versão anterior do eDirectory, deverá habilitar o suporte a IPv6 manualmente.

O eDirectory 8.8 SP8 suporta os seguintes modos de IPv6:

- Pilha dupla
- Túnel
- IPv6 puro

O eDirectory 8.8 SP8 não suporta os seguintes tipos de endereço IPv6:

- Endereços de link local
- Endereços IPv6 mapeados como IPv4
- Endereços IPv6 compatíveis com IPv4

O eDirectory 8.8 SP8 suporta os seguintes formatos de endereço:

- [::]
- [::1
- [2015::12]
- [2015::12]:524

1.4 Melhorias de auditoria

Esta versão melhora a auditoria de XDAS ao prover suporte a endereço IP de cliente em eventos.

2 Plataformas suportadas para instalação do eDirectory

O eDirectory 8.8 SP8 é uma versão compatível com várias plataformas e destinada a melhorar a estabilidade do eDirectory.

2.1 Plataformas obsoletas

O eDirectory 8.8 SP8 não suporta as seguintes plataformas:

- NetWare
- eDirectory de 32 bits e de 64 bits no Solaris
- eDirectory de 32 bits no AIX
- eDirectory de 32 bits no Linux
- eDirectory de 32 bits no Windows

2.2 Linux

Você deve instalar o eDirectory em uma das seguintes plataformas:

- SLES 11 SP1, SP2, e SP3 64 bits
- SLES 10 SP4 de 64 bits
- RHEL 5.7, 5.8 e 5.9
- RHEL 6.2, 6.3 e 6.4

Você pode executar estes sistemas operacionais em um modo virtual nos seguintes hipervisores:

- VMware ESXi
- Xen (no SLES 10, SLES 11 e seus Support Packs)

  Observação: O eDirectory 8.8 SP8 é suportado no serviço de virtualização do SLES 10 XEN que executa o OS SLES 10 de OS convidado. Estes guias estão disponíveis no site de atualização da NetIQ (https://update.novell.com).

  - SUSE-Linux-Enterprise-Server-X86_64-10-0-20061011-020434
  - SLES10-Updates

  Para registrar e atualizar o SUSE Linux Enterprise 10, consulte Registrando o SUSE Linux Enterprise pelo Atendimento ao cliente da NetIQ (http://www.suse.com/products/register.html). Para instalar a atualização mais recente, certifique-se de que o nível de patch mínimo instalado seja o 3.0.2_09763-0.8.

- Virtualização do Windows Server 2008 R2 Virtualization com Hyper-V

Para determinar a versão do SUSE Linux em execução, consulte o arquivo `/etc/SuSE-release`.

Verifique se os patches de glibc mais recentes são aplicados da Errata do Red Hat (http://rhn.redhat.com/errata) nos sistemas Red Hat. A versão mínima obrigatória da biblioteca glibc é a versão 2.1.

2.3 Windows

Você deve instalar o eDirectory em uma das seguintes plataformas:

- Windows Server 2008 (x64) (Standard/Enterprise/Data Center Edition) e seus service packs
- Windows Server 2008 R2 (Standard/Enterprise/Data Center Edition) e seus service packs
- Servidor Windows 2012

Importante

- Você deve usar uma conta que tenha direitos administrativos para instalar o eDirectory 8.8 SP8 no Windows Server 2008 R2.
- Versões da área de trabalho do Windows não são compatíveis.

3 Melhorias de instalação e upgrade

Este capítulo aborda os novos recursos e melhorias de instalação e upgrade do NetIQ eDirectory 8.8.

A tabela a seguir lista os novos recursos e especifica as plataformas nas quais eles são suportados.

Recurso	Linux	Windows
Múltiplos formatos de pacotes para instalação do eDirectory 8.8	✓	✗
Local de instalação personalizado para os arquivos do aplicativo	✓	✓
Local de instalação personalizado para os arquivos de dados	✓	✓
Local de instalação personalizado para os arquivos de configuração	✓	✗
Instalação nonroot	✓	✗
Suporte aprimorado para instalações em clusters de alta disponibilidade	✓	✓
Conformidade com FHS	✓	✗
Conformidade com LSB	✓	✗
Verificações de funcionamento do servidor	✓	✓
Integração do SecretStore	✓	✓
Instalação do eDirectory Instrumentation	✓	✓

Este capítulo inclui as seguintes informações:

3.1 Múltiplos formatos de pacotes para instalação do eDirectory 8.8

No Linux, você terá a opção de escolher dentre diversos formatos de arquivos ao instalar o eDirectory 8.8 no host. Os formatos de arquivos estão relacionados na tabela a seguir.

Tipo de usuário e local de instalação	Linux
Usuário root	
Local padrão	RPM
Local personalizado	Tarball
Usuário nonroot	
Local personalizado	Tarball

Para obter mais informações sobre como instalar e usar tarballs, consulte o *Guia de Instalação do NetIQ eDirectory 8.8 SP8*.

3.2 Instalando o eDirectory 8.8 em um local personalizado

O eDirectory 8.8 lhe concede a flexibilidade de instalar os arquivos do aplicativo, dos dados e de configuração em um local de sua escolha.

Um dos cenários para instalação do eDirectory 8.8 em um local personalizado é quando você já possui uma versão anterior do eDirectory instalada no host e deseja testar o eDirectory 8.8 antes de fazer upgrade. Desta maneira, sua configuração do eDirectory existente permanecerá inalterada e ainda poderá testar esta nova versão. Depois, você poderá decidir se deseja manter sua versão existente ou fazer upgrade para o eDirectory 8.8.

Observação: Os subagentes SLP e SNMP são instalados nos locais padrão.

Esta seção explica como instalar os diversos arquivos em um local personalizado:

- Seção 3.2.1, “Especificando um local personalizado para instalação dos arquivos do aplicativo” na página 18
- Seção 3.2.2, “Especificando um local personalizado para instalação dos arquivos de dados” na página 19
- Seção 3.2.3, “Especificando um local personalizado para instalação dos arquivos de configuração” na página 19

3.2.1 Especificando um local personalizado para instalação dos arquivos do aplicativo

Durante a instalação do eDirectory, é possível instalar os arquivos do aplicativo em um local diferente de sua escolha.

Linux

Para instalar o eDirectory 8.8 em um local personalizado, você pode usar o arquivo de instalação tarball e descompactar o eDirectory 8.8 em um local de sua escolha.

Windows

Já era possível especificar um local personalizado para os arquivos do aplicativo com o Assistente de instalação antes do eDirectory 8.8.

3.2.2 Especificando um local personalizado para instalação dos arquivos de dados

Ao configurar o eDirectory, você pode salvar arquivos de dados em um local de sua escolha. Os arquivos de dados incluem os diretórios `data`, `dib` e `log`.

Linux

Para configurar os arquivos de dados em um local personalizado, use a opção `-d` ou `-D` do utilitário ndsconfig.

Opção	Descrição
-d *local_personalizado*	Cria o diretório `DIB` (o banco de dados do eDirectory) no caminho mencionado. **Observação:** Esta opção já estava disponível antes do eDirectory 8.8.
-D *local_personalizado*	Cria os diretórios `data` (contendo dados como pids e IDs de soquete), `dib` e `log` no caminho mencionado.

Windows

No Windows, será solicitado digitar o caminho do DIB durante a instalação. Digite o caminho de sua escolha.

3.2.3 Especificando um local personalizado para instalação dos arquivos de configuração

Ao configurar o eDirectory, selecione o caminho onde deseja salvar os arquivos de configuração.

Linux

Para configurar o arquivo de configuração `nds.conf` em um local diferente, use a opção `--config-file` do utilitário ndsconfig.

Para instalar os outros arquivos de configuração (como `modules.conf`, `ndsimon.conf` e `ice.conf`) em um local diferente, faça o seguinte:

1. Copie todos os arquivos de configuração para um novo local.
2. Defina o novo local digitando o seguinte:

   ```
   ndsconfig set n4u.nds.configdir local_personalizado
   ```

Windows

Não é possível especificar um local personalizado para os arquivos de configuração no Windows.

3.3 Instalação nonroot

O eDirectory 8.8 e superior suportam instalação e configuração dos servidores do eDirectory por um usuário nonroot. Versões anteriores do eDirectory podiam ser instaladas e configuradas apenas por um usuário root com uma única instância do eDirectory sendo executada em um host.

No eDirectory 8.8 ou superior, qualquer usuário nonroot pode usar um build de tarball para instalar o eDirectory. Podem existir diversas instâncias de instalações binárias do eDirectory realizadas pelo mesmo usuário ou usuários diferentes. Contudo, mesmo para instalações de usuários nonroot, serviços no nível do sistema como Novell International Cryptographic Infrastructure (NICI), SNMP e SLP poderão ser instalados apenas com privilégios root. O NICI é um componente obrigatório, enquanto SNMP e SLP são componentes opcionais para a funcionalidade do eDirectory. Além disso, com instalação em pacote, apenas uma instância poderá ser instalada pelo usuário root.

Após a instalação, o usuário nonroot pode configurar instâncias do servidor do eDirectory usando sua instalação de tarball individual ou usando uma instalação binária. Isto significa que poderão existir múltiplas instâncias de servidores do eDirectory executadas em um mesmo host, pois qualquer usuário, root ou nonroot, pode configurar diferentes instâncias do servidor do eDirectory em um único host usando uma instalação de pacote ou de tarball. Para obter mais detalhes sobre o recurso de Múltiplas instâncias, consulte "Múltiplas instâncias" e "Upgrade de múltiplas instâncias" no *Guia de Instalação do NetIQ eDirectory 8.8 SP8*.

A instalação e configuração nonroot aplicam-se somente às plataformas Linux. Para obter mais informações sobre instalação e configuração nonroot, consulte "Instalação de usuário nonroot do eDirectory 8.8" no *Guia de Instalação do NetIQ eDirectory 8.8 SP8*.

3.4 Suporte aprimorado para instalações em clusters de alta disponibilidade

O eDirectory 8.8 SP8 simplifica sua instalação e gerenciamento em clusters do Linux e do Windows, melhorando o suporte a cluster e habilitando uma alta disponibilidade. O eDirectory também fornece alta disponibilidade através da sincronização de réplica, que pode ser combinada com clusters para obter um nível superior de disponibilidade.

Para obter mais informações sobre como instalar o eDirectory em clusters, consulte o *Guia de Instalação do NetIQ eDirectory 8.8 SP8*.

3.5 Compatibilidade com padrões

O eDirectory 8.8 está em conformidade com os seguintes padrões:

3.5.1 Conformidade com FHS

Para evitar conflitos de arquivos com outros arquivos do aplicativo deste produto, o eDirectory 8.8 segue o Filesystem Hierarchy Standard (FHS). Esse recurso está disponível apenas no Linux.

O eDirectory seguirá esta estrutura de diretório apenas se instalado em seu local padrão. Se você tiver escolhido um local personalizado, a estrutura do diretório será *local_personalizado/caminho_padrão*.

Por exemplo, se escolher instalá-lo no diretório `eDir88`, a mesma estrutura de diretório seria seguida no diretório `eDir88`, de maneira que as páginas de manual seriam instaladas no diretório `/eDir88/opt/novell/man`.

A tabela a seguir lista a alteração na estrutura do diretório:

Tipos de arquivos armazenados no diretório	Nome e caminho do diretório
Binários executáveis e scripts shell estáticos	`/opt/novell/eDirectory/bin`
Binários executáveis para uso root	`/opt/novell/eDirectory/sbin`
Binários de biblioteca estática ou dinâmica	`/opt/novell/eDirectory/lib`
Arquivos de configuração	`/etc/opt/novell/eDirectory/conf`
Dados dinâmicos de leitura/gravação de tempo de execução como o DIB	`/var/opt/novell/eDirectory/data`
Arquivos de registro	`/var/opt/novell/eDirectory/log`
Páginas de manual do Linux	`/opt/novell/man`

Exportar variáveis ambientais

Com a implementação do FHS no eDirectory 8.8, é necessário atualizar as variáveis ambientais do caminho e exportá-las. Isto gera os seguintes problemas:

- Será necessário lembrar de todos os caminhos exportados, de maneira que sempre ao abrir um shell, será necessário exportar esses caminhos para começar a usar os utilitários.
- Se desejar usar mais de um conjunto binário, será necessário abrir mais de um shell ou desconfigurar e reconfigurar os caminhos para um conjunto binário diferente com frequência.

Para resolver o problema acima, use o script `/opt/novell/eDirectory/bin/ndspath` da seguinte maneira:

- Coloque o script ndspath como prefixo do utilitário e execute o utilitário desejado da seguinte maneira:

  ```
  custom_location/opt/novell/eDirectory/bin/ndspath utility_name_with_parameters
  ```

- Exporte os caminhos no shell atual da seguinte maneira:

```
. custom_location/opt/novell/eDirectory/bin/ndspath
```

- Após digitar o comando acima, execute os utilitários normalmente. Obtenha o script no seu perfil, bashrc ou scripts similares. Portanto, sempre que efetuar login ou abrir um novo shell, será possível usar os utilitários diretamente.

3.5.2 Conformidade com LSB

O eDirectory 8.8 está agora em conformidade com o Linux Standard Base (LSB). O LSB também recomenda conformidade com FHS. Todos os pacotes do eDirectory no Linux possuem o prefixo *novell*. Por exemplo, o `NDSserv` agora é `novell-NDSserv`.

3.6 Verificações de funcionamento do servidor

O eDirectory 8.8 introduz verificações de funcionamento do servidor para ajudar a determinar se o funcionamento do servidor está seguro antes de fazer o upgrade.

As verificações de funcionamento do servidor são executadas por padrão a cada upgrade e ocorrem antes do upgrade real do pacote. Contudo, também é possível executar a ferramenta de diagnóstico ndscheck para realizar verificações de funcionamento.

3.6.1 Necessidade de verificações de funcionamento

Nas versões anteriores do eDirectory, o upgrade não verificava o funcionamento do servidor antes de prosseguir. Se o funcionamento estivesse instável, a operação de upgrade falharia e o eDirectory ficaria em um estado inconsistente. Em alguns casos, não seria possível nem mesmo voltar para as configurações anteriores ao upgrade.

Esta nova ferramenta de verificação de funcionamento resolve este problema, garantindo que o servidor esteja pronto para fazer o upgrade.

3.6.2 O que torna um servidor saudável?

O utilitário de verificação de funcionamento do servidor realiza certas verificações de funcionamento para garantir que a árvore esteja funcionando adequadamente. A árvore é declarada saudável quando todas as verificações de funcionamento são concluídas com êxito.

3.6.3 Realizando verificações de funcionamento

Você pode realizar verificações de funcionamento do servidor de duas maneiras:

- “Com o upgrade” na página 23
- “Como utilitário independente” na página 23

Observação: É necessário possuir privilégios administrativos para executar o utilitário de verificação de funcionamento. O mínimo privilégio que pode ser definido para executar o utilitário é Público. Contudo, com o privilégio Público, alguns dos objetos de Protocolo Central do Netware (NCP) e informações de partição não estão disponíveis.

Com o upgrade

As verificações de funcionamento são executadas por padrão a cada upgrade do eDirectory.

Linux

A cada upgrade, as verificações de funcionamento são executadas por padrão antes da operação de upgrade real ser iniciada.

