Identity Console
Guia de administração

Setembro de 2022

Informações legais

Para saber mais sobre informações legais, marcas registradas, isenções de responsabilidades, garantias, exportação e outras restrições de uso, direitos restritos do Governo dos EUA, política de patente e conformidade de FIPS, consulte https://www.netiq.com/company/legal.

Índice

Sobre este manual e a biblioteca

O *Guia de Administração* fornece informações conceituais sobre o produto Identity Console (NetIQ Identity Console). Este manual define a terminologia e inclui cenários de implementação.

Para a versão mais atual do *Guia de Administração do NetIQ Identity Console*, consulte a versão em inglês da documentação no site de documentação online do NetIQ Identity Console.

Público-alvo

Este guia é dirigido a administradores de rede.

Outras informações na biblioteca

A biblioteca fornece os seguintes recursos informativos:

Installation Guide (Guia de Instalação)

Descreve como instalar o Identity Console. Ele é dirigido aos administradores de rede.

Sobre a NetIQ Corporation

Nós somos uma empresa global de software corporativo com foco nos três desafios constantes do seu ambiente — mudança, complexidade e risco — e em como podemos ajudar você a 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 a seus investimentos existentes, de suporte contínuo e treinamento pós-implantação, além de alguém com quem a colaboração 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 **Add Comment** (Adicionar Comentário) na parte inferior de qualquer página nas versões em HTML da documentação publicada em https://www.netiq.com/pt-br/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 uma 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 O que é o Identity Console?

O Identity Console é um console de administração baseado na Web avançado que fornece acesso virtual, seguro e personalizado aos utilitários de administração de rede de qualquer lugar na Internet e no browser da Web. O Identity Console facilita muito a descentralização das tarefas administrativas.

Recursos do Identity Console

O Identity Console fornece os seguintes recursos:

- Administrando usuários, esquema, partições, réplicas, direitos e objetos do eDirectory, etc.
- Gerenciamento de drivers e conjuntos de drivers do Identity Manager
- Gerenciar e ver as estatísticas de desempenho do driver
- Inspecionando objetos, vendo o fluxo de dados do driver, gerenciando direitos, ordens de serviço etc.
- Gerenciado o status da sincronização de senhas e as configurações para drivers
- Gerenciado políticas de senha e métodos de login
- Gerenciando certificados
- Administrando vários recursos de rede
- Medida de segurança aprimorada para proteger seus dados
- Escalabilidade aprimorada para gerenciar objetos maiores do eDirectory
- Login seguro no portal do Identity Console via One SSO Provider (OSP)
- Desenvolvido com a mais recente tecnologia de interface do usuário da Indústria
- Fácil de instalar e configurar via containers do Docker

2 Como acessar o Identity Console?

Você pode acessar o Identity Console e o conjunto completo de recursos que ele fornece usando qualquer browser da Web com suporte. Embora seja possível acessar o Identity Console em um browser da Web não listado, não garantimos nem suportamos a funcionalidade completa em nenhum browser que não seja oficialmente compatível.

Importante: Para obter mais informações sobre browsers da Web suportados, consulte o *Identity Console Installation Guide* (Guia de Instalação do Identity Console).

Acessando o Identity Console

Para acessar o Identity Console baseado no servidor, siga as etapas a seguir:

1. Digite o seguinte no campo Endereço (URL) de um browser da Web com suporte.

   Login seguro: `https://<server-ip-address/hostname>:<port>/identityconsole/`

   Nos exemplos, o endereço IP em *<server-ip-address>* deve ser IPv4. A porta padrão a ser usada é 9000.
2. Efetue login usando seu DN de usuário e senha.
3. Especifique o IP ou DNS da árvore do eDirectory com ou sem porta segura LDAP.

Observação

- Atualizar qualquer guia no Identity Console fará com que o usuário efetue logout por motivos de segurança.
- Abrir guias duplicadas do Identity Console no browser fará com que o usuário efetue logout por motivos de segurança.
- O DN deve ser especificado no formato `cn=admin,ou=sa,o=system`.
- Quando o eDirectory estiver configurado com uma porta não padrão, você precisará especificar o número da porta.

---

3 Navegando na interface do Identity Console

Esta seção descreve como navegar pela interface da web do Identity Console.

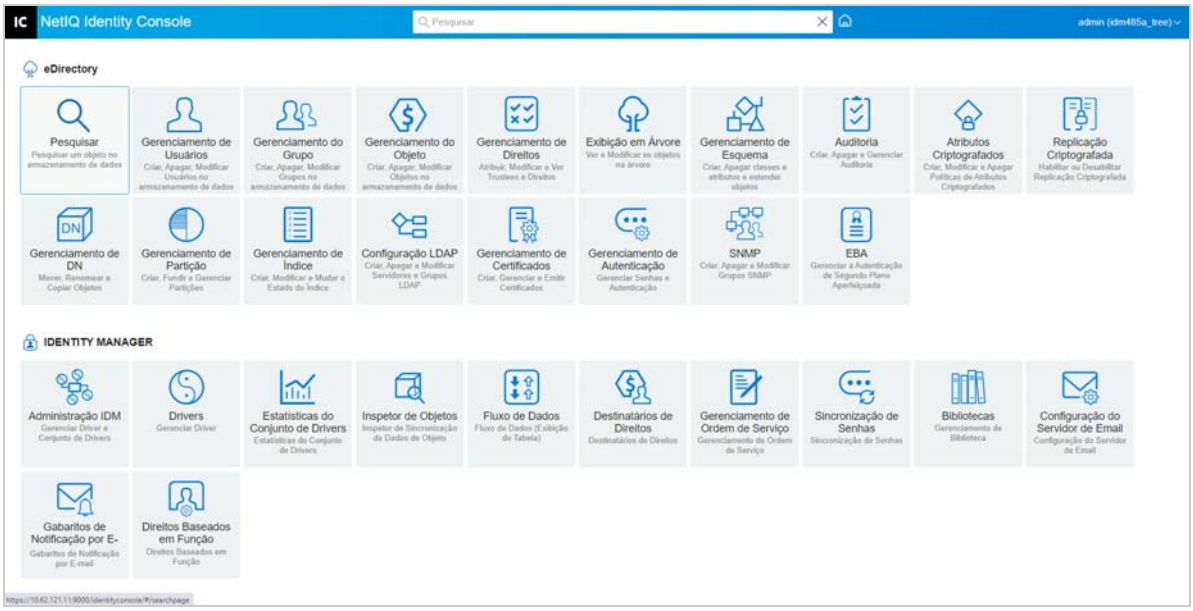
Pesquisa (Versão Prévia de Tecnologia)

A **Pesquisa (Versão Prévia de Tecnologia)** fornece um layout introdutório para a funcionalidade de pesquisa. Nesta visualização, você pode especificar palavras-chave e o campo de pesquisa determina a fonte de informações para pesquisar e exibir resultados correspondentes. Ao utilizar esta opção, você pode procurar um recurso e acessá-lo com facilidade em qualquer página do aplicativo Identity Console.

Interface do Identity Console

A Interface do Identity Console é composta por módulos do eDirectory e do Identity Manager.

Figura 3-1 *Interface do Identity Console*



Importante: Várias animações em GIF usadas neste guia funcionam somente com a documentação Online. Caso decida mudar para o PDF, apenas as capturas de tela ficarão visíveis.

Tabela 3-1 *Explicação de vários módulos do Portal Web do Identity Console*

Nome do módulo	Descrição
Pesquisar	Pesquisar por um objeto no armazenamento de dados. Para obter mais informações, consulte o Capítulo 4, “Realizando pesquisas” na página 25.
Gerenciamento de Usuário	Criar, apagar e modificar usuários no armazenamento de dados. Para obter mais informações, consulte Capítulo 5, “Gerenciando usuários” na página 29.
Gerenciamento de grupos	Criar, apagar e modificar grupos no armazenamento de dados. Para obter mais informações, consulte Capítulo 6, “Gerenciando grupos” na página 39.
Gerenciamento de Objeto	Criar, apagar e modificar objetos no armazenamento de dados. Para obter mais informações, consulte o Capítulo 7, “Gerenciando objetos” na página 45.
Gerenciamento de Direitos	Atribuir, modificar e ver trustees e direitos. Para obter mais informações, consulte o Capítulo 8, “Gerenciando direitos” na página 53.
Exibição em árvore	Ver e modificar os objetos na árvore. Para obter mais informações, consulte Capítulo 9, “Exibição em árvore” na página 57.
Gerenciamento de Esquema	Criar e apagar classes, classes auxiliares, atributos e estender objetos. Para obter mais informações, consulte o Capítulo 10, “Gerenciando esquema” na página 61.
Auditoria	Habilitar, desabilitar e gerenciar a auditoria do CEF. Para obter mais informações, consulte o Capítulo 11, “Gerenciando eventos de auditoria” na página 69.
Atributos criptografados	Criar, modificar, apagar e ver a política de atributos criptografados. Para obter mais informações, consulte Capítulo 12, “Gerenciando atributos criptografados” na página 75.
Replicação Criptografada	Habilitar, desabilitar e ver a replicação criptografada. Para obter mais informações, consulte o Capítulo 13, “Gerenciando a replicação criptografada” na página 79.
Gerenciamento de DN	Mover, renomear e copiar objetos. Para obter mais informações, consulte Capítulo 7, “Gerenciando objetos” na página 45.
Gerenciamento de Partição	Criar, fundir e mover partições e réplicas. Para obter mais informações, consulte Capítulo 14, “Gerenciando partições e réplicas” na página 81.
Gerenciamento de Índice	Crie, modifique e mude o estado dos índices. Para obter mais informações, consulte Capítulo 15, “Gerenciando índices” na página 85.

Nome do módulo	Descrição
Configuração do LDAP	Crie, apague e modifique objetos LDAP. Para obter mais informações, consulte Capítulo 16, “Configurando objetos LDAP” na página 89.
Gerenciamento de certificados	Crie e gerencie certificações do servidor e certificados CA. Para obter mais informações, consulte Capítulo 17, “Gerenciando certificados” na página 93.
Gerenciamento de autenticação	Crie e gerencie sequências e métodos de login e pós-login. Você também pode gerenciar políticas de senha e conjuntos de verificação usando este módulo. Para obter mais informações, consulte Capítulo 18, “Gerenciando a Metodologia de Autenticação” na página 111.
SNMP	Crie, apague e modifique grupos SNMP. Para obter mais informações, consulte Capítulo 19, “Gerenciando objetos grupo SNMP” na página 127.
EBA	Gerencie a autenticação em segundo plano aprimorada. Para obter mais informações, consulte Capítulo 20, “Gerenciando a autenticação em segundo plano aprimorada” na página 131.
Administração IDM	Gerencie drivers e conjuntos de drivers do Identity Manager. Para obter mais informações, consulte Capítulo 21, “Gerenciando drivers e conjuntos de drivers” na página 135. Você também pode gerenciar as propriedades do conjunto de drivers usando este módulo. Para obter mais informações, consulte Capítulo 22, “Gerenciando propriedades de conjunto de drivers” na página 141.
Propriedades do driver	Gerencie as propriedades de vários drivers. Para obter mais informações, consulte Capítulo 23, “Gerenciando propriedades do driver” na página 155.
Estatísticas do conjunto de drivers	Gerencie e veja as estatísticas do conjunto de drivers. Para obter mais informações, consulte Capítulo 24, “Gerenciando estatísticas do conjunto de drivers” na página 185.
Objeto Inspetor	Gerencie a associação de objetos e a sincronização de dados. Para obter mais informações, consulte Capítulo 25, “Inspecionando objetos do Identity Manager” na página 187.
Fluxo de dados	Gerencie e veja o fluxo de dados dos drivers. Para obter mais informações, consulte Capítulo 26, “Gerenciando o fluxo de dados” na página 189.
Destinatários de direitos	Gerencie os destinatários de direitos. Para obter mais informações, consulte Capítulo 27, “Gerenciando destinatários de direitos” na página 191.

Nome do módulo	Descrição
Gerenciamento de ordens de serviço	Gerencie as ordens de serviço. Para obter mais informações, consulte Capítulo 28, “Gerenciando ordens de serviço” na página 193.
Sincronização de senhas	Gerencie a sincronização e o status de senhas. Para obter mais informações, consulte Capítulo 29, “Gerenciando status e sincronização de senhas” na página 197.
Gestão de bibliotecas	Gerencie bibliotecas. Para obter mais informações, consulte Capítulo 30, “Gerenciando bibliotecas” na página 201.
Configuração do servidor de e-mail	Gerencie as opções do servidor de e-mail. Para obter mais informações, consulte Capítulo 31, “Gerenciando opções de servidor de e-mail” na página 203
Gabaritos de notificação por e-mail	Gerencie gabaritos de e-mail. Para obter mais informações, consulte Capítulo 32, “Gerenciando gabaritos de e-mail” na página 205

Gerenciamento do eDirectory usando o Identity Console

Esta seção descreve várias tarefas que você pode executar para gerenciar seus servidores do eDirectory usando o portal Identity Console.

4 Realizando pesquisas

A guia Pesquisa permite que você especifique uma operação de pesquisa a ser realizada na árvore do diretório e exiba os resultados. Essa opção permite pesquisar vários objetos, usuários, grupos etc. Para realizar uma operação de pesquisa para vários objetos no armazenamento de dados, siga as etapas a seguir:

1. Especifique o nome do objeto na pesquisa. Use o asterisco (*) como caractere curinga para especificar parte de um nome. Por exemplo: `ldap*`, `*cert`, `*server*` etc. Se você usar apenas asterisco nesse campo, o Identity Console retornará todos os resultados da pesquisa com base no **Tipo** e **Contexto** selecionados.

   Observação: Ao utilizar o Browser de Contexto, você pode pesquisar toda a árvore do eDirectory especificando asterisco (*) no campo de pesquisa. Você também pode filtrar os objetos no Browser de Contexto usando a pesquisa com caractere curinga. Por exemplo, `admin*`. Esse comportamento do Browser de Contexto é suportado em vários módulos no Identity Console.

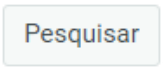
   ---

2. Selecione o tipo de objeto para a pesquisa no campo **Tipo**. O Identity Console exibe somente objetos do tipo especificado. O tipo **Usuário** é selecionado por padrão nesse campo.

   Clique no ícone  para definir configurações de pesquisa de nível de atributo adicionais. Para obter mais informações, consulte “Configurando a pesquisa avançada” na página 26.

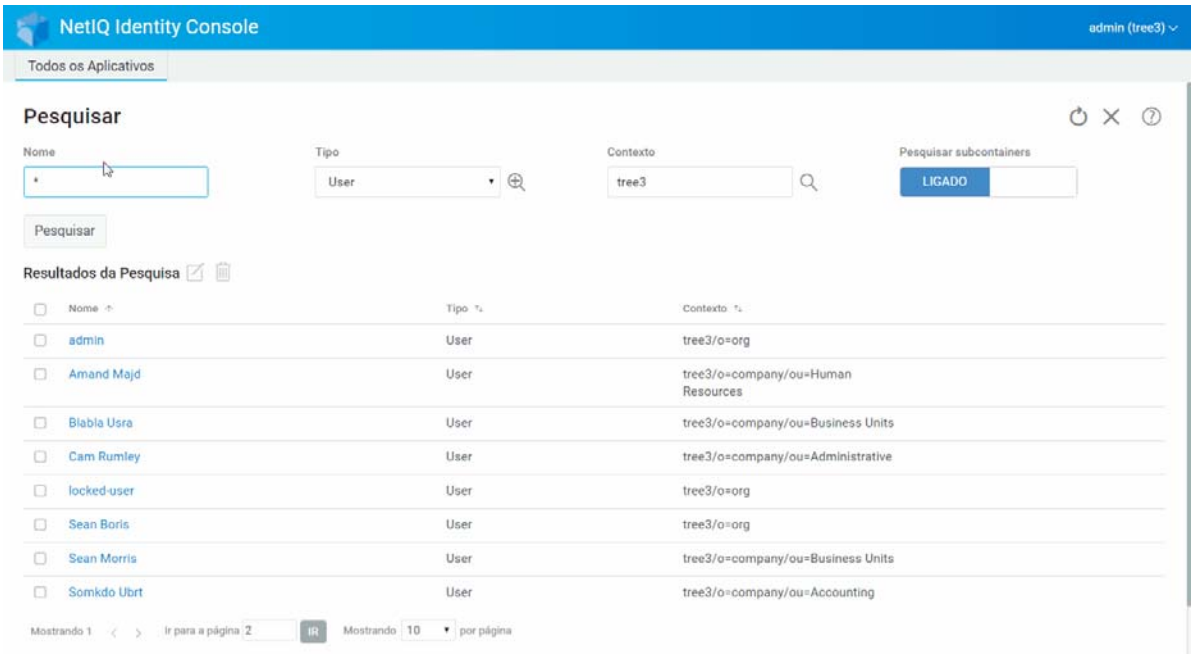
3. Especifique o container inicial para a operação de pesquisa no campo **Contexto**.

4. Se você deseja que a pesquisa inclua containers subordinados, selecione **ATIVADO** para a opção Pesquisar subcontainers.

5. Clique no botão 

.

Figura 4-1 *Executando uma Operação de Pesquisa*



Configurando a pesquisa avançada

A Seleção Avançada fornece um ambiente mais configurável para pesquisar o diretório em busca dos objetos desejados.

Tipo de Objeto: Especifica a classe base do objeto que você esta procurando. Por exemplo, Usuário.

Classes Auxiliares: Clique no ícone + para especificar uma Classe Auxiliar a ser incluída na pesquisa.

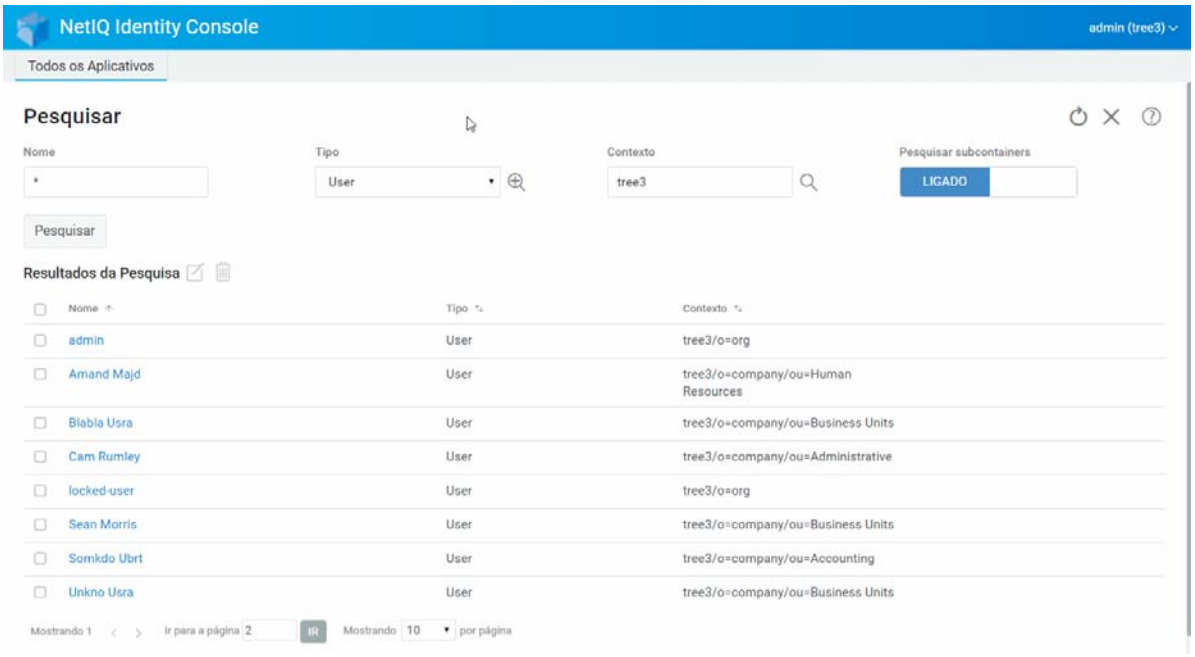
Atributo: Especifica um atributo (propriedade) que você deseja utilizar como parte do filtro.

Operador: Especifica o operador lógico a ser aplicado no filtro. As opções são.

Valor: Especifica o valor de atributo que você está usando como filtro. Você pode usar o asterisco (*) como curinga para indicar parte de um valor. Por exemplo, smi*, *th e *mit*.

Além disso, você pode encadear vários filtros de atributos em um grupo de filtros usando o ícone + Rule para adicionar um segundo atributo à lista. Ao usar vários filtros de atributo, vincule-os com um AND ou OR lógico.

Figura 4-2 *Configurando a pesquisa avançada*



5 Gerenciando usuários

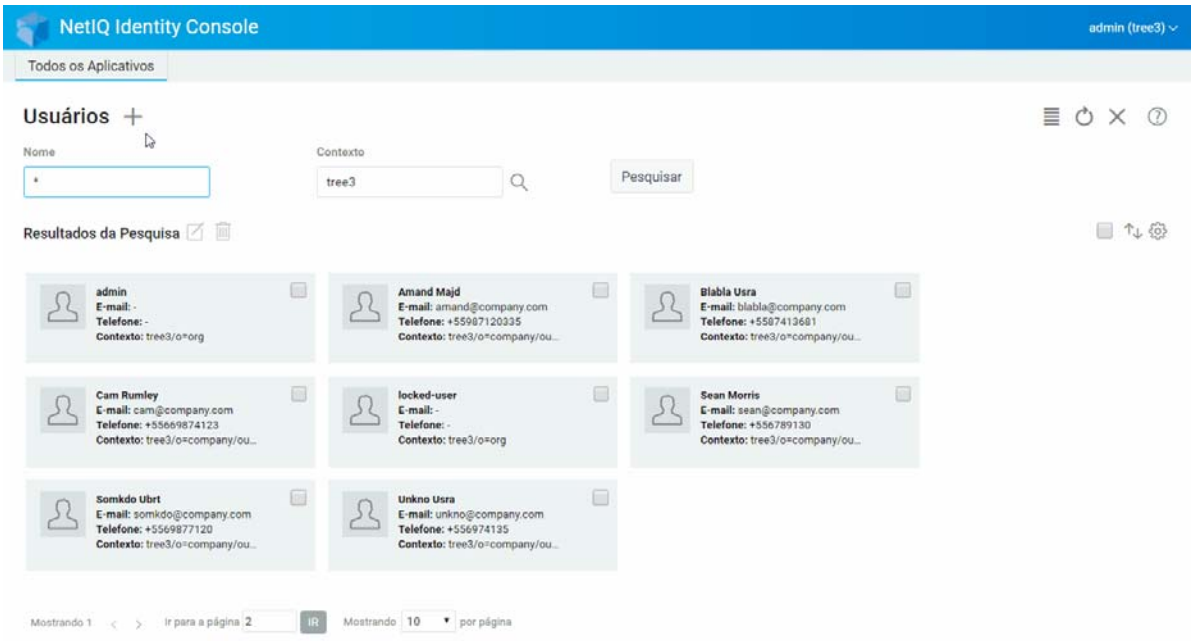
Gerenciar usuários e seu acesso à rede é um objetivo central do armazenamento de dados. Usando o Portal Web do Identity Console, você pode executar as seguintes tarefas relacionadas ao usuário:

Criando um usuário

Para criar um novo objeto Usuário:

1. Clique na opção **Gerenciamento de Usuários** na landing page do Identity Console.
2. Clique no ícone  .
3. Na página Criar Usuário, forneça, no mínimo, as informações relacionadas ao usuário necessárias e clique no botão  .
   - **Nome de Usuário**
   - **Contexto**
   - **Sobrenome**
   - **Senha**
4. Uma confirmação aparece indicando que o objeto Usuário foi criado.

Figura 5-1 *Criando usuários*

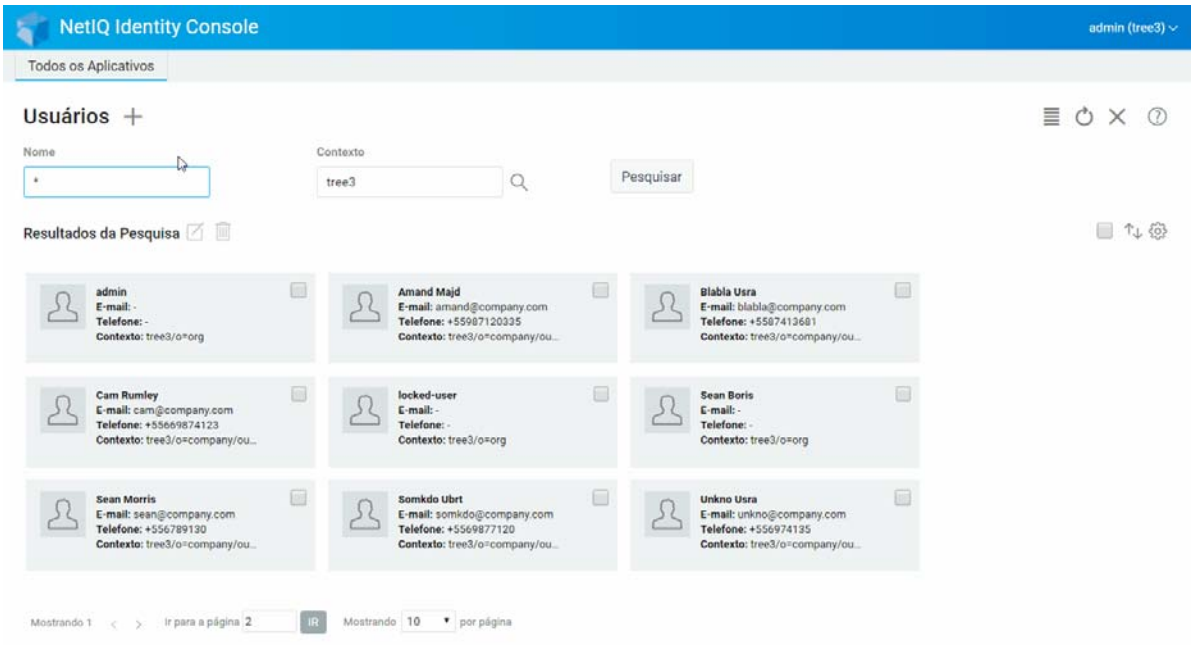


Apagando um usuário

Para apagar um objeto Usuário:

1. Clique na opção **Gerenciamento de Usuários** na landing page do Identity Console.
2. Digite o nome e contexto do objeto ou use o recurso de pesquisa para encontrá-lo e clique no botão Pesquisar.
3. Selecione o objeto Usuário da lista de usuários e clique no ícone 🗑.
4. Aparecerá uma confirmação indicando que o objeto Usuário foi apagado.

Figura 5-2 *Apagando um usuário*

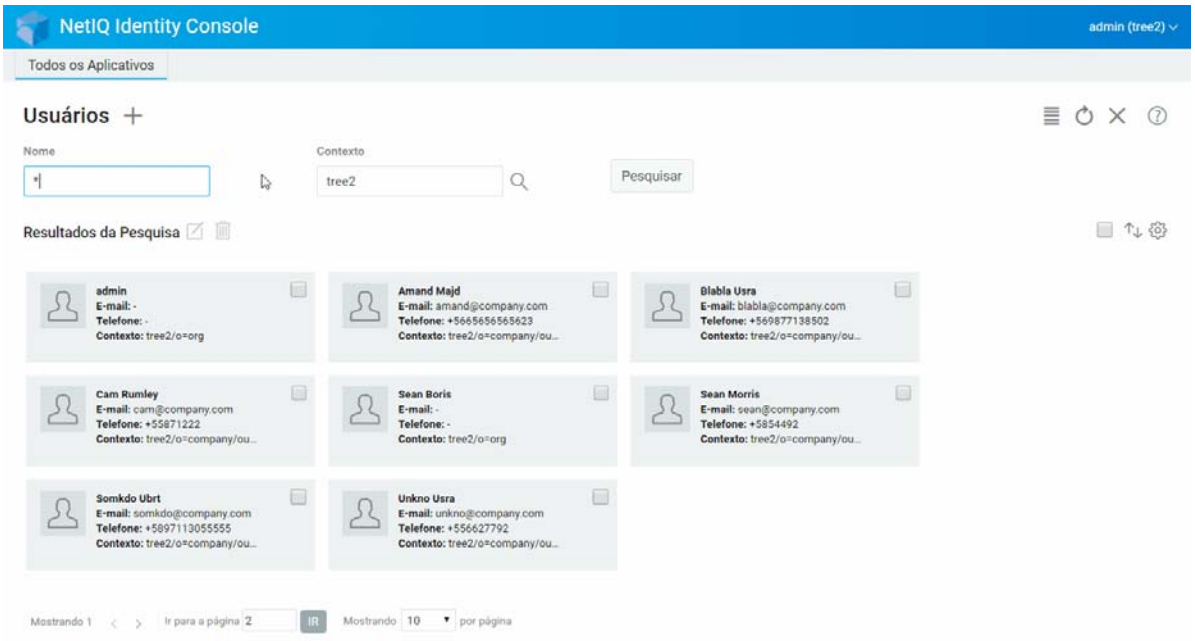


Modificando usuários

Para modificar um objeto Usuário:

1. Clique na opção **Gerenciamento de Usuários** na landing page do Identity Console.
2. Digite o nome e contexto do objeto ou use o recurso de pesquisa para encontrá-lo e clique no botão Pesquisar.
3. Selecione o objeto Usuário da lista de usuários e clique no ícone .
4. Faça suas mudanças e clique no botão Gravar.
5. Uma confirmação aparece indicando que o objeto Usuário foi modificado.

Figura 5-3 *Modificando um usuário*

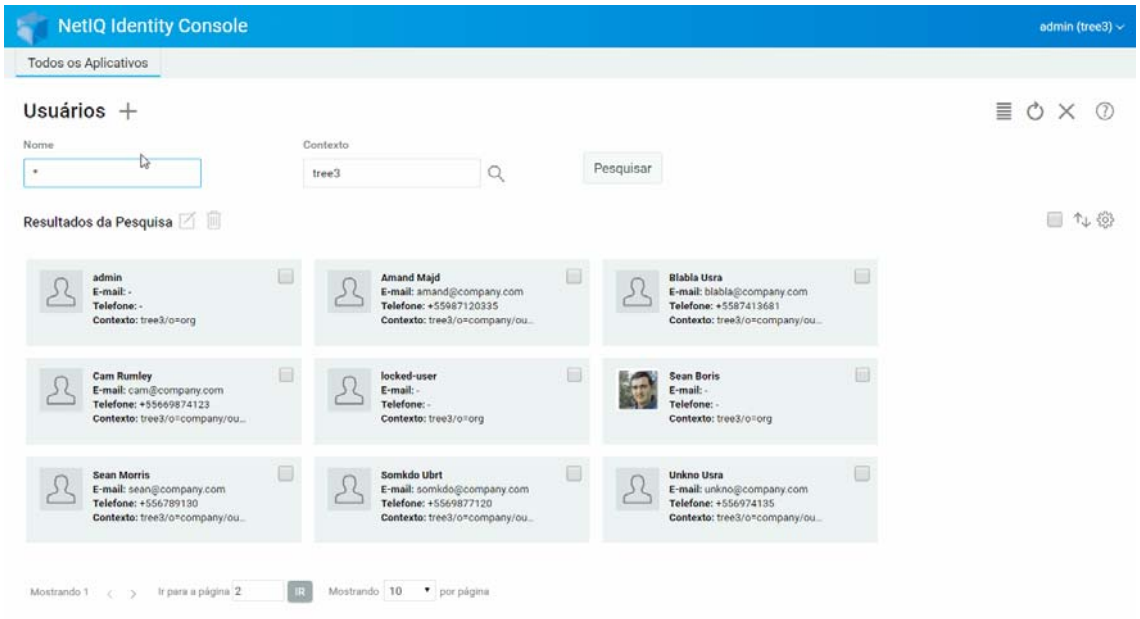


Pesquisando por um usuário

Para pesquisar um objeto Usuário:

1. Clique na opção **Gerenciamento de Usuários** na landing page do Identity Console.
2. Você pode pesquisar um usuário pelo nome ou pelo nome e contexto. Após especificar as informações necessárias, clique no ícone Pesquisar.