Para ignorar as verificações de funcionamento, é possível usar a opção -j no utilitário nds-install.

Windows

As verificações de funcionamento do servidor ocorrem como parte do assistente de instalação. É possível habilitar ou desabilitar as verificações de funcionamento quando solicitado.

Como utilitário independente

É possível executar verificações de funcionamento do servidor como utilitário independente sempre que desejar. A tabela a seguir explica os utilitários de verificação de funcionamento.

Tabela 3-1 *Utilitários de verificação de funcionamento*

Plataforma	Nome do utilitário
Linux	ndscheck Sintaxe: `ndscheck -h hostname:port -a admin_FDN -F logfile_path --config-file configuration_file_name_and_path` **Observação:** Você pode especificar `-h` ou `--config-file`, mas não ambas as opções.
Windows	ndscheck

3.6.4 Tipos de verificações de funcionamento

Ao fazer upgrade ou executar o utilitário ndscheck, os seguintes tipos de verificações de funcionamento são realizados:

- Funcionamento básico do servidor
- Partições e funcionamento de réplica

Ao executar o utilitário ndscheck, os resultados das verificações de funcionamento são exibidos na tela e registrados no `ndscheck.log`. Para obter mais informações sobre arquivos de registro, consulte Seção 3.6.6, “Arquivos de Registro” na página 25.

Se as verificações forem realizadas como parte de um upgrade, depois de sua realização, dependendo da criticidade do erro, você será solicitado a prosseguir com o processo de upgrade ou o processo será abortado. Os detalhes dos erros são descritos em Seção 3.6.5, “Categorização de saúde” na página 24.

Funcionamento básico do servidor

Este é o primeiro estágio de verificação de funcionamento. O utilitário de verificação de funcionamento verifica o seguinte:

1. O serviço do eDirectory está ativado. O DIB está aberto e é capaz de ler algumas informações básicas da árvore como o nome da árvore.
2. O servidor está escutando os respectivos números de porta.

   Para LDAP, ele obtém TCP e os números de porta SSL e verifica se o servidor está escutando estas portas.

   Igualmente, para HTTP, ele obtém TCP e números de porta segura de HTTP e verifica se o servidor está escutando estas portas.

Partições e funcionamento de réplica

Após verificar o funcionamento básico do servidor, a próxima etapa é verificar as partições e o funcionamento de réplica da seguinte maneira:

1. Verificar o funcionamento das réplicas das partições mantidas localmente.
2. Ler o anel de réplicas de cada uma das partições mantidas pelo servidor e verificar se todos os servidores no anel de réplica estão ativos e se todas as réplicas estão no estado LIGADO.
3. Verificar a sincronização de horário de todos os servidores no anel de réplicas. Isto mostra a diferença de tempo entre os servidores.

3.6.5 Categorização de saúde

Com base nos erros encontrados ao verificar o funcionamento de um servidor, poderão existir três categorias de funcionamento. O status das verificações de funcionamento é registrado em um arquivo de registro. Para obter mais informações, consulte o Seção 3.6.6, “Arquivos de Registro” na página 25.

As três categorias de funcionamento são Normal, Aviso e Crítico.

Normal

O funcionamento do servidor é normal quando todas as verificações de funcionamento são concluídas com êxito.

O processo de upgrade prossegue sem interrupção.

Aviso

O funcionamento do servidor está na categoria de aviso quando erros menores são encontrados durante a verificação de funcionamento.

Se a verificação de funcionamento for executada como parte do upgrade, você será solicitado a abortar ou continuar.

Avisos normalmente ocorrem nos seguintes cenários:

1. O servidor não está escutando as portas LDAP e HTTP, normais, seguras ou ambas.

2. Não é possível fazer contato com servidores não mestre no anel de réplicas.
3. Servidores no anel de réplicas não estão em sincronia.

Crítico

O funcionamento do servidor está crítico quando erros críticos são encontrados ao verificar o funcionamento.

Se a verificação de saúde for executada como parte de um upgrade, a operação de upgrade será abortada.

O estado crítico ocorre normalmente nos seguintes casos:

1. Não é possível ler ou abrir o DIB. O DIB pode estar bloqueado ou corrompido.
2. Não é possível contatar qualquer servidor no anel de réplicas.
3. As partições mantidas localmente estão ocupadas.
4. A réplica não está no estado LIGADO.

3.6.6 Arquivos de Registro

Cada operação de verificação de funcionamento do servidor, seja com upgrade ou pelo utilitário independente, mantém o status do funcionamento em um arquivo de registro.

O conteúdo do arquivo de registro é similar às mensagens exibidas na tela quando as verificações ocorrem.

O arquivo de registro da verificação de funcionamento contém o seguinte:

- Status das verificações de funcionamento (normal, aviso ou crítico).
- URLs para o site de suporte da NetIQ.

A tabela a seguir fornece os locais do arquivo de registro nas diversas plataformas:

Tabela 3-2 *Locais do arquivo de registro de verificação de funcionamento*

Plataforma	Nome do arquivo de registro	Localização do Arquivo de Registro
Linux	`ndscheck.log`	Depende do local especificado com o utilitário `ndscheck -F`. Se você não usou a opção `-F`, o local do arquivo `ndscheck.log` será determinado pelas outras opções usadas na linha de comando do ndscheck como mostrado a seguir: 1. Se você usou a opção `-h`, o arquivo `ndscheck.log` é salvo no diretório pessoal do usuário. 2. Se você usou a opção `--config-file`, o arquivo `ndscheck.log` é salvo no diretório de registros da instância do servidor. Também é possível selecionar uma instância em uma lista de múltiplas instâncias.

Plataforma	Nome do arquivo de registro	Localização do Arquivo de Registro
Windows	`ndscheck.log`	*`install_directory`*

3.7 Integração do SecretStore com o eDirectory

O eDirectory 8.8 lhe concede a opção de configurar o Novell SecretStore 3.4 durante a configuração do eDirectory. Antes do eDirectory 8.8, era necessário instalar o SecretStore manualmente.

O SecretStore é uma solução de gerenciamento de senha simples e segura. Ele permite usar uma autenticação única no eDirectory para acessar a maioria dos aplicativos de mainframe do Linux, Windows e da Web.

Após autenticar-se no eDirectory, os aplicativos habilitados para SecretStore armazenam e recuperam as credenciais de login adequadas. Ao usar o SecretStore, você elimina a necessidade de lembrar ou sincronizar todas as diversas senhas necessárias para acessar aplicativos, sites e mainframes protegidos por senha.

Para configurar o SecretStore 3.4 juntamente com o eDirectory, faça o seguinte:

- **Linux:**

  Use o parâmetro `ndsconfig add -m ss`. Nele, `ss` indica SecretStore e é um parâmetro opcional. Se você não mencionar o nome do módulo, todos os módulos serão instalados. Se não desejar configurar o SecretStore, passe o valor `no_ss` para esta opção ao especificar `-m no_ss`.

- **Windows:**

  Ao instalar o eDirectory, há uma opção de especificar se deseja configurar o módulo do SecretStore. Por default, essa opção está assinalada.

Para obter mais informações sobre o uso do SecretStore, consulte o *Guia de Administração do Novell eDirectory 3.4* (https://www.netiq.com/documentation/secretstore34/).

3.8 Instalação do eDirectory Instrumentation

O eDirectory Instrumentation anteriormente fazia parte do Novell Audit. A partir da versão do eDirectory 8.8 SP3, o eDirectory Instrumentation deve ser instalado separadamente.

Para obter informações detalhadas sobre como instalar, configurar e desinstalar o eDirectory Instrumentation, consulte o *Guia de Instalação do NetIQ eDirectory 8.8 SP8*.

3.9 Para obter mais informações

Consulte os itens a seguir para obter mais informações sobre qualquer um dos recursos abordados neste capítulo:

- *Guia de Instalação do NetIQ eDirectory 8.8 SP8*
- *Guia de Administração do NetIQ eDirectory 8.8 SP8*
- No Linux: as páginas de manual `nds-install`, `ndsconfig` e `ndscheck`

4 Backup e restauração do NICI

O Novell International Cryptography Infrastructure (NICI) armazena chaves e dados do usuário em um sistema de arquivos e nos diretórios e arquivos específicos do sistema e do usuário. Esses diretórios e arquivos são protegidos ao definir as permissões adequadas usando o mecanismo fornecido pelo sistema operacional. Isto é realizado com o programa de instalação NICI.

Desinstalar o NICI do sistema não remove os diretórios e arquivos do sistema ou do usuário. Portanto, a única razão para restaurar esses arquivos para um estado anterior seria recuperá-los de uma falha catastrófica do sistema ou em caso de erro humano. É importante compreender que sobrescrever um conjunto de diretórios e arquivos do usuário do NICI existente pode inutilizar um aplicativo existente.

A chave do banco de dados é necessária para abrir o DIB protegido por chaves NICI. Por isso, se um backup do eDirectory for realizado independentemente de um backup do NICI, ele será inútil.

Alterações dos mecanismos de backup e restauração NICI anteriores

Anteriormente, o backup e restauração NICI deveriam ser realizados manualmente. Nesta versão, uma nova solução de backup e restauração NICI foi adicionada. Um switch (`-e`) foi adicionado à solução de backup do eDirectory (backup eMBox e DSBK), que habilita:

1. Fazer backup com as chaves NICI quando um backup do eDirectory é executado
2. Restaurar as chaves NICI quando uma restauração do eDirectory é executada

Consulte "Fazendo backup e restauração de NICI" no *Guia de Administração do NetIQ eDirectory 8.8 SP8*.

5 O utilitário ndspassstore

O ndspassstore é um novo utilitário usado para armazenar senhas criptografadas para o usuário sadmin ou o usuário do eDirectory. Este utilitário está disponível nas plataformas Linux e Windows. Este utilitário coleta o nome do usuário e a senha como entradas e armazena-os como pares de valor de chave criptografados.

Nesta versão, este utilitário é usado para definir a senha sadmin.

Este utilitário está disponível por padrão em `C:\Novell\NDS` no Windows e em `/opt/novell/eDirectory/bin` no Linux.

Sinopse de comando

É possível usar o utilitário ndspassstore ao digitar o comando a seguir no console do servidor:

```
ndspassstore -a <adminContext> -w <password>
```

Opção	Uso
-a adminContext	Esta opção é usada para aceitar o adminContext que é um nome totalmente exclusivo de um usuário que possui direitos administrativos.
-w senha	Esta opção é usada para aceitar a senha (senha do usuário) para autenticação.

6 Múltiplas instâncias

Tradicionalmente, apenas uma instância do NetIQ eDirectory seria configurada em um único host. Com o suporte ao recurso de múltiplas instâncias no eDirectory 8.8, é possível configurar o seguinte:

- Múltiplas instâncias do eDirectory em um único host.
- Múltiplas árvores em um único host.
- Múltiplas réplicas na mesma árvore ou partição em um único host.

O eDirectory 8.8 também fornece um utilitário (ndsmanage) para monitorar as instâncias com facilidade.

A tabela a seguir lista as plataformas que suportam múltiplas instâncias:

Recurso	Linux	Windows
Suporte a múltiplas instâncias	✓	✗

Este capítulo inclui as seguintes informações:

6.1 Necessidade de múltiplas instâncias

As múltiplas instâncias surgem da necessidade de:

- Potencializar hardware de alto nível ao configurar mais de uma instância do eDirectory.
- Testar sua configuração com um host único antes de investir no hardware necessário.

6.2 Cenários de exemplo para implementação de múltiplas instâncias

Múltiplas instâncias que pertencem à mesma árvore ou a diversas árvores podem ser usadas efetivamente nos cenários a seguir.

eDirectory em uma grande empresa

- Em grandes empresas, é possível fornecer serviços do eDirectory de equilíbrio de carga e de alta disponibilidade.

  Por exemplo, se você possui três servidores de réplica executando serviços LDAP nas portas 1524, 2524 e 3524, respectivamente, poderá configurar uma nova instância do eDirectory e fornecer uma alta disponibilidade de serviço LDAP em uma nova porta 636.
- Você pode otimizar hardware de alto nível em vários departamentos de uma configuração ao configurar múltiplas instâncias em um único host.

eDirectory em uma configuração de avaliação

- **Universidades:** Muitos entusiastas (alunos) podem avaliar o eDirectory no mesmo host usando múltiplas instâncias.
- **Treinamento para administração do eDirectory:**
  - Os participantes podem experimentar a administração usando múltiplas instâncias.
  - Os instrutores podem usar um único host para ensinar uma classe de alunos. Cada aluno pode ter sua própria árvore.

6.3 Usando múltiplas instâncias

O eDirectory 8.8 torna muito fácil a tarefa de configurar múltiplas instâncias. Para usar múltiplas instâncias com eficiência, é necessário planejar a configuração para então configurar as múltiplas instâncias.

- Seção 6.3.1, “Planejamento da configuração” na página 32
- Seção 6.3.2, “Configurando múltiplas instâncias” na página 32

6.3.1 Planejamento da configuração

Para usar este recurso com eficiência, recomendamos planejar as instâncias do eDirectory e garantir que cada instância possua identificadores de instância fixos como nome do host, número da porta, nome do servidor ou arquivo de configuração.

Ao configurar múltiplas instâncias, você deverá planejar o seguinte:

- Localização do arquivo de configuração
- Localização dos dados variáveis (como arquivos de registro)
- Localização do DIB
- A interface NCP™, porta com identificação exclusiva para cada instância e portas para outros serviços (como LDAP, LDAPS, HTTP e porta segura HTTP)
- Nome do servidor exclusivo para cada instância

6.3.2 Configurando múltiplas instâncias

Você pode configurar múltiplas instâncias do eDirectory usando o utilitário ndsconfig. A tabela a seguir lista as opções do ndsconfig que você precisa incluir ao configurar múltiplas instâncias.

Observação: Todas as instâncias compartilham a mesma chave de servidor (NICI).

Opção	Descrição
--config-file	Especifica o caminho e nome de arquivo absolutos para armazenamento do arquivo de configuração `nds.conf`. Por exemplo, para armazenar o arquivo de configuração no diretório `/etc/opt/novell/eDirectory/`, use `--config-file /etc/opt/novell/eDirectory/nds.conf`.
-b	Especifica os números de porta que a nova instância deverá escutar. **Observação:** `-b` e `-B` são usados com exclusividade.

-B	Especifica o número da porta com o endereço IP ou a interface. Por exemplo:
	
	`-B eth0@524`
	
	ou
	
	`-B 100.1.1.2@524`
	
	Observação: `-b` e `-B` são usados com exclusividade.

-D	Cria os diretórios `data`, `dib` e `log` no caminho especificado para a nova instância.
S	Especifica o nome do servidor.

Usando as opções mencionadas acima, você poderá configurar uma nova instância do eDirectory.

Você também poderá configurar uma nova instância usando o utilitário ndsmanage. Para obter mais informações, consulte o "Criando uma instância pelo ndsmanage" na página 34.