Figura 5-4 *Pesquisando um usuário*

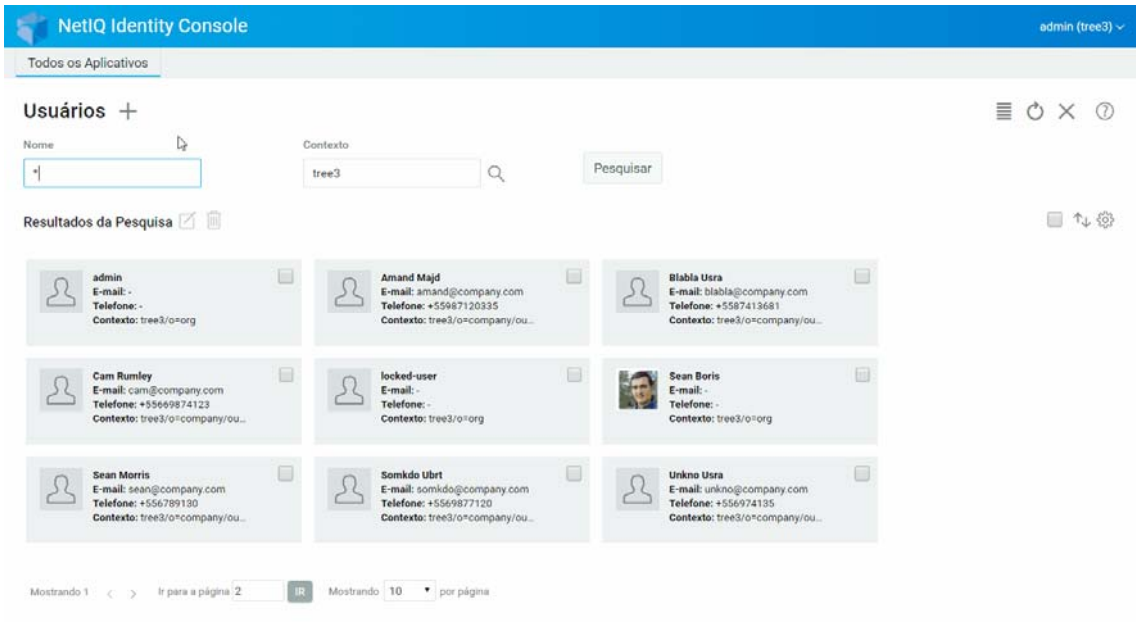


Definindo restrições de senha

As restrições de senha permitem executar as seguintes ações:

- Permitir que os usuários mudem suas respectivas senhas
- Impor uma senha para login
- Especificar a força da senha
- Impor mudança periódica de senha
- Especificar a data de vencimento da senha
- Impor a criação de senha exclusiva
- Especificar o período de login extra, caso a senha tenha expirado.

Figura 5-5 *Restrições de senha*

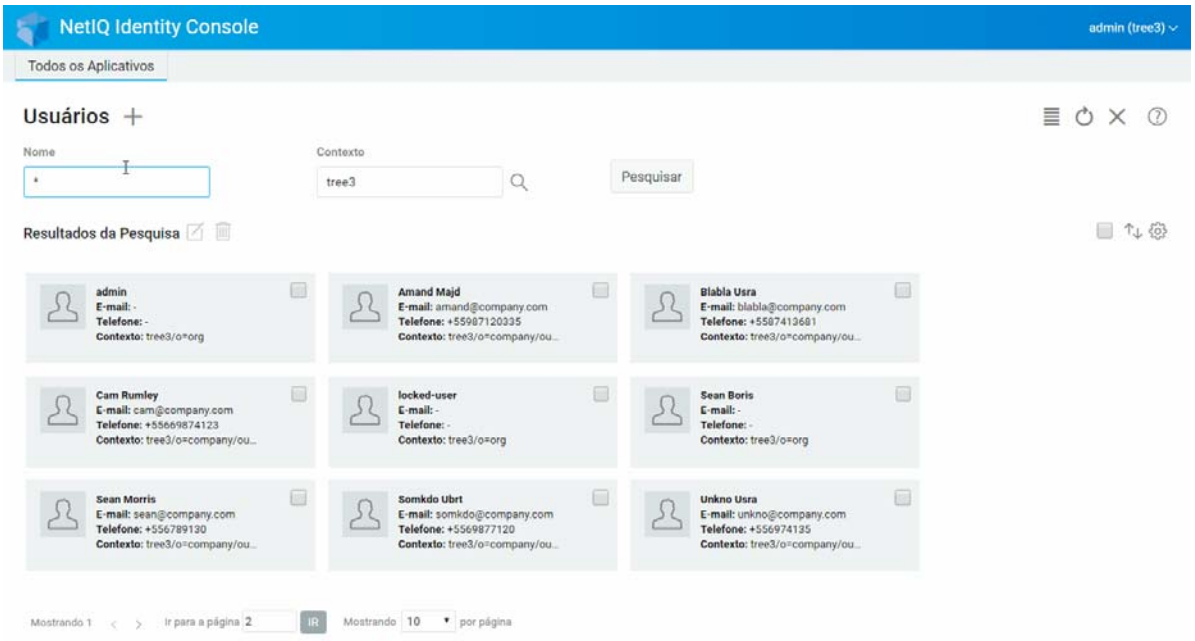


Desabilitando e habilitando uma conta do usuário

Para desabilitar uma conta do usuário, execute as seguintes etapas:

1. Selecione um usuário cuja conta precisa ser desabilitada e clique no ícone .
2. Clique na guia **Restrições** e na página **Modificar Usuário**.
3. Expanda a guia **Restrições de Login** e marque a caixa de seleção **Conta Desabilitada**.
4. Clique no ícone Gravar.
5. Agora, a conta do usuário está desabilitada. Para habilitar qualquer conta do usuário desabilitada, anule a seleção da caixa **Conta Desabilitada**.

Figura 5-6 *Desabilitando e habilitando uma conta do usuário*

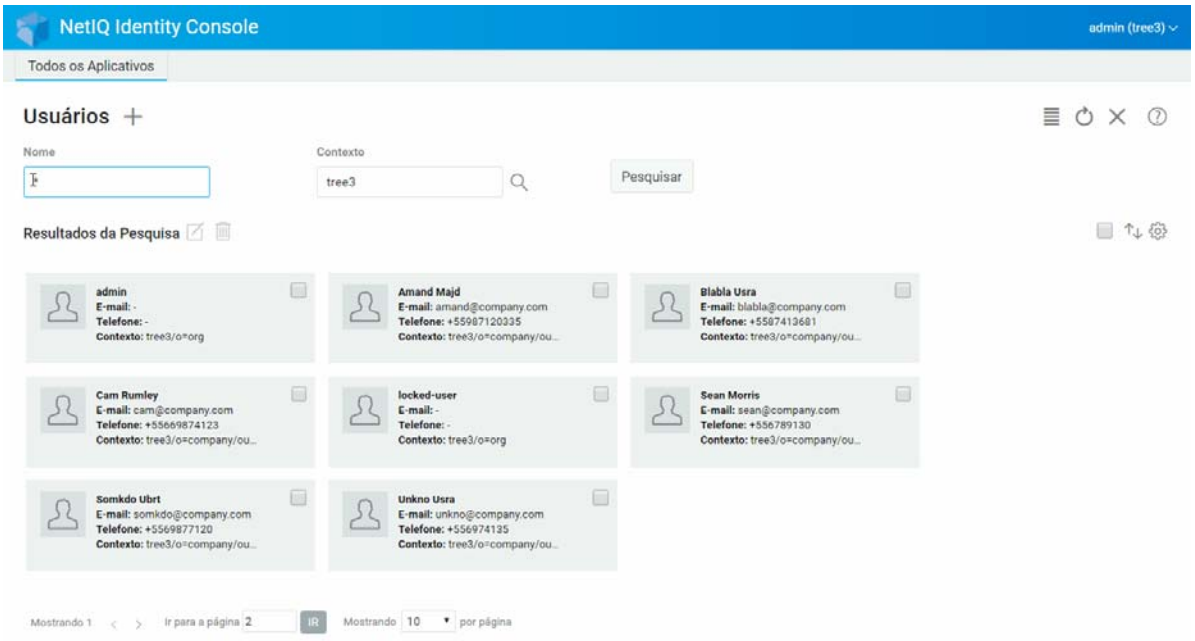


Definindo a data de vencimento da conta

Para definir a data de vencimento da conta para usuários, execute as seguintes etapas:

1. Selecione o usuário cuja data de vencimento da conta precisa ser definida e clique no ícone .
2. Clique na guia **Restrições** e na página **Modificar Usuário**.
3. Expanda a guia **Restrições de Login** e marque a caixa de seleção **Conta com data de vencimento** e especifique a **Data de vencimento**.
4. Clique no ícone Gravar.

Figura 5-7 *Definindo a data de vencimento da conta*

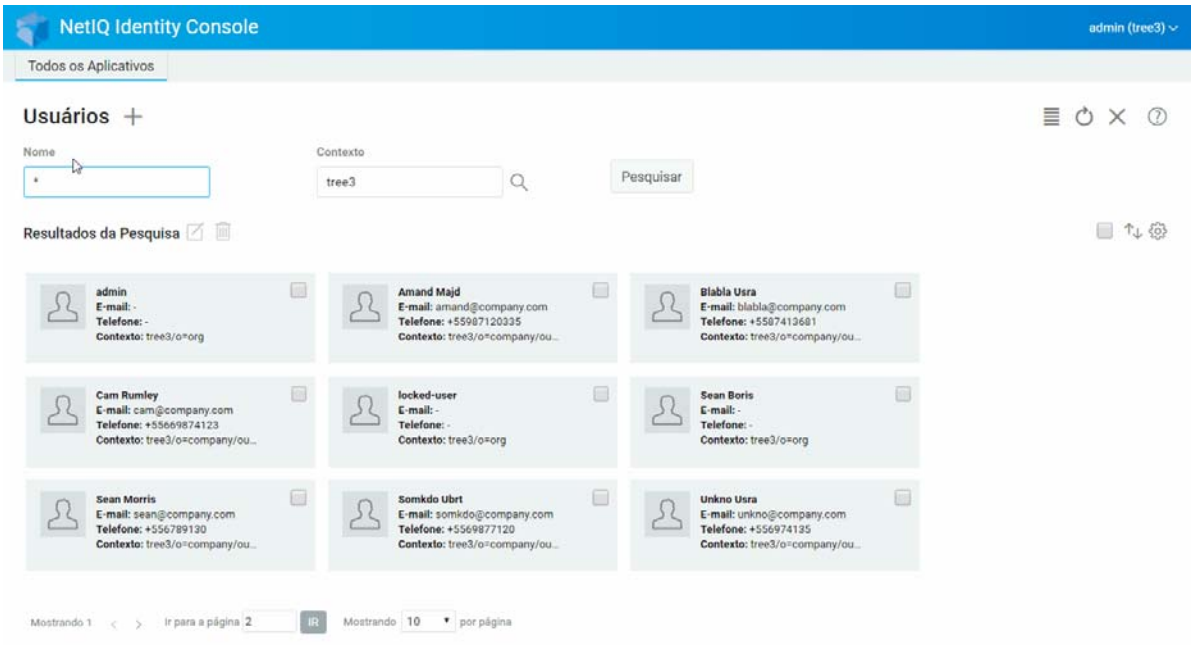


Verificando e limpando o bloqueio de intrusão

Você pode ver mais informações sobre o bloqueio de intrusão para qualquer conta do usuário usando o Portal Web do Identity Console. Para ver mais informações sobre o Bloqueio de Intrusão:

1. Selecione o usuário para o qual as informações do bloqueio de intrusão precisam ser verificadas e clique no ícone .
2. Clique na guia **Restrições** e na página **Modificar Usuário**.
3. Expanda a guia **Bloqueio de Intrusão** e veja as informações do bloqueio de intrusão.
4. Agora selecione a guia **Limpar bloqueio** e clique no botão Limpar Bloqueio.
5. Clique no botão Gravar.

Figura 5-8 *Verificando e limpando o bloqueio de intrusão*



6 Gerenciando grupos

Grupos geralmente contêm um número de membros. Qualquer usuário que cria um grupo torna-se automaticamente o proprietário do grupo. As seguintes operações podem ser executadas usando o recurso de Gerenciamento de Grupos:

Para obter mais informações sobre como usar e configurar objetos Grupo, consulte o *NetIQ eDirectory 9.2 Administration Guide* (https://www.netiq.com/documentation/edirectory-92/edir_admin/data/bookinfo.html) (Guia de administração do NetIQ eDirectory 9.2).

Criando um grupo

Para criar um grupo:

1. Clique na opção **Gerenciamento de Grupos** na landing page do Identity Console.
2. Clique no ícone +.
3. Na página Criar Grupo, digite as seguintes informações:
   - Especifique o nome do grupo
   - Especifique o Contexto

   Selecione **Grupo Dinâmico** para tornar o novo grupo um grupo dinâmico, da classe `dynamicGroup`. Caso contrário, o grupo é criado como um grupo estático.

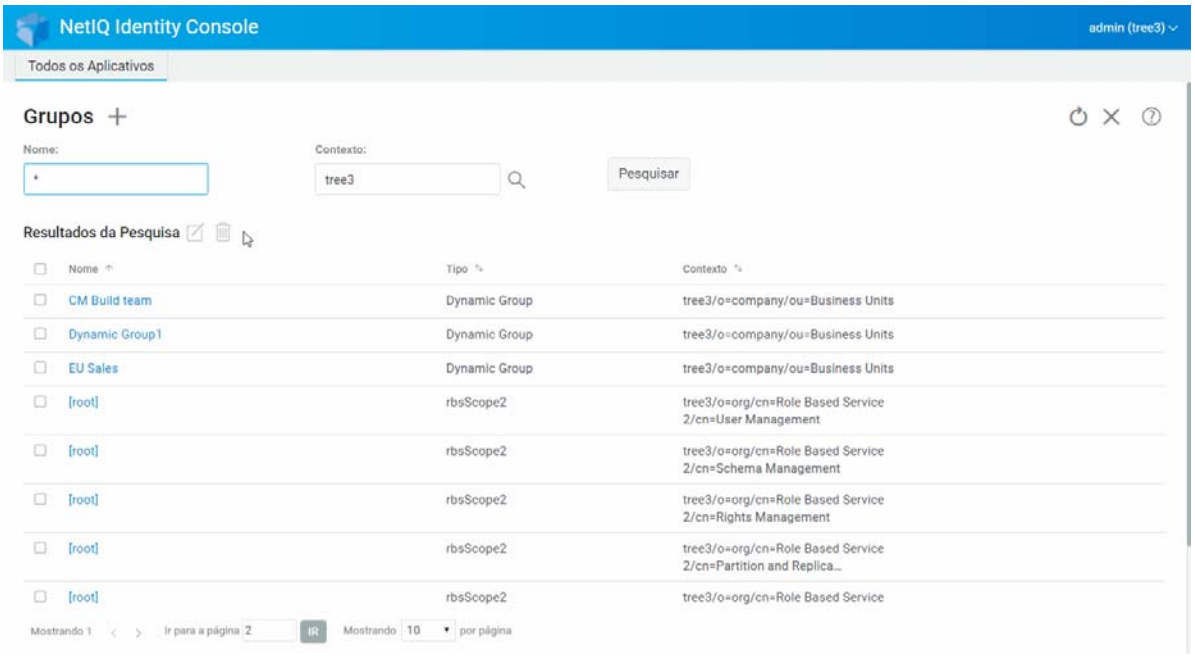
   Selecione **Grupo Aninhado** para tornar o novo grupo um grupo aninhado, de modo que o grupo seja criado com a classe auxiliar `nestedGroupAux`.

   Observação: Você pode converter um grupo estático em um grupo dinâmico ou aninhado usando o procedimento mencionado em Modificando objetos. Isso estende o objeto Grupo selecionado para pertencer à classe `dynamicGroupAux` ou à classe `nestedGroupAux`, respectivamente.

   Um grupo pode ser aninhado ou dinâmico. Não é possível criar um grupo que seja aninhado e dinâmico ao mesmo tempo.

   ---
4. Após especificar as informações necessárias, clique no botão Criar.
5. Uma confirmação aparece, indicando que o grupo foi criado.

Figura 6-1 *Criando um grupo*

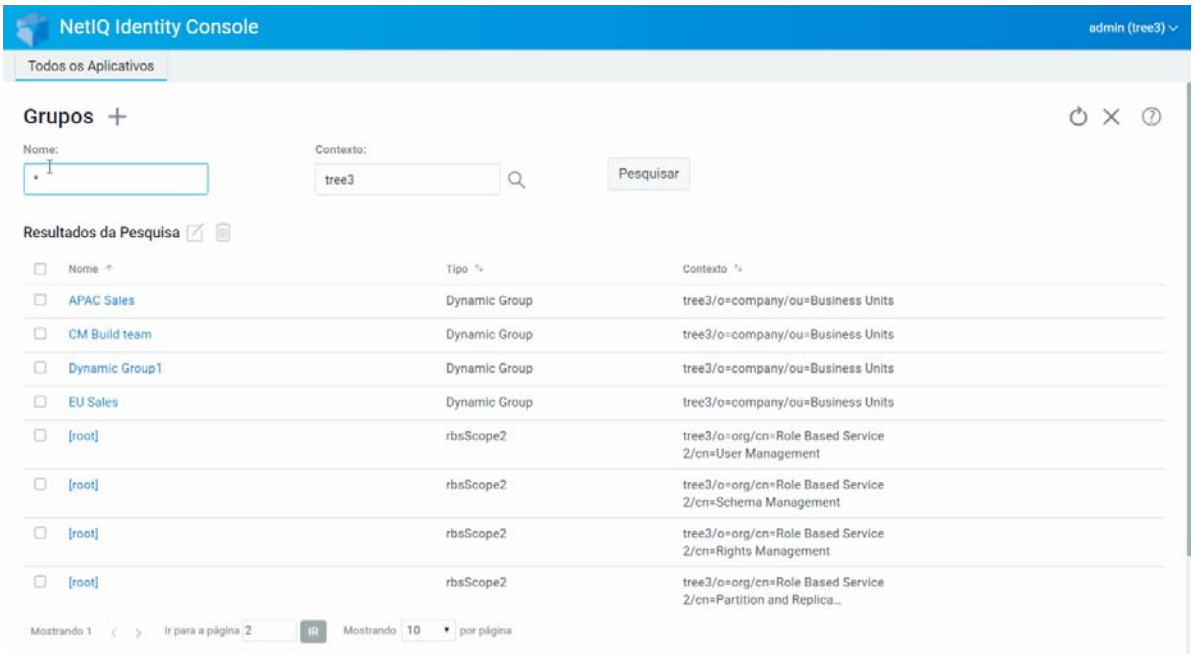


Apagando grupos

Para apagar grupos:

1. Clique na opção **Gerenciamento de Grupos** na landing page do Identity Console.
2. Especifique o nome e o contexto do grupo ou use o recurso de pesquisa para encontrá-lo e clique no botão Pesquisar.
3. Selecione o grupo que precisa ser apagado e clique no ícone 🗑.
4. Uma confirmação aparece, indicando que o grupo foi apagado.

Figura 6-2 *Apagando grupos*

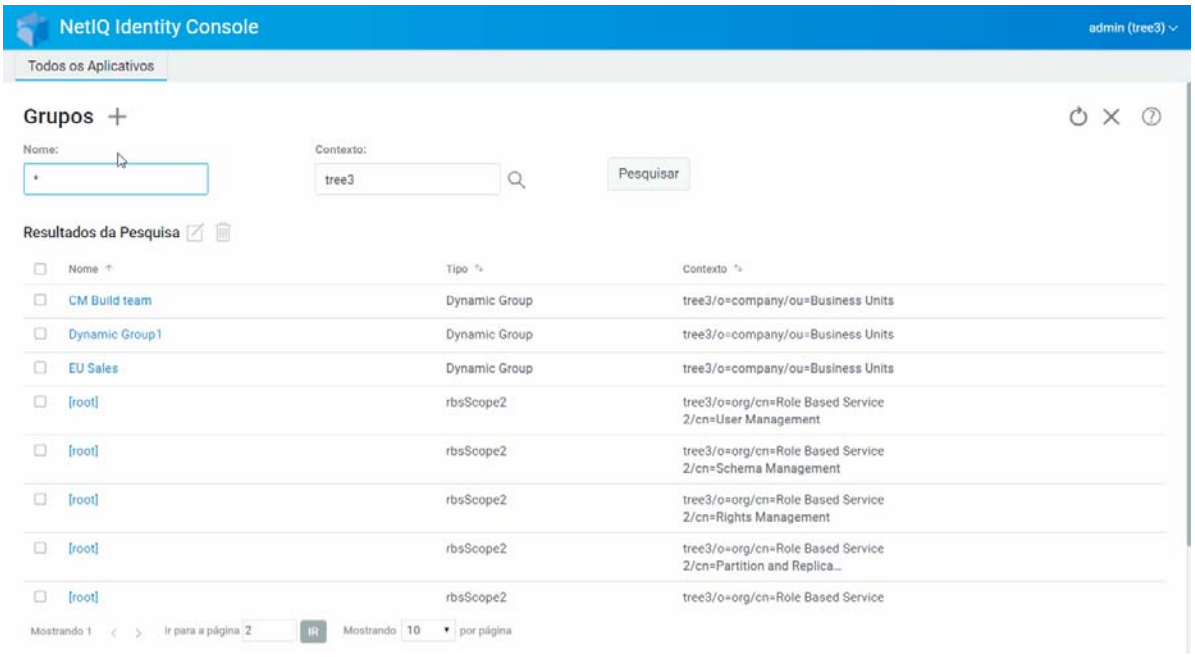


Modificando grupos

Para modificar grupos:

1. Clique na opção **Gerenciamento de Grupos** na landing page do Identity Console.
2. Digite o nome e o contexto do grupo e clique no botão Pesquisar.
3. Selecione o grupo que precisa ser modificado e clique no ícone.
4. Faça suas mudanças e clique no botão Gravar.
5. Uma confirmação aparece indicando que o grupo foi modificado.

Figura 6-3 *Modificando grupos*

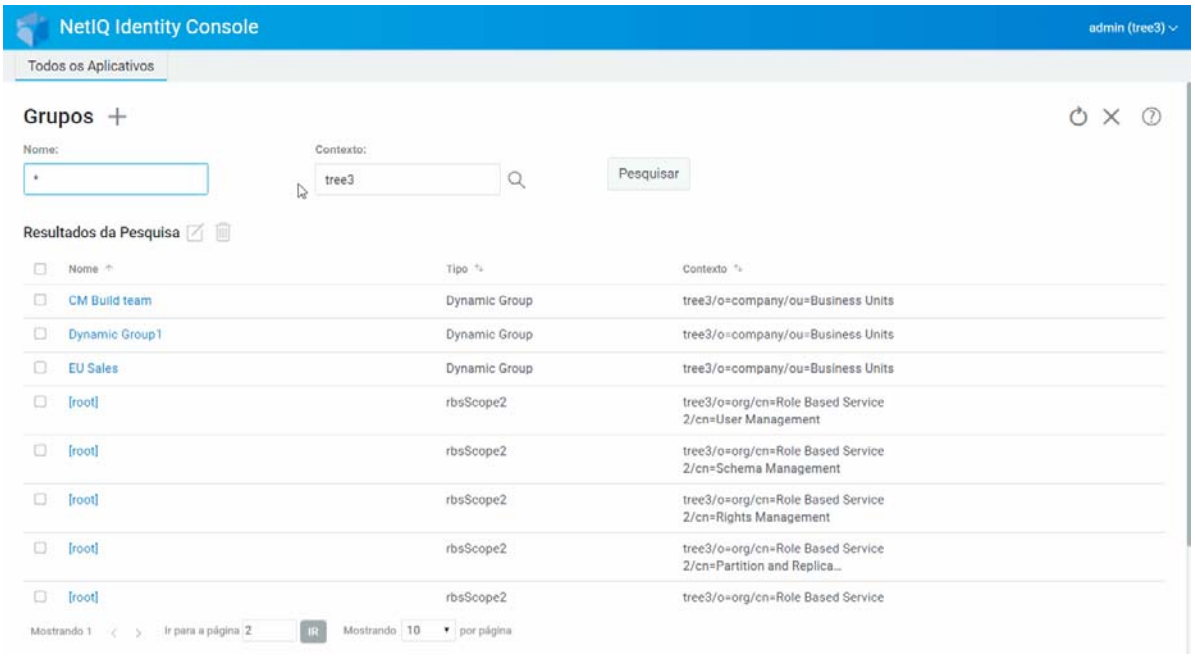


Adicionando ou modificando membros de grupos

Para adicionar ou modificar membros de grupos:

1. Clique na opção **Gerenciamento de Grupos** na landing page do Identity Console.
2. Digite o nome e o contexto do grupo e clique no botão Pesquisar.
3. Selecione o grupo e clique no ícone .
4. Clique na guia **Membros** e na página **Modificar Grupo**.
5. Use o ícone para adicionar um novo membro ao grupo. Caso decida remover membros do grupo, clique no ícone .
6. Após fazer as mudanças, clique no botão Gravar.
7. Uma confirmação aparece indicando que o grupo foi modificado.

Figura 6-4 *Adicionando ou modificando membros de grupos*

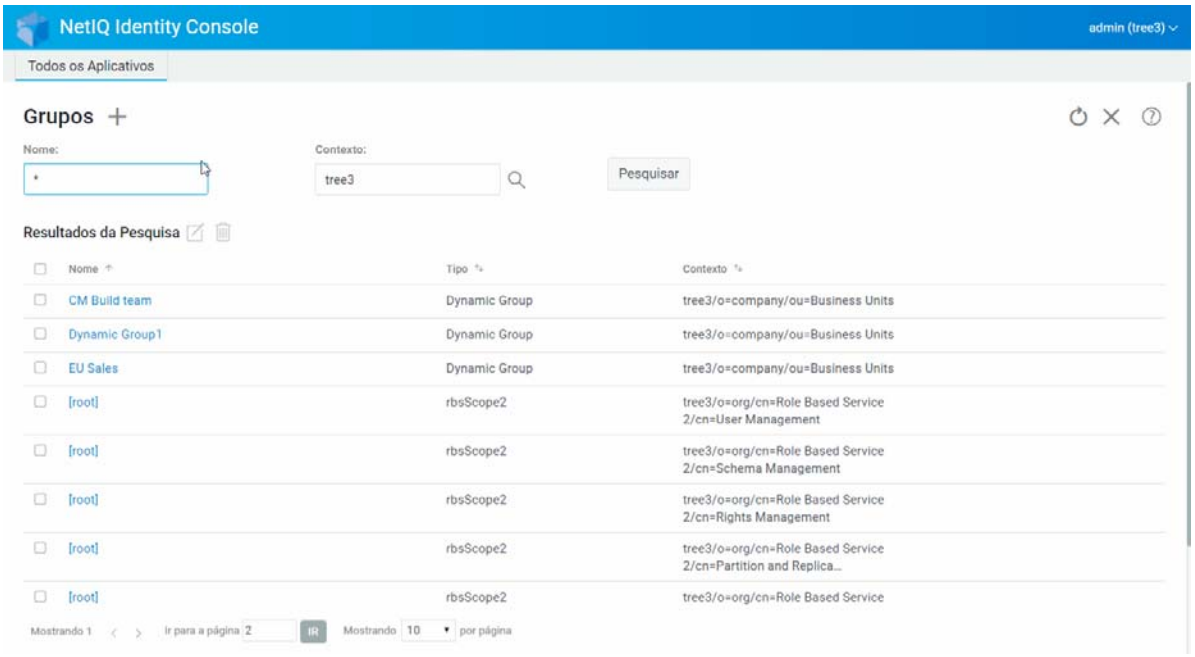


Pesquisando grupos

Para pesquisar grupos:

1. Clique na opção **Gerenciamento de Grupos** na landing page do Identity Console.
2. Você pode pesquisar um grupo pelo nome ou pelo nome e contexto.
3. Após especificar as informações necessárias, clique no ícone Pesquisar.

Figura 6-5 *Pesquisando grupos*



7 Gerenciando objetos

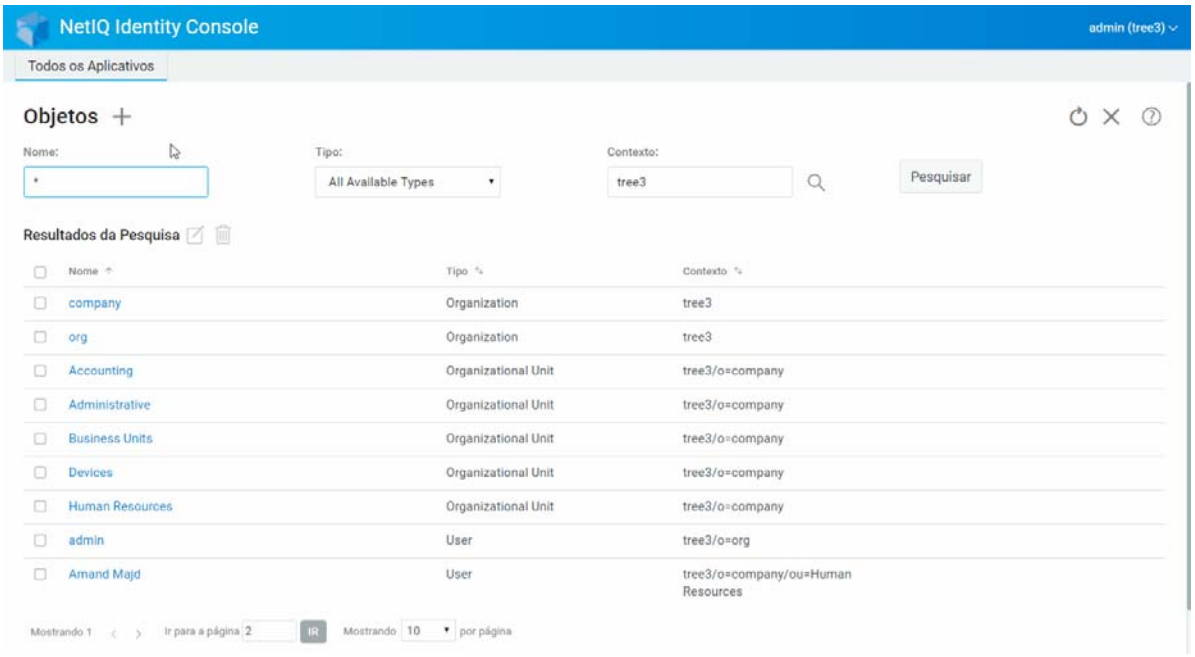
O Identity Console permite gerenciar vários objetos no seu armazenamento de dados. Usando este módulo, você pode criar, modificar, apagar e pesquisar objetos.

Criando um objeto

Para criar um novo objeto:

1. Clique na opção **Gerenciamento de Objeto** na landing page do Identity Console.
2. Clique no ícone +.
3. Na página Criar Objeto, digite as seguintes informações:
   - Especifique o nome do objeto
   - Especifique o Tipo
   - Especifique o Contexto
4. Após digitar todas as informações necessárias, clique em **Próximo** > **Criar**.
5. Uma confirmação aparece indicando que o objeto foi criado.

Figura 7-1 *Criando um objeto*

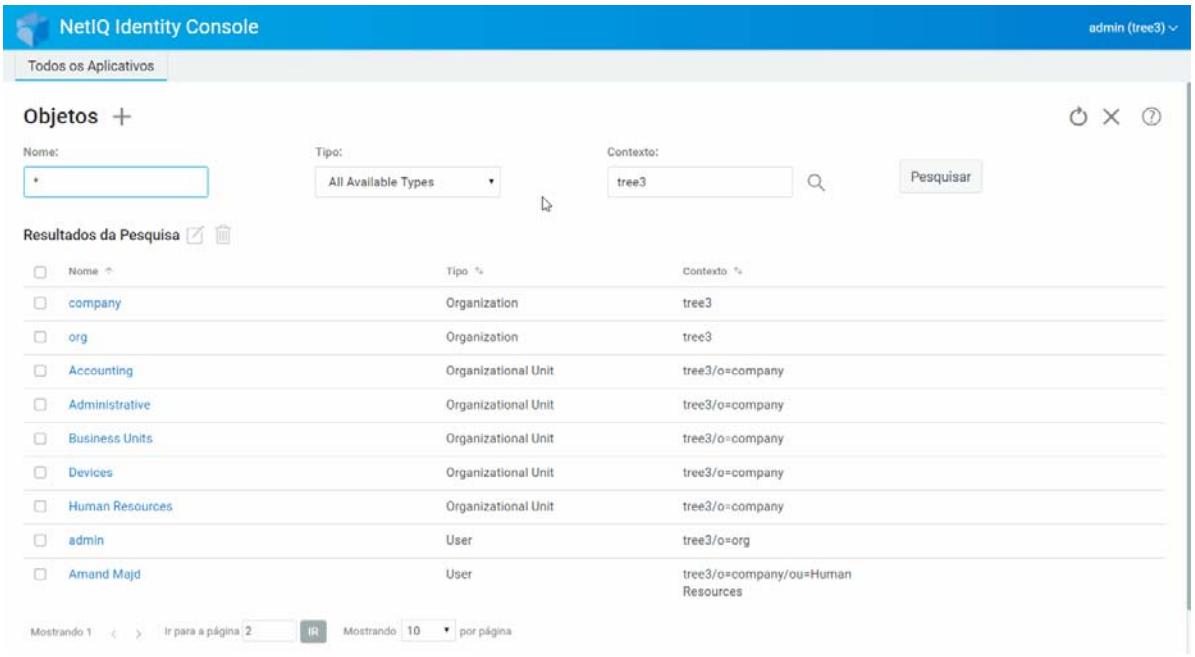


Apagando objetos

Para apagar objetos:

1. Clique na opção **Gerenciamento de Objeto** na landing page do Identity Console.
2. Digite o nome, tipo e contexto do objeto ou use o recurso de pesquisa para encontrá-lo e clique no botão Pesquisar.
3. Selecione o objeto da lista de pesquisa e clique no ícone 🗑.
4. Aparecerá uma confirmação indicando que o objeto foi apagado.

Figura 7-2 *Apagando objetos*

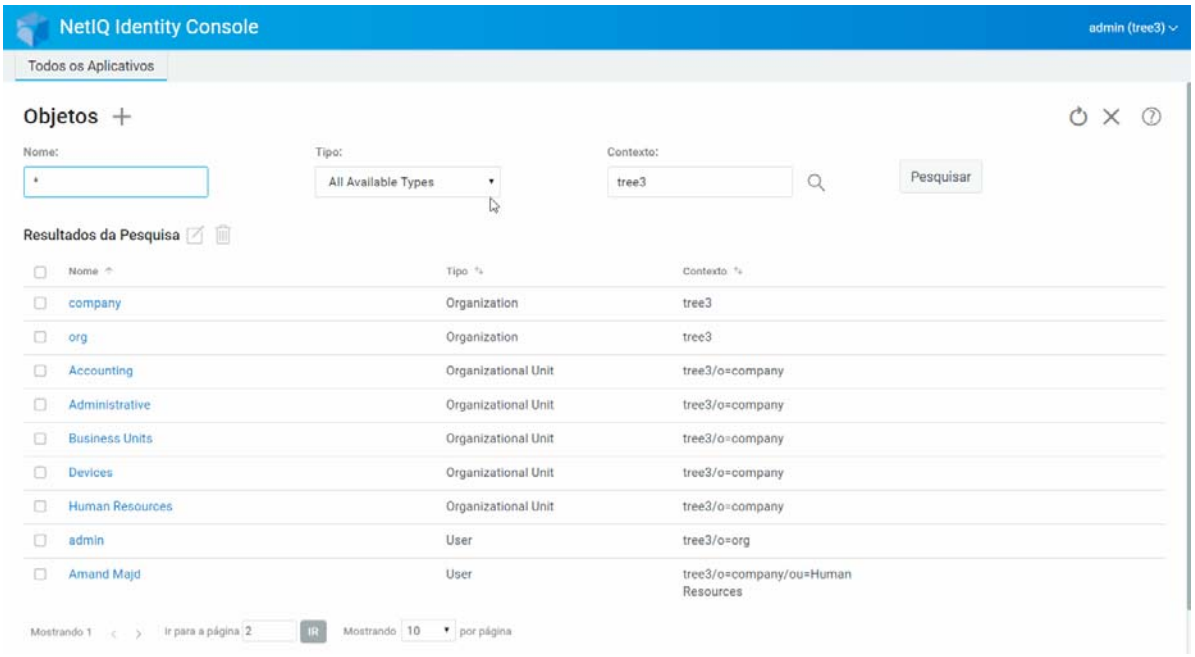


Modificando objetos

Para modificar objetos:

1. Clique na opção **Gerenciamento de Objetos** na landing page do Identity Console.
2. Digite o nome, o tipo e o contexto do objeto. Clique no botão Pesquisar.
3. Selecione o objeto da lista de pesquisa e clique no ícone .
4. Faça suas mudanças e clique no botão Gravar.
5. Aparecerá uma confirmação indicando que o objeto foi modificado.

Figura 7-3 *Modificando objetos*

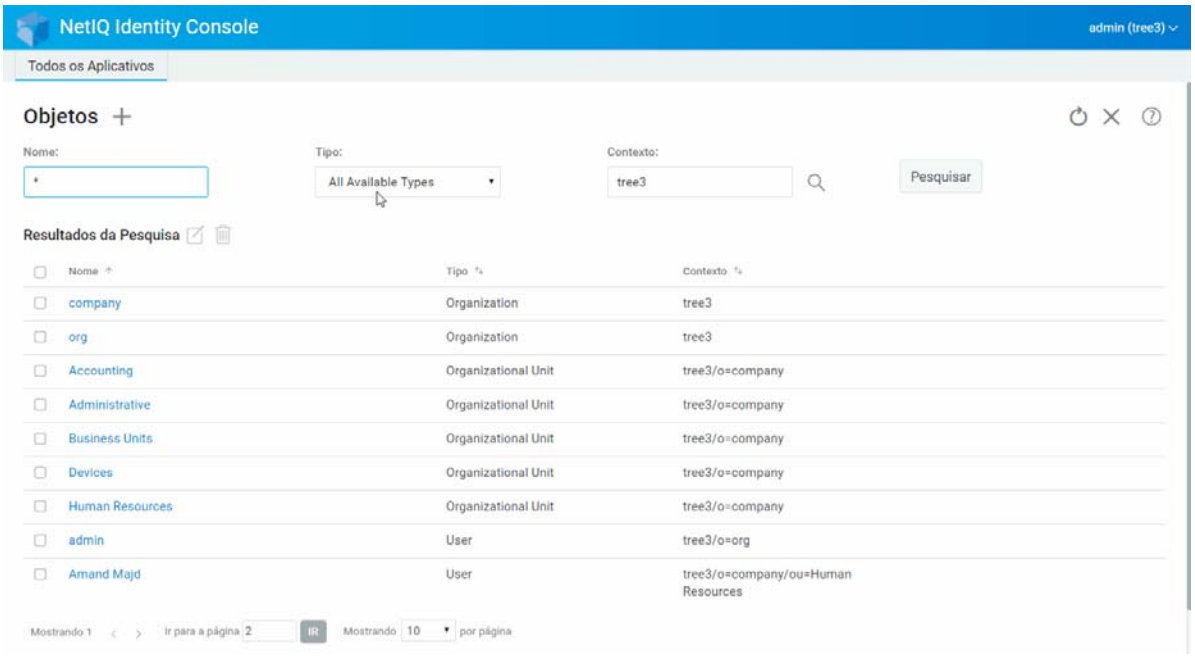


Pesquisando um objeto

Para pesquisar um objeto:

1. Clique na opção **Gerenciamento de Objeto** na landing page do Identity Console.
2. Você pode pesquisar um objeto pelo nome ou por nome, tipo e contexto.
3. Após especificar as informações necessárias, clique no botão Pesquisar.

Figura 7-4 *Pesquisando um objeto*



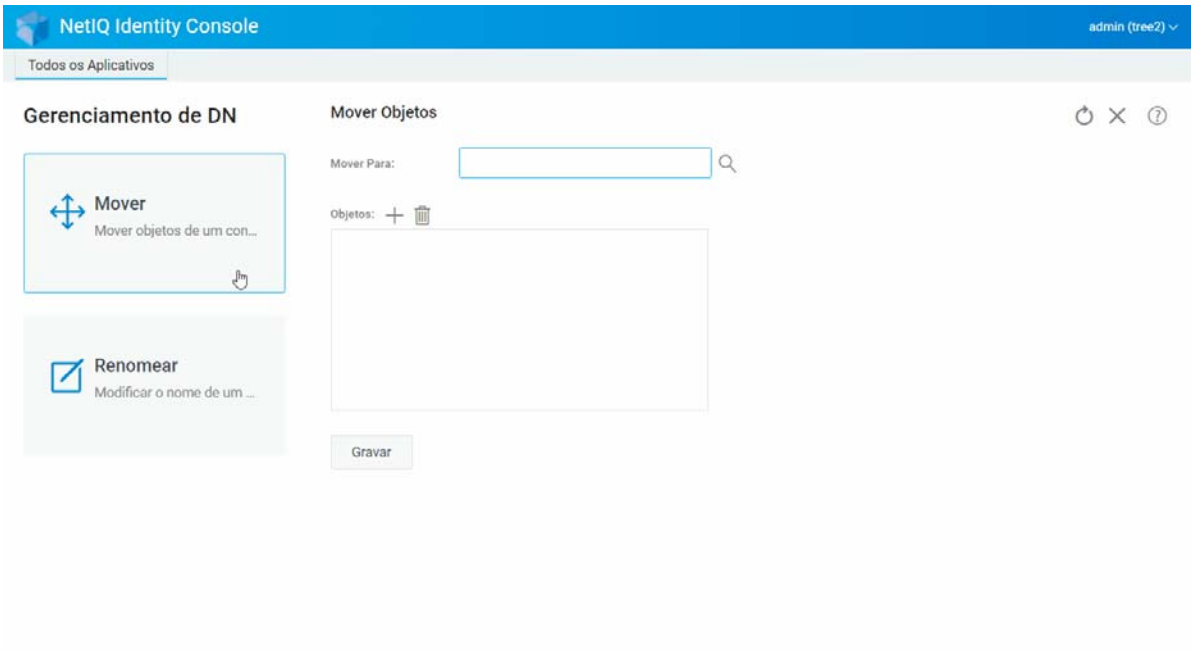
Movendo um objeto

Para mover um objeto:

1. Clique na opção **Gerenciamento de DN** na landing page do Identity Console.
2. A opção **Mover Objeto** será selecionada por padrão.
3. No campo **Mover Para**, selecione o container para o qual deseja mover o objeto.
4. Clique no ícone + para adicionar o objeto que deseja mover para um container diferente.

   Se quiser remover um objeto selecionado, clique no ícone 🗑.
5. Clique no botão Gravar.
6. Aparecerá uma mensagem de confirmação indicando que a operação de movimentação de objeto foi concluída com sucesso.

Figura 7-5 *Movendo um objeto*

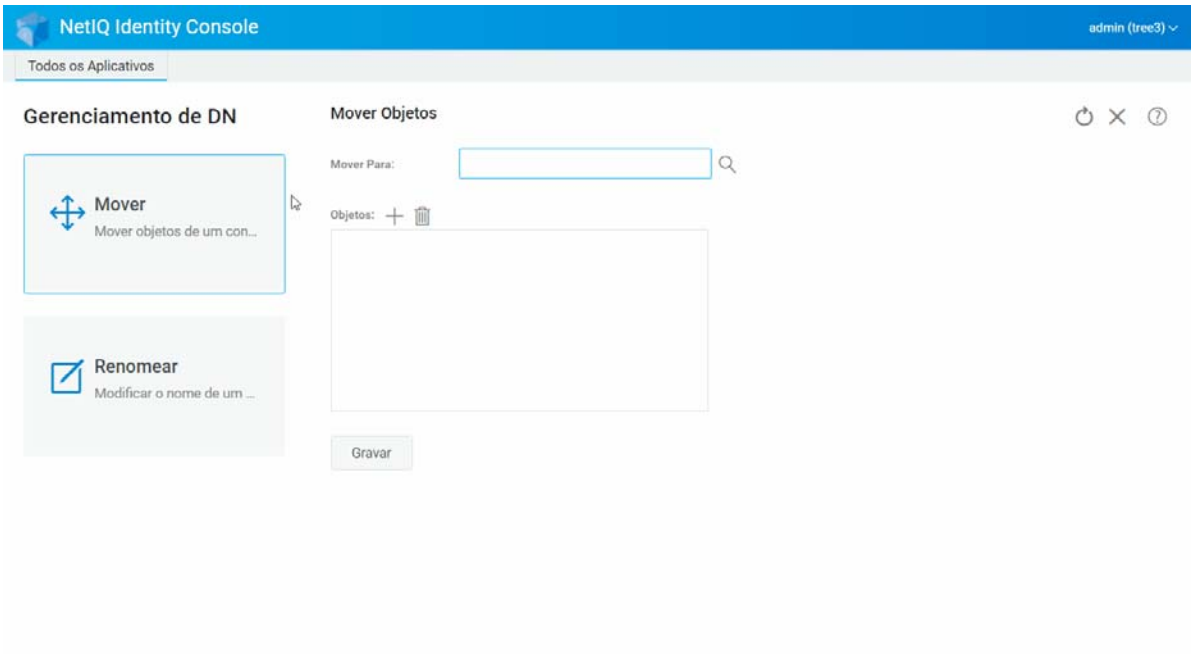


Renomeando um objeto

Para renomear um objeto:

1. Clique na opção **Gerenciamento de DN** na landing page do Identity Console.
2. Selecione a opção **Renomear Objeto**.
3. Use o recurso de pesquisa para encontrar o objeto que precisa ser renomeado no campo **Nome do objeto**.
4. Especifique somente o novo nome do objeto no campo **Novo Nome**. Não especifique o Contexto.
5. Selecione para gravar o nome antigo, se desejar.
6. Clique no botão Gravar.
7. Aparecerá uma mensagem de confirmação indicando que a operação de renomeação de objeto foi bem-sucedida.

Figura 7-6 *Renomeando um objeto*



8 Gerenciando direitos

Direitos se refere a trustees e direitos de trustee do eDirectory. Quando você cria uma árvore, as atribuições padrão de direitos fornecem à sua rede segurança e acesso generalizados. O Identity Console permite que você execute as seguintes tarefas relacionadas a direitos:

- “Modificando o filtro de direitos herdados” na página 53
- “Modificando os direitos de trustee” na página 54
- “Visualizando os direitos efetivos” na página 55

Para obter mais informações sobre direitos do eDirectory, consulte o *NetIQ eDirectory 9.2 Administration Guide* (https://www.netiq.com/documentation/edirectory-92/edir_admin/data/bookinfo.html) (Guia de administração do NetIQ eDirectory 9.2).

Modificando o filtro de direitos herdados

O eDirectory fornece um mecanismo de filtro de direitos herdados (IRF) para bloquear a herança de direitos em itens subordinados individuais.

Para obter mais informações sobre Filtros de Direitos Herdados, consulte o *NetIQ eDirectory 9.2 Administration Guide* (https://www.netiq.com/documentation/edirectory-92/edir_admin/data/bookinfo.html) (Guia de administração do NetIQ eDirectory 9.2).

1. Clique na opção **Gerenciamento de Direitos** na landing page do Identity Console
2. Selecione **Filtro de Direitos Herdados**.

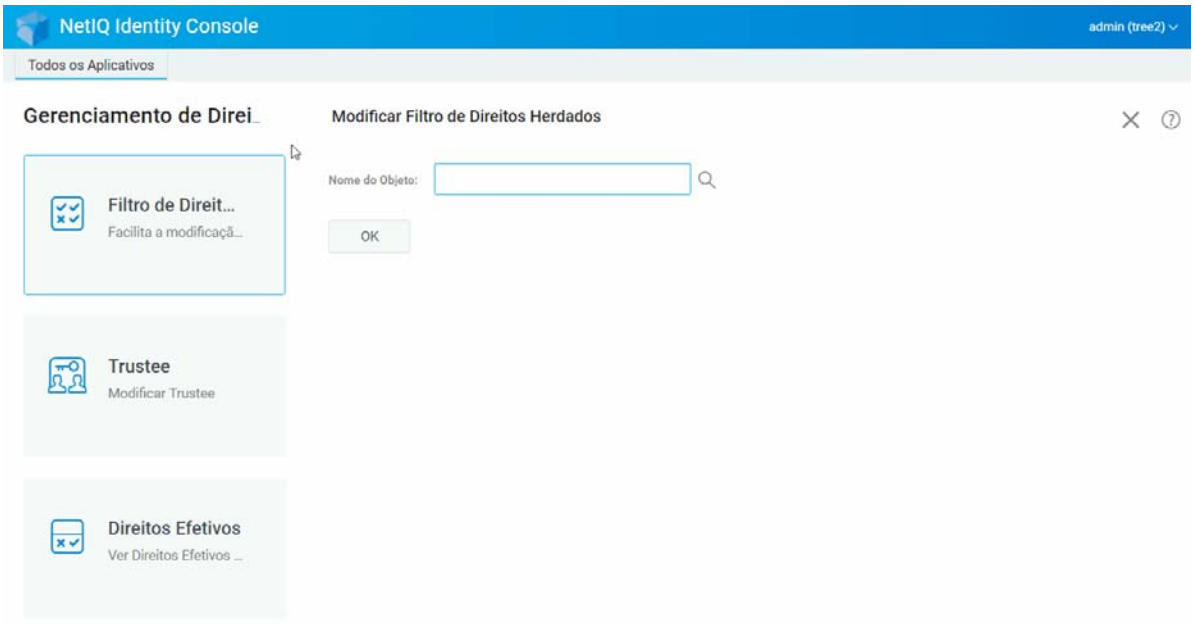
   Observação: O Filtro de Direitos Herdados é selecionado por padrão.

3. Especifique o nome completo do objeto cujo filtro de direitos herdados você deseja modificar ou use o ícone  do Seletor de Objetos para localizá-lo e clique em **OK**.

   Isso exibe uma lista dos filtros de direitos herdados já definidos nesse objeto.
4. Em **Propriedades**, edite a lista de filtros de direitos herdados conforme necessário e clique em **Aplicar**.

   Para editar a lista de filtros, é necessário que você tenha o direito Supervisor ou Controlar Acesso à propriedade ACL do objeto. Você pode definir filtros que bloqueiam os direitos herdados ao objeto como um todo, a todas as propriedades do objeto e a propriedades individuais.

Figura 8-1 *Modificando o filtro de direitos herdados*



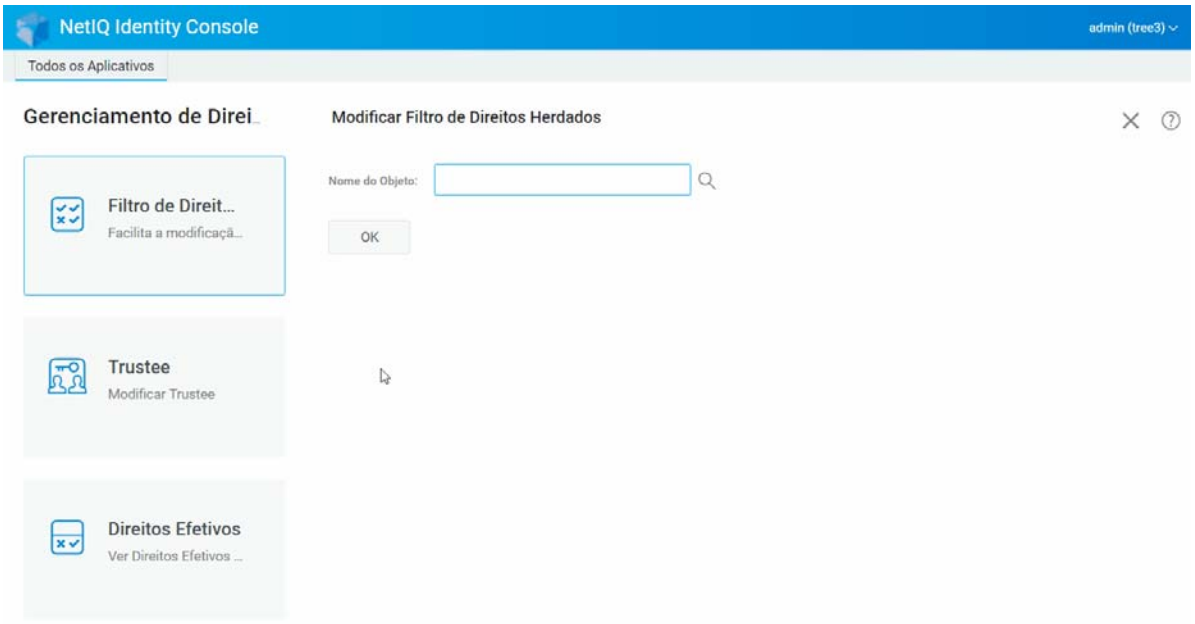
Modificando os direitos de trustee

Um trustee é um objeto ao qual ao qual foram concedidos direitos explícitos para outro objeto em sua árvore de diretório. Para modificar a lista de trustees em para um determinado objeto:

1. Clique na opção **Gerenciamento de Direitos** na landing page do Identity Console
2. Selecione **Trustee**.
3. Especifique ou use o ícone do Seletor de Objetos para localizar o nome do objeto cuja lista de trustees deseja ver e clique em **OK**.

   Isso abre a lista dos trustees atualmente designados do objeto.
4. Modifique a lista de trustees conforme necessário e clique em **OK**.
   - Adicione um trustee clicando no ícone .
   - Remova um trustee marcando sua caixa de seleção e clicando no ícone .
   - Modifique a designação de direitos de um trustee, selecionando o link **Direitos Designados** para esse trustee.

Figura 8-2 *Modificando os direitos de trustee*



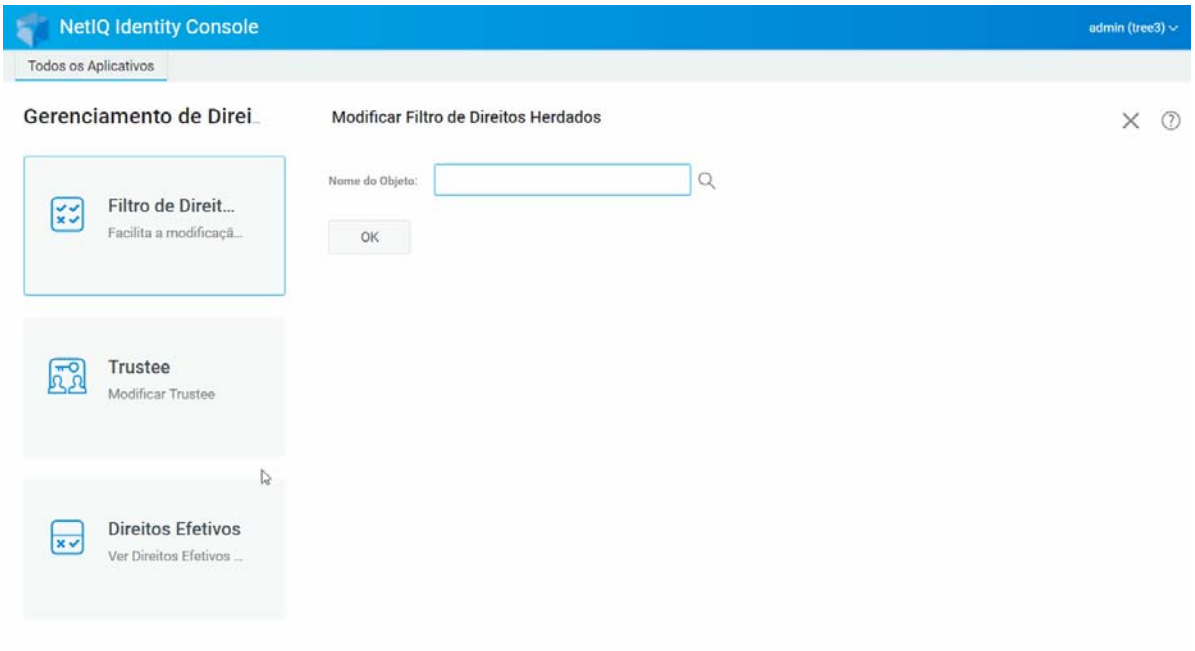
Visualizando os direitos efetivos

Direitos efetivos é a combinação de direitos explícitos e herdados que um objeto possui em qualquer ponto da árvore de diretório. Para ver os direitos efetivos de um objeto sobre outro objeto:

1. Clique na opção **Gerenciamento de Direitos** na landing page do Identity Console
2. Selecione **Direitos Efetivos**.
3. Especifique ou use o ícone de Seletor de Objetos para encontrar o nome do trustee cujos direitos você deseja ver e clique em **OK**.
4. No campo Nome do objeto, especifique o nome do objeto cujos direitos efetivos do trustee você deseja ver.

   O eDirectory calcula os direitos efetivos e os exibe no campo **Direitos Efetivos**.

Figura 8-3 *Visualizando os direitos efetivos*



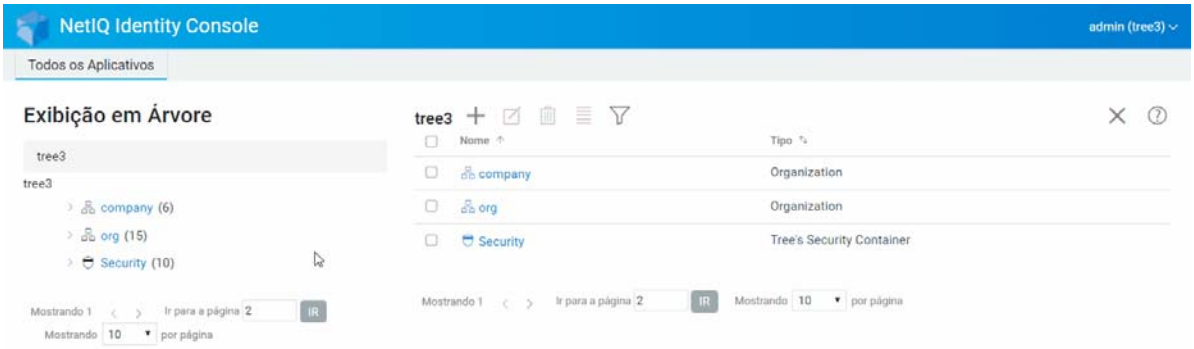
9 Exibição em árvore

A Exibição em árvore permite procurar em uma árvore de diretório para criar, apagar e modificar vários objetos nessa árvore. A Exibição em árvore tem um frame de navegação e um frame de conteúdo.

Frame de navegação da Exibição em árvore

Nessa Exibição em árvore, o frame de navegação exibe a estrutura do diretório. O frame de navegação exibe objetos Containers, incluindo Volume (sistema de arquivos) etc. Todas as opções exibidas no frame de navegação podem ser clicadas para ajudá-lo a procurar na estrutura de diretórios. Por padrão, o frame de navegação exibe até 10 objetos subordinados por container, mas você pode mudar essa configuração abaixo do painel do frame de navegação na Exibição em Árvore.

Figura 9-1 *O frame de navegação na Exibição em árvore*



Frame de conteúdo da Exibição em Árvore

Selecionar um dos objetos Container no frame de Navegação faz com que o frame de Conteúdo exiba todos os objetos desse container. O frame de Conteúdo é onde você vê e modifica objetos diretório. O frame de Conteúdo inclui um cabeçalho com diversas ações disponíveis:

Barra de título: A barra de título do frame de Conteúdo exibe o nome do objeto container selecionado no momento.

Cabeçalho de Lista de Objetos: O cabeçalho de lista de objetos dá acesso ao seguinte:

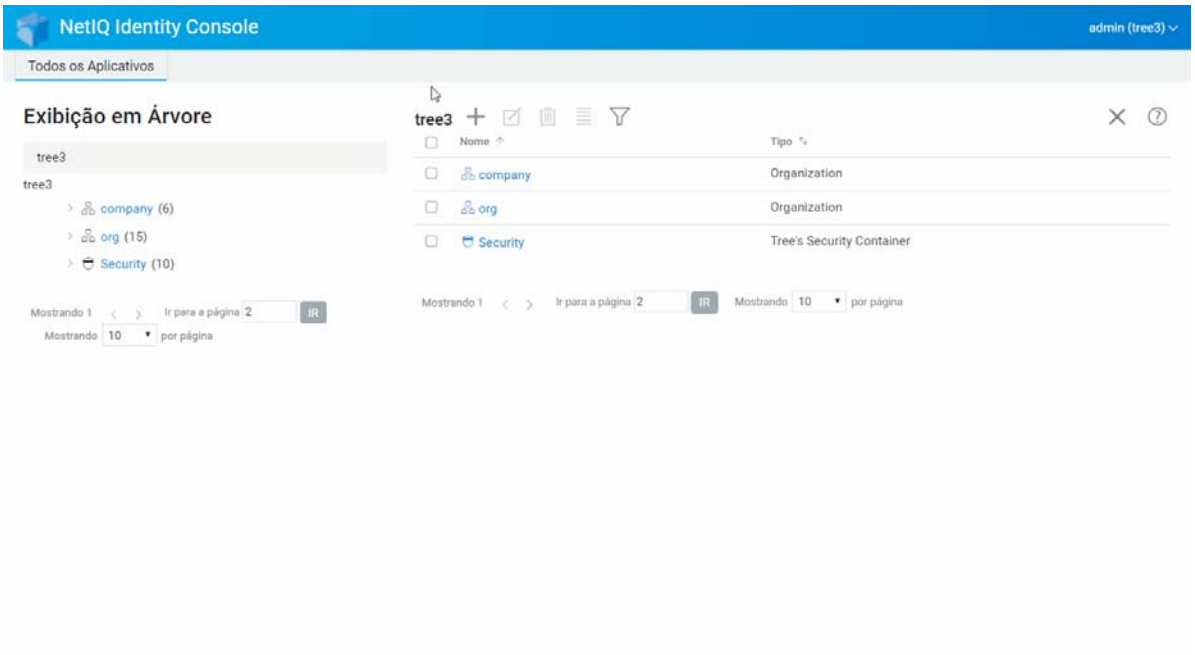
- **Adicionar**: Clique no ícone  para adicionar um novo objeto.
- **Modificar**: Selecione um objeto e clique no ícone  para modificar. Isso abre o livro de propriedades do objeto selecionado para que você possa modificar os atributos dele. Vários objetos não podem ser modificados juntos.
- **Apagar**: Selecione um objeto e clique no ícone  para apagar os objetos selecionados. Vários objetos podem ser apagados juntos. Objetos não folha não podem ser apagados.
- **Ações**: Selecione um objeto e clique no ícone  que abre um menu suspenso de tarefas com suporte para esses objetos selecionados. Para executar uma tarefa, selecione-a no menu suspenso e forneça as informações necessárias.
- **Contagem de Objetos**: A Exibição em árvore lista o número de objetos na página atual no final da página. Por padrão, o frame de conteúdo exibe até 20 objetos subordinados por container, mas você pode mudar essa configuração.
- **Selecionar Tudo**: A caixa de seleção no cabeçalho funciona como uma caixa de seleção “selecionar tudo” para a página de objetos atual.
- **Classificar**: As colunas **Nome** e **Tipo** são classificáveis. Clique em um desses itens para alternar a classificação dos objetos entre ordem alfabética crescente ou decrescente.
- **Filtro de Pesquisa**: Clique no ícone  . para iniciar a janela pop-up do filtro. Usando esta opção, você pode criar um filtro que limite os objetos exibidos na lista de objetos. Você pode filtrar por tipo ou nome de objeto, conforme necessário.

  Selecione a opção  para abrir a caixa de diálogo Filtro Avançado que permite criar um filtro usando praticamente qualquer atributo de objeto. Para obter mais informações, consulte “Configurando a pesquisa avançada” na página 26.