6.4 Gerenciando múltiplas instâncias

Esta seção inclui as seguintes informações:

6.4.1 O utilitário ndsmanage

O utilitário ndsmanage permite realizar o seguinte:

- Listar as instâncias configuradas
- Criar uma nova instância
- Realizar o seguinte na instância selecionada:
  - Listar as réplicas do servidor
  - Iniciar a instância
  - Parar a instância

- Executar o DSTrace (ndstrace) para a instância
- Desconfigurar a instância

- Iniciar e parar todas as instâncias

Listando as instâncias

A tabela a seguir descreve como listar as instâncias do eDirectory.

Tabela 6-1 *Uso do ndsmanage para listar as instâncias*

Sintaxe	Descrição
ndsmanage	Lista todas as instâncias configuradas por você.
ndsmanage -a|--all	Lista as instâncias de todos os usuários que usam uma instalação específica do eDirectory.
ndsmanage *nome de usuário*	Lista as instâncias configuradas por um usuário específico

Os campos a seguir são exibidos para cada instância:

- Caminho do arquivo de configuração
- Servidor FND e porta
- Status (mostra se a instância está ativa ou inativa)

Observação: Este utilitário lista todas as instâncias configuradas em um único binário.

Consulte Figura 6-1 na página 34 para obter mais informações.

Criando uma instância pelo ndsmanage

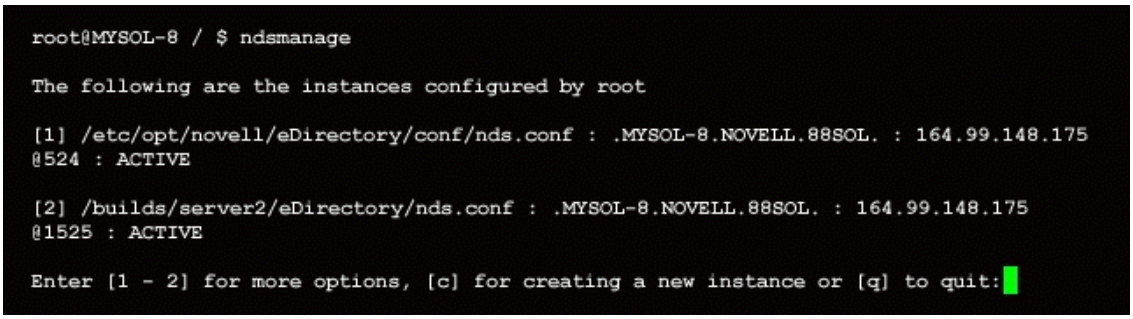
Para criar uma nova instância pelo ndsmanage:

1. Digite o seguinte comando:

   ```
   ndsmanage
   ```

   Se você possui duas instâncias configuradas, a tela a seguir é exibida:

Figura 6-1 *Tela de saída do utilitário ndsmanage*



2 Digite c para criar uma nova instância.

É possível criar uma nova árvore ou adicionar um servidor a uma árvore existente. Siga as instruções na tela para criar uma nova instância.

Realizando operações para uma instância específica.

É possível realizar as seguintes operações para cada instância:

- "Iniciando uma instância específica" na página 35
- "Parando uma instância específica" na página 35
- "Desconfigurando uma instância" na página 36

Para outras não listadas acima, também é possível executar o DSTrace para a instância selecionada.

Iniciando uma instância específica

Para iniciar uma instância configurada por você, faça o seguinte:

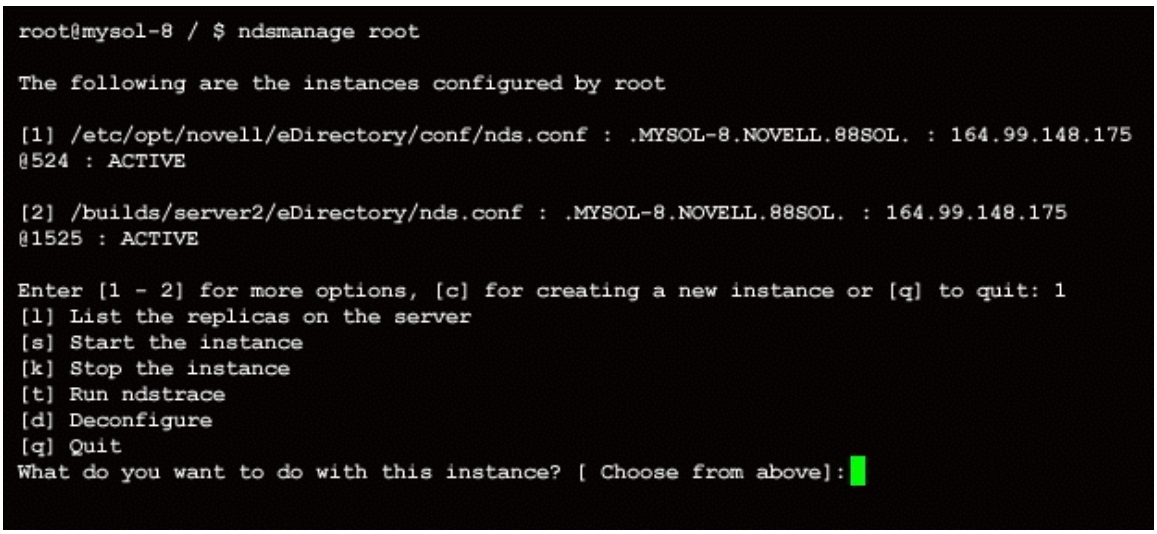
1 Digite o seguinte:

```
ndsmanage
```

2 Selecione a instância que deseja iniciar.

O menu expande-se para incluir as opções que podem ser realizadas na instância específica.

Figura 6-2 *Tela de saída do utilitário ndsmanage com opções de instância*



3 Digite s para iniciar a instância.

Como alternativa, você também pode digitar o seguinte no prompt de comando:

```
ndsmanage start --config-file
arquivo_de_configuração_da_instância_configurada_por_você
```

Parando uma instância específica

Para parar uma instância configurada por você, faça o seguinte:

1 Digite o seguinte:

```
ndsmanage
```

2 Selecione a instância que deseja parar.

O menu expande-se para incluir as opções que podem ser realizadas na instância específica. Para obter mais informações, consulte o Tela de saída do utilitário ndsmanage com opções de instância (página 35).

3 Digite `k` para parar a instância.

Como alternativa, você também pode digitar o seguinte no prompt de comando:

```
ndsmanage stop --config-file
arquivo_de_configuração_da_instância_configurada_por_você
```

Desconfigurando uma instância

Para desconfigurar uma instância, faça o seguinte:

1 Digite o seguinte:

```
ndsmanage
```

2 Selecione a instância que deseja desconfigurar.

O menu expande-se para incluir as opções que podem ser realizadas na instância específica. Para obter mais informações, consulte o Tela de saída do utilitário ndsmanage com opções de instância (página 35).

3 Digite `d` para desconfigurar a instância.

Iniciando e parando todas as instâncias

Você pode iniciar e parar todas as instâncias configuradas por você.

Iniciando todas as instâncias

Para iniciar todas as instâncias configuradas por você, digite o seguinte no prompt de comando:

```
ndsmanage startall
```

Para iniciar uma instância específica, consulte "Iniciando uma instância específica" na página 35.

Parando todas as instâncias

Para parar todas as instâncias configuradas por você, digite o seguinte no prompt de comando:

```
ndsmanage stopall
```

Para parar uma instância específica, consulte "Parando uma instância específica" na página 35.

6.4.2 Identificando uma instância específica

Ao configurar múltiplas instâncias, você deverá atribuir um nome de host, número de porta e caminho do arquivo de configuração exclusivo para cada instância. Este nome de host e número da porta serão os identificadores da instância.

A maioria dos utilitários possui a opção `-h` *`hostname:port`* ou `--config-file` *`local_do_arquivo_de_configuração`* que permite especificar uma instância específica. Consulte as páginas de manual dos utilitários para ver mais informações.

6.4.3 Invocando um utilitário para uma instância específica

Se desejar executar um utilitário para uma instância específica, será necessário incluir o identificador da instância no comando do utilitário. Os identificadores de instância são o caminho do arquivo de configuração, o nome do host e o número da porta. É possível usar o `--config-file` *`local_do_arquivo_de_configuração`* ou `-h` *`hostname`*`:`*`port`* para fazer isto.

Se você não incluir os identificadores de instância no comando, o utilitário exibirá as diversas instâncias de sua propriedade e solicitará selecionar a instância para a qual você deseja executar o utilitário.

Por exemplo, para executar o DSTrace para um utilitário específico usando a opção `--config-file`, digite o seguinte:

`ndstrace --config-file` *`configuration_filename_with_location`*

6.5 Cenários de exemplo para múltiplas instâncias

Mary é um usuário nonroot que deseja configurar duas árvores em uma única máquina host para um único binário.

6.5.1 Planejamento da configuração

Mary especifica os identificadores de instâncias a seguir.

- **Instância 1:**

Número da porta que a instância deverá escutar	1524
Caminho do arquivo de configuração	`/home/maryinst1/nds.conf`
Diretório DIB	`/home/mary/inst1/var`

- **Instância 2:**

Número da porta que a instância deverá escutar	2524
Caminho do arquivo de configuração	`/home/mary/inst2/nds.conf`
Diretório DIB	`/home/mary/inst2/var`

6.5.2 Configurando as instâncias

Para configurar as instâncias com base nos identificadores de instância mencionados acima, Mary deverá digitar os seguintes comandos.

- **Instância 1:**

```
ndsconfig new -t mytree -n o=novell -a cn=admin.o=company -b 1524 -D
/home/mary/inst1/var --config-file /home/mary/inst1/nds.conf
```

- **Instância 2:**

```
ndsconfig new -t corptree -n o=novell -a cn=admin.o=company -b 2524 -D
/home/mary/inst2/var --config-file /home/mary/inst2/nds.conf
```

6.5.3 Invocando o utilitário para uma instância

Se Mary desejar executar o utilitário DSTrace para a instância 1 que está escutando a porta 1524, com o arquivo de configuração no local `/home/mary/inst1/nds.conf` e seu arquivo DIB localizado em `/home/mary/inst1/var`, ela poderá executar o utilitário da seguinte maneira:

```
ndstrace --config-file /home/mary/inst1/nds.conf
```

ou

```
ndstrace -h 164.99.146.109:1524
```

Se Mary não especificar os identificadores de instância, o utilitário exibirá todas as instâncias possuídas por Mary e solicitará que ela selecione uma instância.

6.5.4 Listando as instâncias

Se Mary desejar saber detalhes das instâncias no host, ela poderá executar o utilitário ndsmanage.

- Para exibir todas as instâncias possuídas por Mary:

  ```
  ndsmanage
  ```

- Para exibir todas as instâncias possuídas por John (cujo nome de usuário é john):

  ```
  ndsmanage john
  ```

- Para exibir todas as instâncias de todos os usuários que usam uma instalação específica do eDirectory:

  ```
  ndsmanage -a
  ```

6.6 Para obter mais informações

Consulte os documentos a seguir para obter mais informações sobre suporte a múltiplas instâncias:

- *Guia de Instalação do NetIQ eDirectory 8.8 SP8*
- Para Linux: páginas de manual ndsconfig e ndsmanage

7 Autenticação no eDirectory através do SASL-GSSAPI

O mecanismo SASL-GSSAPI do NetIQ eDirectory 8.8 permite autenticar o eDirectory através de LDAP usando um bilhete Kerberos e sem precisar digitar a senha de usuário do eDirectory. O bilhete Kerberos deverá ser obtido autenticando um servidor Kerberos.

Este recurso é útil principalmente para usuários do aplicativo LDAP em ambientes que já possuem infraestrutura Kerberos implementada. Portanto, tais usuários deverão ser capazes de autenticar o servidor LDAP sem fornecer uma senha de usuário LDAP separada.

Para facilitar isto, o eDirectory introduz o mecanismo SASL-GSSAPI.

A implementação atual do SASL-GSSAPI está em conformidade com o RFC 2222 (http://www.ietf.org/rfc/rfc2222.txt?number=2222) e suporta apenas o Kerberos v5 como mecanismo de autenticação.

Este capítulo inclui as seguintes informações:

7.1 Conceitos

7.1.1 O que é o Kerberos?

O Kerberos é um protocolo padrão que fornece uma maneira de autenticar entidades em uma rede. Ele é baseado em um modelo confiável de outra empresa. Ele envolve segredos compartilhados e utiliza criptografia de chave simétrica.

Para obter mais informações, consulte RFC 1510 (http://www.ietf.org/rfc/rfc1510.txt?number=1510).

7.1.2 O que é SASL?

A Simple Authentication and Security Layer (SASL, Camada Simples de Autenticação e Segurança) fornece uma camada de abstração de autenticação para aplicativos. Ela é uma metodologia à qual os métodos de autenticação podem ser conectados.

Para obter mais informações, consulte RFC 2222 (http://www.ietf.org/rfc/rfc2222.txt?number=2222).

7.1.3 O que é GSSAPI?

O Generic Security Services Application Program Interface (GSSAPI, Interface de Programa de Aplicativo de Serviços e Segurança) fornece autenticação e outros serviços de segurança através de um conjunto padrão de APIs. Ele suporta diferentes mecanismos de autenticação. O Kerberos v5 é o mais comum.

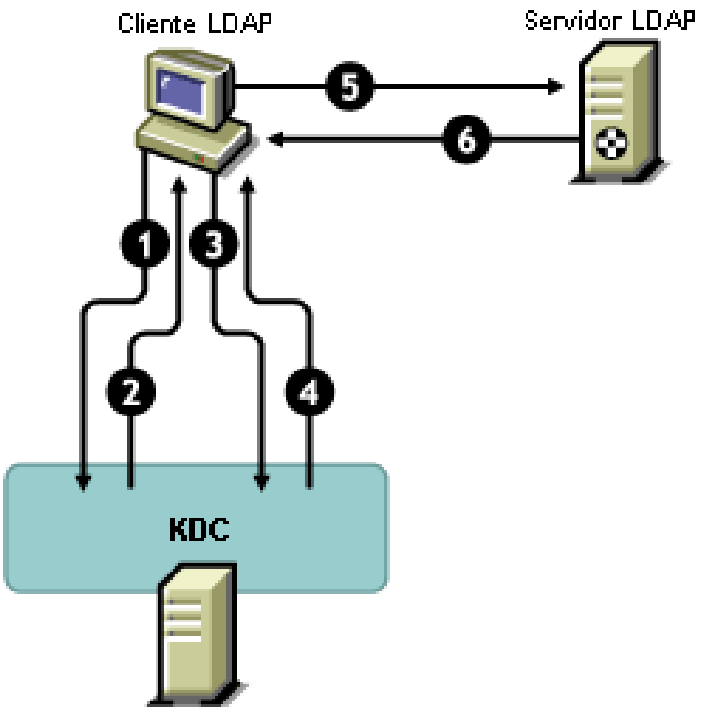
Para obter mais informações sobre APIs GSS, consulte RFC 1964 (http://www.ietf.org/rfc/rfc1964.txt?number=1964).

Esta implementação SASL-GSSAPI está na seção 7.2 do RFC 2222 (http://www.ietf.org/rfc/rfc2222.txt?number=2222).

7.2 Como o GSSAPI funciona com o eDirectory?

O diagrama a seguir ilustra como o GSSAPI funciona com um servidor LDAP.