Para executar uma ação em um objeto, selecione a caixa correspondente e selecione o ícone da ação  do cabeçalho da Lista de Objetos. Selecione o objeto (nível atual) para realizar uma ação no container em que você está navegando no momento. As seguintes ações podem ser executadas usando essa opção:

- “Modificando o filtro de direitos herdados” na página 53
- “Modificando os direitos de trustee” na página 54
- “Estendendo um objeto” na página 66
- “Renomeando um objeto” na página 50
- Definir Senha
- “Visualizando os direitos efetivos” na página 55

Figura 9-2 *Frame de conteúdo na Exibição em árvore*



10 Gerenciando esquema

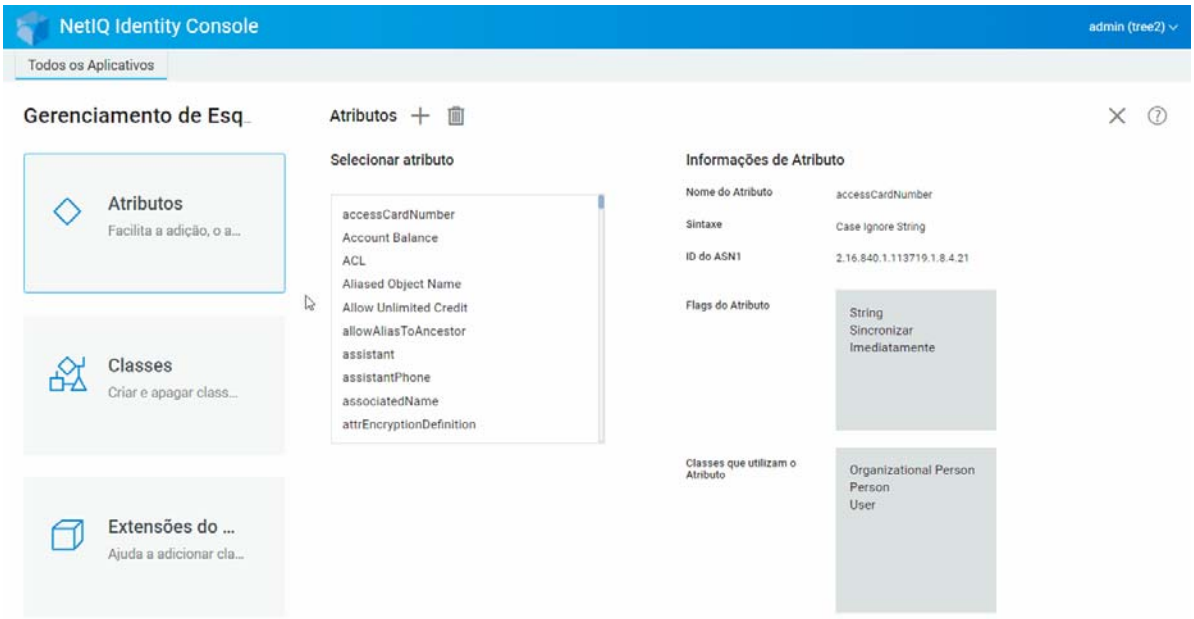
O esquema do diretório define os tipos de objetos que podem ser criados em sua árvore (como Usuários, Impressoras, Grupos etc.) e quais informações são necessárias ou opcionais no momento em que o objeto é criado. O Identity Console fornece as seguintes tarefas relacionadas ao esquema:

Criando um atributo

Você pode definir seus próprios tipos de atributos personalizados e adicioná-los como atributos opcionais nas classes do objeto existentes. No entanto, você não pode adicionar atributos obrigatórios às classes existentes. Criar um atributo:

1. Clique na opção **Gerenciamento de Esquema** na landing page do Identity Console.
2. Clique no ícone +.
3. Na página Criar Atributo, digite as seguintes informações:
   - Nome do Atributo
   - ID do ASN1 (opcional)
   - Sintaxe
   - Flags de Atributos
4. Após digitar todas as informações necessárias, clique no botão Criar.
5. Uma confirmação aparece, indicando que o atributo foi criado.

Figura 10-1 *Criando um atributo*



Criando uma classe

Usando a opção **Gerenciamento de Esquema**, você pode definir suas próprias classes. Você pode estender objetos individuais com as propriedades definidas em suas classes. Para criar uma classe:

1. Clique na opção **Gerenciamento de Esquema** na landing page do Identity Console e selecione **Classes**.
2. Clique no ícone +.
3. Na página Criar Atributo, digite as seguintes informações:
   - Nome da Classe
   - ID do ASN1 (opcional)
   - Flags de Classe: Selecione um dos seguintes flags de classe:
     - **Classe efetiva:** Defina este flag se quiser criar uma classe efetiva, que pode ser utilizada para criar objetos.
     - **Classe não efetiva:** Usada como marcador de espaço de um grupo de atributos. Uma classe não efetiva não pode ser utilizada para criar objetos, mas pode ser especificada como uma classe a partir da qual outras classes podem herdar atributos. Por exemplo, a classe Pessoa é uma classe não efetiva que retém os atributos herdados pela classe Usuário.
     - **Classe auxiliar:** Uma coleção de atributos que podem ser associados somente a objetos individuais e não a classes inteiras.
     - **Classe do container:** Defina este flag se quiser fazer desta classe uma classe de container. Quando forem usados para criar objetos, esses objetos se tornarão objetos Container (como OU). Não defina esse flag para uma classe de objeto Folha.

Observação: Se você selecionar Classes Efetivas e Não Efetivas, também precisará especificar valores para Superclasse. Caso escolha a Classe Auxiliar, a Superclasse será opcional para você.

4 Após digitar todas as informações necessárias, clique em **Próximo**.

5 Na próxima tela, selecione os atributos opcionais, obrigatórios e de nomeação e clique em **OK**.

6 Uma confirmação aparece indicando que a classe foi criada.

Designando atributos para uma classe

Você poderá adicionar atributos opcionais às classes existentes se for necessário mudar as informações da sua organização ou se estiver se preparando para fundir árvores. Adicionar um atributo a uma classe existente:

Observação: Os atributos obrigatórios só podem ser definidos enquanto uma classe estiver sendo criada. Um atributo obrigatório é aquele que deve ser completado quando um objeto estiver sendo criado.

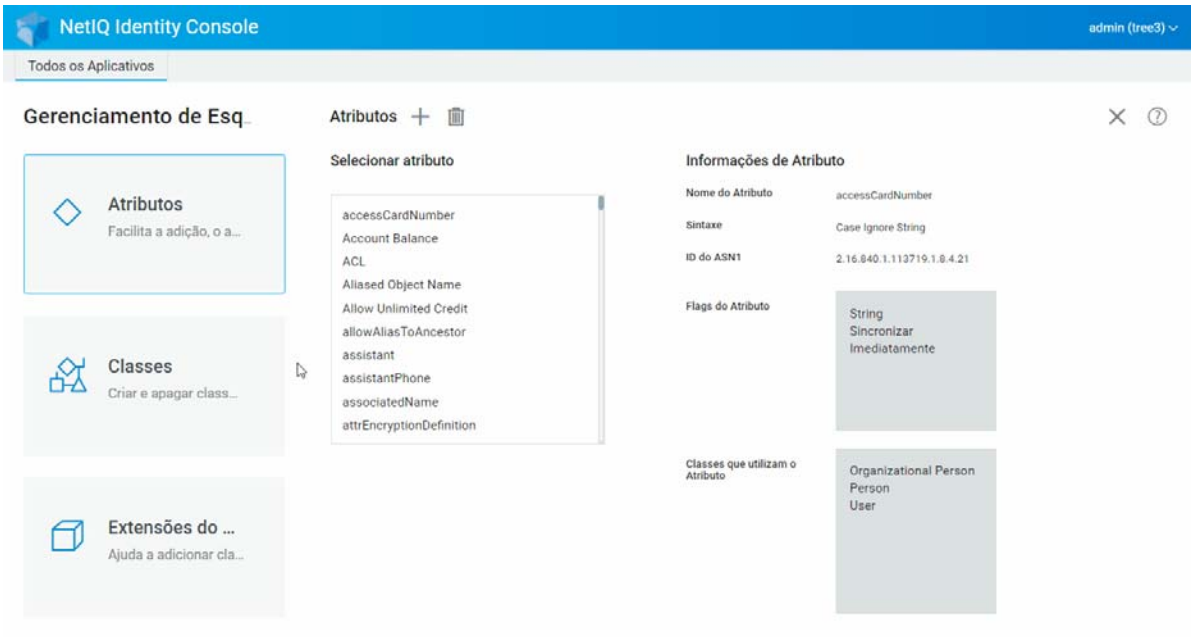
1 Clique na opção **Gerenciamento de Esquema** na landing page do Identity Console e selecione **Classes**.

2 Clique em qualquer classe listada em **Selecionar classe**.

3 As informações da classe correspondente são exibidas no lado direito da tela.

4 Clique no botão + ao lado da opção **Atributos**, selecione os atributos que deseja adicionar e clique em **Adicionar** > **Gravar**.

Figura 10-2 *Designando atributos para uma classe*

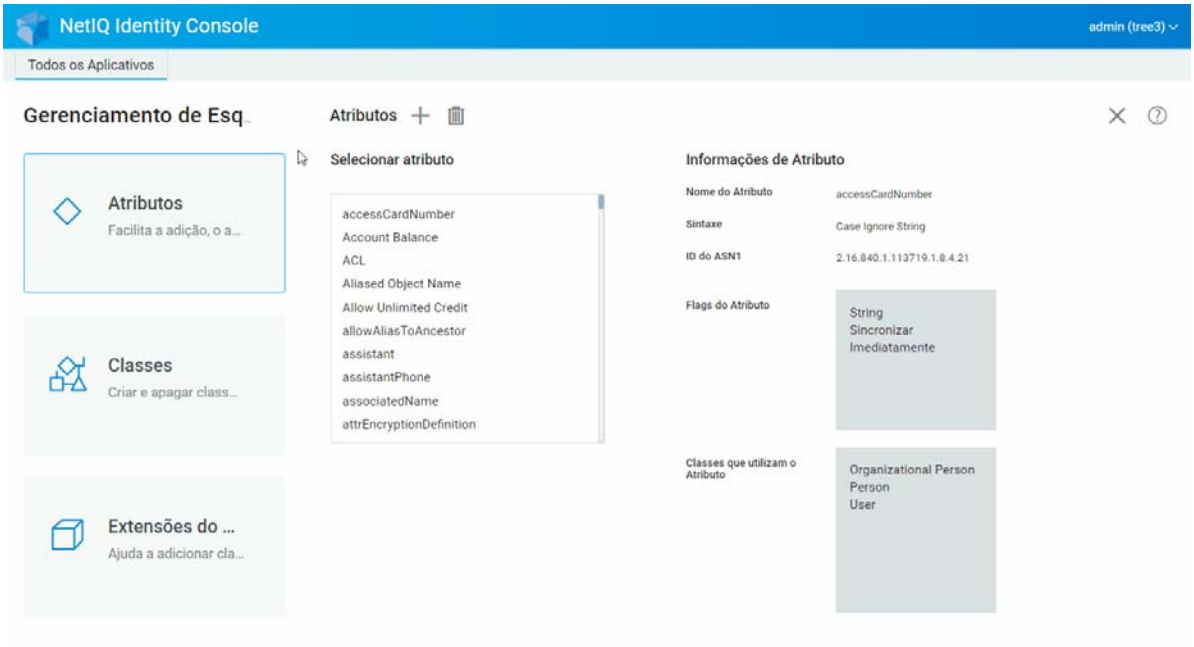


Exibindo informações de atributo

Você pode ver os detalhes estruturais de um atributo, tais como Sintaxe, flags e Classes que usam o atributo. Para ver as informações de um atributo:

1. Clique na opção **Gerenciamento de Esquema** na landing page do Identity Console e selecione **Atributos**.
2. Clique em qualquer atributo listado em **Selecionar atributo**.
3. As informações do atributo correspondente são exibidas no lado direito da tela.

Figura 10-3 *Exibindo informações de atributo*



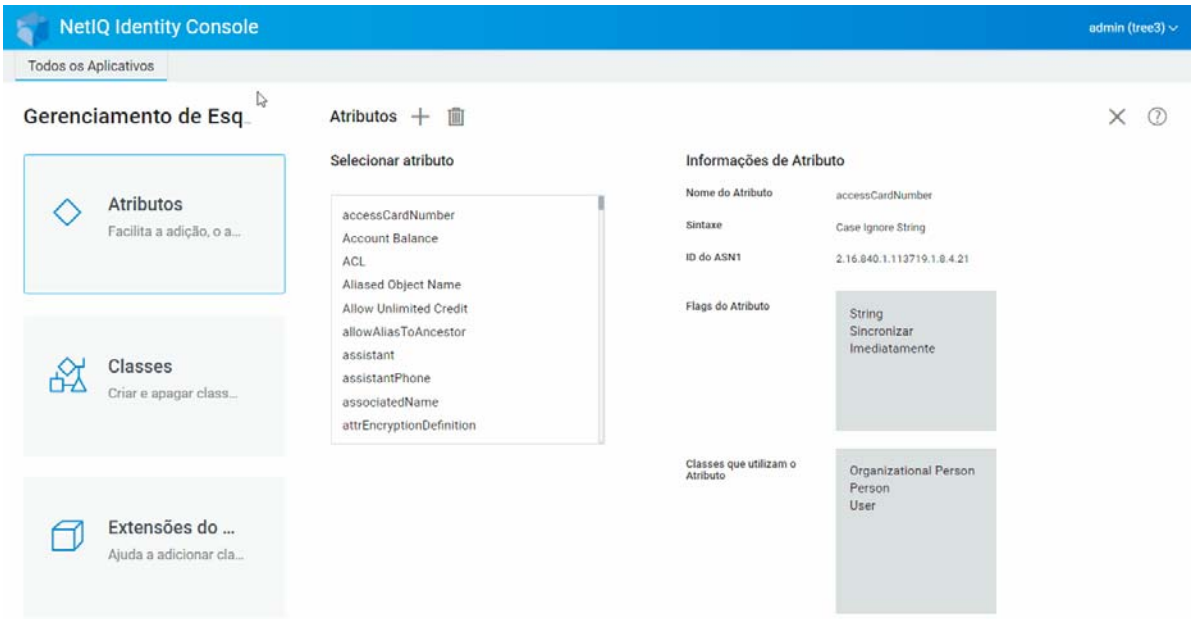
Apagando um atributo

Você pode apagar atributos não utilizados que não fazem parte do esquema base da sua árvore do eDirectory. Isso pode ser útil após a fusão de duas árvores de diretório, ou se um atributo tiver se tornado obsoleto com o tempo. Para excluir um atributo:

1. Clique na opção **Gerenciamento de Esquema** na landing page do Identity Console e selecione **Atributos**.
2. Selecione o atributo que deseja apagar na lista **Selecionar atributo** e clique no ícone .

   Observação: O ícone será habilitado somente quando for selecionado um atributo que pode ser apagado.
3. Clique em **OK** para confirmar o apagamento.

Figura 10-4 *Apagando um atributo*



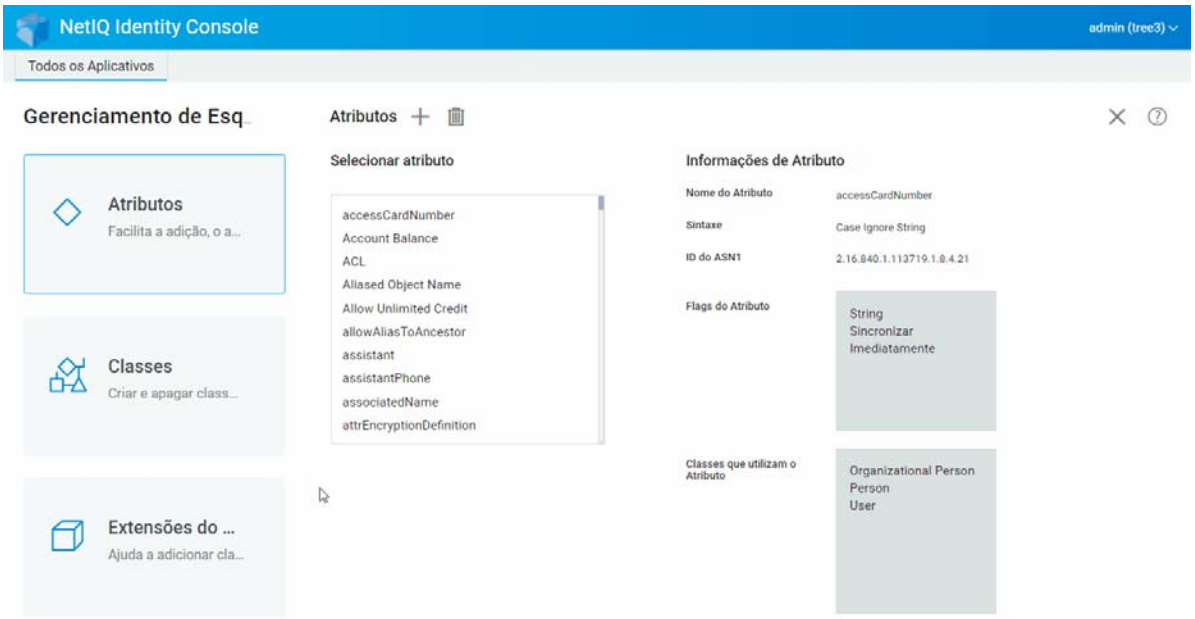
Apagando uma classe

Você pode apagar classes não utilizadas que não fazem parte do esquema base da sua árvore do eDirectory. O Identity Console impede que você apague as classes que estão sendo usadas no momento em partições replicadas localmente. Para apagar uma classe:

1. Clique na opção **Gerenciamento de Esquema** na landing page do Identity Console e selecione **Classes**.
2. Selecione a classe que deseja apagar na lista **Selecionar classe** e clique no ícone  .

   Observação: O ícone  será habilitado somente quando for selecionada uma classe que pode ser apagada.
3. Clique em **OK** para confirmar o apagamento.

Figura 10-5 *Apagando uma classe*



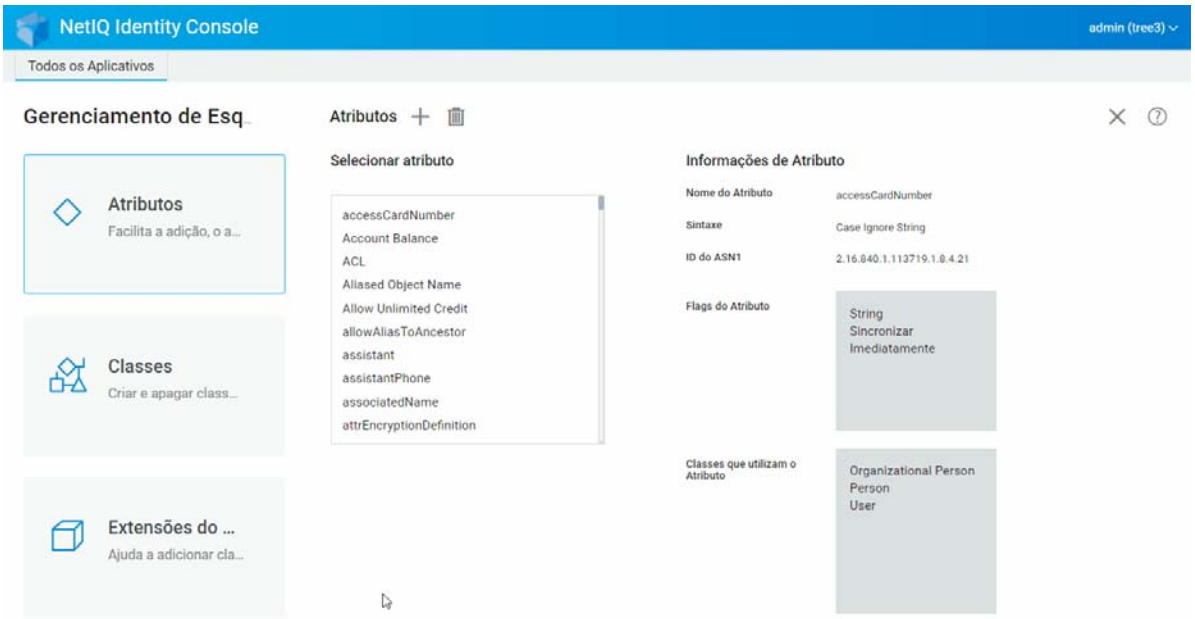
Estendendo um objeto

Realize as seguintes etapas para estender um objeto:

1. Clique na opção **Gerenciamento de Esquema** na landing page do Identity Console e selecione **Extensão do Objeto**.
2. Especifique o nome do objeto ou use o seletor de objetos para selecionar o objeto a ser estendido, clique no ícone .
3. Clique no ícone , selecione a classe auxiliar e clique em **OK**.

   Observação: Se qualquer atributo obrigatório estiver anexado à classe auxiliar selecionada, será solicitado que você digite os valores necessários na janela pop-up **Atributos Obrigatórios**.
4. Uma mensagem de confirmação aparece indicando que a classe auxiliar foi adicionada ao objeto.
5. Para remover uma classe auxiliar de um objeto, selecione a classe e clique no ícone .

Figura 10-6 *Estendendo um objeto*



11 Gerenciando eventos de auditoria

Este capítulo explica como gerenciar vários eventos de auditoria usando o Identity Console. Usando este recurso, é possível habilitar ou desabilitar eventos de auditoria para o servidor NCP.

Configurando eventos de auditoria CEF

1. Efetue login no Identity Console usando seu nome de usuário e senha.
2. Selecione **Auditoria**.
3. Selecione o servidor NCP que deseja monitorar e clique em **OK**.

   Observação: Após habilitar os eventos CEF para qualquer servidor NCP pela primeira vez, poucos eventos serão selecionados por padrão.

   ---

4. Configure os eventos de auditoria CEF:
   - **Configuração de eventos:** Habilite ou desabilite os seguintes eventos com base na auditoria necessária para seu ambiente:

Observação: Categorias de eventos individuais na seção de configuração de eventos serão recolhidas por padrão. Você pode expandir cada categoria para selecionar eventos individuais.

Opções	Descrição
Eventos de Segurança	Selecione os eventos de segurança para os quais você deseja registrar eventos. Você pode registrar eventos para adicionar ou apagar membros, detectar intrusos, mudar a senha, autenticar usuários, etc.
Eventos de Objeto	Selecione os eventos de objeto para os quais você deseja registrar eventos. Você pode registrar eventos para criar, apagar, renomear, mover e pesquisar objetos.
Eventos de Atributo	Selecione os eventos de atributo para os quais você deseja registrar eventos. Você pode registrar eventos para ler e apagar atributos e para adicionar, apagar e comparar o valor de atributo.
Eventos de LDAP	Selecione os eventos LDAP para os quais você deseja registrar eventos.

- **Configurações avançadas:** Usando as configurações avançadas, você pode executar as ações a seguir.
  - **Global:** Você pode selecionar ou limpar entradas duplicadas das configurações globais.
    - **Não enviar eventos replicados:** Selecione esta opção para parar de receber eventos duplicados devido à replicação de outros servidores.
  - **Valores do evento de registro:** Os eventos são registrados em um arquivo texto. Valores de evento com mais de 768 bytes de tamanho são considerados “valores altos”. É possível registrar eventos de qualquer tamanho.
    - **Registrar valores altos:** Selecione esta opção para registrar eventos com mais de 768 bytes.
    - **Registrar valores de atributos:** Selecione esta opção para exibir os valores de atributo. Isso é aplicável somente aos eventos **Adicionar Valor** e **Apagar Valor**.
    - **Registrar valores de atributos criptografados:** Selecione esta opção para exibir os valores de atributos criptografados. Isso é aplicável somente aos eventos **Adicionar Valor** e **Apagar Valor**.

    Observação: Se o tamanho do evento for maior do que 768 bytes, o valor do evento será truncado e gravado no arquivo de registro.

Entendendo os Tipos de Evento CEF

Você pode configurar o CEF para registrar eventos nas seguintes categorias:

- Segurança

- Objetos
- Atributos
- LDAP

Você pode auditar o seguinte conjunto padrão de tipos de evento:

Configurações	Tipo de Evento
Segurança	◆ ACL Mudado ◆ Adicionar Membro ◆ Apagar Membro ◆ Intruso Detectado ◆ Login Desabilitado ◆ Login Habilitado ◆ Login ◆ Mudar Segurança Igual a ◆ Configuração de Auditoria ◆ Mudar Senha ◆ Desbloquear Conta ◆ Logout ◆ Conexão ◆ Personificar ◆ Autenticar ◆ Verificar Senha ◆ Mudar Configurações de Login ◆ Consultar Credenciais
Objetos	◆ Criar Objeto ◆ Apagar Objeto ◆ Renomear Objeto ◆ Mover Objeto ◆ Leitura de DSA ◆ Pesquisar
Atributos	◆ Ler Atributo ◆ Apagar Atributo ◆ Adicionar Valor ◆ Apagar Valor ◆ Comparar Valor do Atributo

Configurações	Tipo de Evento
LDAP	◆ Vincular LDAP ◆ Resposta de Vincular LDAP ◆ Desvincular LDAP ◆ Conexão de LDAP ◆ Pesquisar LDAP ◆ Resposta de Pesquisar LDAP ◆ Resposta de Entrada de Pesquisar LDAP ◆ Adicionar LDAP ◆ Resposta de Adicionar LDAP ◆ Comparação de LDAP ◆ Resposta de Comparar LDAP ◆ Modificar LDAP ◆ Resposta de Modificar LDAP ◆ Apagar LDAP ◆ Resposta de Apagar LDAP ◆ DN de Modificação de LDAP ◆ Resposta de DN de Modificação de LDAP ◆ Abandono de LDAP ◆ Operação Estendida de LDAP ◆ Operação Estendida do Sistema de LDAP ◆ Resposta de Operação Estendida de LDAP ◆ Modificar Configuração do Servidor LDAP ◆ Operação de LDAP Desconhecida ◆ Modificar Senha de LDAP

Configurando a filtragem de auditoria do CEF

Usando filtros e notificações de eventos, o CEF é capaz de relatar quando um tipo específico de evento ocorre ou quando não ocorre. Você também pode filtrar eventos para um ou mais atributos ou classes de objeto específicos, dependendo do tipo de evento. O CEF avalia todos os eventos gerados em relação aos filtros configurados no servidor do eDirectory e registra apenas os eventos correspondentes a esses filtros.

Esta seção fornece as informações necessárias para configurar os filtros e as notificações do sistema.

- “Filtrando eventos do eDirectory com filtro de exclusão” na página 73
- “Filtrando eventos de objeto CEF” na página 73
- “Filtrando eventos de atributo CEF” na página 74

Filtrando eventos do eDirectory com filtro de exclusão

Clique no link **Filtro de Exclusão** para configurar a filtragem para esses atributos e essas classes de objeto para os quais você não deseja que um evento seja gerado. Você pode selecionar atributos e classes de objeto.

Para configurar a filtragem para Eventos indesejados do eDirectory:

1. No Identity Console, selecione **Auditoria** na home page.
2. Selecione o servidor NCP que deseja monitorar e clique em **OK**.
3. Agora vá até **Configurações Avançadas** e clique em **Filtro de Exclusão** em **Filtros**.

   A janela de Filtragem de Exclusão do CEF aparece.
4. Na lista **Classes de Objeto Disponíveis**, selecione as classes de objeto para as quais você não deseja coletar eventos e, em seguida, clique na seta para a direita para movê-los para a lista **Classes do Objeto Selecionadas**.
5. Na lista **Atributos Disponíveis**, selecione qualquer número de atributos. Selecione o atributo e clique na seta para a direita para adicionar o atributo à lista de atributos selecionada.
6. Clique em **OK**.

Usando o filtro configurado, o módulo de auditoria do CEF para de gerar eventos para todas as classes e atributos de objetos selecionados.

Filtrando eventos de objeto CEF

Você pode configurar a filtragem de objetos para procurar apenas um evento ou eventos específicos. Por exemplo, se quiser ser notificado quando alguém criar uma conta do usuário no eDirectory, você poderá criar um filtro selecionando a classe Objeto Usuário para registrar eventos para criar um novo objeto Usuário.

Para configurar a filtragem de contas, clique no link Eventos de Objeto, selecione a classe e clique em **OK** para sair do aplicativo.

Para configurar filtros para eventos de Gerenciamento de Contas:

1. No Identity Console, selecione **Auditoria** na home page.
2. Selecione o servidor NCP que deseja monitorar e clique em **OK**.
3. Agora vá até **Configurações Avançadas** e clique em **Eventos de Objeto** em **Filtros**.

   A janela de Filtragem de Objeto do CEF aparece.
4. Na lista **Classes de Objeto Disponíveis**, selecione qualquer classe de objeto e clique na seta para a direita para movê-la para a lista **Classes do Objeto Selecionadas** e clique em **OK**.

Usando o filtro configurado, o módulo de auditoria CEF verifica todos os eventos gerados para as classes de objeto selecionadas e registra esses eventos.

Filtrando eventos de atributo CEF

Clique no link **Eventos de Atributo** para configurar a filtragem para os Eventos de Atributo. Por exemplo, se você quiser ser notificado quando alguém adicionar um novo valor de atributo no eDirectory, poderá criar um filtro para registrar eventos para adicionar um novo valor.

Para configurar a filtragem para Eventos de Atributo:

1. No Identity Console, selecione **Auditoria** na home page.
2. Selecione o servidor NCP que deseja monitorar e clique em **OK**.
3. Agora vá até **Configurações Avançadas** e clique em **Eventos de Atributo** em **Filtros**.

   A janela **Filtragem da Configuração de Atributos** é mostrada.
4. Na lista **Classes de Objeto Disponíveis**, selecione as classes do objeto para as quais você deseja coletar eventos e clique na seta para a direita para movê-las para a lista **Classes de Objeto Selecionadas**.
5. Na lista **Atributos Disponíveis**, selecione qualquer número de atributos para as classes de objeto selecionadas. Selecione o atributo e clique na seta para a direita para adicionar o atributo à lista de atributos selecionada.

   Observação: Se você selecionar uma classe de objeto, todos os Eventos de Atributo para todos os atributos nessa classe de objeto serão selecionados. Nesse caso, você obterá todos os Eventos de Atributo para todos os atributos nas classes de objeto selecionadas.

   ---
6. Clique em **OK**.

Com o filtro configurado, o módulo de auditoria CEF verifica os eventos gerados para todos os atributos e classes de objeto selecionados e registra esses eventos.

12 Gerenciando atributos criptografados

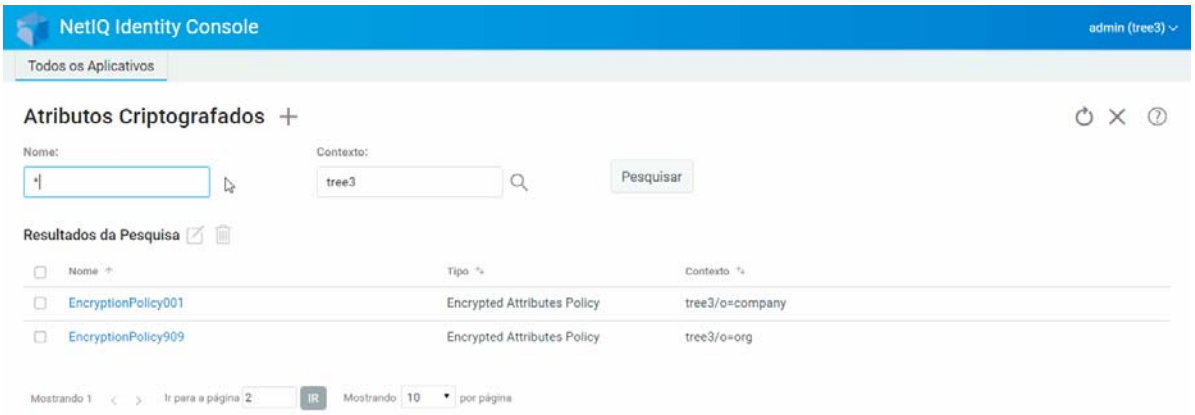
O Identity Console pode ler com segurança os atributos criptografados do servidor eDirectory. Usando o Identity Console, você pode criar, modificar ou apagar várias políticas para esses atributos criptografados.

Criando uma política para atributos criptografados

Para criar uma nova política de atributo:

1. Clique na opção **Atributos Criptografados** na landing page do Identity Console.
2. Clique no ícone +.
3. Na página Criar Política de Atributos Criptografados, digite as seguintes informações:
   - Especifique o nome da política
   - Digite ou selecione o Contexto
   - Selecione o servidor NCP
   - Selecione atributos
4. Após especificar todas as informações necessárias, clique em **Terminar**.
5. Uma confirmação aparece indicando que a política foi criada.

Figura 12-1 *Criando uma política de atributos criptografados*

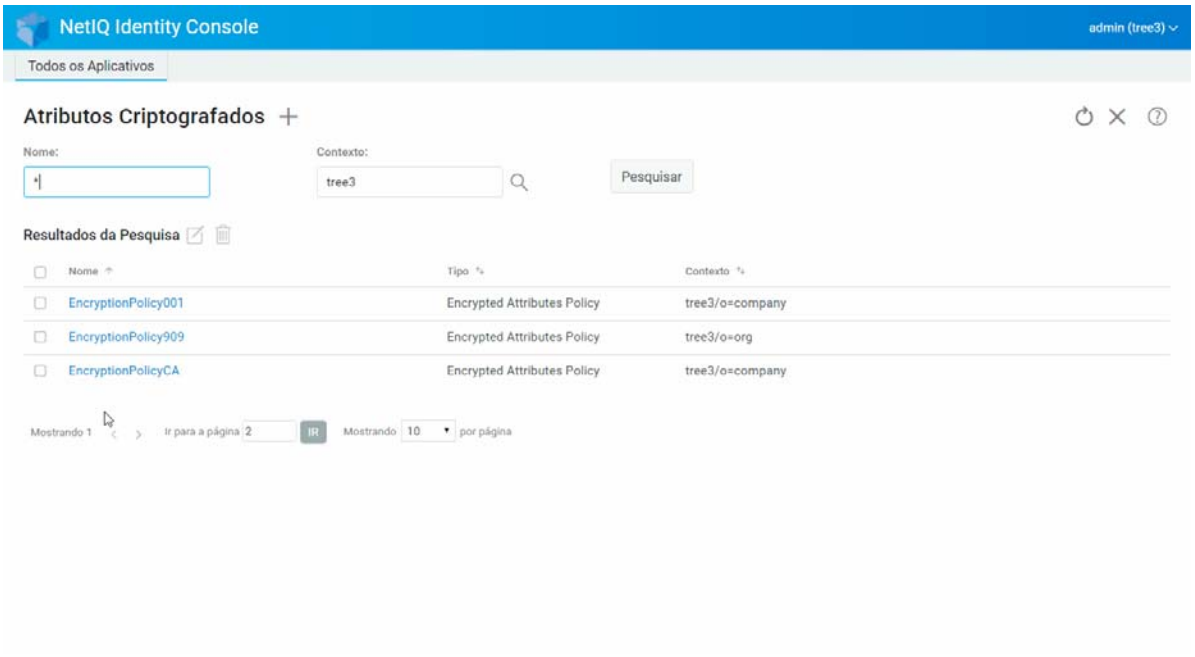


Apagando uma política de atributos criptografados

Para apagar uma política de atributos criptografados:

1. Clique na opção **Atributos Criptografados** na landing page do Identity Console.
2. Especifique o nome e o contexto do atributo ou use o recurso de pesquisa para encontrá-lo e clique no botão Pesquisar.
3. Selecione o(s) atributo(s) na lista e clique no ícone 🗑.
4. Uma confirmação aparece indicando que a política foi apagada.

Figura 12-2 *Apagando uma política de atributos criptografados*

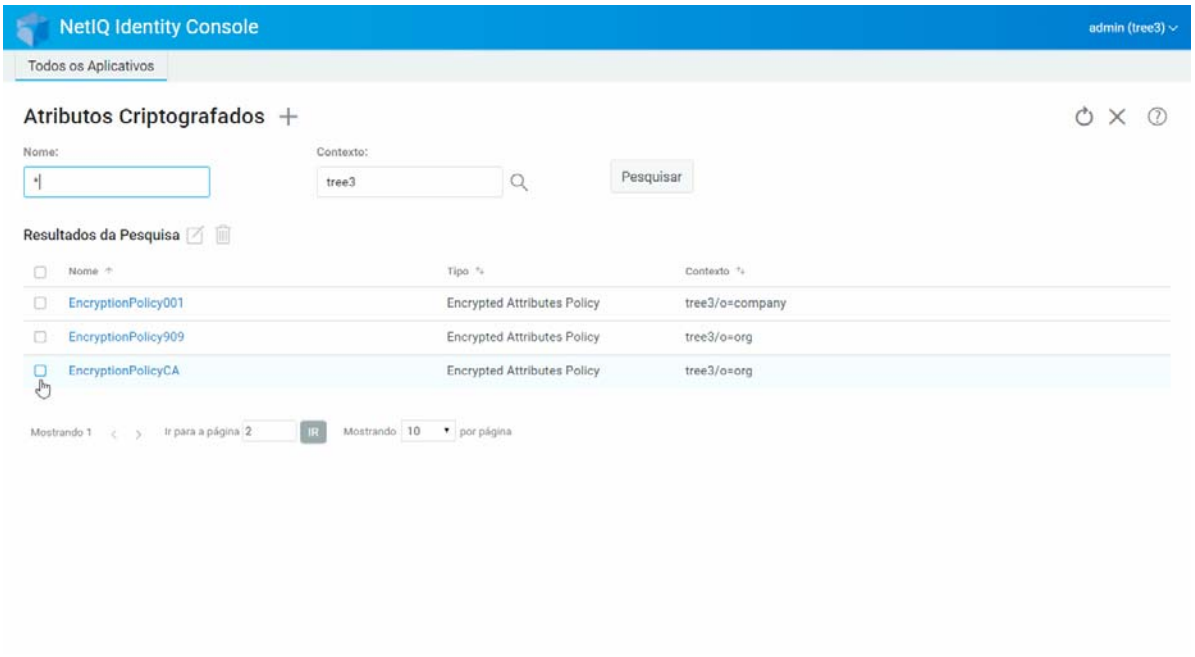


Modificando uma política de atributos criptografados

Para modificar uma política de atributos criptografados:

1. Clique na opção **Atributos Criptografados** na landing page do Identity Console.
2. Digite o nome e o contexto do objeto e clique no botão Pesquisar.
3. Selecione o atributo na lista de objetos e clique no ícone .
4. Faça suas mudanças e clique no botão Gravar.
5. Uma confirmação aparece indicando que a política foi modificada.

Figura 12-3 *Modificando uma política de atributos criptografados*



13 Gerenciando a replicação criptografada

Para habilitar a replicação criptografada, você precisa configurar uma partição para replicação criptografada. As configurações são armazenadas no objeto Raiz da partição. Você pode optar por habilitar a replicação criptografada no nível da partição. Quando você habilita a replicação criptografada no nível da partição, a replicação entre todas as réplicas que hospedam a partição é criptografada. Por exemplo, considere a partição P1 com réplicas R1, R2, R3 e R4. Você pode criptografar a replicação entre todas as réplicas.

Habilitando a replicação criptografada para partições

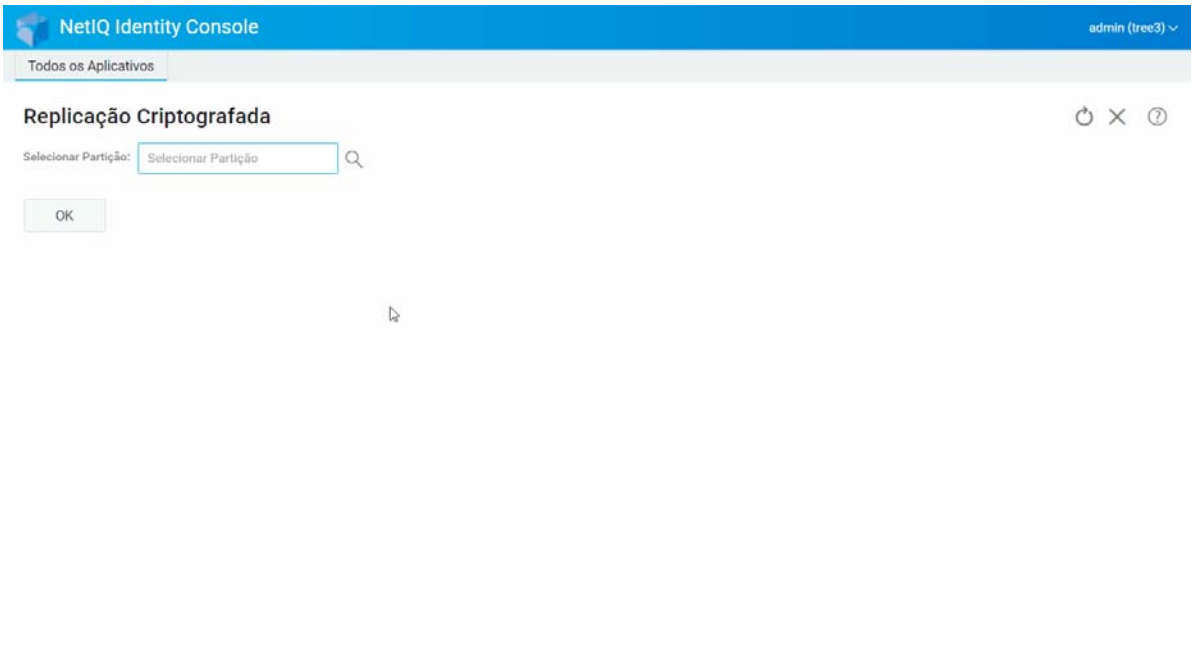
Para habilitar a replicação criptografada para partições:

Observação: Para habilitar uma partição para replicação criptografada, todos os servidores que hospedam a partição devem ser servidores eDirectory 9.2 ou posterior.

---

1. Clique na opção **Replicação Criptografada** na landing page do Identity Console.
2. Especifique ou procure a partição para a qual você deseja habilitar a replicação criptografada.
3. Selecione a opção **Habilitar Replicação Criptografada**. Ao desabilitar a replicação criptografada para uma partição, anule a seleção dessa opção.
4. Clique em **Terminar**.
5. Uma confirmação aparece indicando que a replicação criptografada foi habilitada.

Figura 13-1 *Habilitando a replicação criptografada para partições*



14 Gerenciando partições e réplicas

Operações de partição e réplica permitem que você gerencie o design e distribuição do eDirectory em seus servidores de diretório.

Partições criam divisões lógicas na árvore do eDirectory. Por exemplo, se escolher uma Unidade Organizacional e criá-la como uma partição nova, você dividirá a Unidade Organizacional e todos os seus objetos subordinados da partição pai. A Unidade Organizacional que você escolher se tornará a raiz de uma partição nova. As réplicas da partição nova existirão nos mesmos servidores das réplicas da partição pai, e os objetos na partição nova pertencerão ao objeto raiz da partição nova.

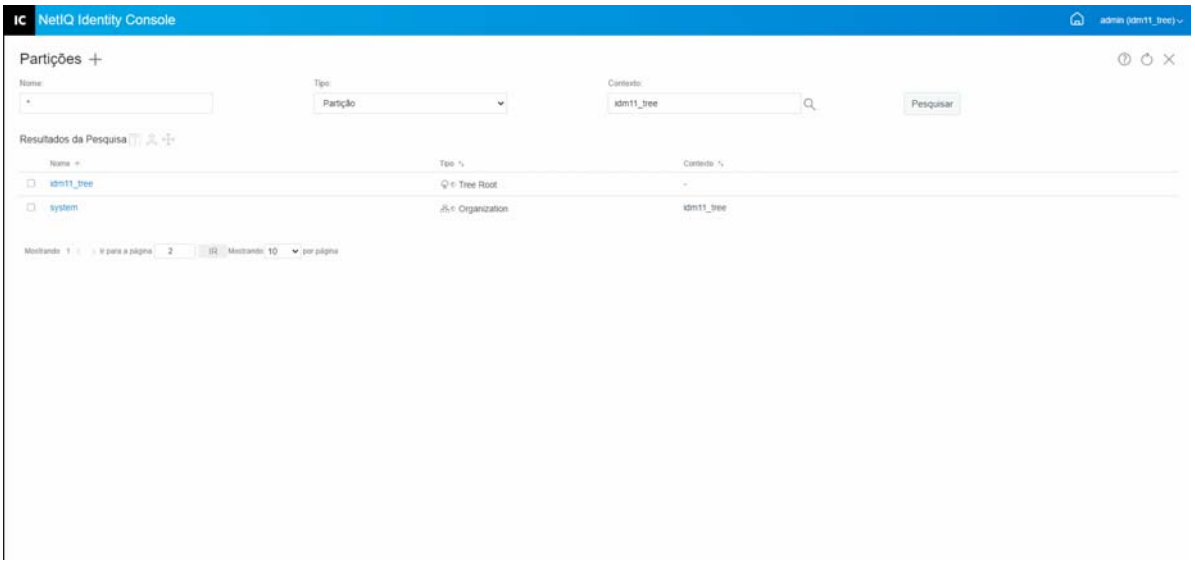
As seguintes tarefas podem ser executadas usando o módulo Partição:

Criando uma partição

Para criar uma nova partição:

1. Clique na opção **Gerenciamento de Partição** na landing page do Identity Console.
2. Clique no ícone +.
3. Na página Criar Partição, especifique o container a ser usado como raiz para a nova partição ou use o ícone 🔍 do Seletor de Objetos para localizá-lo e clique em **Criar**.
4. Uma confirmação aparece indicando que a partição foi criada.

Figura 14-1 *Criando uma nova partição*

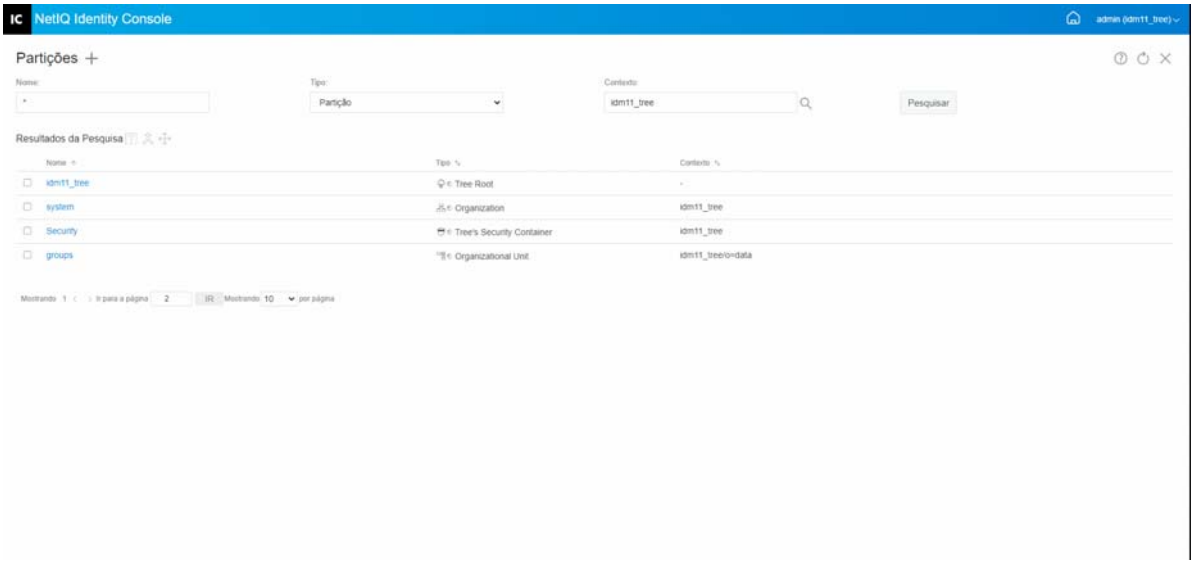


Fundir partições

Para fundir partições com a respectiva partição-mãe:

1. Clique na opção **Gerenciamento de Partição** na landing page do Identity Console.
2. Digite o nome, tipo e contexto da partição ou use o recurso de pesquisa para encontrá-lo e clique no botão Pesquisar.
3. Selecione a partição na lista de pesquisa, clique no ícone  e clique em **OK**.
4. Uma confirmação aparece indicando que a partição foi mesclada.

Figura 14-2 *Mesclando partições*



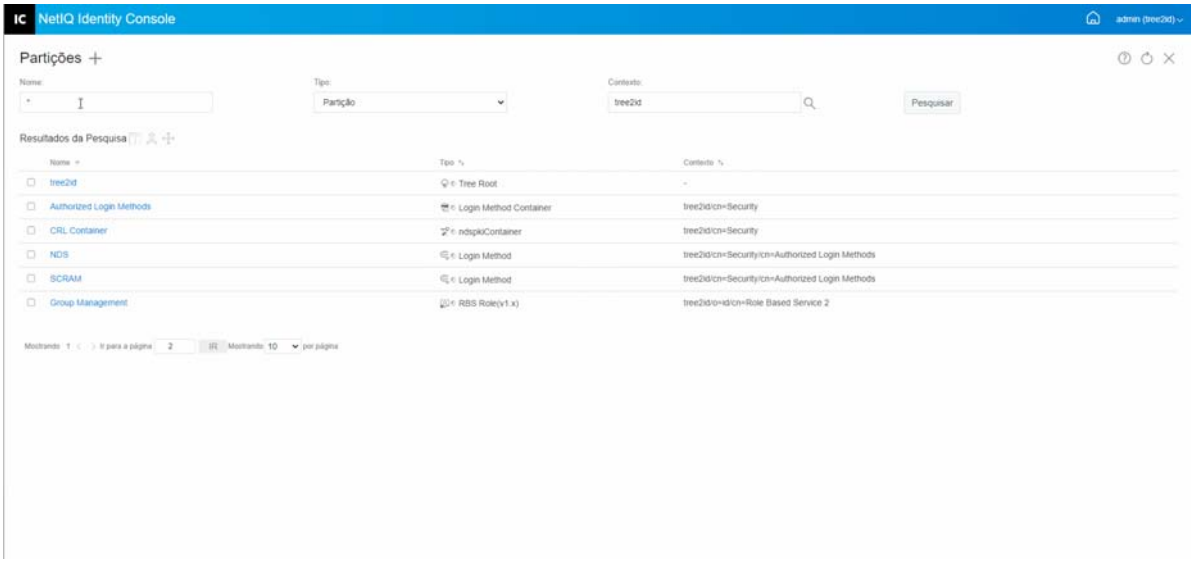
Modificando partições

Para modificar partições:

1. Clique na opção **Gerenciamento de Partição** na landing page do Identity Console.
2. Digite o nome, o tipo e o contexto da partição, depois clique no botão Pesquisar.
3. Selecione a partição da lista de pesquisa e clique no ícone .
4. Clique na opção **Editar** em **Filtro** para mudar filtros de réplica e as respectivas classes e atributos e clique em **OK**.

   Caso você tenha selecionado **Servidor** no campo **Tipo**, verá a lista de todos os servidores. Se você clicar em cada servidor, verá uma lista de todas as partições em cada um deles.
5. Uma confirmação aparece indicando que a partição foi modificada.

Figura 14-3 *Modificando partições*



Movendo uma Partição

Mover uma partição permite que você mova uma subárvore na árvore do diretório. Esta operação também é conhecida como operação de poda e inserção. Você pode mover apenas partições que não possuam partições subordinadas. Se houver partições subordinadas, você deve primeiro fundir essas partições antes da operação de movimentação.

Quando você mover uma partição, o eDirectory mudará todas as referências para o objeto raiz da partição. Embora o nome do objeto permaneça inalterado, o nome completo do container (e de todos seus subordinados) muda.

Observação: Quando mover uma partição, siga as regras de contenção do eDirectory. Por exemplo, não será possível mover uma Unidade Organizacional diretamente da raiz da árvore do diretório, porque as regras de contenção da raiz permitem apenas objetos Local, País ou Organização, mas não objetos Unidade Organizacional.

Para mover uma partição:

1 Clique na opção **Gerenciamento de Partição** na landing page do Identity Console.

2 Digite o nome, o tipo e o contexto da partição, depois clique no botão Pesquisar.

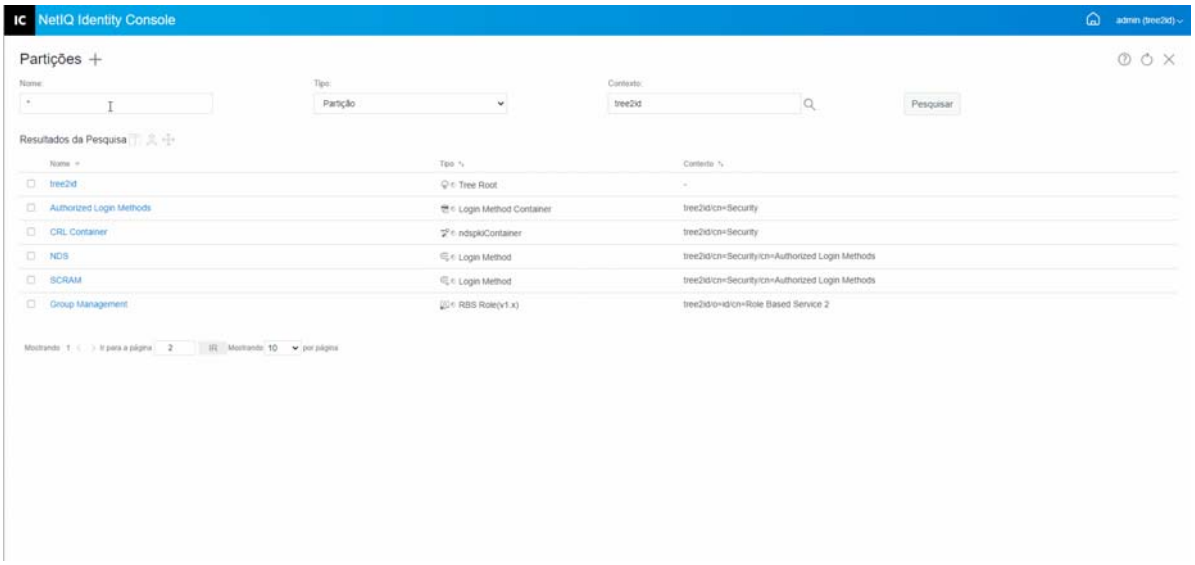
3 Selecione a partição da lista de pesquisa e clique no ícone ✣.

4 Selecione o objeto Container de destino para o qual você deseja mover a partição especificada e clique em **OK**.

Observação: A opção **Criar um álias no lugar da partição movida** cria um indicador para a nova localização da partição. Isso permite que quaisquer operações dependentes da antiga localização continuem ininterruptas até que você as atualize para refletir a nova localização. Os usuários poderão continuar efetuando login na rede e encontrando objetos na localização original do diretório.

5 Aparecerá uma mensagem de confirmação indicando que a operação de movimentação de partição foi concluída com sucesso.

Figura 14-4 *Movendo uma partição*



15 Gerenciando índices

O Index Manager é um atributo do objeto Servidor que permite gerenciar os índices do banco de dados. Esses índices são usados pelo eDirectory para melhorar consideravelmente o desempenho da consulta.

O NetIQ eDirectory é enviado com um conjunto de índices que fornece a funcionalidade de consulta básica. Esses índices padrão são para os atributos a seguir.

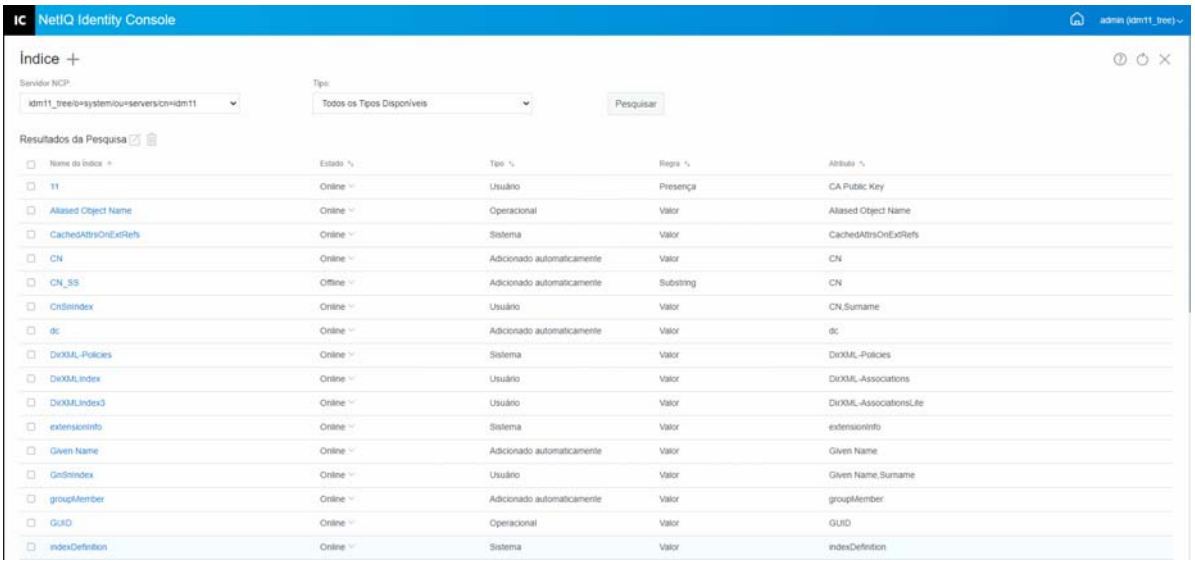
As tarefas a seguir podem ser executadas usando o módulo de índice:

Criando um índice

Para criar um novo índice:

1. Clique na opção **Gerenciamento de Índice** na landing page do Identity Console.
2. Clique no ícone +.
3. Digite o nome do índice.
4. Selecione os servidores na lista de servidores NCP disponíveis.
5. Selecione o(s) atributo(s) necessário(s).
6. Selecione a regra do índice:
   - 6a **Substring:** Corresponde a um subconjunto de uma string de valor de atributo. Por exemplo, uma consulta para localizar um Sobrenome com “der” retornaria correspondências para “Derington”, “Anderson” e “Lauder”. Um índice de substring é o índice que exige mais recursos para ser criado e mantido.
   - 6b **Presença:** Necessita apenas da presença de um atributo em vez de valores de atributos específicos. Uma consulta para localizar todas as entradas com um atributo Login Script usaria um índice de presença.
   - 6c **Valor:** Corresponde o valor inteiro da primeira parte do valor de um atributo. Por exemplo, a correspondência de valor pode ser usada para localizar entradas com Sobrenome igual a “Jensen” e entradas cujo Sobrenome comece com “Jen”.
7. Clique no botão Criar.
8. Uma confirmação aparece indicando que o índice foi criado.

Figura 15-1 *Criando um novo índice*

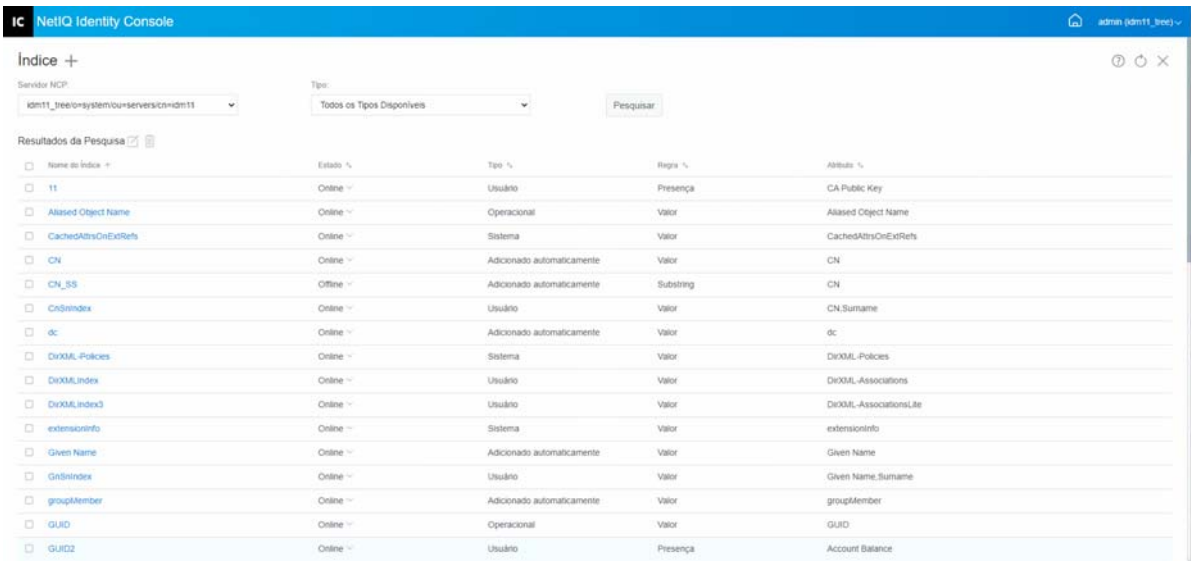


Apagando um índice

Para apagar um índice:

1. Clique na opção **Gerenciamento de Índice** na landing page do Identity Console.
2. Selecione o servidor NCP e o tipo do índice e clique no botão Pesquisar.
3. Selecione o índice na lista de pesquisa e clique no ícone 🗑.
4. Aparecerá uma confirmação indicando que o índice foi apagado.

Figura 15-2 *Apagando um índice*



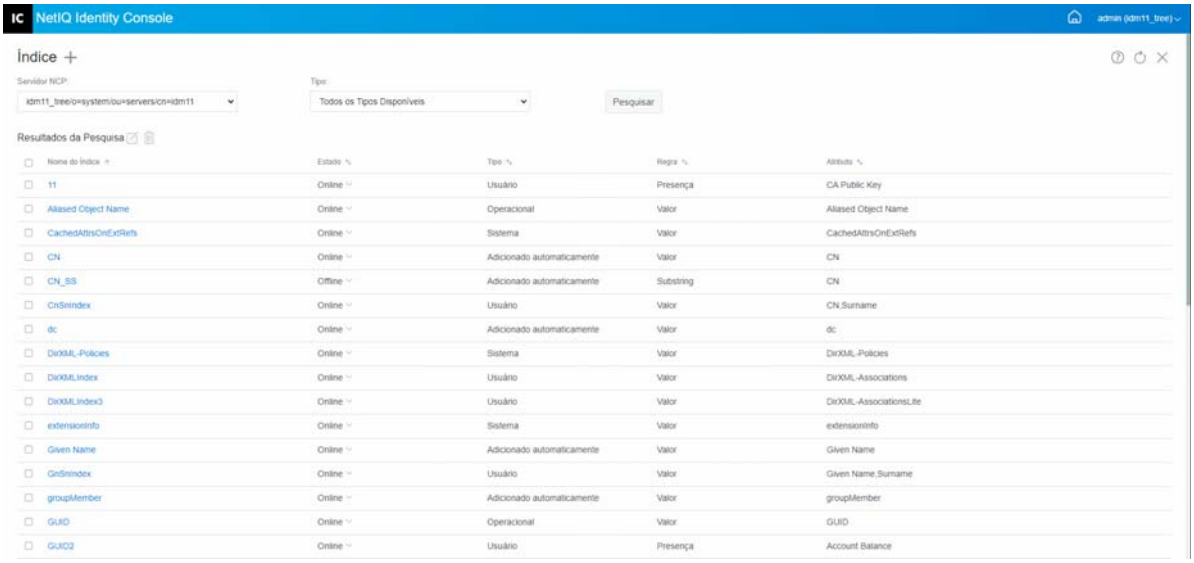
Copiando um índice

Se você concluiu que um índice específico é útil em um determinado servidor e vê a necessidade desse índice em outro servidor, pode copiar a definição de índice de um servidor para outro. Ao revisar dados predicados, você também pode encontrar um caso exatamente oposto: um índice que estava atendendo a uma necessidade de vários servidores não é mais útil em um deles. Nesse caso, você pode apagar o índice apenas daquele servidor que não está se beneficiando do índice.

Para copiar um índice:

1. Clique na opção **Gerenciamento de Índice** na landing page do Identity Console.
2. Selecione o servidor NCP e o tipo do índice e clique no botão Pesquisar.
3. Selecione o índice na lista de pesquisa e clique no ícone .
4. Selecione o(s) servidor(es) NCP em que você deseja copiar o índice e clique no botão Gravar.
5. Aparecerá uma confirmação indicando que o índice foi modificado.

Figura 15-3 *Copiando um índice*



Mudando o estado de um índice

Durante os horários de pico, você pode querer ajustar o desempenho colocando os índices temporariamente offline. Por exemplo, para obter uma velocidade adicional de carga em massa, você pode querer suspender todos os índices definidos pelo usuário. Como cada adição ou

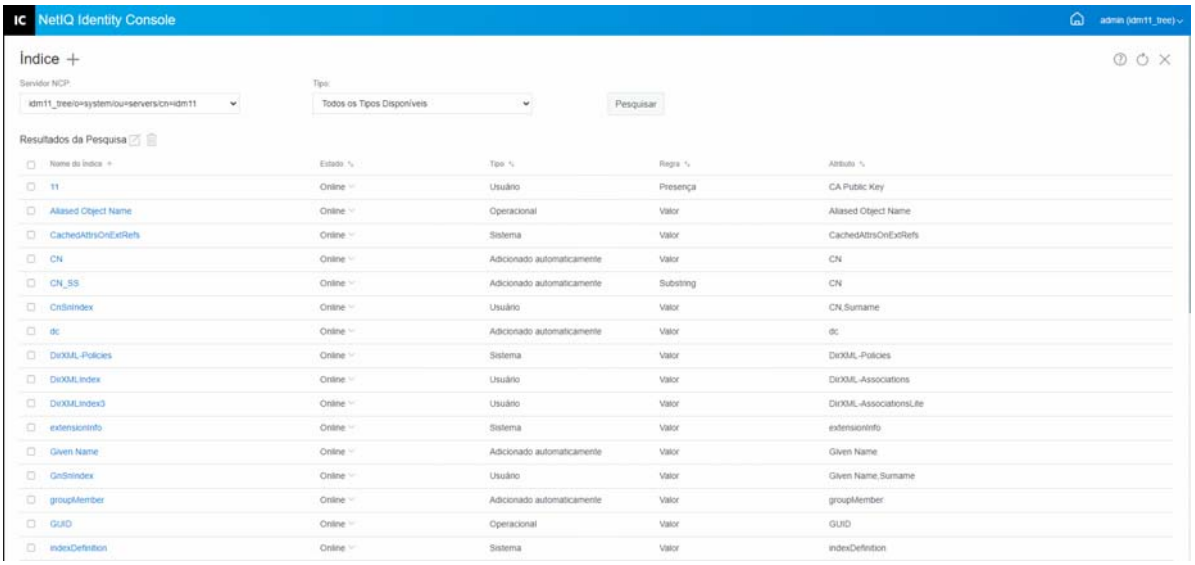
modificação de objeto requer a atualização de índices definidos, a permanência de todos os índices como ativos pode retardar o carregamento em massa de dados. Depois que o carregamento em massa é concluído, os índices podem ser colocados novamente online.