Figura 7-1 *Como o GSSAPI funciona?*



Na figura acima, os números indicam o seguinte:

1. Um usuário do eDirectory envia uma solicitação pelo cliente do LDAP para o servidor do Kerberos KDC (Centro de Distribuição de Chave) para um bilhete inicial conhecido como bilhete fornecedor de bilhetes (TGT).

   Um Kerberos KDC pode ser a partir do MIT ou Microsoft*.
2. O KDC responde ao cliente LDAP com um TGT.
3. O cliente LDAP envia o TGT de volta ao KDC e solicita um bilhete de serviço LDAP.
4. O KDC responde ao cliente LDAP com o bilhete de serviço LDAP.
5. O cliente LDAP realiza um ldap_sasl_bind no servidor LDAP e envia o bilhete de serviço LDAP.
6. O servidor LDAP valida o bilhete de serviço LDAP com a ajuda do mecanismo GSSAPI e, com base no resultado, retorna um ldap_sasl_bind de êxito ou falha ao cliente do LDAP.

7.3 Configurando o GSSAPI

1. O plug-in do iManager para o SASL-GSSAPI não funcionará se o iManager não for configurado para usar conexão SSL/TLS com o eDirectory. Uma conexão segura é obrigatória para proteger a chave master e principais chaves do domínio.

   Por padrão, o iManager geralmente é configurado para conexão SSL/TLS com o eDirectory. Se desejar configurar o Método de Login do Kerberos para GSSAPI em uma árvore que não aquela que abriga a configuração do iManager, será necessário configurar o iManager para conexão SSL/TLS com o eDirectory.

   Para obter informações sobre como configurar o iManager com conexão SSL/TLS com o eDirectory, consulte o *Guia de Administração do NetIQ iManager 2.7* (https://www.netiq.com/documentation/imanager/imanager_admin/data/hk42s9ot.html).

   O plug-in do iManager para SASL-GSSAPI (`kerberosPlugin.npm`) está disponível como parte dos arquivos `eDir_88_iMan26_Plugins.npm` e `eDir_88_iMan27_Plugins.npm`. Faça download do NPMs no site de download da Novell (http://download.novell.com).
2. Para usar um bilhete do Kerberos para autenticar um servidor do eDirectory:
   - **2a** Estender o esquema do Kerberos.
   - **2b** Criar um contêiner de domínio.
   - **2c** Extrair uma Chave Principal de Serviço ou Chave Compartilhada do KDC.
   - **2d** Criar o objeto principal de serviço do LDAP.
   - **2e** Associar um nome principal do Kerberos a um Objeto de Usuário.

Para obter mais informações sobre as etapas acima, consulte "Configurando o GSSAPI com o eDirectory" no *Guia de Administração do NetIQ eDirectory 8.8 SP8*.

7.4 Como o LDAP usa o GSSAPI?

Após configurar o GSSAPI, ele é adicionado juntamente com outros métodos SASL ao atributo `supportedSASLMechanisms` no `rootDSE`. `rootDSE (entrada específica de DSA [Agente do Sistema do Diretório])` é uma entrada localizada na raiz da Árvore de Informações de Diretório (DIT). Para obter mais informações, consulte "Compreendendo como o LDAP funciona com o eDirectory" no *Guia de Administração do NetIQ eDirectory 8.8 SP8*.

O servidor LDAP solicita SASL dos mecanismos instalados ao obter sua configuração e suporte automaticamente do que estiver instalado. O servidor LDAP também relata os mecanismos SASL atualmente suportados em seu `rootDSE` ao usar o atributo `supportedSASLMechanisms`.

Portanto, ao configurar o GSSAPI, ele torna-se o mecanismo padrão. Contudo, para realizar especificamente uma operação de LDAP no mecanismo SASL GSSAPI, é possível mencionar o GSSAPI na linha de comando.

Por exemplo, para realizar uma pesquisa em OpenLDAP usando o mecanismo GSSAPI, digite o seguinte:

```
ldapsearch -Y GSSAPI -h 164.99.146.48 -b "" -s base
```

7.5 Termos comumente usados

A tabela a seguir define a terminologia usada comumente com o Kerberos e o GSSAPI.

Tabela 7-1 *Terminologia Kerberos/GSSAPI*

Termo	Definição
KDC (Key Distribution Center - Centro de Distribuição de Chaves)	Servidor do Kerberos que autentica usuários e emite bilhetes.
Principal	Uma entidade (usuário ou instância de servidor) registrada junto ao KDC.
Domínio	Um domínio ou agrupamento de princípios atendido por um conjunto de KDCs.
Bilhete de Serviço (ST)	Um registro contendo as informações do cliente, informações do serviço e uma chave de sessão que é criptografada com a chave compartilhada do serviço principal específico.
Bilhete Fornecedor de Bilhetes (TGT)	Um tipo de bilhete com o qual o cliente pode obter bilhetes adicionais do Kerberos.

8 Cumprimento de senhas universais diferenciando maiúsculas e minúsculas

No NetIQ eDirectory 8.8, é possível habilitar uma Senha Universal e tornar a senha sensível à diferenciação de minúsculas ou maiúsculas ao acessar o servidor do eDirectory 8.8 através dos seguintes clientes e utilitários:

- Novell Client 4.9 e posterior
- Utilitários de administração atualizados para o eDirectory 8.8
- NetIQ iManager 2.7 e posterior, exceto quando executado no Windows

Você pode usar qualquer versão do LDAP SDK para ter senhas que diferenciam maiúsculas e minúsculas.

A tabela a seguir lista as plataformas que suportam o recurso de diferenciação de maiúsculas e minúsculas:

Recurso	Linux	Windows
Cumprimento de senha universal diferenciando maiúsculas e minúsculas	✓	✓

Este capítulo inclui as seguintes informações:

8.1 Necessidade de senhas que diferenciem maiúsculas e minúsculas

Fazer com que a senha diferencie maiúsculas e minúsculas confere maior segurança ao login do diretório. Por exemplo, se você possui uma senha aBc que diferencia maiúsculas e minúsculas, todas as combinações de login com abc, Abc ou ABC falhariam.

No eDirectory 8.8 e posterior, é possível fazer com que as senhas diferenciem maiúsculas e minúsculas para todos os clientes atualizados para o eDirectory 8.8.

Ao fazer cumprir o uso de senhas que diferenciem maiúsculas e minúsculas, você evita que clientes Novell legados acessem o servidor do eDirectory 8.8. Consulte Seção 8.4, “Evitando que clientes legados da Novell acessem o servidor do eDirectory 8.8” na página 46 para obter mais informações.

8.2 Como fazer com que a senha diferencie maiúsculas e minúsculas?

No eDirectory 8.8 e posterior, é possível fazer com que suas senhas diferenciem maiúsculas e minúsculas para todos os clientes ao habilitar a senha universal. Por padrão, a senha universal é desabilitada.

8.2.1 Pré-requisitos

Por padrão, o LDAP e outros utilitários do servidor usam o login do NDS primeiramente e, se ele falhar, usam o login de Senha Simples. Para que o recurso de senha que diferencia maiúsculas e minúsculas funcione, o login precisará ser realizado pelo Novell Modular Authentication Service (NMAS). Portanto, você precisará definir a variável do ambiente `NDSD_TRY_NMASLOGIN_FIRST` para verdadeiro para habilitar o recurso de senha que diferencia maiúsculas de minúsculas.

Conclua o procedimento a seguir para disponibilizar o recurso de senha que diferencia maiúsculas de minúsculas:

1. Defina a variável de ambiente
   - Linux:

     Acrescente isto `/opt/novell/eDirectory/sbin/pre_ndsd_start` ao fim.

     ```
     NDSD_TRY_NMASLOGIN_FIRST=true
     export NDSD_TRY_NMASLOGIN_FIRST
     ```

   - Windows:

     Clique com o botão direito em Meu Computador e selecione Propriedades. Na guia Avançado, clique em Variáveis do ambiente. Em Variáveis do sistema, acrescente a variável e defina o valor para verdadeiro.
2. Reinicie o servidor do eDirectory.

Observação: Usar NMAS na autenticação aumenta o tempo decorrente para login.

8.2.2 Fazendo com que sua senha diferencie maiúsculas e minúsculas

1. Faça login no eDirectory usando uma senha existente.

   No caso de uma nova instalação, a senha existente é aquela definida ao configurar o eDirectory 8.8.

   Neste exemplo, sua senha é "novell".

   Observação: Esta senha não faz distinção entre maiúsculas e minúsculas.
2. Habilitar Senha Universal.

   Para obter mais informações, consulte a seção "Implementando uma senha universal" no *Guia de Administração Novell Password Management 3.3* (http://www.netiq.com/documentation/password_management33/pwm_administration/data/allq21t.html).
3. Efetue logout do eDirectory.
4. Efetue login no eDirectory usando a senha existente em letras maiúsculas ou minúsculas conforme desejado.

   A senha fará agora distinção entre maiúsculas e minúsculas.

Por exemplo, digite "NoVELL".

Sua senha será "NoVELL". Portanto, "novell" ou qualquer outra combinação de maiúsculas e minúsculas que não "NoVELL" será inválida.

Se estiver migrando para senhas com distinção de maiúsculas e minúsculas, consulte Seção 8.3.1, “Migrando para senhas com distinção entre maiúsculas e minúsculas” na página 45.

Qualquer nova senha definida diferenciará maiúsculas e minúsculas dependendo do nível (objeto ou partição) para o qual a Senha universal foi definida.

8.2.3 Gerenciando senhas com distinção de maiúsculas e minúsculas

É possível gerenciar a distinção entre maiúsculas e minúsculas de suas senhas ao habilitar ou desabilitar a Senha universal pelo iManager. Para obter mais informações, consulte a seção “Implementando uma senha universal” no *Guia de Administração do NetIQ Password Management 3.3* (http://www.netiq.com/documentation/password_management33/pwm_administration/data/allq21t.html).

8.3 Fazendo upgrade de clientes e utilitários legados da Novell

A seguir são exibidas as versões mais recentes dos clientes da Novell e utilitários da NetIQ:

- Novell Client 4.9
- Utilitários de administração com o eDirectory 8.8
- NetIQ iManager 2.7 e posterior

Os clientes e utilitários anteriores às versões mencionadas acima são clientes legados da Novell.

É possível definir distinção entre maiúsculas e minúsculas para clientes legados da Novell após fazer upgrade destes para suas versões mais recentes. O eDirectory 8.8 torna a migração de senhas existentes para senhas com distinção entre maiúsculas e minúsculas uma tarefa fácil e flexível. Consulte Seção 8.3.1, “Migrando para senhas com distinção entre maiúsculas e minúsculas” na página 45 para obter mais informações.

Caso não faça o upgrade dos clientes legados para suas versões mais recentes, esses clientes poderão ser impedidos de usar o eDirectory 8.8 no nível do servidor. Consulte Seção 8.4, “Evitando que clientes legados da Novell acessem o servidor do eDirectory 8.8” na página 46 para obter mais informações.

8.3.1 Migrando para senhas com distinção entre maiúsculas e minúsculas

A senha universal é desabilitada por padrão e, portanto, suas senhas existentes não serão afetadas até habilitá-la no iManager. Para obter instruções passo a passo, consulte Seção 8.2, “Como fazer com que a senha diferencie maiúsculas e minúsculas?” na página 44.

O exemplo a seguir explica a migração para senhas com distinção entre maiúsculas e minúsculas:

Sessão de login 1: a senha universal está desabilitada por padrão.

- Efetue login usando sua senha existente. Por exemplo, digamos que sua senha é netiq.

- Esta senha não faz distinção entre maiúsculas e minúsculas. Portanto, tanto netiq quanto NetIQ são senhas válidas.
- Após efetuar login, você habilita a senha universal. Consulte a seção "Implementando uma senha universal" no *Guia de Administração do NetIQ Password Management 3.3* (http://www.netiq.com/documentation/password_management33/pwm_administration/data/allq21t.html).

Sessão de login 2: a senha universal foi habilitada na sessão anterior.

- Efetue login usando sua senha existente. Por exemplo, digamos que você digite sua senha como noVell.
- Quando a senha universal está habilitada, esta senha faz distinção entre maiúsculas e minúsculas. Por isso, será necessário lembrar como a senha foi digitada desta vez.

Sessão de login 3 e logins posteriores.

- Se você efetuar login usando a senha netIQ, esta será válida.
- Se você efetuar login usando a senha NetIQ (ou qualquer outra versão exceto noVell) esta será inválida.

8.4 Evitando que clientes legados da Novell acessem o servidor do eDirectory 8.8

No eDirectory 8.7.1 e 8.7.3, era possível evitar que clientes legados da Novell configurassem ou alterassem a senha de NDS. Com o eDirectory 8.8, também é possível evitar que eles efetuem login no eDirectory 8.8 e verifiquem as senhas.

Para permitir ou proibir que clientes legados da Novell usem o eDirectory 8.8, será necessário configurar o login de NDS pelo iManager ou pelo LDAP.

Esta seção inclui as seguintes informações:

8.4.1 Necessidade de evitar que clientes legados da Novell acessem o servidor do eDirectory 8.8

As senhas de clientes legados da Novell não fazem distinção entre maiúsculas e minúsculas. Portanto, no eDirectory 8.8 e posterior, quando desejar assegurar o uso obrigatório de senhas com distinção entre maiúsculas e minúsculas, poderá ser necessário bloquear clientes legados de acessar o diretório.

Nas versões anteriores ao Novell Client 4.9, não havia suporte à senha universal. Isto porque as alterações de login e senha iam diretamente para a senha de NDS em vez de para o NMAS. Agora, ao usar a senha universal, alterar as senhas através de clientes legados poderá criar um problema

chamado "flutuação de senha". Isto significa que a senha de NDS e a senha universal não estarão sincronizadas. Para evitar o problema, uma opção é bloquear alterações de senha realizadas em clientes anteriores à versão 4.9.

Consulte a próxima seção, Gerenciando configurações de login de NDS, para obter mais informações sobre como impedir que clientes legados acessem o servidor do eDirectory 8.8 eDirectory 8.8.

8.4.2 Gerenciando configurações de login de NDS

Ao configurar o login de NDS, é possível permitir ou proibir que clientes legados da Novell acessem o servidor do eDirectory 8.8. É possível gerenciar as configurações de login do NDS pelo iManager 2.6 e pelo LDAP.

No eDirectory 8.8 e posterior, você pode configurar a definição e alteração de senhas pelo LDAP ou pelo iManager.

Esta seção inclui informações sobre o seguinte:

Configuração de NDS em diferentes níveis

É possível configurar o login do NS em um ou em todos os níveis a seguir:

- Nível da partição
- Nível do objeto

Se você não especificar a configuração em qualquer um dos níveis, a configuração de login do NDS será habilitada em todos os níveis.