Para deixar um índice offline:

1. Clique na opção **Gerenciamento de Índice** na landing page do Identity Console.
2. Selecione o servidor NCP e o tipo do índice e clique no botão Pesquisar.
3. Clique na lista suspensa para **Estado** na lista de índices. Um índice pode ter os seguintes estados:
   - **Online:** Atualmente em execução
   - **Offline:** Suspenso. O índice pode ser iniciado novamente.

Observação: O estado dos Índices dos tipos Sistema e Operacional não pode ser mudado. Tais índices também não podem ser apagados.

Figura 15-4 *Colocando um índice offline*



16 Configurando objetos LDAP

Uma instalação do eDirectory cria um objeto servidor LDAP e um objeto Grupo LDAP. A configuração padrão para serviços LDAP está localizada no diretório desses dois objetos. Você pode modificar a configuração padrão usando a tarefa de Gerenciamento LDAP no Identity Console.

O objeto servidor LDAP representa dados de configuração específicos a um servidor. No entanto, o objeto Grupo LDAP contém informações de configuração que podem ser compartilhadas de modo prático entre vários servidores LDAP. Esse objeto fornece dados de configuração comuns e representa um grupo de servidores LDAP. Os servidores têm dados comuns.

Você pode associar vários objetos servidor LDAP a um objeto Grupo LDAP. Todos os servidores LDAP associados obtêm, então, as respectivas configurações específicas a um servidor no objeto servidor LDAP de cada um deles, mas obtêm informações comuns ou compartilhadas do objeto Grupo LDAP.

As seguintes tarefas podem ser executadas usando o módulo LDAP:

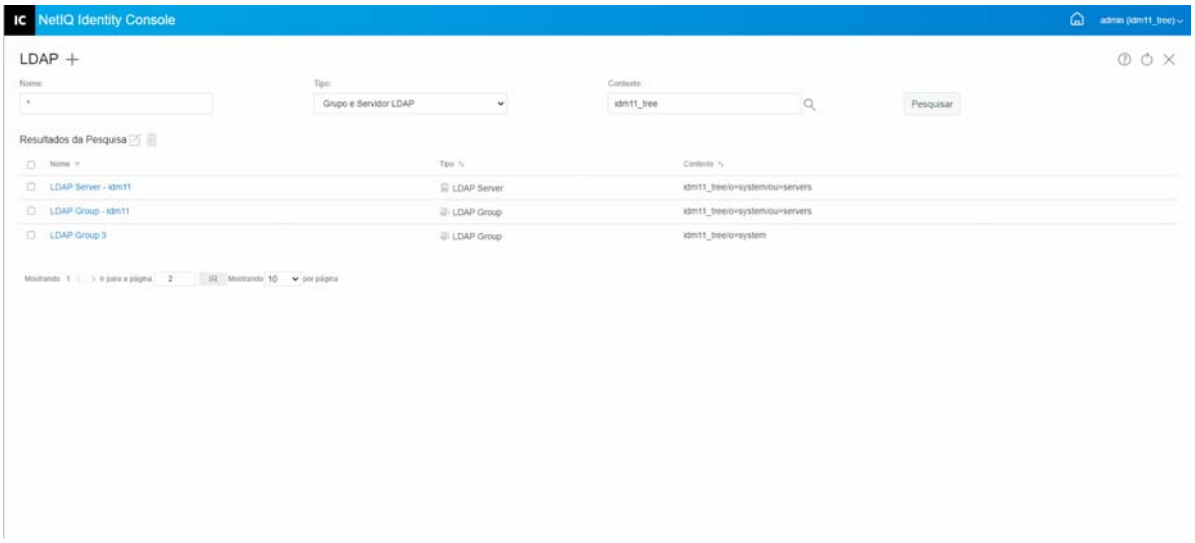
- “Criando objetos LDAP” na página 89
- “Apagando objetos LDAP” na página 90
- “Modificando objetos LDAP” na página 91

Criando objetos LDAP

Para criar um novo objeto LDAP:

1. Clique na opção **Configuração LDAP** na landing page do Identity Console.
2. Clique no ícone +.
3. Na página Criar Objeto LDAP, especifique o nome, o tipo e o contexto ou use o ícone de Pesquisar Contexto para localizá-lo e clique em **Criar**.
4. Uma confirmação aparece, indicando que o objeto LDAP foi criado.

Figura 16-1 *Criando um objeto LDAP*

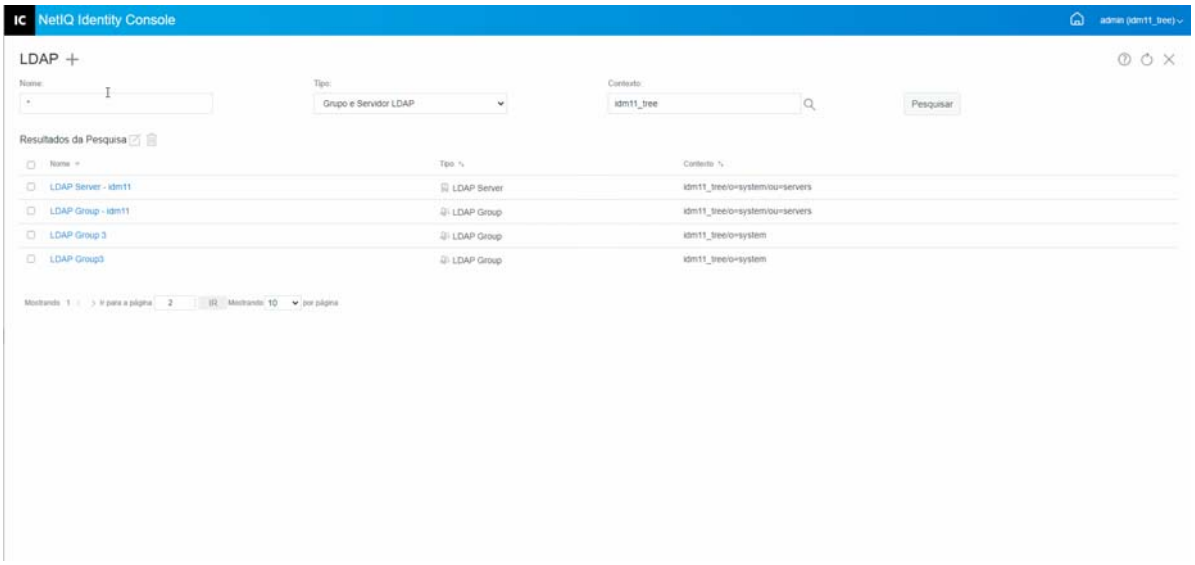


Apagando objetos LDAP

Para apagar objetos LDAP:

1. Clique na opção **Configuração LDAP** na landing page do Identity Console.
2. Especifique o nome, o tipo e o contexto do objeto LDAP, depois clique no botão Pesquisar.
3. Selecione o(s) objeto(s) LDAP na lista de pesquisa e clique no ícone 🗑.
4. Uma confirmação aparece, indicando que os objetos LDAP foram apagados.

Figura 16-2 *Apagando objetos LDAP*

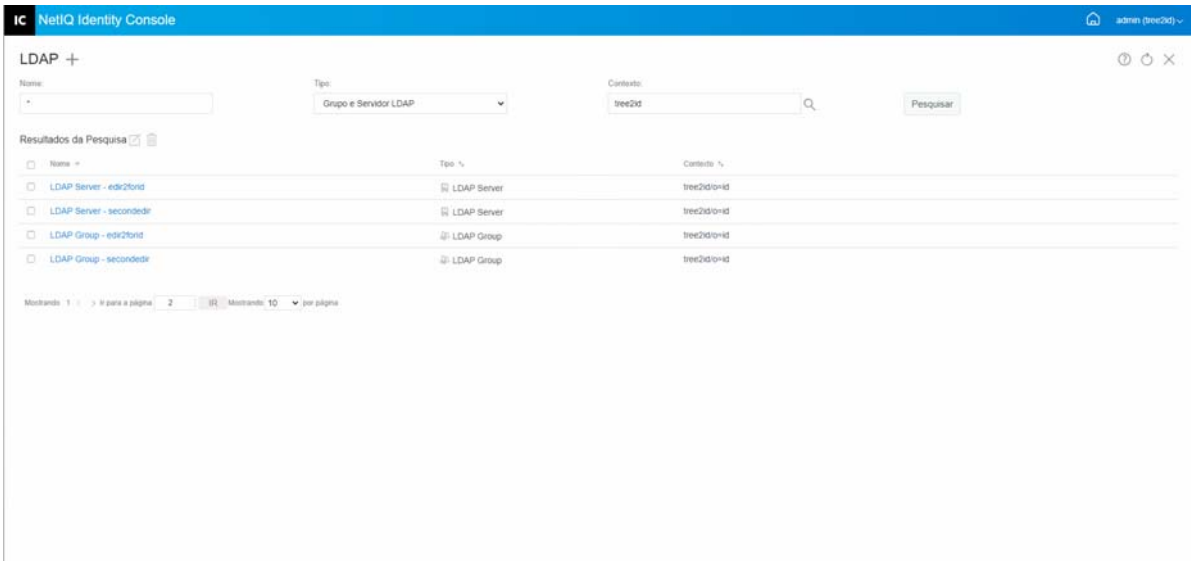


Modificando objetos LDAP

Para modificar objetos LDAP:

1. Clique na opção **Configuração LDAP** na landing page do Identity Console.
2. Digite o nome, o tipo e o contexto do objeto LDAP, depois clique no botão Pesquisar.
3. Selecione o objeto LDAP da lista de pesquisa e clique no ícone .
4. Modifique os atributos e informações para o objeto LDAP específico conforme necessário e clique no botão Gravar. Para obter mais informações sobre os atributos para objetos LDAP, consulte Configuração de objetos grupo LDAP e de servidor LDAP no Linux no *Guia de administração do NetIQ eDirectory*.
5. Uma confirmação aparece, indicando que o objeto LDAP foi modificado.

Figura 16-3 *Modificando objetos LDAP*



17 Gerenciando certificados

O Servidor de Certificação NetIQ é instalado automaticamente quando você instala o eDirectory. O Servidor de Certificação fornece serviços de criptografia de chave pública integrados nativamente ao eDirectory que permitem gerar, emitir e gerenciar certificados de servidor e de usuário. Esses serviços permitem proteger as transmissões de dados confidenciais em canais de comunicação pública como a Internet.

Observação: Se quiser usar o módulo Gerenciamento de Certificados com o Identity Console, você deverá fazer upgrade do seu servidor do eDirectory para 9.2.4 HF2.

O Identity Console fornece as seguintes tarefas de gestão de certificados:

Gerenciando a autoridade de certificação

Por padrão, o processo de instalação do Servidor de Certificação do NetIQ cria a CA (autoridade de certificação) organizacional para você. Você é solicitado a especificar um nome de CA Organizacional. Quando você clica em Terminar, a CA Organizacional é criada com os parâmetros padrão e colocada no container de segurança. Se você quiser mais controle sobre a criação da CA Organizacional, poderá criá-la manualmente usando o portal Identity Console. Além disso, se você apagar a CA Organizacional, precisará recriá-la.

Ao utilizar o módulo de autoridade de certificação, você pode executar as seguintes tarefas:

Criando um objeto CA Organizacional

Para criar um objeto CA Organizacional, execute as seguintes etapas:

1. Clique nas opções **Gerenciamento de Certificados** > **Gerenciamento de CA** na landing page do Identity Console.
2. Se não houver nenhum objeto autoridade de certificação organizacional, isso abrirá a caixa de diálogo Criar um objeto autoridade de certificação organizacional e o assistente correspondente, que criará o objeto. Siga os prompts para criar o objeto.

   Observação: Verifique se o caminho de arquivo CRL especificado aqui está relacionado ao caminho de instalação do eDirectory.
3. Depois de terminar de criar a autoridade de certificação, recomendamos que você faça um backup do par de chaves públicas/privadas da CA e armazene isso em um lugar seguro e seguro. Para obter mais informações, consulte "Fazendo backup de certificados de CA Organizacional" na página 94.

Fazendo backup de certificados de CA Organizacional

Recomendamos que você faça backup da sua chave privada da CA Organizacional no caso de o servidor de host da CA Organizacional enfrentar uma falha irrecuperável. Se ocorrer uma falha, você poderá usar o arquivo de backup para restaurar a sua CA Organizacional para qualquer servidor na árvore.

Observação: A capacidade de fazer backup de uma CA Organizacional está disponível apenas para autoridades de certificação Organizacionais criadas com o Servidor de Certificação versão 9.0 ou posterior. Em versões anteriores do Servidor de Certificação, a chave privada da CA Organizacional foi criada de modo a impossibilitar a exportação.

O arquivo de backup contém a chave privada, o certificado autoassinado, o certificado de chave pública e vários outros certificados da CA, necessários para que ela opere. Essas informações são armazenadas no formato PKCS #12 (também conhecido como PFX).

O backup da CA Organizacional deverá ser realizado quando ela estiver funcionando corretamente.

Para fazer backup da CA Organizacional, execute as seguintes etapas:

1. Clique nas opções **Gerenciamento de Certificados** > **Gerenciamento de CA** na landing page do Identity Console.
2. Clique na guia **Certificados**.
3. Selecione o **Certificado autoassinado** ou o **Certificado de chave pública**. Ambos os certificados são gravados no arquivo durante a operação de backup. Recomendamos que você selecione o certificado autoassinado para certificados RSA e ECDSA separadamente.
4. Clique no ícone  .

5 Escolha exportar a chave privada, especifique uma senha com 6 ou mais caracteres alfanuméricos para usar na criptografia do arquivo PFX, selecione PKCS12 como formato de exportação e clique em **OK**.

6 O arquivo de backup criptografado é gravado no local especificado. Agora ele está pronto para ser armazenado em um local seguro para uso emergencial.

Restaurando uma CA Organizacional

Se o objeto CA Organizacional tiver sido apagado ou corrompido, ou se o servidor de host da CA Organizacional tiver sofrido uma falha irrecuperável, a CA Organizacional poderá ser restaurada para operação integral usando um arquivo de backup criado como descrito em "Fazendo backup de certificados de CA Organizacional" na página 94.

Para restaurar a CA Organizacional, execute as seguintes etapas:

1 Clique nas opções **Gerenciamento de Certificados** > **Gerenciamento de CA** na landing page do Identity Console.

2 Clique no ↑↓ na parte superior da tela (ao lado do **Gerenciamento de Autoridade de Certificação**) para apagar a CA Organizacional existente.

3 Agora você será solicitado a configurar uma nova CA Organizacional. Esse procedimento faz com que a caixa de diálogo Criar um objeto autoridade de certificação organizacional e o assistente correspondente que cria o objeto sejam abertos.

4 Na caixa de diálogo de criação, especifique o servidor que deve hospedar a CA Organizacional e o nome do objeto CA Organizacional.

5 Selecione **Importar**.

6 Selecione os certificados RSA e ECDSA. O Servidor de Certificação exige que ambos os certificados tenham o mesmo nome do assunto. No entanto, o Servidor de Certificação não suporta a importação de certificados de CA autoassinados externos. No entanto, permite importar certificados de CA subordinados.

7 Nas telas subsequentes, procure e selecione o nome do arquivo para RSA e ECDSA.

8 Digite a senha usada para criptografar o arquivo quando o backup foi feito e clique em **OK**.

9 A chave privada e os certificados da CA Organizacional foram restaurados e a CA está totalmente funcional. O arquivo agora pode ser armazenado novamente para uso futuro.

Validando os certificados da CA Organizacional

Se você suspeitar de um problema com um certificado ou suspeitar que ele pode não ser mais válido, você poderá validar facilmente o certificado usando o Identity Console. Qualquer certificado na árvore do eDirectory pode ser validado, incluindo certificados emitidos por autoridades de certificação externas.

O processo de validação do certificado inclui várias verificações dos dados no certificado, bem como os dados na cadeia de certificação. Uma cadeia de certificação é composta por um certificado de CA raiz e, opcionalmente, os certificados de uma ou mais autoridades de certificação intermediárias.

Para validar um certificado:

1. Clique nas opções **Gerenciamento de Certificados** > **Gerenciamento de CA** na landing page do Identity Console.
2. Clique na guia **Certificados**.
3. Selecione o **Self Signed Certificate** (Certificado Autoassinado) ou o **Public Key Certificate** (Certificado de Chave Pública).
4. Clique no ícone para validar os certificados de CA selecionados.

Substituindo os certificados da CA Organizacional

Se os certificados ficarem corrompidos ou inválidos por algum motivo, ou se você apenas quiser substituir os certificados existentes, execute as seguintes etapas:

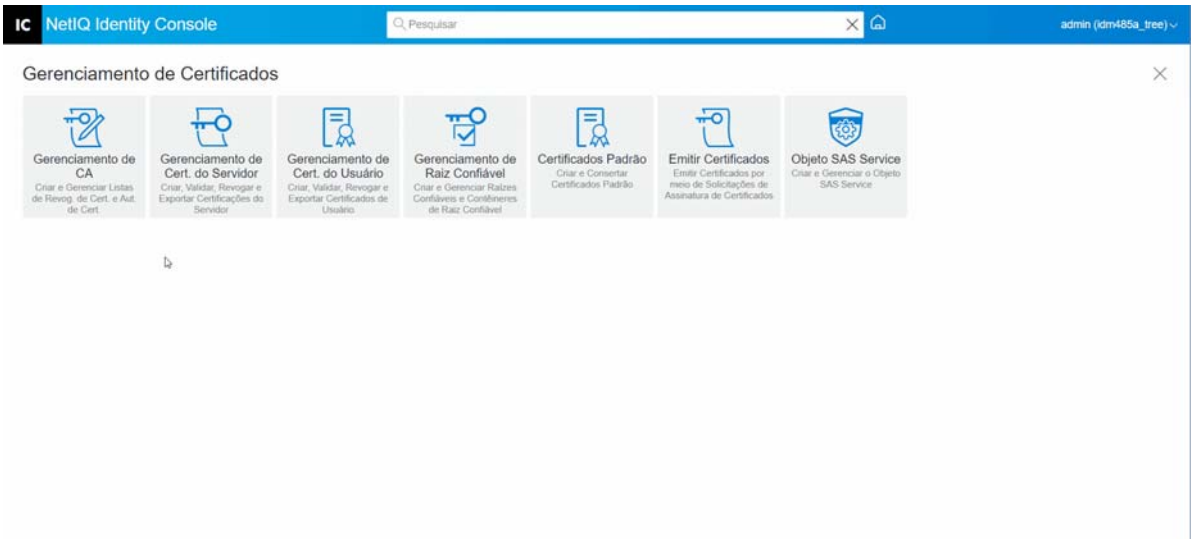
1. Clique nas opções **Gerenciamento de Certificados** > **Gerenciamento de CA** na landing page do Identity Console.
2. Clique na guia **Certificados**.
3. Selecione o **Self Signed Certificate** (Certificado Autoassinado) ou o **Public Key Certificate** (Certificado de Chave Pública).
4. Clique no ícone para substituir o certificado de CA selecionado.
5. Importe um certificado de CA no formato `.pfx` ou `.p12` e especifique uma senha para criptografar a chave privada.
6. Clique em **OK**.

Revogando os certificados da CA Organizacional

Para revogar um certificado:

1. Clique nas opções **Gerenciamento de Certificados** > **Gerenciamento de CA** na landing page do Identity Console.
2. Clique na guia **Certificados**.
3. Selecione o **Self Signed Certificate** (Certificado Autoassinado) ou o **Public Key Certificate** (Certificado de Chave Pública).
4. Clique no ícone .
5. Leia e entenda o risco envolvido com a revogação de certificados de servidor.
6. Selecione uma razão válida para revogação da lista suspensa, selecione a data de invalidade e especifique qualquer outro comentário.
7. Clique em **OK** para terminar a revogação.

Figura 17-1 *Gerenciando a autoridade de certificação*



Gerenciando certificados de servidor

Ao utilizar o módulo de Gestão de Certificados de Servidor, o administrador pode executar as seguintes tarefas:

- “Criando objetos certificação do servidor” na página 97
- “Exportando objetos certificação do servidor” na página 98
- “Validando objetos certificação do servidor” na página 98
- “Substituindo um objeto certificação do servidor” na página 98
- “Revogando objetos certificação do servidor” na página 99
- “Apagando objetos certificação do servidor” na página 99

Criando objetos certificação do servidor

Para criar um objeto certificação do servidor, execute as seguintes etapas:

1. Clique nas opções **Gerenciamento de Certificados** > **Gerenciamento de Cert. do Servidor** na landing page do Identity Console.
2. Clique no ícone +.
3. Na página **Criar certificado de servidor**, especifique um **Apelido**, um servidor e selecione qualquer uma das seguintes opções:
   - **Padrão (parâmetros padrão):** Permite criar um objeto certificação do servidor padrão do tipo RSA ou ECDSA.
   - **Personalizado (parâmetros especificados pelo usuário):** Permite especificar os parâmetros personalizados para o objeto certificação do servidor.
   - **Importar (permite importar um arquivo PKCS12):** Permite importar um arquivo PKCS12 no formato `.pfx` ou `.p12`.

4 Depois de especificar os parâmetros, clique em **Próximo** para revisar o resumo do certificado.

5 Na tela **Resumo**, clique em **OK** para criar um objeto certificação do servidor.

Exportando objetos certificação do servidor

Para exportar objetos certificação do servidor, execute as seguintes etapas:

1 Clique nas opções **Gerenciamento de Certificados** > **Gerenciamento de Cert. do Servidor** na landing page do Identity Console.

2 Selecione o servidor apropriado na lista suspensa.

3 Selecione o certificado de servidor apropriado na lista e clique no ícone .

4 Na próxima tela, selecione a caixa de seleção para **Exportar a chave privada** e especifique uma senha para proteger a chave privada. Confirme a senha e selecione o formato de exportação.

Observação: Os certificados de servidor podem ser exportados apenas no formato PKCS12.

---

5 Clique em **OK** exportar o objeto certificação do servidor.

Validando objetos certificação do servidor

Para validar um objeto certificação do servidor, execute as seguintes etapas:

1 Clique nas opções **Gerenciamento de Certificados** > **Gerenciamento de Cert. do Servidor** na landing page do Identity Console.

2 Selecione o servidor apropriado na lista suspensa.

3 Selecione o certificado de servidor apropriado na lista e clique no ícone .

4 Uma confirmação aparece, indicando uma validação bem-sucedida do objeto certificação do servidor.

Substituindo um objeto certificação do servidor

Se os certificados de servidor se tornarem corrompidos ou inválidos por algum motivo ou se você apenas quiser substituir os certificados padrão existentes, execute as seguintes etapas:

1 Clique nas opções **Gerenciamento de Certificados** > **Gerenciamento de Cert. do Servidor** na landing page do Identity Console.

2 Selecione o servidor apropriado na lista suspensa.

3 Selecione o certificado de servidor apropriado na lista e clique no ícone .

4 Leia e entenda o risco envolvido na substituição de certificados de servidor e clique em **OK**.

5 Na próxima tela, procure o novo certificado de servidor no formato `.pfx` ou `.p12`, selecione-o e especifique uma senha.

6 Clique em **OK** para substituir o certificado de servidor.

Revogando objetos certificação do servidor

Para revogar um objeto certificação do servidor, execute as seguintes etapas:

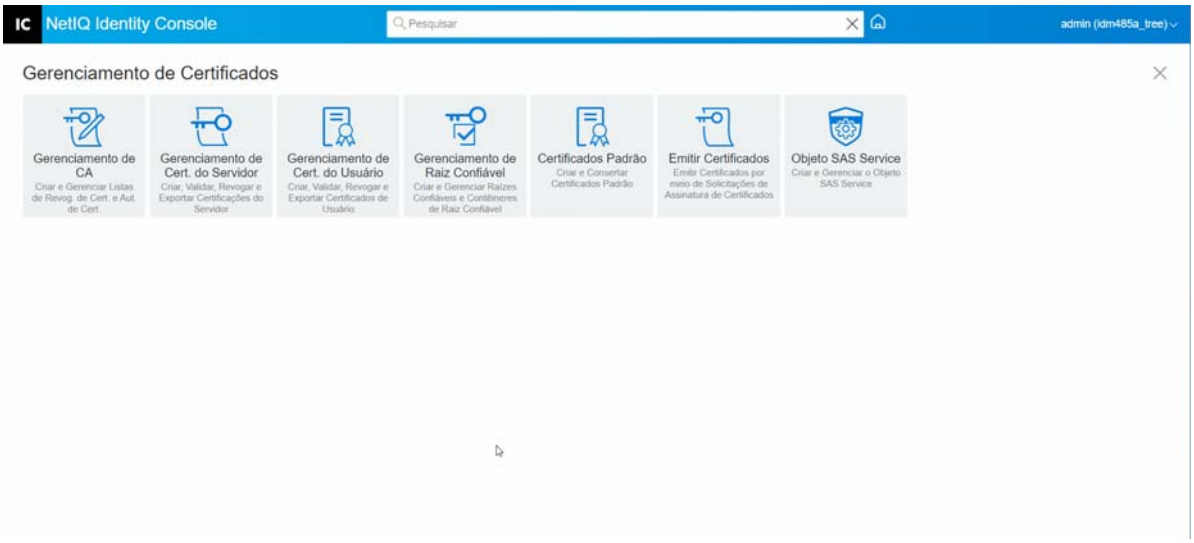
1. Clique nas opções **Gerenciamento de Certificados** > **Gerenciamento de Cert. do Servidor** na landing page do Identity Console.
2. Selecione o servidor apropriado na lista suspensa.
3. Selecione o certificado de servidor apropriado na lista e clique no ícone ⊘.
4. Leia e entenda o risco envolvido na revogação de certificados de servidor e clique em **OK**.
5. Na próxima tela, selecione uma razão válida para revogação na lista suspensa, selecione a data de invalidade e especifique qualquer outro comentário.
6. Clique em **OK** para terminar a revogação.

Apagando objetos certificação do servidor

Para remover objetos certificação do servidor, execute as seguintes etapas:

1. Clique nas opções **Gerenciamento de Certificados** > **Gerenciamento de Cert. do Servidor** na landing page do Identity Console.
2. Selecione o servidor apropriado na lista suspensa.
3. Selecione o certificado de servidor apropriado na lista e clique no ícone 🗑.
4. Na próxima tela, clique em **OK**.
5. Uma confirmação aparece, indicando que o objeto certificação do servidor foi apagado com êxito.

Figura 17-2 *Gerenciando certificados de servidor*



Gerenciando certificados de usuário

Ao utilizar o módulo Gestão de Certificados de usuário, você pode executar a seguinte tarefa:

Criando objetos certificado de usuário

Para criar um objeto certificado de usuário, execute as seguintes etapas:

1. Clique nas opções **Gerenciamento de Certificados** > **Gerenciamento de Cert. do Usuário** na landing page do Identity Console.
2. Clique no ícone +.
3. Na página **Criar certificado de usuário**, especifique um **Apelido**, um servidor e selecione qualquer uma das seguintes opções:
   - **Padrão (parâmetros padrão):** Permite criar um objeto certificado de usuário padrão do tipo RSA ou ECDSA.
   - **Personalizado (parâmetros especificados pelo usuário):** Permite especificar os parâmetros personalizados para o objeto certificado de usuário.
   - **Importar:** Permite importar um arquivo de certificado no formato CERT ou PKCS12.
4. Depois de especificar os parâmetros, clique em **Próximo** para revisar o resumo do certificado.
5. Na tela **Resumo**, clique em **OK** para criar um objeto certificado de usuário.

Exportando objetos certificado de usuário

Para exportar objetos certificado de usuário, execute as seguintes etapas:

1. Clique nas opções **Gerenciamento de Certificados** > **Gerenciamento de Cert. do Usuário** na landing page do Identity Console.
2. Selecione o servidor apropriado na lista suspensa.
3. Selecione o certificado de usuário apropriado na lista e clique no ícone .
4. Na próxima tela, selecione a caixa de seleção para **Exportar a chave privada** e especifique uma senha para proteger a chave privada. Confirme a senha e selecione o formato de exportação.

   Observação: Os certificados de usuário podem ser exportados apenas no formato PKCS12.
5. Clique em **OK** para exportar o objeto certificado de usuário.

Validando objetos certificado de usuário

Para validar um objeto certificado de usuário, execute as seguintes etapas:

1. Clique nas opções **Gerenciamento de Certificados** > **Gerenciamento de Cert. do Usuário** na landing page do Identity Console.
2. Selecione o servidor apropriado na lista suspensa.
3. Selecione o certificado de usuário apropriado na lista e clique no ícone .
4. Uma confirmação aparece, indicando uma validação bem-sucedida do objeto certificado de usuário.

Revogando objetos certificado de usuário

Para revogar um objeto certificado de usuário, execute as seguintes etapas:

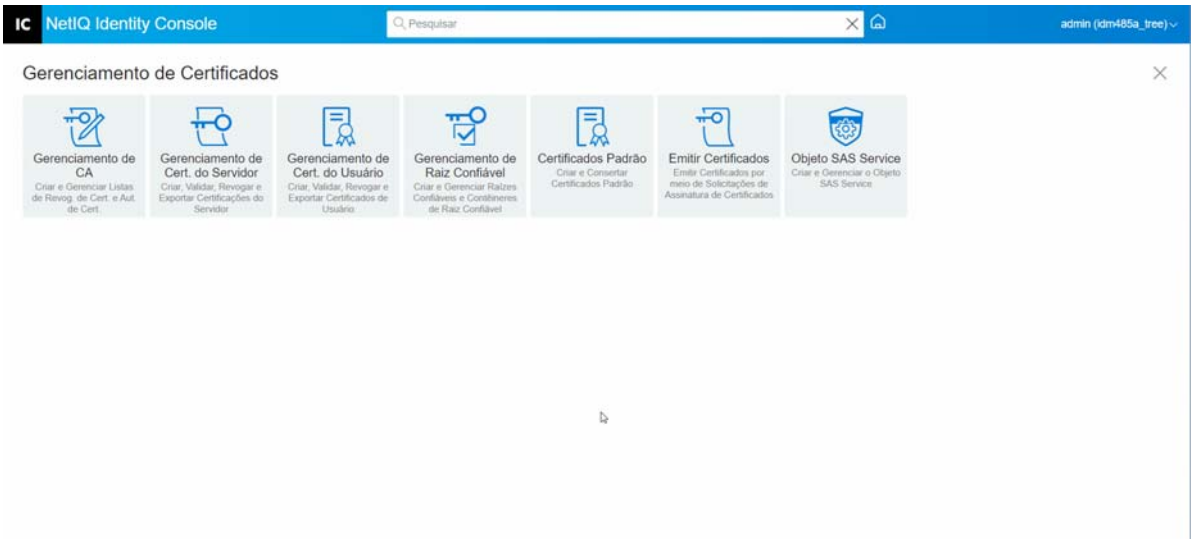
1. Clique nas opções **Gerenciamento de Certificados** > **Gerenciamento de Cert. do Usuário** na landing page do Identity Console.
2. Selecione o servidor apropriado na lista suspensa.
3. Selecione o certificado de usuário apropriado na lista e clique no ícone .
4. Leia e entenda o risco envolvido com a revogação de certificados de usuário.
5. Selecione uma razão válida para revogação da lista suspensa, selecione a data de invalidade e especifique qualquer outro comentário.
6. Clique em **OK** para terminar a revogação.