A configuração de nível de objeto sempre se sobrepõe à configuração de nível de partição. Isto é descrito na tabela a seguir:

Tabela 8-1 *Configuração do do NDS*

Configuração no nível de objeto	Configuração no nível de partição	Configuração
Não especificado	Habilitado	Habilitado
Habilitado	Não especificado	Habilitado
Não especificado	Desabilitado	Desabilitado
Desabilitado	Não especificado	Desabilitado
Habilitado	Habilitado	Habilitado
Habilitado	Desabilitado	Habilitado
Desabilitado	Habilitado	Desabilitado
Desabilitado	Desabilitado	Desabilitado

Em todos os níveis (objeto e partição), é possível configurar o login de NDS para realizar o seguinte:

- Efetuar login no diretório usando a senha de NDS ou verificando a senha de NDS.
- Definindo uma nova senha e alterando a senha existente

Efetuando login no diretório ou verificando a senha de NDS

Efetuar login/verificar a senha de NDS significa:

- Efetuar login no diretório usando uma senha de NDS.
- Verificar a senha existente no diretório.

Login/verificação de senha de NDS está habilitado por padrão. Ao desabilitar a chave de login/verificação, você não poderá efetuar login na versão mais recente do eDirectory ou verificar as senhas. Você pode habilitar ou desabilitar o login/verificação de senha de NDS nos níveis de partição e de objeto. Se o login/verificação estiver desabilitado, você não poderá definir ou alterar senhas de NDS.

Você pode configurar o login/verificação de senha de NDS pelo iManager ou pelo LDAP. Para obter mais informações, consulte a "Gerenciando as configurações de NDS pelo iManager" na página 48 e a "Gerenciando as configurações de NDS pelo LDAP" na página 49.

Definindo uma nova senha ou alterando a senha de NDS

Definir/alterar uma senha de NDS significa

- Definir uma nova senha para um objeto.
- Alterar a senha existente de um objeto.

A definição/alteração de senha de NDS está habilitada por padrão. Ao desabilitar a chave de definição/alteração, você não poderá mais definir uma nova senha ou alterar a senha existente no eDirectory. Você pode habilitar ou desabilitar a definição/alteração de senha de NDS nos níveis de partição e de objeto. Se o login/verificação estiver desabilitado, você não poderá definir/alterar senhas.

Antes, você podia definir/alterar senhas de NDS apenas pelo LDAP. Agora, pode fazê-lo também pelo iManager. Para obter mais informações, consulte a "Gerenciando as configurações de NDS pelo iManager" na página 48 e a "Gerenciando as configurações de NDS pelo LDAP" na página 49.

Gerenciando as configurações de NDS pelo iManager

Esta seção inclui as seguintes informações:

Você pode ativar a chave de login/verificação ou a chave de definição/alteraçãonas configurações de login de NDS.

Habilitando/desabilitando a configuração de NDS para uma partição

Para habilitar o login de NDS para clientes anteriores ao eDirectory 8.8:

1. No iManager, clique no botão *Funções e tarefas*  .
2. Selecione *NMAS* > *Obrigação de senha universal*.

3 No plug-in de Obrigação de senha universal. selecione *Configuração do NDS para uma partição.*

4 Siga as instruções na configuração de NDS para um assistente de partição e configure o login e o gerenciamento de senha no nível da partição.

Ajuda está disponível no assistente.

Habilitando/desabilitando a configuração de NDS para um objeto

Para habilitar o login de NDS para clientes anteriores ao eDirectory 8.8:

1 No iManager, clique no botão *Funções e tarefas*  .

2 Selecione *NMAS* > *Obrigação de senha universal*.

3 No assistente, selecione *Configuração de NDS para um objeto*.

4 Siga as instruções na Configuração de NDS para um assistente de objeto para configurar o login e gerenciamento de senha no nível do objeto.

Ajuda está disponível no assistente.

Gerenciando as configurações de NDS pelo LDAP

Importante: É altamente recomendável usar o iManager para gerenciar as configurações de NDS e não o LDAP.

Você pode gerenciar as configurações através do LDAP usando um atributo do eDirectory em um contêiner de raiz da partição ou objeto. Os atributos fazem parte do esquema no eDirectory 8.7.1 ou posterior e não são suportados no eDirectory 8.7 ou anterior.

O método usado pelos clientes legados para definir as configurações de login de NDS é chamado de gerenciamento de login de NDAP e o método usado para configurações de senha de NDS é o gerenciamento de senha de NDAP.

Esta seção fornece informações sobre:

- "Habilitando/desabilitando a configuração de NDS para uma partição" na página 49
- "Habilitando/desabilitando configurações de NDS para um objeto" na página 50

Habilitando/desabilitando a configuração de NDS para uma partição

Gerenciamento de senha de login e verificação

Use o atributo `ndapPartitionLoginMgmt` para habilitar ou desabilitar o gerenciamento de senha de login e verificação para uma partição.

`ndapPartitionLoginMgmt` Valor do atributo	Descrição
Não presente ou não especificado	O gerenciamento de login de NDAP está habilitado.
0	O gerenciamento de login de NDAP está desabilitado.
1	O gerenciamento de login de NDAP está habilitado.

Definir e alterar a senha de NDS

Use o atributo `ndapPartitionPasswordMgmt` para habilitar ou desabilitar a definição e alteração de uma senha de NDS para uma partição.

`ndapPartitionPasswordMgmt` Valor do atributo	Descrição
Não presente ou não especificado	O gerenciamento de senha de NDAP está habilitado.
0	O gerenciamento de senha de NDAP está desabilitado.
1	O gerenciamento de senha de NDAP está habilitado.

Habilitando/desabilitando configurações de NDS para um objeto

Login e verificação de senha de NDS

Use o atributo `ndapLoginMgmt` para habilitar ou desabilitar o gerenciamento de login e verificação de NDS para um objeto.

`ndapLoginMgmt` Valor do atributo	Descrição
Não presente ou não especificado	O gerenciamento de login do NDAP depende da configuração no nível da partição.
0	O gerenciamento de login de NDAP será desabilitado se desativado no nível da partição.
1	O gerenciamento de login será habilitado independentemente da definição de configuração no nível da partição.

Definir e alterar a senha de NDS

Use o atributo `ndapPasswordMgmt` para habilitar ou desabilitar a definição e alteração de uma senha de NDS para um objeto.

`ndapPasswordMgmt` Valor do atributo	Descrição
Não presente ou não especificado	O gerenciamento de senha do NDAP depende da configuração no nível da partição.
0	O gerenciamento de senha de NDAP será desabilitado se desativado no nível da partição.
1	O gerenciamento de senha será habilitado independentemente da definição de configuração no nível da partição.

Observação: Para obter mais informações sobre a criação e gerenciamento de políticas de sincronização prioritária, consulte "Usando ferramentas LDAP no Linux" e "Utilitário de importação, conversão e exportação da NetIQ" no *Guia de Administração do NetIQ eDirectory 8.8 SP8*.

8.4.3 Operações de partição

Ao dividir uma partição, as configurações de NDS não são herdadas pela partição-filha. Ao fundir partições, as configurações de NDS do pai são retidas pela partição NDS resultante.

8.4.4 Obrigatoriedade de senhas com distinção entre maiúsculas e minúsculas em uma árvore mista

Se existir uma árvore com um servidor do eDirectory 8.8 ou posterior e um servidor do eDirectory 8.7 ou anterior, e se os dois servidores compartilharem uma partição, desabilitar a configuração de login nesta partição gerará resultados não confiáveis. O servidor 8.8 assegurará o uso obrigatório da definição, evitando que clientes legados acessem o diretório. Contudo, o servidor 8.7 não assegurará tal definição, de maneira que será possível acessar o diretório pelo servidor 8.7.

8.5 Para obter mais informações

Consulte os itens a seguir para obter mais informações sobre senhas com distinção entre maiúsculas e minúsculas:

- Ajuda online do iManager
- A seção "Implementando uma senha universal" no *Guia de Administração do NetIQ Password Management 3.3* (http://www.netiq.com/documentation/password_management33/pwm_administration/data/allq21t.html)

9 Suporte à política de senha do Microsoft Windows Server 2008

Nas versões anteriores do eDirectory, os usuários poderiam usar a política de complexidade padrão da Microsoft ou a sintaxe legada da Novell. Contudo, o NetIQ eDirectory 8.8 SP8 suporta o uso de políticas de senha em conformidade com os requisitos de complexidade de senha do Microsoft Windows Server 2008, que diferem dos requisitos da política de complexidade anterior da Microsoft. Você pode usar o iManager para criar uma política usando a opção de sintaxe da Política de senha do novo Microsoft Server 2008 e configurar esta política conforme necessário para seu ambiente.

Este capítulo inclui as seguintes informações:

9.1 Criando políticas de senha do Windows Server 2008

Você pode usar o iManager para criar políticas que usam os requisitos de complexidade do Microsoft Windows Server 2008 e atribuir usuários no seu ambiente do eDirectory para a nova política. Para obter instruções detalhadas sobre a criação de políticas de senhas, consulte o *Guia de Administração do NetIQ Password Management 3.3.2* (http://www.netiq.com/documentation/password_management33/pwm_administration/data/bookinfo.html).

Observação

- Antes de criar uma nova política de senha usando a sintaxe da política de senha do Microsoft Server 2008, confirme que possui a versão mais recente do plug-in de Gerenciamento de Senha do Novell iManager. Para obter mais informações sobre instalação dos módulos de plug-in, consulte o *Guia de Administração do NetIQ iManager 2.7* (https://www.netiq.com/documentation/imanager/imanager_admin/data/hk42s9ot.html).
- Você também deverá assegurar que ambas as regras de senha universal e senha avançada estejam habilitadas para a política que deseja criar ou configurar.

9.2 Gerenciando políticas de senha do Windows Server 2008

Você poderá gerenciar políticas que usam requisitos de complexidade de política de senha do Windows Server 2008 usando o iManager. Para obter mais informações, consulte a seção "Gerenciando senhas usando políticas de senha" *no* Guia de Administração do Novell Password Management 3.3.2 (http://www.netiq.com/documentation/password_management33/pwm_administration/data/ampxjj0.html).

9.3 Para obter mais informações

Consulte os itens a seguir para obter mais informações sobre políticas de senha no eDirectory:

- Ajuda online do iManager
- *Guia de Administração do Novell Password Management 3.3.2* (http://www.netiq.com/documentation/password_management33/pwm_administration/data/bookinfo.html)
- *Guia de Administração do Novell Modular Authentication Services 3.3.4* (http://www.netiq.com/documentation/nmas33/admin/data/a20gkue.html)

10 Sincronização de Prioridade

Sincronização prioritária é um novo recurso presente no NetIQ eDirectory 8.8 que complementa o processo de sincronização atual no eDirectory. Através da sincronização prioritária, é possível sincronizar dados críticos modificados, tais como senhas, imediatamente.

Você pode sincronizar seus dados críticos através da sincronização prioritária quando não puder aguardar pela sincronização normal. O processo de sincronização prioritária é mais rápido do que o processo de sincronização normal. A sincronização prioritária apenas é suportada entre dois ou mais servidores do eDirectory 8.8 ou posterior agindo como host de uma mesma partição.

A tabela a seguir lista as plataformas que suportam o recurso Sincronização prioritária:

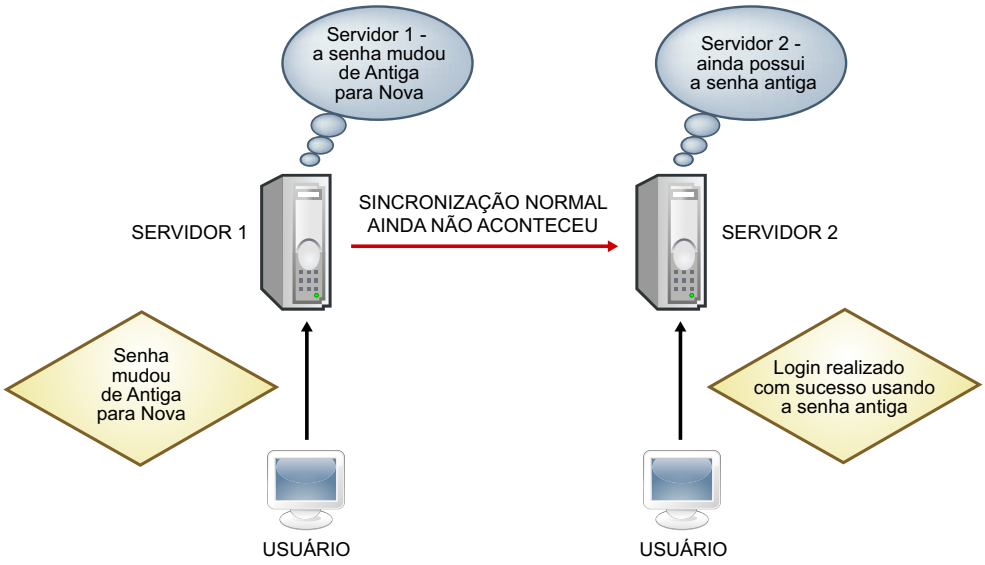
Lista de recursos	Linux	Windows
Sincronização de Prioridade	✓	✓

Este capítulo inclui as seguintes informações:

10.1 Necessidade de sincronização prioritária

A sincronização normal pode levar algum tempo, durante o qual os dados modificados não estariam disponíveis em outros servidores. Por exemplo, suponha que em sua configuração há diversos aplicativos que se comunicam com o diretório. Você muda sua senha no Servidor1. Com a sincronização normal, levará algum tempo para que esta mudança seja sincronizada com o Servidor2. Portanto, um usuário ainda seria capaz de autenticar-se no diretório através de um aplicativo que se comunica com o Servidor2 usando a senha antiga.

Figura 10-1 *Necessidade de sincronização prioritária*



Em grandes implementações, quando os dados críticos de um objeto são modificados, as alterações precisam ser sincronizadas imediatamente. O processo de sincronização prioritária resolve este problema.

10.2 Usando a sincronização prioritária

Para sincronizar as modificações de data através de sincronização prioritária, será necessário fazer o seguinte:

1. Habilitar a sincronização prioritária, configurar o número de threads e o tamanho da fila da sincronização prioritária pelo iMonitor.
2. Definir as políticas de sincronização prioritária identificando os atributos que são críticos pelo iManager.
3. Aplicar as políticas de sincronização prioritária às partições pelo iManager.

10.3 Para obter mais informações

Consulte os itens a seguir para obter mais informações sobre sincronização prioritária:

- *Guia de Administração do NetIQ eDirectory 8.8 SP8*
- Ajuda online do iManager e do iMonitor

11 Criptografia de Dados

No NetIQ eDirectory 8.8 e posterior, você pode criptografar dados específicos quando armazenados no disco e quando são transmitidos entre dois ou mais servidores do eDirectory 8.8. Isto concede maior segurança a dados confidenciais.

A tabela a seguir lista as plataformas que suportam o recurso de criptografia de dados:

Recurso	Linux	Windows
Atributos Criptografados	✓	✓
Replicação criptografada	✓	✓

Este capítulo inclui as seguintes informações:

11.1 Criptografando atributos

O eDirectory 8.8 permite criptografar dados sensíveis armazenados em disco. Atributos criptografados é um recurso específico do servidor.

Você poderá acessar os atributos criptografados apenas por canais seguros exceto se escolher oferecer acesso também por canais de texto sem criptografia. Consulte Seção 11.1.3, “Acessando atributos criptografados” na página 58 para obter mais informações.

Esta seção inclui as seguintes informações:

O recurso de atributos criptografados é suportado apenas em servidores do eDirectory 8.8 ou posterior.

11.1.1 Necessidade de atributos criptografados

Antes do eDirectory 8.8, os dados eram armazenados como texto sem criptografia no disco. Houve a necessidade de proteger os dados e conceder acesso aos dados apenas por canais seguros.

Você pode usar este recurso em cenários onde precisa proteger dados confidenciais como números de cartão de crédito de clientes bancários.

11.1.2 Como criptografar atributos

Você pode criptografar atributos ao criar e definir políticas de atributos criptografados e depois aplicar tais políticas aos servidores. É possível criar, definir, aplicar e gerenciar as políticas de atributos criptografados pelo iManager e pelo LDAP.

1. Criação e definição de uma política de atributo criptografada:
   - **1a** Determine os atributos para criptografia.
   - **1b** Determine também o esquema de criptografia para os atributos.
2. Aplique a política de atributos criptografados a um servidor.

11.1.3 Acessando atributos criptografados

Você poderá acessar os atributos criptografados apenas por meio de canais seguros como porta LDAP SSL ou porta segura HTTP. Você poderá escolher conceder acesso aos atributos criptografados por canais de texto sem criptografia usando o plug-in do iManager. Para obter mais informações, consulte o *Guia de Administração do NetIQ eDirectory 8.8 SP8*.

11.2 Criptografando replicação

A replicação criptografada refere-se à criptografia de dados transmitidos entre dois ou mais servidores do eDirectory 8.8.

A replicação criptografada complementa a sincronização normal no eDirectory.

Esta seção inclui as seguintes informações:

- Seção 11.2.1, “Necessidade de replicação criptografada” na página 58
- Seção 11.2.2, “Habilitando a replicação criptografada” na página 59

11.2.1 Necessidade de replicação criptografada

Antes do eDirectory 8.8, os dados eram transmitidos por fio durante a replicação como texto sem criptografia. Houve a necessidade de proteger dados confidenciais durante a transferência criptografando-os, especialmente se as réplicas eram separadas geograficamente e conectavam-se pela Internet.

Este recurso pode ser usado nos seguintes cenários:

- Se os servidores do diretório estiverem dispersos por várias localizações geográficas através de WAN e Internet e se houver necessidade de criptografar dados sensíveis durante transmissões.
- Se você desejar que apenas algumas partições da sua árvore sejam protegidas, poderá indicar seletivamente as partições que contêm os dados sensíveis para ser criptografados na replicação.
- Se você precisar de replicação criptografada entre réplicas específicas de uma partição que contém dados sensíveis.
- Se achar que a rede da sua configuração é hostil e desejar proteger dados sensíveis durante a replicação.

11.2.2 Habilitando a replicação criptografada

Você pode habilitar a replicação criptografada usando o iManager. É possível habilitar a replicação criptografada no nível de partição ou de réplica.

Importante: Antes de habilitar a replicação criptografada, certifique-se de que ambos os servidores de origem e de destino possuam os certificados padrão. Se você tiver feito qualquer alteração nesses certificados, como renomeá-los, a replicação criptografada falhará.

11.3 Para obter mais informações

Consulte os itens a seguir para obter mais informações sobre criptografia de dados no eDirectory:

- *Guia de Administração do NetIQ eDirectory 8.8 SP8*
- Ajuda online do iManager e do iMonitor

12 Desempenho em massa

O NetIQ eDirectory 8.8 fornece melhorias para aumentar o desempenho em massa.

Para obter mais informações sobre como aumentar o desempenho em massa, consulte as seguintes seções do *Guia de Administração do NetIQ eDirectory 8.8 SP8*:

- "Configurações de cache do eDirectory"
- "Configuração do tamanho da transação LBURP"
- "Aumentando o número de solicitações assíncronas em ICE"
- "Número elevado de threads de gravador de LDAP"
- "Desabilitando a validação do esquema em ICE"
- "Desativando modelos ACL"
- "Backlinker"
- "Habilitando/desabilitando o cache em linha"
- "Aumentando o período do tempo de espera do LBURP"
- "Utilitário em massa offline"

13 Plug-ins ICE do iManager

Antes do NetIQ eDirectory 8.8, algumas das opções de linha de comando do utilitário de importação, conversão e exportação da Novell (ICE) não possuíam opções correspondentes no plug-in do iManager.

A tabela a seguir lista as plataformas que suportam este recurso:

Recurso	Linux	Windows
Melhorias do ICE iManager	✓	✓

O assistente ICE no iManager 2.7 com o eDirectory 8.8 oferece os seguintes recursos:

- Adição de esquema faltante
- Comparação de esquema
- Geração de um arquivo de ordem

13.1 Adição de esquema faltante

No eDirectory 8.8, o iManager fornece opções para adicionar esquemas faltantes a um esquema do servidor. Este processo envolve comparar a origem e o destino. Se houver esquemas adicionais no esquema de origem, eles serão acrescentados ao esquema de destino. A origem pode ser um arquivo ou um servidor LDAP e o destino deverá ser um servidor LDAP.

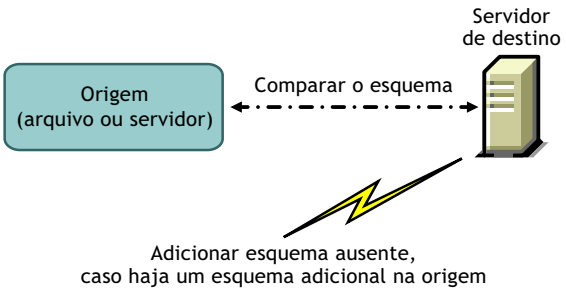
Através do assistente ICE no iManager, você poderá adicionar o esquema faltante usando as opções a seguir:

- Adicionar esquemas de um arquivo
- Adicionar esquemas de um servidor

13.1.1 Adicionar esquemas de um arquivo

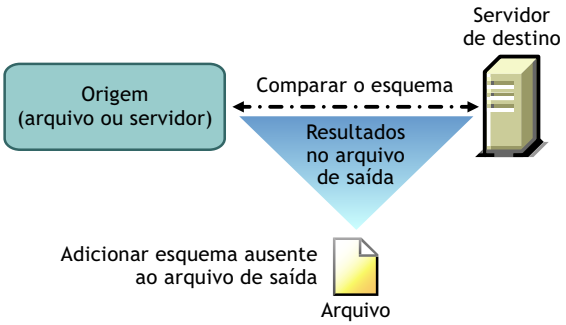
O ICE pode comparar o esquema na origem e no destino. A origem é um arquivo ou servidor LDAP e o destino deverá ser um servidor LDAP. O arquivo do esquema de origem pode estar nos formatos LDIF ou SCH.

Figura 13-1 *Comparar e adicionar o esquema de um arquivo*



Se desejar apenas comparar o esquema e não adicionar o esquema adicional ao servidor de destino, selecione a opção *Comparar, mas não adicionar*. Neste caso, o esquema adicional não é adicionado ao servidor e destino, porém as diferenças entre os esquemas estarão disponíveis como um link no fim da operação.

Figura 13-2 *Comparar esquemas e adicionar os resultados a um arquivo de saída*



Para obter mais informações, consulte "Utilitários de gerenciamento do NetIQ eDirectory" no *Guia de Administração do NetIQ eDirectory 8.8 SP8*.

13.1.2 Adicionar esquemas de um servidor

A origem e o destino são servidores LDAP.

Se desejar apenas comparar o esquema e não adicionar o esquema adicional ao servidor de destino, selecione a opção *Comparar, mas não adicionar*. Neste caso, o esquema adicional não é adicionado ao servidor e destino, porém as diferenças entre os esquemas estarão disponíveis como um link no fim da operação.

Para obter mais informações, consulte "Utilitários de gerenciamento do NetIQ eDirectory" no *Guia de Administração do NetIQ eDirectory 8.8 SP8*.

13.2 Comparando os esquemas

Usando o iManager, é possível comparar os esquemas entre uma origem e um destino. A origem pode ser um arquivo ou um servidor e o destino deverá ser um arquivo LDIF.

O iManager compara o esquema entre uma origem e um destino e armazena os resultados em um arquivo de saída.

Através do assistente ICE no iManager, você poderá comparar os esquemas usando as opções a seguir:

- Comparar arquivos de esquema
- Comparar esquemas entre um servidor e um arquivo

13.2.1 Comparar arquivos de esquema

A opção *Comparar arquivos de esquema* compara esquemas entre um arquivo de origem e outro de destino e, então, aloca o resultado em um arquivo de saída. Para adicionar o esquema faltante ao arquivo de destino, aplique os registros do arquivo de saída ao arquivo de destino.

Para obter mais informações, consulte "Utilitários de gerenciamento do NetIQ eDirectory" no *Guia de Administração do NetIQ eDirectory 8.8 SP8*.

13.2.2 Comparar esquemas entre um servidor e um arquivo

A opção *Comparar esquemas entre um servidor e um arquivo* compara os esquemas entre um servidor de origem e um arquivo de destino e aloca o resultado em um arquivo de saída. Para adicionar o esquema faltante ao arquivo de destino, aplique os registros do arquivo de saída ao arquivo de destino.

Para obter mais informações, consulte "Utilitários de gerenciamento do NetIQ eDirectory" no *Guia de Administração do NetIQ eDirectory 8.8 SP8*.

13.3 Gerando um arquivo de ordem

Esta opção cria um arquivo de ordem para uso com a sub-rotina delim para importar dados de um arquivo de dados delimitado. O assistente ajuda a criar esse arquivo de ordem que contém uma lista de atributos para uma classe de objetos específica.

Para obter mais informações, consulte "Utilitários de gerenciamento do NetIQ eDirectory" no *Guia de Administração do NetIQ eDirectory 8.8 SP8*.

13.4 Para obter mais informações

Para obter mais informações sobre este recurso, consulte:

- *Guia de Administração do NetIQ eDirectory 8.8 SP8*
- Ajuda online do iMonitor

14 Backup baseado em LDAP

O recurso de backup baseado em LDAP foi introduzido no NetIQ eDirectory 8.8. Este recurso é usado para fazer backup dos atributos e valores dos atributos em um objeto por vez.

A tabela a seguir lista as plataformas que suportam este recurso:

Recurso	Linux	Windows
Backup baseado em LDAP	✓	✓

Este recurso permite realizar um backup incremental onde o backup do objeto ocorre apenas se houver alteração no mesmo.

O backup baseado em LDAP fornece um conjunto de interfaces para backup e restauração de objetos do eDirectory expostos pelas bibliotecas do LDAP para operações estendidas de C a LDAP.

Para obter mais informações sobre bibliotecas LDAP para C SDK, consulte a documentação de bibliotecas para LDAP para C (http://developer.novell.com/ndk/doc/cldap/ldaplibc/data/hevgtl7k.html).

Para obter um exemplo de como fazer o backup e restauração de objetos do eDirectory através do LDAP, consulte o código de amostra backup.c (http://developer.novell.com/ndk/doc/samplecode/cldap_sample/extensions/backup.c.html).

14.1 Necessidade do backup baseado em LDAP

O backup baseado em LDAP tenta resolver problemas decorridos no backup e restauração atuais.

Os problemas que este recurso resolve são:

- Fornece uma interface consistente através da qual quaisquer aplicativos ou desenvolvedores de backup de terceiros poderão fazer backup do eDirectory em todas as plataformas suportadas.
- Fornece uma solução de backup incremental para objetos.

14.2 Para obter mais informações

Para obter mais informações sobre este recurso, consulte:

- Bibliotecas LDAP para C (http://developer.novell.com/documentation/cldap/ldaplibc/data/hevgtl7k.html)
- Código de amostra: backup.c (http://developer.novell.com/documentation/samplecode/cldap_sample/extensions/backup.c.html)

15 LDAP Obter lista de privilégios efetivos

O API LDAP Obter lista de privilégios efetivos foi introduzido no NetIQ eDirectory 8.8 SP6.

A tabela a seguir lista as plataformas que suportam este recurso:

Recurso	Linux	Windows
LDAP Obter lista de privilégios efetivos	✓	✓

Este recurso pode ser usado para obter privilégios efetivos para um certo assunto de DN em um DN alvo específico para um dado conjunto de atributos. Ele fornece uma interface para obter a lista de privilégios através das bibliotecas LDAP para C por meio das operações estendidas de LDAP.

Para obter mais informações sobre bibliotecas LDAP para C SDK, consulte a documentação de bibliotecas para LDAP para C (http://developer.novell.com/ndk/doc/cldap/ldaplibc/data/hevgtl7k.html).

15.1 Necessidades da interface LDAP obter lista de privilégios efetivos

A interface LDAP Obter lista de privilégios efetivos tenta resolver problemas com o API Obter privilégios efetivos.

Os problemas que este recurso resolve são:

- Requer apenas uma solicitação para o diretório para obter os direitos efetivos de múltiplos atributos.
- Reduz o tempo de jornada para o diretório obter os direitos efetivos de múltiplos atributos.
- Identifica qualquer falha de entrada na solicitação ou no diretório.

15.2 Para obter mais informações

Para obter mais informações sobre este recurso, consulte:

- Bibliotecas LDAP para C (http://developer.novell.com/documentation/cldap/ldaplibc/data/hevgtl7k.html).
- Código de amostra: getpriv.c (http://developer.novell.com/documentation/samplecode/cldap_sample/extensions/getpriv.c.html).

16 Gerenciando registros de erro no eDirectory 8.8

Muitos clientes relataram que os registros de erros no NetIQ eDirectory não ajudavam muito a identificar e resolver os problemas mais comuns. O registro de erros é iniciado automaticamente durante a instalação do eDirectory.

Este capítulo consiste nas seguintes seções:

16.1 Níveis de gravidade de mensagem

Todas as mensagens possuem um nível de gravidade atrelado para ajudar a determinar sua criticidade. Os níveis de gravidade, em ordem decrescente, são os seguintes:

16.1.1 Fatal

Uma mensagem fatal indica um problema significativo, tal como perda de dados ou de funcionalidade.

Exemplos:

- Se o servidor do eDirectory falhar em carregar módulos de sistema como o NCPEngine e o DSLoader ao carregar módulos, um erro fatal será relatado e registrado.
- Se o servidor do eDirectory falhar em vincular a porta segura 636, um erro fatal será relatado e registrado.

16.1.2 Aviso

Uma mensagem que não é necessariamente grave, porém poderá ser uma possível causa para um problema futuro.

Exemplos:

- Falhas de conexão entre dois servidores em uma árvore, resultando na adição do servidor ao cache de endereço inválido. O servidor pode recuperar-se deste estado específico ao reiniciar o cache de endereço inválido.
- Se o aplicativo do cliente do LDAP realizar uma vinculação e fechar a conexão sem se desvincular, o servidor LDAP deverá registrar um aviso de registro com a mensagem de aviso adequada.
- Se o servidor do eDirectory consumir todos os descritores de arquivo e alcançar o limite, como resultado, o servidor não será capaz de processar qualquer solicitação recebida, levando a uma falha do aplicativo.

16.1.3 Erro

Uma mensagem que poderia ser devido à operação inválida, porém não causará qualquer problema.