Apagando objetos certificado de usuário

Para remover objetos certificado de usuário, execute as seguintes etapas:

1. Clique nas opções **Gerenciamento de Certificados** > **Gerenciamento de Cert. do Usuário** na landing page do Identity Console.
2. Selecione o servidor apropriado na lista suspensa.
3. Selecione o certificado de usuário apropriado na lista e clique no ícone .
4. Na próxima tela, clique em **OK**.
5. Uma confirmação aparece, indicando que o objeto certificado de usuário foi apagado com êxito.

Figura 17-3 *Gerenciando certificados de usuário*



Gerenciando containers e raiz confiável

Uma raiz confiável fornece a base para a confiança em uma criptografia de chave pública. Raízes confiáveis são usadas para validar certificados assinados por outras autoridades de certificação. As raízes confiáveis habilitam a segurança para autenticação baseada em SSL, e-mail seguro e certificados.

Ao utilizar o módulo Gerenciamento de raiz confiável, você pode executar as seguintes tarefas:

- “Criando um container de raiz confiável” na página 102
- “Criando um objeto certificado raiz confiável” na página 103
- “Exportando objetos certificado de raiz confiável” na página 103
- “Validando objetos certificado de raiz confiável” na página 103
- “Apagando objetos certificado de raiz confiável” na página 104
- “Apagando containers de raiz confiável” na página 104

Criando um container de raiz confiável

Para criar um container de raiz confiável, execute as seguintes tarefas:

1. Clique nas opções **Gerenciamento de Certificados** > **Gerenciamento de Raiz Confiável** na landing page do Identity Console. A caixa de seleção **Contêiner de Raiz Confiável** será selecionada por padrão.
2. Clique no ícone + para criar um novo container de raiz confiável.
3. Especifique um nome para o container de raiz confiável.
4. Use o seletor de objetos para procurar o container apropriado.
5. Clique no botão **OK**.
6. Uma confirmação aparece, indicando que o container de raiz confiável foi criado com sucesso.

Criando um objeto certificado raiz confiável

Para criar um objeto raiz confiável, execute as seguintes etapas:

1. Clique nas opções **Gerenciamento de Certificados** > **Gerenciamento de Raiz Confiável** na landing page do Identity Console. A caixa de seleção **Container de raiz confiável** será selecionada por padrão. Selecione a caixa de seleção **Raiz confiável**.
2. Clique no ícone + para criar um novo objeto raiz confiável.
3. Especifique um nome para o objeto raiz confiável.
4. Selecione o container de raiz confiável apropriado na lista suspensa.
5. Procure o arquivo de certificado apropriado no formato `.der` ou `.b64` e selecione-o.

   Observação: Qualquer tipo de certificado pode ser armazenado em um objeto raiz confiável (certificados de CA, certificados de CA intermediários ou certificados de usuário).
6. Clique no botão **OK**.
7. Uma confirmação aparece, indicando que o objeto raiz confiável foi criado com sucesso.

Exportando objetos certificado de raiz confiável

Para exportar objetos certificado de raiz confiável, execute as seguintes etapas:

1. Clique nas opções **Gerenciamento de Certificados** > **Gerenciamento de Raiz Confiável** na landing page do Identity Console. A caixa de seleção **Container de raiz confiável** será selecionada por padrão. Selecione a caixa de seleção **Raiz confiável**.
2. Selecione o certificado de raiz confiável apropriado na lista e clique no ícone .
3. Na próxima tela, selecione a caixa de seleção para **Exportar a chave privada** e especifique uma senha para proteger a chave privada. Confirme a senha e selecione o formato de exportação.

   Observação: Os certificados de raiz confiável podem ser exportados apenas nos formatos DER ou BASE64.
4. Clique em **OK** para exportar o objeto certificado de raiz confiável.

Validando objetos certificado de raiz confiável

Para validar objetos certificado de raiz confiável, execute as seguintes etapas:

1. Clique nas opções **Gerenciamento de Certificados** > **Gerenciamento de Raiz Confiável** na landing page do Identity Console. A caixa de seleção **Container de raiz confiável** será selecionada por padrão. Selecione a caixa de seleção **Raiz confiável**.
2. Selecione o certificado de raiz confiável apropriado na lista e clique no ícone .
3. Uma confirmação aparece, indicando uma validação bem-sucedida do objeto certificado de raiz confiável.

Apagando objetos certificado de raiz confiável

Para remover objetos certificado de raiz confiável, execute as seguintes etapas:

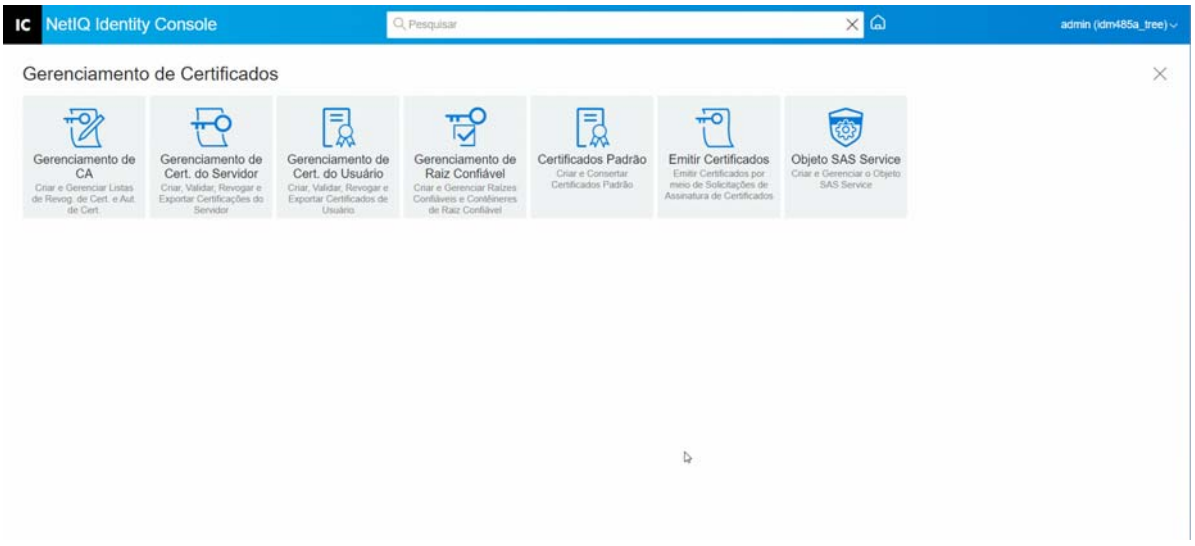
1. Clique nas opções **Gerenciamento de Certificados** > **Gerenciamento de Raiz Confiável** na landing page do Identity Console. A caixa de seleção **Container de raiz confiável** será selecionada por padrão. Selecione a caixa de seleção **Raiz confiável**.
2. Selecione o certificado de raiz confiável apropriado na lista e clique no ícone .
3. Clique em **OK** na tela de aviso.
4. Uma confirmação aparece, indicando uma remoção bem-sucedida do objeto certificado de raiz confiável.

Apagando containers de raiz confiável

Para remover um container de raiz confiável, execute as seguintes etapas:

1. Clique nas opções **Gerenciamento de Certificados** > **Gerenciamento de Raiz Confiável** na landing page do Identity Console. A caixa de seleção **Contêiner de Raiz Confiável** será selecionada por padrão.
2. Selecione o container de raiz confiável apropriado na lista e clique no ícone .
3. Clique em **OK** na tela de aviso.
4. Uma confirmação aparece, indicando uma remoção bem-sucedida do container de raiz confiável.

Figura 17-4 *Gerenciando containers de raiz confiável*



Criando objetos certificação do servidor padrão

A instalação do Servidor de Certificação cria objetos certificação do servidor padrão.

- SSL CertificateDNS - *nome_do_servidor*

- Um certificado para cada endereço IP configurado no servidor (IPAG*xxx.xxx.xxx.xxx - nome_do_servidor*)
- Um certificado para cada nome DNS configurado no servidor (DNSAG*www.exemplo.com - nome_do_servidor*)

Observação: O eDirectory não cria automaticamente o SSL CertificateIP. O SSL CertificateDNS contém todos os IPs listados no Nome Alternativo do Assunto. Quando você tenta criar ou reparar os certificados padrão usando o Identity Console, o certificado SSL CertificateIP não é criado nem reparado por padrão. No entanto, a interface de plug-in fornece uma caixa de seleção que você pode selecionar para anular o comportamento padrão e forçar a criação/reparo do certificado SSL CertificateIP.

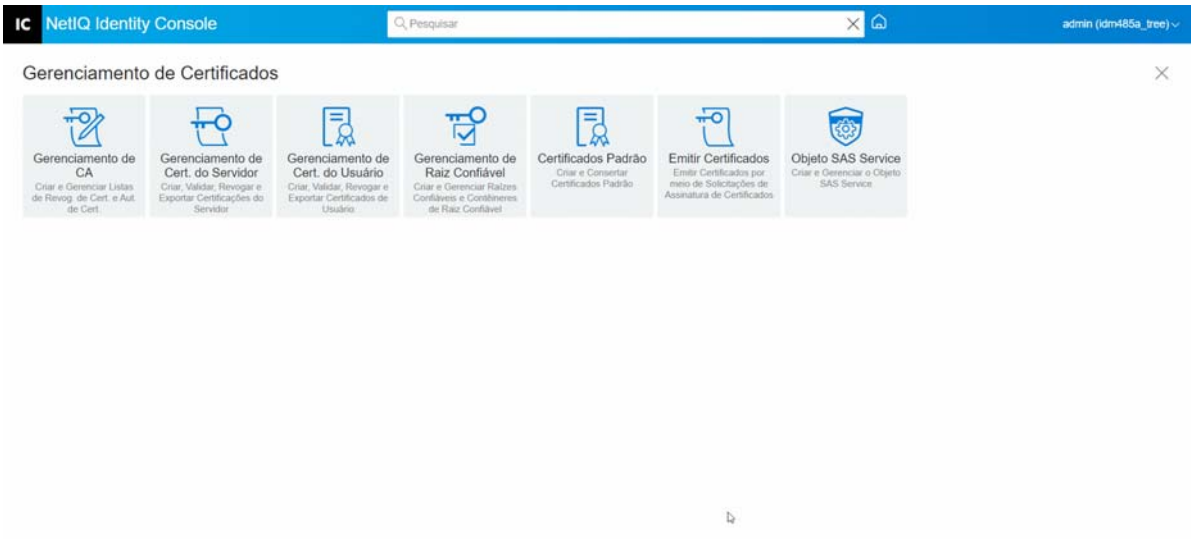
O eDirectory 9.0 ou superior criará automaticamente certificados ECDSA se a CA da organização tiver um certificado ECDSA.

Se esses certificados ficarem corrompidos ou inválidos por algum motivo ou se você apenas quiser substituir os certificados padrão existentes, você poderá usar o Assistente de criação de certificados de servidor padrão, conforme descrito no procedimento a seguir:

1. Clique nas opções **Gerenciamento de Certificados** > **Certificados Padrão** da landing page do Identity Console.
2. Selecione o servidor ou servidores para os quais deseja criar certificados padrão, depois clique em **Próximo**.
3. Selecione Sim se quiser sobregravar os certificados padrão do servidor existentes ou selecione Não se quiser sobregravar os certificados de servidor padrão existentes somente se eles forem inválidos.
4. (Somente servidor único) Se você quiser usar o endereço DNS existente, selecione essa opção. Se você quiser usar um endereço DNS diferente, selecione essa opção e especifique o novo endereço DNS.
5. (Somente servidor único) Se você quiser usar o endereço IP padrão existente, selecione essa opção. Se você quiser usar um endereço IP diferente, selecione essa opção e especifique o novo endereço IP.
6. Clique em **Próximo**.
7. Revise a página de resumo e clique em **Terminar**.

Se quiser mais controle sobre a criação do objeto certificação do servidor, você poderá criá-lo manualmente. Para obter mais informações, consulte “Criando objetos certificação do servidor” na página 97.

Figura 17-5 *Criando objetos certificação do servidor padrão*



Emitindo um certificado de chave pública

A sua CA Organizacional funciona da mesma forma que uma CA externa. Ou seja, ela tem a capacidade de emitir certificados por meio de solicitações de assinatura de certificados (CSRs). É possível emitir certificados usando a CA Organizacional quando um usuário envia uma CSR para que você assine. O usuário interessado em obter o certificado pode pegar o certificado emitido e importá-lo diretamente para o aplicativo habilitado por criptografia.

Esta tarefa permite que você gere certificados para aplicativos habilitados por criptografia que não reconheçam os objetos certificação do servidor.

Para emitir um certificado, execute as seguintes etapas:

1. Clique nas opções **Gerenciamento de Certificados** > **Emitir Certificados** da landing page do Identity Console.
2. Procure um arquivo CSR e selecione-o.
3. Selecione o Tipo de chave apropriado e o Uso de chave correspondente em Especificações de uso de chaves. Essas opções permitem selecionar um tipo de chave. Cada tipo de chave tem valores de uso de chave predefinidos associados a ele:
   - 3a **Não especificado:** Essa opção é selecionada por padrão e não ativa nenhum uso de chave no certificado.
   - 3b **Autoridade de certificação:** Essa opção ativa os usos de chave de Assinatura de certificado e de Assinatura do CRL.
   - 3c **Criptografia:** Essa opção ativa o uso de chave de Criptografia de chave.
   - 3d **Autenticação:** Essa opção ativa o uso de chave Assinatura Digital.
   - 3e **SSL ou TSL:** Essa opção configura a chave de modo que ela possa ser usada em transações de SSL ou TLS.

3f **Personalizado:** Essa opção permite que você selecione manualmente qualquer uma das opções de uso de chave ou todas elas.

3g **Defina a Extensão de uso da chave para Crítica:** Com qualquer tipo de chave exceto Não Especificado selecionado, você pode marcar a extensão de uso da chave como crítica. As extensões críticas deverão ser entendidas pelo software destinatário antes que o certificado possa ser usado para qualquer propósito. Portanto, marcar uma extensão como crítica poderá oferecer risco, pois nem todos os aplicativos poderão usar o certificado. Mas para extensões bem conhecidas, como uso de chave, o risco é mínimo. Em geral, se o uso de chave for especificado, a extensão deverá ser marcada como crítica.

4 Você pode optar por codificar uma extensão de **Uso de chave estendido** no certificado. Para ativar esse recurso, selecione **Habilitar uso de chave estendido**:

4a **Servidor:** Essa opção ativa o uso de chave estendido de Autenticação do Servidor.

4b **Usuário:** Essa opção ativa os usos de chave estendida de Autenticação do usuário e Proteção de e-mail.

4c **Personalizado:** Permite que você selecione um ou todos os Usos de chave estendida.

4d **Qualquer:** Permite que a chave seja utilizada para qualquer uso de chave estendida.

4e **Defina a extensão de uso da chave estendida para Crítica:** As extensões críticas deverão ser entendidas pelo software destinatário antes que o certificado possa ser usado para qualquer propósito. Portanto, marcar uma extensão como crítica poderá oferecer risco, pois nem todos os aplicativos poderão usar o certificado. Como muitos aplicativos não entendem a Extensão de Uso da Chave Estendida, se você tornar essa extensão crítica, haverá um risco significativo de a certificação não ser aceita por um determinado aplicativo; portanto, a extensão só deverá ser definido como crítica quando necessário.

5 Selecione as **Restrições básicas** apropriadas:

5a **Tipo de certificado:**

5a1 **Não especificado:** Selecione essa opção se você não quiser adicionar uma extensão de limitação básica ao certificado.

5a2 **Autoridade de certificação:** Selecione essa opção se desejar adicionar uma extensão de limitação básica da Autoridade de Certificação à certificação. Se a certificação for para uma Autoridade de Certificação, selecione essa opção.

5a3 **Entidade Final:** Selecione essa opção para adicionar uma extensão de limitação básica à certificação especificada como uma certificação de Entidade Final (que não é uma Autoridade de Certificação). Nota: Se o certificado for do tipo Entidade Final, o tamanho do caminho deverá ser definido como Não especificado.

5b **Tamanho do caminho:**

5b1 **Não especificado:** Selecione essa opção se não desejar especificar quantos níveis de CAs subordinadas poderão ser criados abaixo dessa CA.

Observação: Se uma certificação for do tipo Entidade Final, o tamanho do caminho apenas poderá ser definido como Não especificado.

5b2 **Específico:** Selecione essa opção se desejar especificar quantos níveis de CAs subordinadas poderão ser criados abaixo dessa CA. Clique nas setas para cima e para baixo para especificar o tamanho do caminho.

Observação: Se o certificado que estiver sendo criado for uma CA subordinada, o tamanho do caminho deverá estar consistente com a CA superior. Por exemplo, se a CA superior tiver um tamanho de caminho igual a 3, o tamanho de caminho da subordinada deverá ser 2 ou menos. Se a CA superior tiver um tamanho de caminho não especificado, a subordinada também poderá ter um tamanho de caminho não especificado ou qualquer tamanho de caminho específico desejado.

5c **Definir Extensão de limitações básicas para Crítica:** Normalmente, a Extensão de Limitações Básicas deve ser definida para crítica em certificações de CA. As extensões críticas deverão ser entendidas pelo software destinatário antes que o certificado possa ser usado para qualquer propósito. Portanto, marcar uma extensão como crítica poderá oferecer risco, pois nem todos os aplicativos poderão usar o certificado. Mas para extensões bem conhecidas, como Limitações Básicas, o risco é mínimo.

6 Especifique os seguintes parâmetros de certificado:

6a **Nome do Assunto:** Exibe o nome tipificado completo da árvore do eDirectory.

6b **Nome do Assunto:** Exibe o nome tipificado completo da árvore do eDirectory.

6c **Período de validade:** Use a lista suspensa para especificar o período durante o qual o certificado será válido. A faixa é de seis meses até o ano 2036, no máximo (uma limitação de tempo com base no valor de tempo de 32 bits). Se escolher a opção Datas Específicas, você poderá editar os campos Data Efetiva e Data de Vencimento para criar um período de validade personalizado. A data máxima selecionada precisa estar dentro da data de validade da CA.

6c1 **Data efetiva:** Permite que você exiba ou edite a hora e a data em que o certificado se tornará válido.

6c2 **Data de vencimento:** Permite que você exiba ou edite a hora e a data em que o certificado se tornará inválido.

6d **Extensões personalizadas:** Esse recurso permite que o Servidor de Certificação suporte qualquer extensão padrão ou personalizada que você queira incluir ao criar um certificado. As extensões devem ter sido criadas anteriormente e armazenadas em um arquivo (uma extensão por arquivo). As extensões devem ser codificadas por ASN.1, conforme definido na seção 4.2 da IETF RFC 2459/3280.

Se você quiser incluir uma ou mais extensões personalizadas no certificado que estiver criando, clique em Novo, procure um arquivo que contenha a extensão personalizada e adicione-a ao certificado. Para adicionar várias extensões, repita esse processo.

Para apagar um arquivo de extensões personalizadas, selecione-o e clique no ícone  .

7 Selecione o formato de certificado apropriado entre as seguintes opções:

7a **Arquivo no formato DER binário:** Essa opção permite gravar ou exportar um certificado para um arquivo exibido no campo Nome de arquivo. Por padrão, o arquivo de certificado é exportado com uma extensão .DER na raiz da unidade C: de uma estação de trabalho do Identity Console baseada em Windows e no diretório pessoal de uma estação de trabalho do Identity Console baseada em Linux.

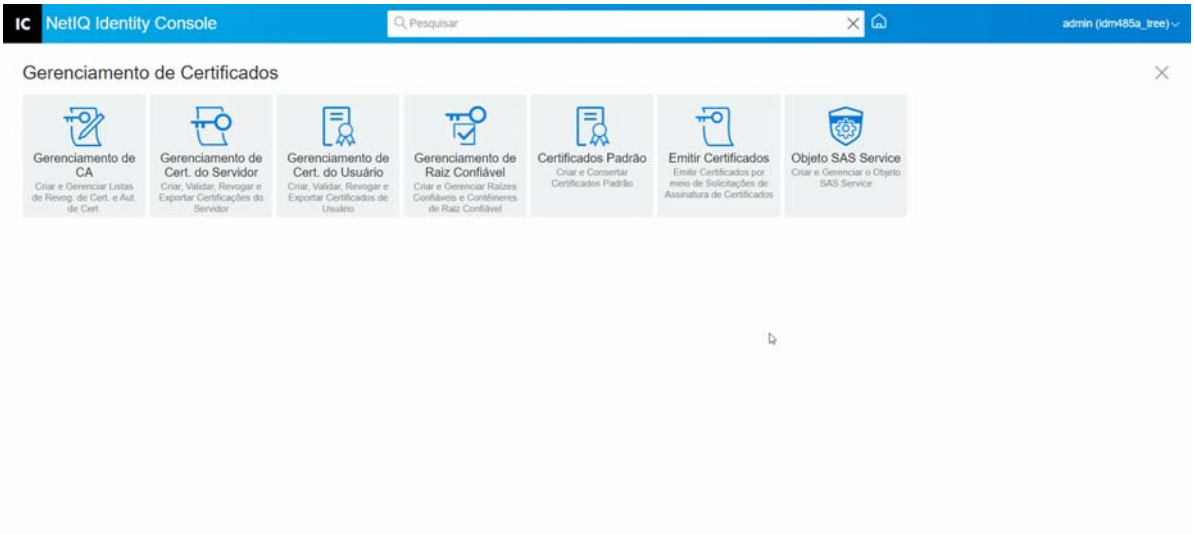
7b **Arquivo no formato Base64:** Essa opção permite gravar um CSR ou exportar um certificado para um arquivo exibido no campo Nome de arquivo. Por padrão, os arquivos de certificado e CSR são exportados com uma extensão .B64 na raiz da unidade C: de uma estação de trabalho do Identity Console baseada em Windows e no diretório pessoal de uma estação de trabalho do Identity Console baseada em Linux.

7c **Arquivo em formato CER:** Essa opção permite gravar um CSR ou exportar um certificado para um arquivo exibido no campo Nome de arquivo. Por padrão, os arquivos de certificado e CSR são exportados com uma extensão .CER na raiz da unidade C: de uma estação de trabalho do Identity Console baseada em Windows e no diretório pessoal de uma estação de trabalho do Identity Console baseada em Linux.

8 Reveja o resumo do certificado na próxima tela e clique em **OK**.

9 Uma confirmação aparece, indicando que o certificado foi emitido com sucesso.

Figura 17-6 *Emitindo um certificado de chave pública*



Gerenciando um objeto SAS Service

O objeto SAS Service facilita a comunicação entre um servidor e os respectivos certificados de servidor. Se você remover um servidor de uma árvore do eDirectory, terá também de apagar o objeto SAS Service associado a esse servidor. Do mesmo modo, se você quiser colocar o servidor de volta na árvore, deverá criar o objeto SAS Service para esse servidor. Se você não fizer isso, não poderá criar novos certificados de servidor.

O objeto SAS Service é criado automaticamente como parte da verificação de saúde do servidor. Você não deve precisar criá-lo manualmente.

O utilitário criará um novo objeto SAS Service apenas se não houver um objeto SAS Service nomeado adequadamente no mesmo container do objeto servidor. Por exemplo, para um servidor chamado WAKE, você terá um objeto SAS Service chamado “SAS Service - WAKE”. O utilitário adiciona os indicadores de DS do objeto servidor para o objeto SAS, e do objeto SAS para o objeto servidor, além de configurar as entradas corretas da ACL no objeto SAS Service.

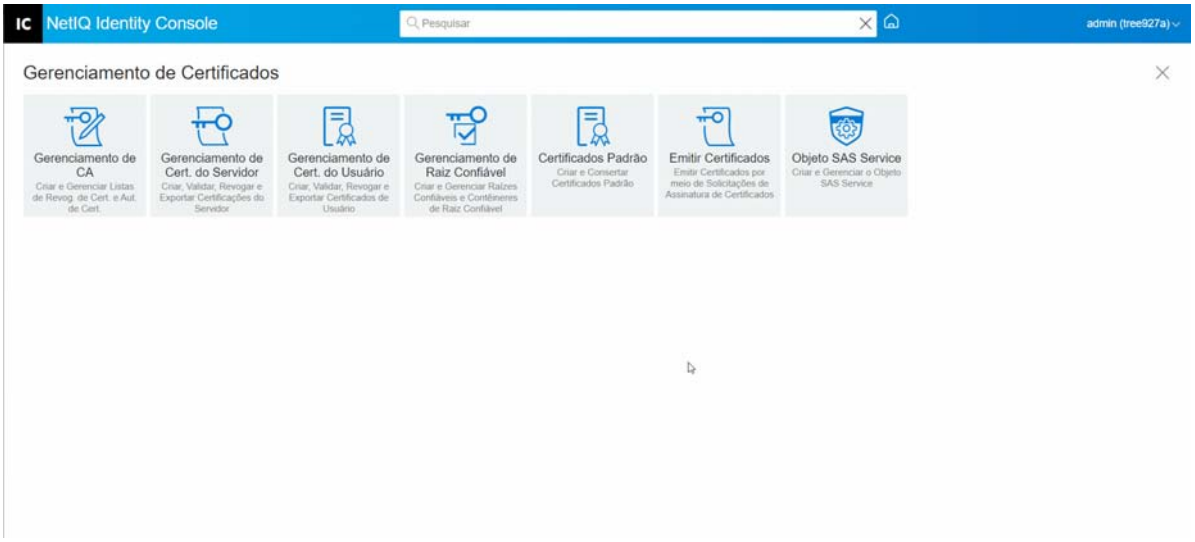
Se um objeto SAS Service com o nome adequado já existir, o utilitário não criará outro. Os indicadores de DS do objeto SAS Service antigo podem estar errados ou ausentes ou as ACLs podem não estar corretas. Nesse caso, você pode apagar o objeto SAS Service corrompido e usar o portal do Identity Console para criar outro.

Criando ou apagando um objeto SAS Service

Para criar ou apagar um objeto SAS Service, execute as seguintes etapas:

1. Clique nas opções **Gerenciamento de Certificados** > **Objeto SAS Service** da landing page do Identity Console.
2. Se não houver nenhum objeto SAS Service criado para um servidor existente, clique no ícone + para criar um novo.
3. Uma mensagem de confirmação aparece, indicando que um objeto SAS Service foi criado com sucesso.
4. Para remover um objeto SAS Service, clique no ícone 🗑.
5. Clique em **OK** na tela de confirmação para remover um objeto SAS Service com sucesso.

Figura 17-7 *Gerenciando objetos SAS Service*



18 Gerenciando a Metodologia de Autenticação

Ao utilizar o Módulo de autenticação, você pode executar as seguintes tarefas:

Gerenciando métodos e sequências de login e pós-login

O NMAS inclui suporte para uma série de métodos de login e pós-login do NetIQ e de terceiros desenvolvedores de autenticação. Alguns métodos requerem hardware e software adicionais. Verifique se você tem todo o hardware e software necessários para os métodos que você usará.

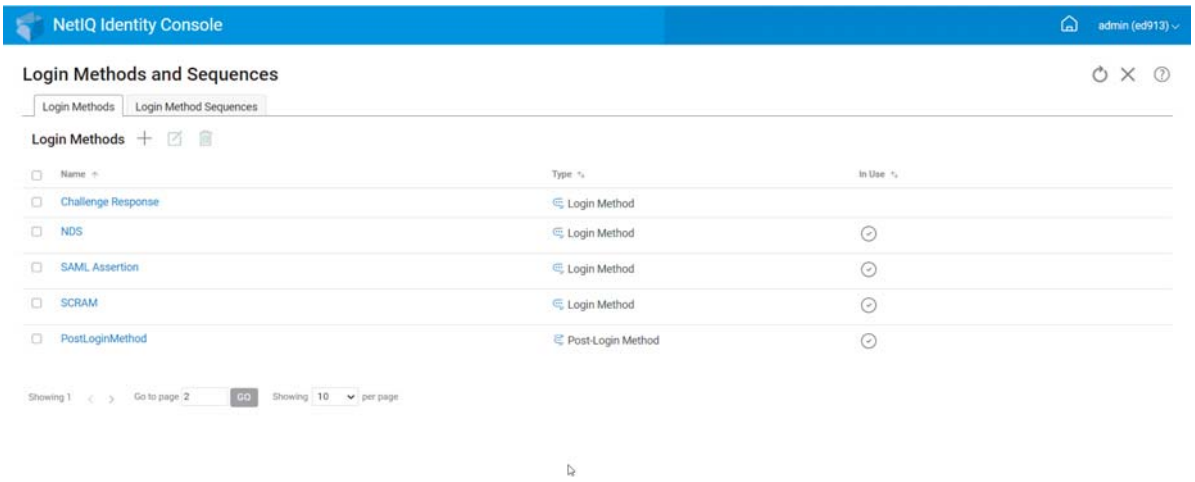
Esta seção descreve como instalar e configurar sequências e métodos de login e pós-login para NMAS.

Instalando um método de login ou pós-login

Para instalar um método de login, execute as seguintes tarefas:

1. Clique nas opções **Gerenciamento de Autenticação** > **Sequências e Métodos de Login** na landing page do Identity Console.
2. Clique no ícone + para instalar um novo método de login.
3. Procure o arquivo do método de login (.zip) que você deseja instalar, selecione-o e clique em **Próximo**.
4. Siga o assistente de instalação para concluir o processo de instalação do método de login.

Figura 18-1 *Instalando um novo método de login*

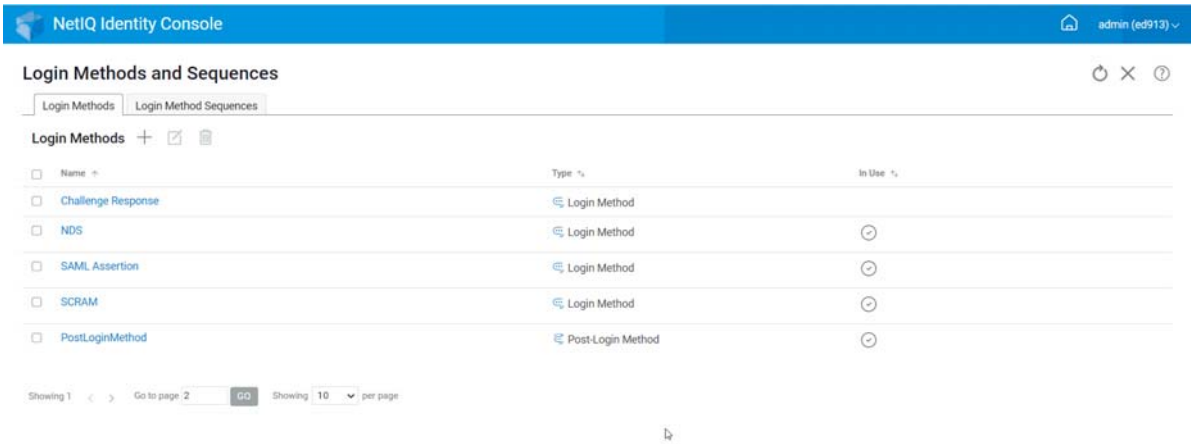


Atualizando um método de login ou pós-login existente

Para atualizar um método de login existente, execute as seguintes etapas:

1. Clique nas opções **Gerenciamento de Autenticação** > **Sequências e Métodos de Login** na landing page do Identity Console.
2. Selecione o método de login que deseja atualizar na lista e clique no ícone ☑.
3. Procure o arquivo do método de login (.zip) que você deseja atualizar, selecione-o e clique em **Próximo**.
4. Siga o assistente de atualização para concluir a atualização do método de login.