Exemplos:

- Quando um aplicativo cliente tentar adicionar um objeto para o qual a definição dos atributos não está definida no esquema, o servidor do eDirectory relatará o erro ERR_NO_SUCH_ATTRIBUTE.
- Quando um usuário tentar efetuar login com uma senha inválida, o servidor do eDirectory relatará o erro ERR_FAILED_AUTHENTICATION.

16.1.4 Informativo

Uma mensagem descrevendo a conclusão com êxito de uma operação ou evento no servidor do eDirectory.

Exemplos:

- Quando um módulo é carregado/descarregado com êxito, pode ser adequado registrar uma mensagem informativa sobre esta operação.
- Quando a configuração de cache de banco de dados é alterada, uma mensagem informativa deverá ser registrada sobre o salvamento com êxito da configuração.

16.1.5 Depurar

Uma mensagem que contém informações que ajudam os desenvolvedores a depurar um programa.

Exemplos:

Ao realizar uma pesquisa em grupo dinâmico, exibe todos os membros do grupo dinâmico com informações de ID de entrada, ID de partição e DN dos membros. Estas informações ajudarão a saber que todos os membros são exibidos no nível do eDirectory.

16.2 Configurando os registros de erro

- Seção 16.2.1, “Linux” na página 73
- Seção 16.2.2, “Windows” na página 73

16.2.1 Linux

Para configurar as definições de registros de erro para mensagens do lado do servidor, use os parâmetros `n4u.server.log-levels` e `n4u.server.log-file` no arquivo de configuração `/etc/opt/novell/eDirectory/conf/nds.conf`.

Definindo o nível de gravidade

Os níveis de gravidade disponíveis são `LogFatal`, `LogWarn`, `LogErr`, `LogInfo` e `LogDbg` (em ordem decrescente de gravidade). Para obter maiores informações sobre os níveis de gravidade, consulte Seção 16.1, “Níveis de gravidade de mensagem” na página 71.

Por padrão, o nível de gravidade é definido como `LogFatal`. Por isso, apenas mensagens com o nível de gravidade fatal serão registradas.

Para definir o nível de gravidade, use o parâmetro `n4u.server.log-levels` no arquivo `nds.conf` da seguinte maneira:

`n4u.server.log-levels=`*`nível_de_gravidade`*

Por exemplo:

- Para definir o nível de gravidade para `LogInfo` e acima, digite:

  `n4u.server.log-levels=LogInfo`

  Com esta configuração, as mensagens com nível de gravidade `LogInfo` e acima (ou seja, `LogFatal`, `LogWarn` e `LogErr`) serão registradas no arquivo de registro.
- Para definir o nível de gravidade para `LogWarn` e acima, digite:

  `n4u.server.log-levels=LogWarn`

  Com esta configuração, mensagens com nível de gravidade `LogWarn` e acima (`LogFatal`) serão registradas no arquivo de registro.

Especificando o nome do arquivo de registro

Para especificar o local do arquivo de registro onde as mensagens serão registradas, use o parâmetro `n4u.server.log-file` no arquivo `nds.conf`. Por padrão, as mensagens são registradas no arquivo `ndsd.log`.

Por exemplo, para registrar mensagens em `/tmp/edir.log`, digite:

`n4u.server.log-file=/tmp/edir.log`

Para registrar mensagens no registro do sistema, use o parâmetro `n4u.server.log-file` da seguinte maneira:

`n4u.server.log-file=syslog`

16.2.2 Windows

- “Definindo o nível de gravidade” na página 74
- “Especificando o nome e o caminho do arquivo de registro” na página 74
- “Especificando o tamanho do arquivo de registro” na página 74

Definindo o nível de gravidade

Os níveis de gravidade disponíveis são `LogFatal`, `LogWarn`, `LogErr`, `LogInfo` e `LogDbg` (em ordem decrescente de gravidade). Para obter maiores informações sobre os níveis de gravidade, consulte Seção 16.1, “Níveis de gravidade de mensagem” na página 71.

Para definir o nível de gravidade, faça o seguinte:

1. Clique em *Iniciar* > *Configurações* > *Painel de Controle* > *NetIQ eDirectory Services*
2. Na guia *Serviços*, selecione *dhlog.dlm*.
3. Digite o nível de registro na caixa *Parâmetros de inicialização*.

   Por exemplo, para definir o nível de registro para `LogErr` e acima, digite:

   ```
   LogLevels=LogErr
   ```
4. Clique em *Configurar*
5. Na guia *ACS Config*, clique no sinal de mais do *DHostLogger*.

   O parâmetro `LogLevel` é atualizado com o valor configurado.

Especificando o nome e o caminho do arquivo de registro

1. Clique em *Iniciar* > *Configurações* > *Painel de Controle* > *NetIQ eDirectory Services*
2. Na guia *Serviços*, selecione *dhlog.dlm*.
3. Digite o caminho do arquivo de registro em *Parâmetros de inicialização* da seguinte maneira:

   ```
   LogFile=file_path
   ```

   Por exemplo, para definir o caminho do arquivo de registro para `/tmp/Err.log`, digite o seguinte nos parâmetros de inicialização:

   ```
   LogFile=/tmp/Err.log
   ```
4. Clique em *Configurar*
5. Na guia *ACS Config*, clique no sinal de mais do *DHostLogger*.

   O parâmetro `LogFile` é atualizado com o valor configurado.

Especificando o tamanho do arquivo de registro

1. Clique em *Iniciar* > *Configurações* > *Painel de Controle* > *NetIQ eDirectory Services*
2. Na guia *Serviços*, selecione *dhlog.dlm*.
3. Digite o caminho do arquivo de registro em *Parâmetros de inicialização* da seguinte maneira:

   ```
   LogSize=size
   ```

   O tamanho padrão do arquivo é 1 MB.
4. Clique em *Configurar*
5. Na guia *ACS Config*, clique no sinal de mais do *DHostLogger*.

   O parâmetro `LogSize` é atualizado com o valor configurado.

16.3 Mensagens DSTrace

Você pode filtrar as mensagens de rastreio com base no ID da thread, ID da conexão e gravidade das mensagens.

Após especificar um filtro para as mensagens, apenas aquelas que forem compatíveis com o filtro serão exibidas na tela. Todas as demais mensagens para as tags habilitadas serão registradas no `ndstrace.log` se o arquivo estiver definido para LIGADO.

Apenas um filtro é aplicável por vez. O filtro deve ser especificado para cada sessão do DSTrace.

Por padrão, o nível de gravidade é definido para INFO, o que significa que todas as mensagens com nível de gravidade superior a INFO serão exibidas. Você pode ver o nível de gravidade ao habilitar a tag `svty`.

Você também pode usar o iMonitor para filtrar as mensagens de rastreio. Para obter mais informações, consulte o Seção 16.4, “Filtragem de mensagens do iMonitor” na página 78.

16.3.1 Linux

Execute o procedimento a seguir para filtrar as mensagens de rastreio:

1. Habilite a filtragem com o seguinte comando:

   ```
   ndstrace tag filter_value
   ```

   Para desabilitar a filtragem, digite o seguinte comando:

   ```
   ndstrace tag
   ```

   Exemplos de filtragem habilitada:

   - Para habilitar a filtragem para o ID de thread 35, digite o seguinte:

     ```
     ndstrace thrd 35
     ```

   - Para habilitar a filtragem para o nível de gravidade fatal, digite o seguinte:

     ```
     ndstrace svty fatal
     ```

     Os níveis de gravidade podem ser `FATAL`, `WARN`, `ERR`, `INFO` e `DEBUG`.

   - Para habilitar a filtragem para o ID de conexão 21, digite o seguinte:

     ```
     ndstrace conn 21
     ```

   Exemplos de filtragem desabilitada:

   - Para desabilitar a filtragem baseada em ID de thread, digite o seguinte:

     ```
     ndstrace thrd
     ```

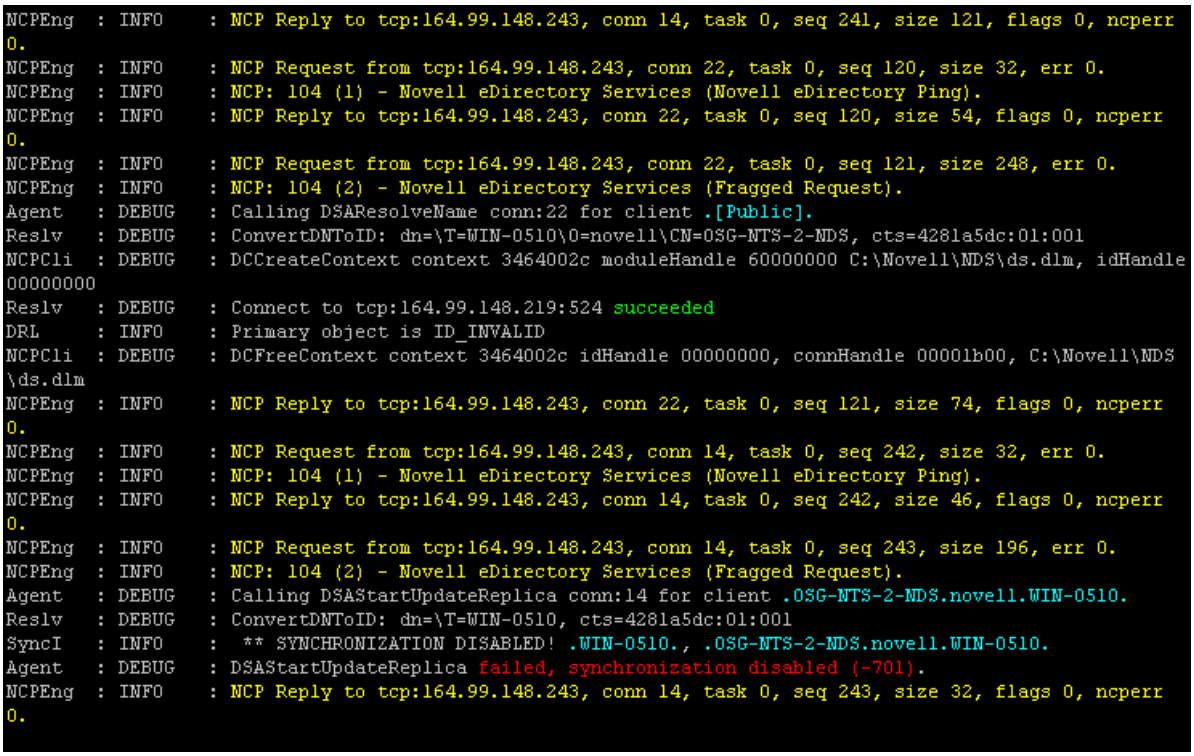
   - Para desabilitar a filtragem baseada em ID de conexão, digite o seguinte:

     ```
     ndstrace conn
     ```

   - Para desabilitar a filtragem baseada em gravidade, digite o seguinte:

     ```
     ndstrace svty
     ```

Figura 16-1 *Exemplo de tela de mensagem de rastreio com filtros*



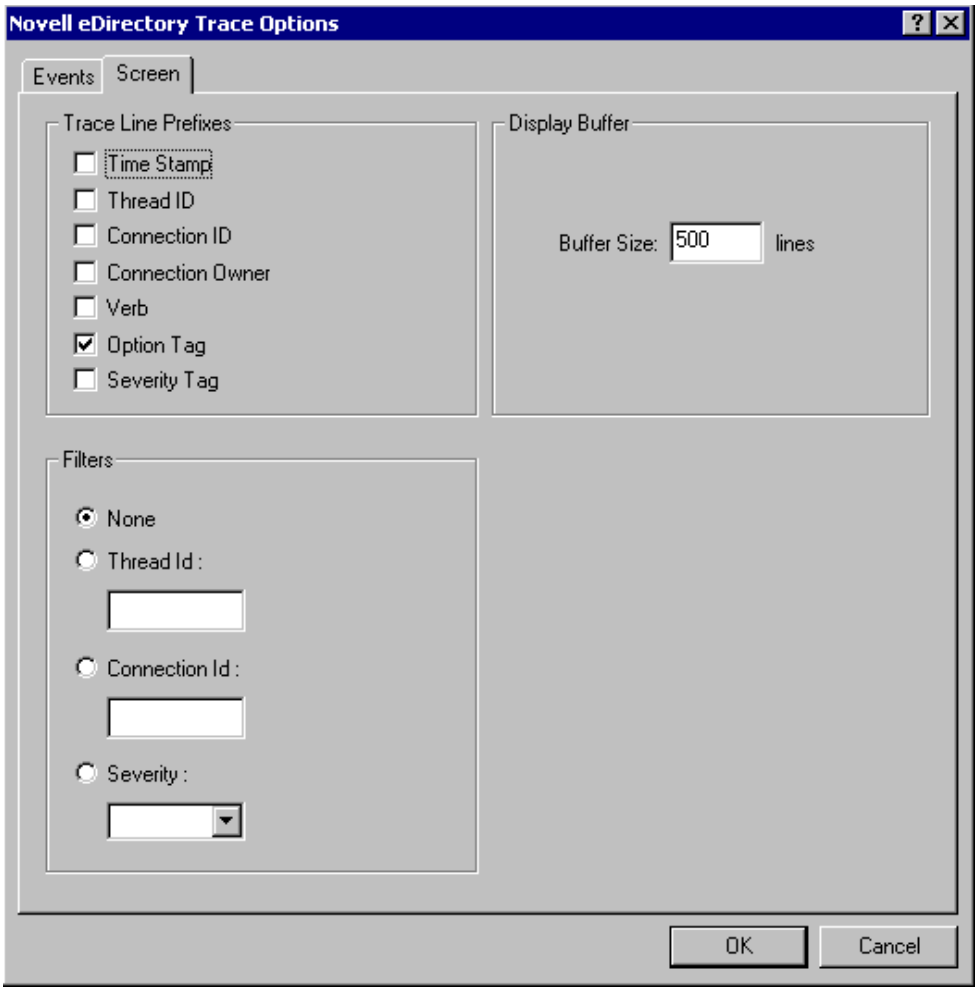
16.3.2 Windows

Execute o procedimento a seguir para filtrar as mensagens de rastreio:

1. Selecione *Iniciar* > *Painel de controle* > *NetIQ eDirectory Services*
2. Na guia *Serviços*, selecione *dstrace.dlm*.
3. Clique em *Editar* > *Opções* na janela de Rastreio.

   A caixa de diálogo de Opções de rastreio do NetIQ eDirectory é exibida.

Figura 16-2 *Tela de opções de rastreio no Windows*



4 Clique na guia *Tela*.

5 Selecione a opção do filtro no grupo *Filtros* e digite o valor do filtro.

Você pode filtrar as mensagens com base em:

- ID do Processo
- ID da Conexão
- Gravidade

Antes de selecionar qualquer filtro, certifique-se de que ele esteja habilitado em *Prefixos de linha de rastreio*.

Você também pode desabilitar a filtragem ao selecionar *Nenhum* ou desmarcar a opção de filtro.

Observação: Se você selecionou *ID de thread* ou *ID de conexão* como sua opção de filtro e digitou um valor que não existe, as mensagens não serão exibidas na tela. Contudo, todas as demais mensagens ainda serão registradas no arquivo `ndstrace.log`.

16.4 Filtragem de mensagens do iMonitor

Você pode filtrar as mensagens de rastreio do iMonitor com base no ID de conexão, ID de thread ou número de erro.

Para filtrar com base no ID de Conexão e de Processo, certifique-se de ter habilitado os mesmos na guia Configuração do rastreamento.

Para obter mais informações, consulte a ajuda online do iMonitor.

16.5 Filtragem de mensagens de SAL

O SAL foi aprimorado para registrar informações abrangentes sobre os erros quando solicitado. As chamadas de função podem ser rastreadas com argumentos nas builds de depuração.

16.5.1 Configurando os níveis de gravidade

Você pode usar o parâmetro `SAL_LogLevels` para configurar os níveis de gravidade das mensagens do SAL. O `SAL_LogLevels` é uma lista separada por vírgulas dos níveis de registro desejados.

Os níveis de registro são explicados na tabela abaixo:

Tabela 16-1 *Parâmetros de filtragem de mensagens de SAL*

Nome do parâmetro	Descrição
`LogCrit`	Mensagens críticas. Este nível é habilitado por padrão. Após um erro crítico ser registrado, o sistema é desligado.
`LogErr`	Todas as mensagens de erro. O sistema continua a funcionar, porém os resultados são imprevisíveis.
`LogWarn`	Mensagens de aviso. Este é apenas um aviso para que você esteja ciente de um erro iminente.
`LogInfo`	Mensagens informativas.
`LogDbg`	Mensagens de depuração usadas no momento do desenvolvimento. Essas mensagens são compiladas de um build da versão para reduzir o tamanho binário.
`LogCall`	Rastreia as chamadas de função. Estas são um subconjunto das mensagens de depuração.
`LogAll`	Habilita todas as mensagens, exceto `LogCall`.

Um "-" no início de um nível de registro específico desabilita este nível.

Exemplos

Para filtrar com base em todos os níveis de registro, exceto `LogInfo` e `LogDbg`, execute as seguintes etapas:

Linux

1. Para o `ndsd`.
2. Digite o seguinte comando:

   ```
   export SAL_LogLevels=LogAll,-LogInfo,-LogDbg
   ```

3. Inicie o `ndsd`.

Windows

1. Desligue o `DHost`.
2. Digite o seguinte comando no prompt de comando:

   ```
   set SAL_LogLevels=LogAll,-LogInfo,-LogDbg
   ```

   ```
   c:\novell\nds>dhost.exe /datadir=c:\novell\nds\DIBFiles\
   ```

3. Reinicie o `DHost`.

16.5.2 Definindo o caminho do arquivo de registro

Você pode usar a variável do ambiente `SAL_LogFile` para especificar o local do arquivo de registro. Este poderá ser um nome de arquivo válido com um caminho válido ou um dos seguintes.

- Console: todas as mensagens são registradas no console.
- Syslog: no Linux, as mensagens vão para o syslog. No Windows, as mensagens são registradas em um arquivo com o nome syslog. Este é o comportamento padrão de registro.

  Todos os erros críticos sempre são registrados no syslog exceto se especificamente desabilitado.

17 Utilitário em massa offline: ldif2dib

O ldif2dib é um novo utilitário introduzido no NetIQ eDirectory 8.8 para dados em massa vindos de arquivos LDIF para o banco de dados do eDirectory. Ele é um utilitário offline e atinge maior velocidade em massa em comparação com outras ferramentas online.

A tabela a seguir lista as plataformas que suportam o ldif2dib.

Recurso	Linux	Windows
ldif2dib	✓	✓

17.1 Necessidade de ldif2dib

O utilitário ldif2dib é necessário quando um grande banco de dados precisa ser preenchido com entradas de um arquivo LDIF. Ferramentas online como ice ou ldapmodify são mais lentas que o ldif2dib neste aspecto, devido aos overheads associados à massa online como verificação de esquemas, tradução de protocolo e verificações de controle de acesso. O ldif2dib permite atingir um rápido tempo ativo quando um grande banco de dados precisa ser preenchido e quando o tempo de inatividade inicial não é um problema.

17.2 Para obter mais informações

Para obter mais informações sobre este utilitário, consulte "Utilitário em massa offline" no *Guia de Administração do NetIQ eDirectory 8.8 SP8*.

18 Backup do eDirectory com SMS

O Novell Storage Management Services (SMS) é uma metodologia API repleta de aplicativos de backup para fornecer uma solução de backup completa. A metodologia SMS é implementada em dois componentes principais:

- SMDR (Storage Management Data Requester)
- TSA (Target Service Agent)

O TSA para o eDirectory (`tsands`) atende a alvos do eDirectory e fornece uma implementação do Novell Storage Management Services API para as árvores de diretório. Os aplicativos podem ser gravados sobre o `SMS API` para oferecer uma solução de backup completa.

O TSA para NDS é suportado no Linux.

19 Auditoria de LDAP

A auditoria é uma das funcionalidades primárias que interessará a um administrador ao avaliar um diretório. O mecanismo de eventos do eDirectory facilita sua auditoria. Devido à grande adoção do protocolo LDAP pelos aplicativos para acessar diretórios, a exigência de operações de auditoria de LDAP tem se tornado cada vez mais predominante.

Este capítulo consiste nas seguintes seções:

19.1 Necessidade de auditoria de LDAP

Este mecanismo de eventos era notavelmente ausente no servidor LDAP do eDirectory existente, que não fornecia informações de LDAP suficientes. Embora o sistema de eventos de NDS gere eventos para todas as operações do eDirectory, a maioria destas informações era insuficiente ou irrelevante para um aplicativo auditar o servidor LDAP. Informações como detalhes de protocolo e de vinculação, endereço de rede, métodos de autenticação, tipos de autenticação, pesquisa de LDA e detalhes de transação, entre tantas outras informações vitais para uma auditoria do servidor LDAP, não estavam disponíveis nos eventos NDS. Os desenvolvedores de aplicativos achavam difícil programar aplicativos de auditoria de LDAP com base nesses eventos.

Como o LDAP é uma importante interface do eDirectory, a fim de oferecer um mecanismo para aplicativos de auditoria do servidor LDAP do eDirectory, foi introduzido um novo subsistema de eventos na versão NetIQ eDirectory 8.8 SP3. Este subsistema gera eventos LDAP específicos com todas as informações relevantes para um aplicativo auditar o servidor LDAP. Isto é conhecido como auditoria de LDAP.

19.2 Usando a auditoria de LDAP.

A auditoria de LDAP permite aos aplicativos monitorar/auditar operações de LDAP como Adição, Modificação e Pesquisa, entre outros, além de obter informações úteis do servidor LDAP como informações de conexão, IP do cliente ao qual o servidor esteve conectado no momento da operação de LDAP, o ID de mensagem, o código resultante da operação e assim em diante.

A auditoria de LDAP pode ser exercida através das Bibliotecas NDK LDAP para C (http://developer.novell.com/documentation/cldap/ldaplibc/data/hevgtl7k.html), que fornecem interface no lado do cliente para este recurso através das novas estruturas e eventos de LDAP.

19.3 Para obter mais informações

Consulte os itens a seguir para obter mais informações sobre eventos de auditoria de LDAP:

- "Configurando serviços de LDAP no NetIQ eDirectory"no *Guia de Administração do NetIQ eDirectory 8.8 SP8*.
- Ferramentas NDK: LDAP (http://developer.novell.com/documentation/cldap/ltoolenu/data/hevgtl7k.html) na documentação das bibliotecas LDAP para C.

Para ver mais informações sobre as ferramentas LDAP, consulte Bibliotecas LDAP para C (http://developer.novell.com/ndk/doc/cldap/index.html?ldaplibc/data/a6eup29.html).

20 Auditoria com XDASv2

A especificação XDASv2 fornece uma classificação padronizada para eventos de auditoria. Ela define um conjunto de eventos genéricos em um nível de sistema globalmente distribuído. A XDASv2 fornece um formato de registro de auditoria portátil e comum para facilitar a fusão e análise de informações de auditoria a partir de múltiplos componentes no nível de sistema distribuído. Os eventos XDASv2 são encapsulados em um sistema de notação hierárquica que ajuda a estender o conjunto de identificador de eventos padrão ou existente.

Com o eDirectory 8.8 SP8, se o agente XDASv2 não puder se comunicar com o servidor syslog, poderá ser configurado para armazenar localmente os eventos de auditoria registrados, garantindo que os dados de auditoria não sejam perdidos. O agente tenta, então, reenviar os eventos de auditoria armazenados, continuando até que a comunicação seja restabelecida. O armazenamento de eventos XDAS é desabilitado por padrão.

Para obter mais informações, consulte o *Guia de Administração do NetIQ XDASv2*.

21 Diversos

Este capítulo aborda recursos novos diversos do NetIQ eDirectory 8.8.

21.1 Gerador de relatórios de dump de cache do iMonitor

A página de cache de alteração no iMonitor exibe apenas um objeto por vez, o que dificulta navegar pelo cache de alteração completo. O eDirectory 8.8 SP8 adiciona um novo relatório de dump de cache de alteração aos relatórios padrão incluídos no iMonitor. Com este relatório, você poderá visualizar todo o cache de uma vez. Este relatório pode ajudar um administrador a compreender melhor as alterações que ocorrem em um servidor específico.

Ao executar um Relatório de dump de cache de alteração, o iMonitor também gera um dump de XML total de todos os objetos no cache, juntamente com os atributos e valores que precisam ser sincronizados entre os servidores.

Para obter mais informações sobre os relatórios do iMonitor, consulte o *Guia de Instalação do NetIQ eDirectory 8.8 SP8*.

21.2 Suporte à sintaxe de número inteiro grande da Microsoft no iManager

O eDirectory 8.8 SP8 fornece uma nova sintaxe para suportar a sintaxe de número inteiro grande da Microsoft. Essa sintaxe pode ser usada para armazenar valores de inteiros grandes ou datas anteriores a 1970 ou além de 2038. Você pode usar o LDAP ou o iManager para criar ou gerenciar os atributos com esta sintaxe.

Observação: O eDirectory usa sua sintaxe existente e valores de 32 bits para marcadores de data e hora internos.

21.3 Armazenamento em cache de objeto de segurança

O contêiner de segurança é criado a partir da partição raiz quando o primeiro servidor é instalado na árvore e contém informações como dados globais, políticas e chaves de segurança.

Após a introdução da senha universal, sempre que um usuário efetuava login no eDirectory pelo NMAS, este acessava as informações no contêiner de segurança para autenticar o login. Quando a partição que possuía o contêiner de segurança não estava presente localmente, o NMAS acessava o servidor, que possuía esta partição. Isto representava um impacto adverso no desempenho da autenticação do NMAS. A situação agravava-se ainda mais em cenários onde o servidor que continha a partição que possuía o contêiner de segurança precisava ser acessado por links de WAN.

Para resolver isto, no eDirectory 8.8, os dados do contêiner de segurança são armazenados no servidor local. Portanto, o NMAS não precisa acessar o contêiner de segurança localizado em uma máquina diferente sempre que um usuário efetuar login, ele pode acessá-lo localmente com facilidade. Isto melhora o desempenho. Adicionar a partição que possui o contêiner de segurança ao servidor local melhora o desempenho, porém pode não ser viável em cenários com muitos servidores.

Se os dados reais do contêiner de segurança mudarem no servidor que possui a partição do contêiner de segurança, o cache local é atualizado por um processo em segundo plano chamado backlinker. Por padrão, o backlinker é executado a cada treze horas, obtendo os dados modificados do servidor remoto. Caso os dados precisem ser sincronizados imediatamente, é possível programar o backlinker no servidor local pelo iMonitor, ndstrace no Linux ou ndscons no Windows. Para obter mais informações, consulte a ajuda online do iMonitor ou a página de manual do ndstrace.

O recurso de armazenamento em cache do objeto de segurança é habilitado por padrão. Se você não desejar que o backlinker armazene nenhum dado, remova `CachedAttrsOnExtRef` do objeto do servidor do NCP.

21.4 Melhoria de desempenho na pesquisa de subárvore

O desempenho de pesquisa de subárvore do eDirectory para uma árvore grande com uma estrutura significativamente aninhada permanece simples independentemente do DN base da pesquisa. Isto foi resolvido usando um atributo `AncestorID`. O atributo `AncestorID` é uma lista de IDs de entrada de todos os antepassados associados a cada entrada. Este atributo `AncestorID` é usado internamente durante a pesquisa de subárvore e, portanto, restringe o escopo da pesquisa.

Este atributo é preenchido com a adição de entradas e após o upgrade de todas as entradas no DIB, sendo repreenchido para todas as entradas na subárvore após esta ser movida. Contudo, uma pesquisa de subárvore não usará o atributo `AncestorID` ao preencher o atributo após um upgrade ou mudança de subárvore. Portanto, o desempenho da subárvore permanece semelhante ao desempenho de pesquisa de subárvore anterior ao eDirectory 8.8.

Para confirmar se os `AncestorIDs` foram atualizados após um upgrade:

Depois de os `AncestorIDs` serem preenchidos, a versão de upgrade de objeto do NDS muda para 6 ou mais. Você pode ver isto usando o iMonitor na seção *Histórico de DIB* de Informações de agente.

Para confirmar se os `AncestorIDs` foram atualizados após uma operação de mudança de subárvore:

Enquanto os `AncestorIDs` estão sendo preenchidos, o atributo`UpdateInProgress` no objeto `Pseudo Server` possui a lista de IDs de entrada da partição Raiz da subárvore. Após os `AncestorIDs` serem preenchidos, o atributo não estará presente no `Pseudo Server`.

O DSRepair atualizará o atributo `AncestorID` se este for inválido.

21.5 Mudanças de host local

Os servidores do eDirectory 8.8 não escutam endereços de loopback. Os utilitários que usam host local precisam ser alterados para usar o nome do host ou a resolução de endereço IP.

Se uma ferramenta ou um utilitário de terceiros resolver por meio do host local, ele(a) deverá ser alterado(a) para resolver por meio de um nome de host ou um endereço IP e não por meio do endereço do host local.

21.6 Sub-rotina de arquivo 256 no Solaris

A implementação do anterior, Solaris 2.*x* stdio streams podia usar apenas um máximo de 256 descritores de arquivos. Isto não era suficiente para o eDirectory funcionar corretamente. O eDirectory 8.8 oferece uma biblioteca de referência para ultrapassar este limite.

21.7 Gerenciador de memória no Solaris

As versões anteriores do eDirectory no Solaris usavam o Geodesic*, um produto de outra empresa, como gerenciador de memória. Nesta versão, o eDirectory 8.8 não inclui qualquer alocador de memória de outras empresas, mas sim utiliza o gerenciador de memória nativo.

Isto não possui qualquer impacto sobre o desempenho do eDirectory. Na maioria dos casos, o desempenho melhorou ou permaneceu o mesmo de alocadores de outras empresas.

21.8 Grupos aninhados

O eDirectory 8.8 SP2 suporta agrupamentos de grupos, fornecendo uma forma de agrupamento mais estruturada. Este recurso é chamado Grupos aninhados. Atualmente, o aninhamento é permitido para grupos estáticos.

O aninhamento pode possuir múltiplos níveis, até o máximo de 200.

Para obter mais informações sobre grupos aninhados, consulte o *Guia de Administração do NetIQ eDirectory 8.8 SP8*.