Figura 18-2 *Atualizando um método de login existente*

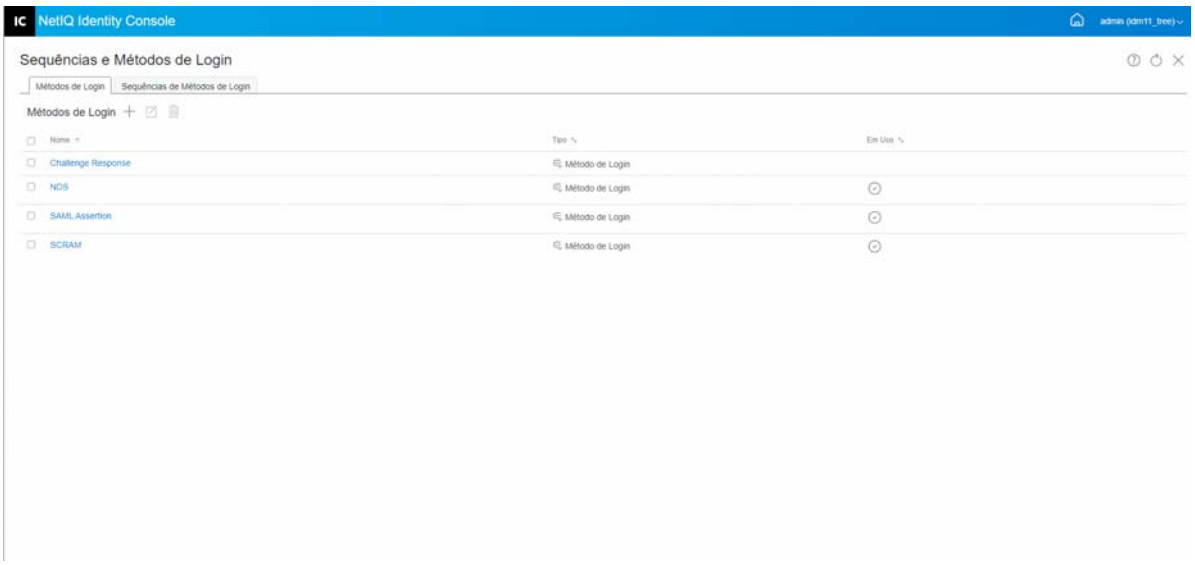


Desinstalando métodos de login ou pós-login

Para desinstalar um ou mais métodos de login ou pós-login, execute as seguintes etapas:

1. Clique nas opções **Gerenciamento de Autenticação** > **Sequências e Métodos de Login** na landing page do Identity Console.
2. Selecione o(s) método(s) de login que você deseja desinstalar na lista e clique no ícone 🗑.
3. Na próxima tela, clique em **OK**.
4. Uma mensagem de confirmação aparece, indicando que um ou mais métodos de login foram desinstalados.

Figura 18-3 *Desinstalando um método de login*



Criando nova sequência de métodos de login

Quando você tiver vários métodos de login criados para o seu ambiente, poderá decidir em qual ordem esses métodos deverão ser usados. Para criar uma nova sequência de métodos de login, execute as seguintes etapas:

1. Clique nas opções **Gerenciamento de Autenticação** > **Sequências e Métodos de Login** na landing page do Identity Console.
2. Selecione a guia **Sequências de Métodos de Login**.
3. Clique no ícone + para criar uma nova sequência de métodos de login.
4. Especifique um **nome** e selecione o **Tipo de sequência**.
5. Selecione os métodos de login e pós-login necessários na lista de métodos de login e pós-login disponíveis.

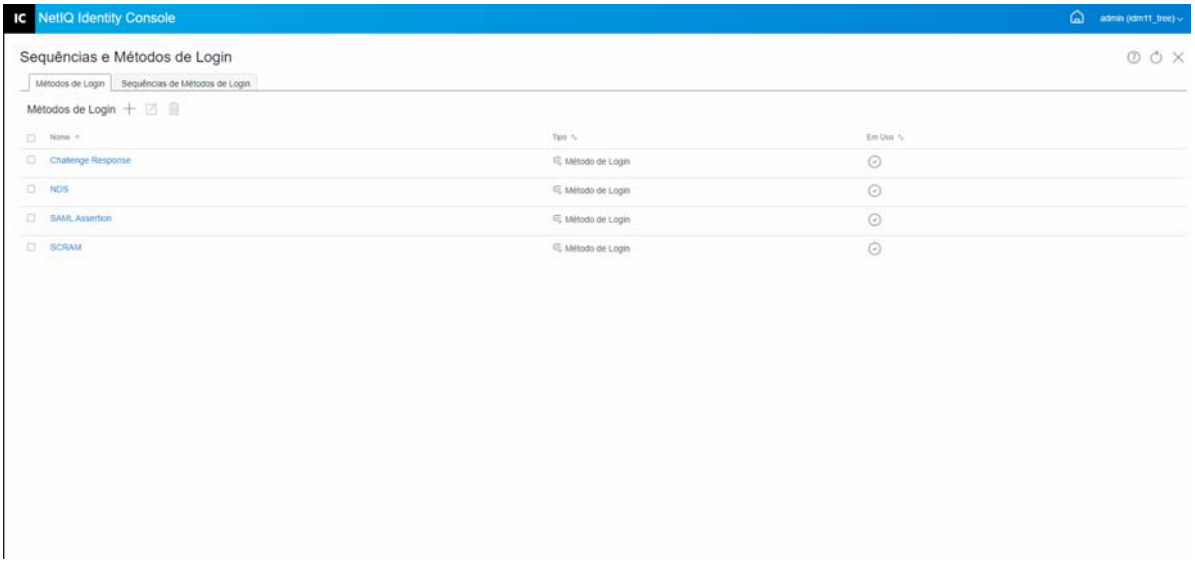
Observação: Você pode decidir a ordem dos métodos de login clicando na seta para cima e para baixo visível nos objetos método de login.

---

6 Clique no botão **Criar**.

7 Uma mensagem de confirmação aparece, indicando que uma nova sequência de métodos de login foi criada com sucesso.

Figura 18-4 *Criando uma sequência de métodos de login*



Modificando uma sequência de métodos de login

Para modificar uma sequência de métodos de login existente, execute as seguintes etapas:

1 Clique nas opções **Gerenciamento de Autenticação** > **Sequências e Métodos de Login** na landing page do Identity Console.

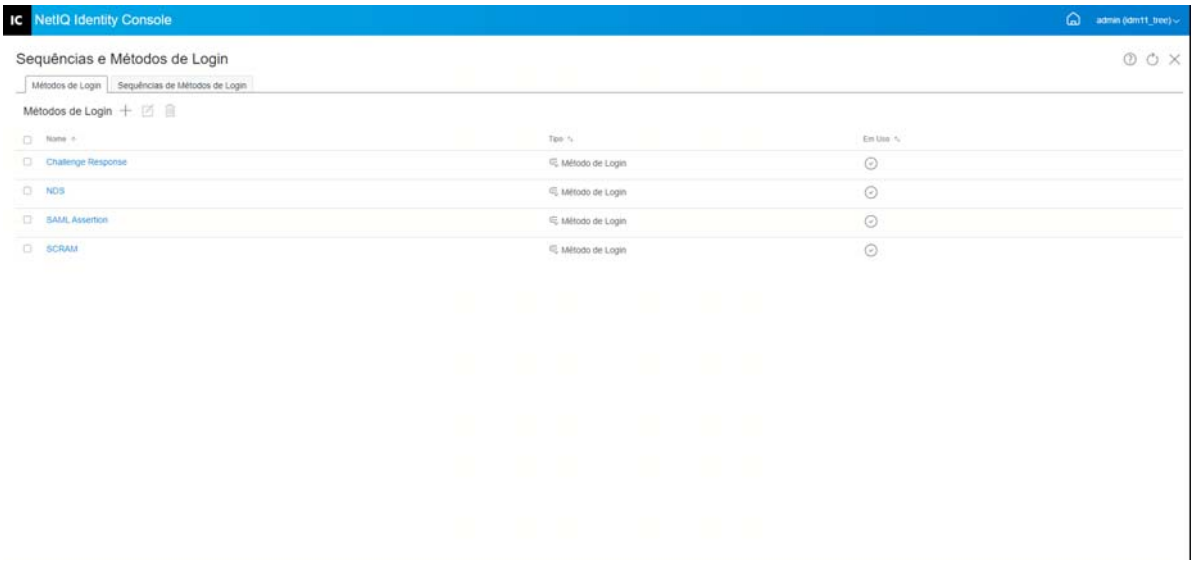
2 Selecione a guia **Sequências de Métodos de Login**.

3 Clique no ícone ☑ para modificar uma sequência de métodos de login existente.

4 Faça as mudanças necessárias na página **Modificar a Sequência do Método de Login** e clique em **Gravar**.

5 Uma mensagem de confirmação aparece, indicando que a sequência do método de login foi modificada com sucesso.

Figura 18-5 *Modificando uma sequência de métodos de login*

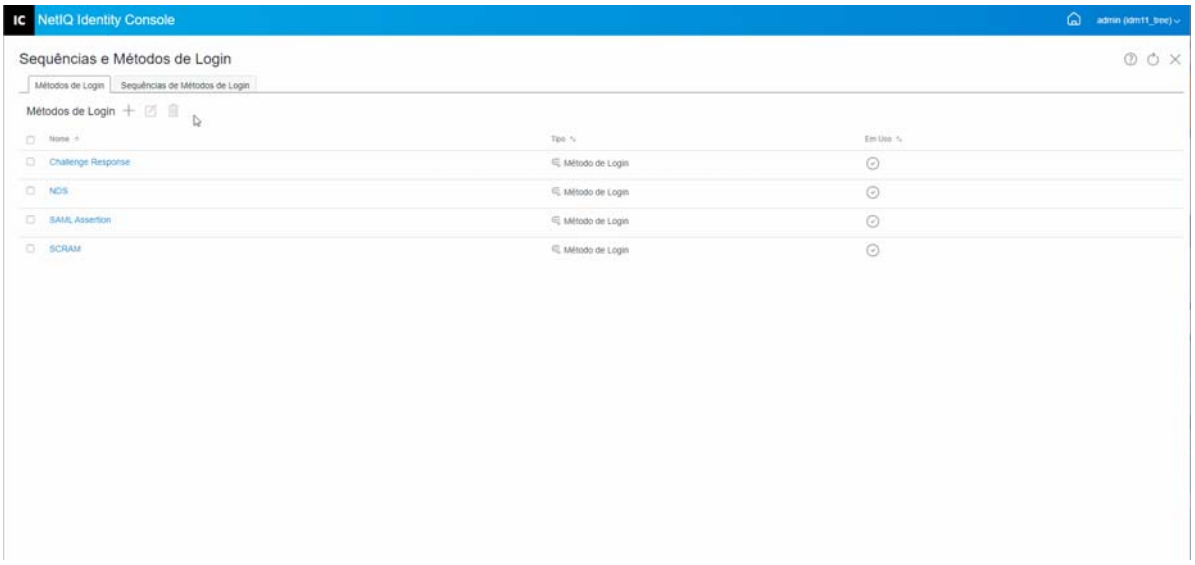


Autorizando ou desautorizando uma sequência de métodos de login

Uma sequência de métodos de login deve ser autorizada e definida como padrão para associá-los aos usuários, containers e partições. Para autorizar uma sequência de método de login, execute as seguintes etapas:

1. Clique nas opções **Gerenciamento de Autenticação** > **Sequências e Métodos de Login** na landing page do Identity Console.
2. Selecione a guia **Sequências de Métodos de Login**.
3. Selecione a sequência de métodos de login apropriada na lista e clique no ícone ⊙.
4. Para desautorizar uma sequência de métodos de login, selecione a sequência de métodos de login e clique no ícone ⊗.
5. Alternativamente, você também pode autorizar ou desautorizar uma sequência de métodos de login no menu suspenso, na coluna **Autorizado**, na lista de Sequências de Métodos de Login.

Figura 18-6 *Autorizando ou desautorizando uma sequência de métodos de login*

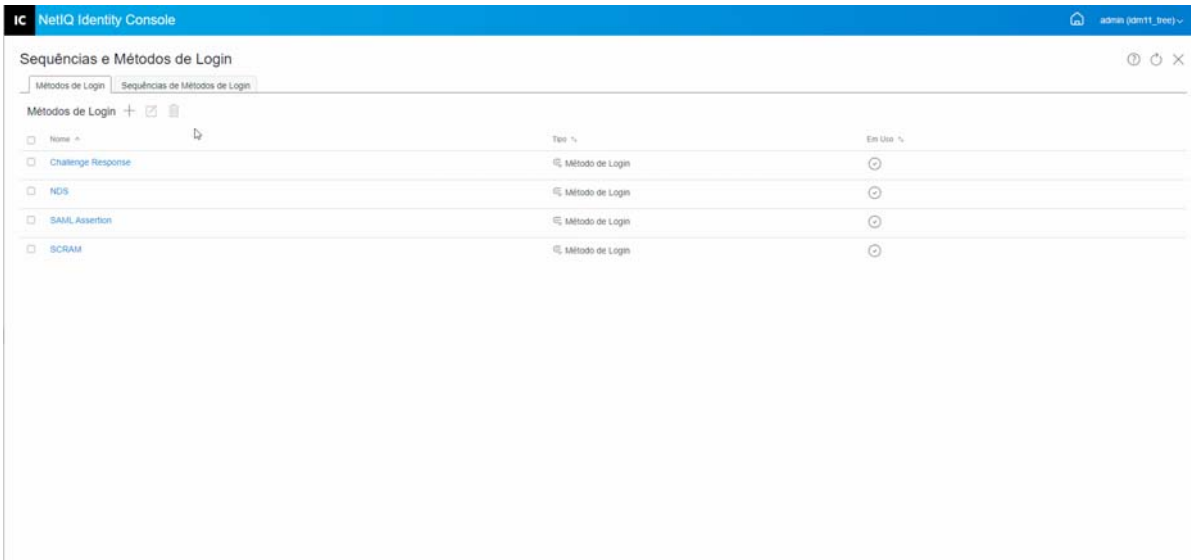


Definindo uma sequência de métodos de login padrão

Para definir uma sequência de login padrão para que os usuários não sejam obrigados a especificar uma sequência de login ao efetuar login:

1. Clique nas opções **Gerenciamento de Autenticação** > **Sequências e Métodos de Login** na landing page do Identity Console.
2. Selecione a guia **Sequências de Métodos de Login**.
3. Habilite o ícone  para definir uma sequência de métodos de login autorizada como padrão.

Figura 18-7 *Definindo uma sequência de métodos de login padrão*

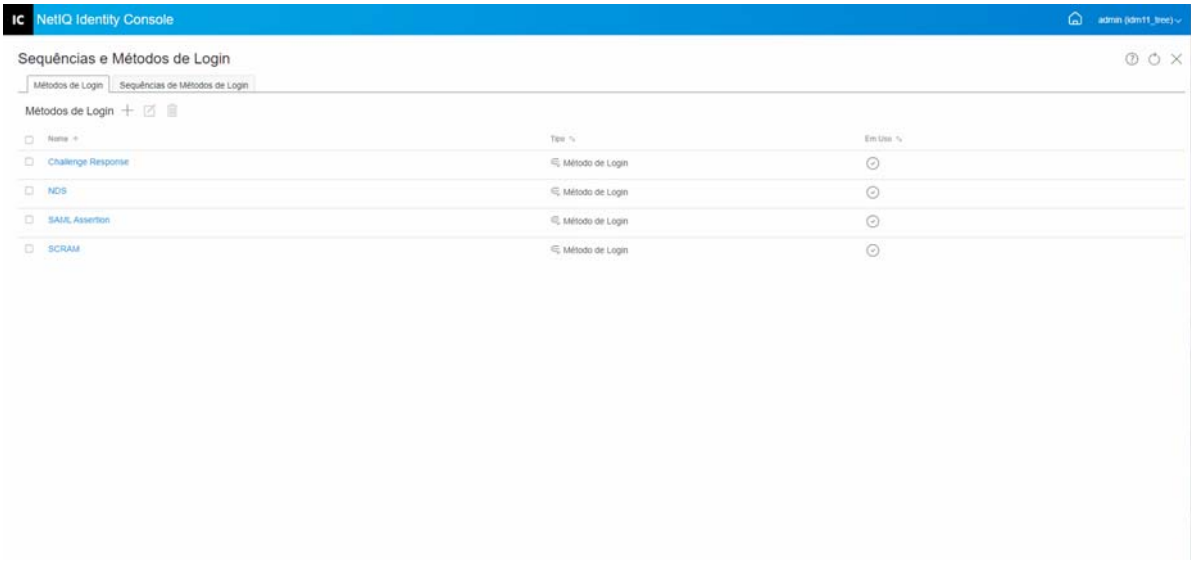


Apagando sequências de métodos de login

Para apagar uma sequência de métodos de login:

1. Clique nas opções **Gerenciamento de Autenticação** > **Sequências e Métodos de Login** na landing page do Identity Console.
2. Selecione a guia **Sequências de Métodos de Login**.
3. Selecione a sequência de métodos de login apropriada na lista e clique no ícone .
4. Clique em **OK** na próxima tela de confirmação.

Figura 18-8 *Apagando uma sequência de métodos de login*



Gerenciando políticas de senha

Uma política de senha é uma coleção de regras definidas pelo administrador que especificam os critérios para a criação e a substituição de senhas do usuário final. O NMAS permite que você assegure o uso obrigatório de políticas de senha que você atribui aos usuários no eDirectory. As políticas de senha também podem incluir recursos de autoatendimento de senha esquecida, para reduzir as chamadas de suporte técnico para senhas esquecidas. Outro recurso de autoatendimento é o Autoatendimento para redefinição de senha, que permite que os usuários mudem as respectivas senhas, visualizando as regras especificadas pelo administrador na política de senha. Os usuários acessam esses recursos através do Aplicativo de usuário do Identity Manager ou do Identity Console.

Ao utilizar o módulo Políticas de senha, você pode executar as seguintes tarefas:

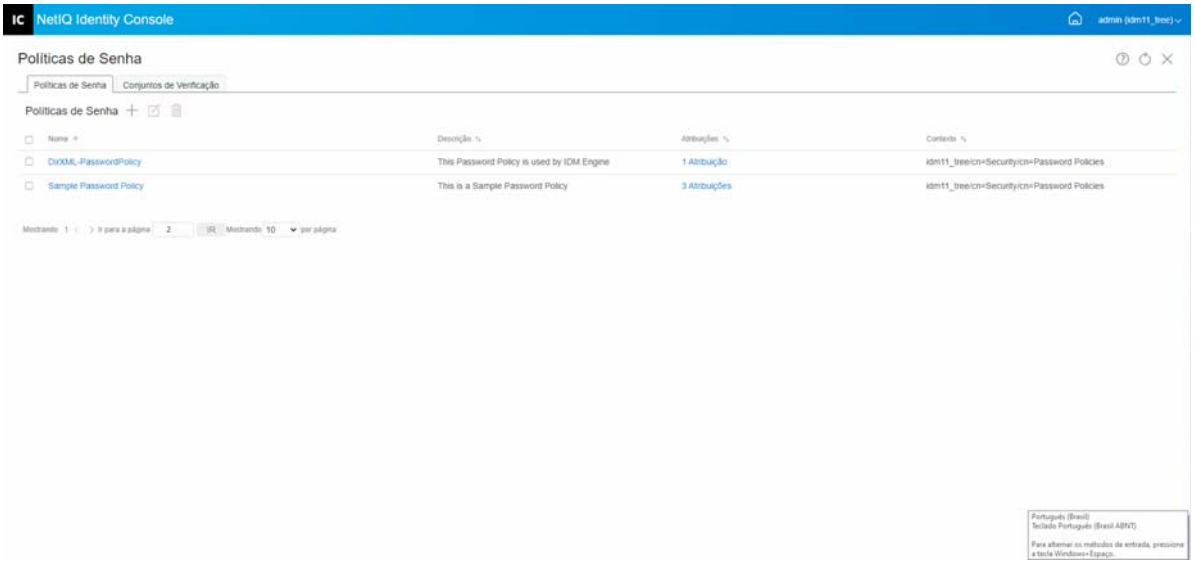
- “Criando uma política de senha com configurações padrão” na página 118
- “Criando uma política de senha com configurações personalizadas” na página 118
- “Modificando uma política de senha” na página 121
- “Apagando políticas de senha” na página 122

Criando uma política de senha com configurações padrão

Para criar uma nova política de senha, siga estas etapas:

1. Clique nas opções **Gerenciamento de Autenticação** > **Políticas de Senha** da landing page do Identity Console.
2. Clique no ícone + para criar uma nova política de senha.
3. Especifique o nome, o contexto, a descrição e uma mensagem de mudança de senha na próxima tela.
4. Se você quiser criar uma política de senha com as configurações padrão, marque a caixa para **Criar uma política de senha com base nas configurações padrão** e clique em **Próximo** para exibir a página **Resumo**.
5. Verifique os detalhes na página **Resumo** e clique em **Criar**.
6. Uma mensagem de confirmação aparece, indicando que a política de senha foi criada com sucesso.

Figura 18-9 *Criando uma política de senha com configurações padrão*



Criando uma política de senha com configurações personalizadas

Para criar uma política de senha com configurações personalizadas, execute as seguintes etapas:

1. Clique nas opções **Gerenciamento de Autenticação** > **Políticas de Senha** da landing page do Identity Console.
2. Clique no ícone + para criar uma nova política de senha.
3. Especifique o nome, o contexto, a descrição e uma mensagem de mudança de senha na próxima tela.
4. Se você quiser criar uma política de senha com configurações personalizadas, clique em **Próximo**.

5 Execute as seguintes ações na página **Configuração**:

5a Habilitar senha universal: Habilitar a senha universal para uma política permite que você use opções no recurso Políticas de senha. No entanto, antes de habilitar a senha universal para uma política, você precisa atender aos pré-requisitos da senha universal no ambiente.

5b Habilitar as regras de senha avançadas: Essa opção habilita as regras de senha encontradas em Regras de senha avançadas. Essas regras ajudam você a proteger seu ambiente, dando-lhe controle sobre critérios como a vida útil de uma senha e o conteúdo de uma senha, como combinação de letras, números, letras maiúsculas ou minúsculas e caracteres especiais. Você pode apagar senhas que não considera seguras, como o nome de sua empresa.

5c Sincronização de Senhas: Essas opções determinam como a senha universal é sincronizada no eDirectory com outros tipos de senha do cofre de identidade. A Sincronização de Senhas contém as seguintes opções:

5c1 Remover a senha do NDS ao definir a senha: Se essa opção estiver selecionada, a senha do NDS será desabilitada quando a senha universal for definida Os usuários não poderão usar métodos ou utilitários mais antigos que efetuam login diretamente com a senha do NDS em vez de se comunicar com o NMAS. Se essa opção for definida, a próxima opção (**Sincronizar a senha do NDS ao definir a senha**) será desabilitada por padrão.

5c2 Sincronizar a senha do NDS ao definir a senha: Se você selecionar essa opção, a definição da senha universal em aplicativos como o Identity Console também mudará a senha do NDS.

5c3 Sincronizar senha simples ao definir a senha: Essa opção fornece a compatibilidade com clientes da NetIQ e de terceiros usando senha simples e aprovisionamento de usuário.

5c4 Sincronizar senha de distribuição ao definir senha: Esta opção determina se o mecanismo de metadiretório pode recuperar ou definir uma senha universal de usuário no eDirectory.

5d Recuperação de senha universal: As seguintes opções estão disponíveis:

5d1 Permitir que o usuário recupere a senha: Permite que o agente do usuário recupere a senha. Essa opção determina se o recurso de Autoatendimento de senha esquecida pode recuperar uma senha em nome de um usuário para que a senha possa ser enviada por e-mail para ele. Se você não selecionar esta opção, o recurso correspondente ficará esmaecido na guia Senha esquecida, na política de senha.

5d2 Permitir que o administrador recupere a senha: Selecione essa caixa se você tiver um serviço específico que precise dela. O Identity Manager não tem necessidade de que os administradores recuperem senhas. No entanto, alguns serviços de terceiros podem aproveitar essa opção.

5d3 Permita as seguintes opções para recuperação de senha: Selecione o usuário apropriado que deve recuperar a senha clicando no ícone +.

5e Autenticação:

5e1 Verificar se as senhas existentes estão em conformidade com a política de senha (a verificação ocorre durante o login): Essa opção será útil se você estiver distribuindo uma nova política de senha ou mudando as Regras avançadas de senha de uma política existente e desejar verificar se as senhas existentes são compatíveis com as regras novas ou mudadas.

Se você selecionar essa opção, quando os usuários efetuarem login, as senhas existentes deles serão analisadas para verificar se elas cumprem as Regras avançadas de senha na política de senha nova ou mudada. Se uma senha existente não for compatível, o usuário será obrigado a mudá-la.

Depois de concluir o procedimento, clique em **Próximo**.

6 As **Regras avançadas de senha** ajudam você a proteger o seu ambiente, dando-lhe controle sobre detalhes de senha, como a vida útil da senha, a frequência de mudança de senha e o quê uma senha contém.

Caracteres especiais são aqueles que não são números (0-9) e não são caracteres alfabéticos.

Execute as seguintes ações na página Regras Avançadas de Senha:

6a Você pode gerenciar configurações de sintaxe de senha usando a Política de Complexidade da Microsoft (anterior ao Microsoft Windows Server 2008), a Política de Senha do Microsoft Server 2008 ou a sintaxe Novell.

6b Especifique as opções necessárias para Mudar senha, Vida útil da senha, Comprimento e composição da senha e Exclusão da senha no assistente e clique em **Próximo**.

7 Você pode reduzir os custos de suporte técnico ao habilitar o autoatendimento de **Senha esquecida** para os usuários que esquecerem uma senha. Esses recursos de autoatendimento estão disponíveis para os usuários através do portal do Identity Console. Execute as seguintes ações na página Senha Esquecida:

Observação: Se habilitar a Senha Esquecida, você também deverá especificar se um conjunto de verificação será necessário para ajudar o usuário a efetuar login.

7a **Conjuntos de verificação:** Se você usar conjuntos de verificação, os usuários não poderão usar o autoatendimento de Senha Esquecida até que respondam às perguntas do conjunto de verificação. Para garantir que os usuários sejam solicitados a digitar essas informações através do portal Identity Console, selecione a opção **Exigir Conjunto de Verificação**.

7b **Ação:** As opções disponíveis nessa guia permitem que o seu usuário redefina a senha usando conjuntos de verificação e senha universal para habilitar a senha atual ou a dica de senha a ser enviada por e-mail e para exibir a opção de dica de senha.

7c **Autenticar:** Selecione a caixa **Forçar o usuário a configurar Perguntas de Verificação e/ou Dica após a autenticação** para garantir que os usuários sejam solicitados a especificar os conjuntos de verificação ou a dica de senha.

Depois de concluir o procedimento, clique em **Próximo**.

8 Uma política só entra em vigor quando você a atribui a um ou mais objetos. A Novell recomenda que você atribua políticas no ponto hierárquico mais alto possível da árvore, para simplificar a administração. Uma política de senha pode ser atribuída aos seguintes objetos:

8a **Objeto política de login:** Recomendamos que você crie uma política de senha padrão para todos os usuários na árvore e atribua-a ao objeto política de login, que está localizado no container de Segurança.

8b **Um container que é a raiz de uma partição:** Se você atribuir uma política a um container que for a raiz de uma partição, todos os usuários dessa partição, incluindo usuários em subcontainers, herdarão a designação da política.

8c **Um container que não é a raiz de uma partição:** Se você atribuir uma política a um container que não é a raiz de uma partição, apenas os usuários mantidos nesse container específico herdarão a designação da política. Os usuários que são mantidos em subcontainers não herdam a política.

Para aplicar a política a todos os usuários abaixo de um container que não é uma raiz de partição, atribua a política individualmente a cada subcontainer.

8d **Um usuário:** Você pode atribuir uma política a um ou mais usuários.

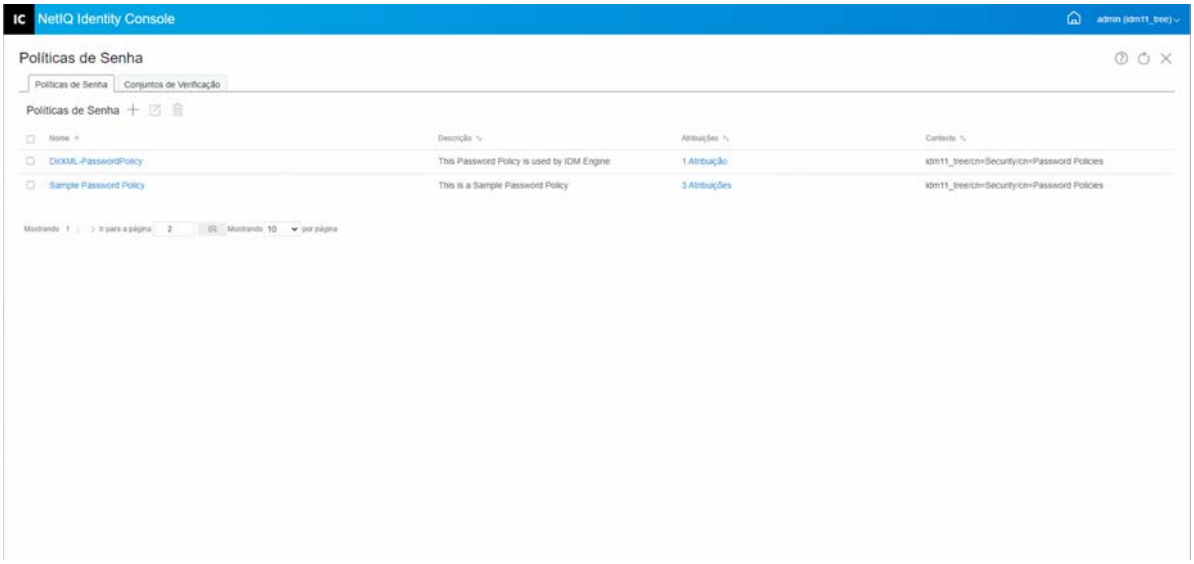
Para atribuir uma política, clique no ícone +. Em seguida, procure e selecione o objeto apropriado para atribuir uma política de senha.

Caso você queira remover uma associação de políticas, selecione a política da lista e clique no ícone 🗑.

9 Verifique os detalhes na página **Resumo** e clique em **Criar**.

10 Uma mensagem de confirmação aparece, indicando que a política de senha foi criada com sucesso.

Figura 18-10 *Criando uma política de senha com configurações personalizadas*



Modificando uma política de senha

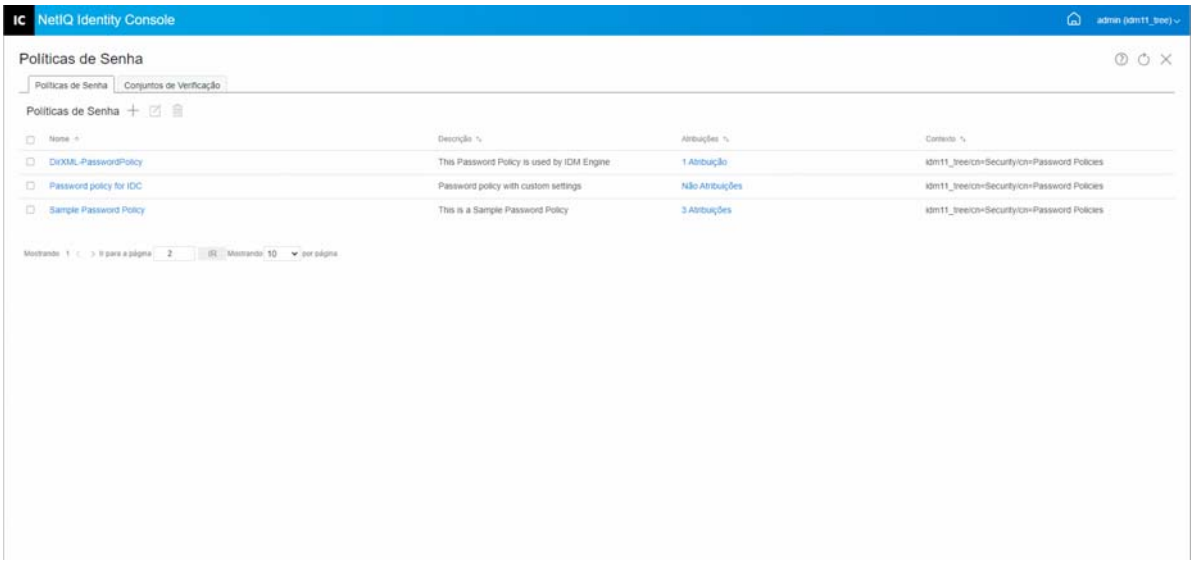
Para modificar uma política de senha existente, execute as seguintes etapas:

1 Clique nas opções **Gerenciamento de Autenticação** > **Políticas de Senha** da landing page do Identity Console.

2 Selecione a política de senha apropriada na lista e clique no ícone ☑.

3 Faça as mudanças necessárias na página **Modificar política de senha** e clique em **Gravar**.

Figura 18-11 *Modificando uma política de senha*

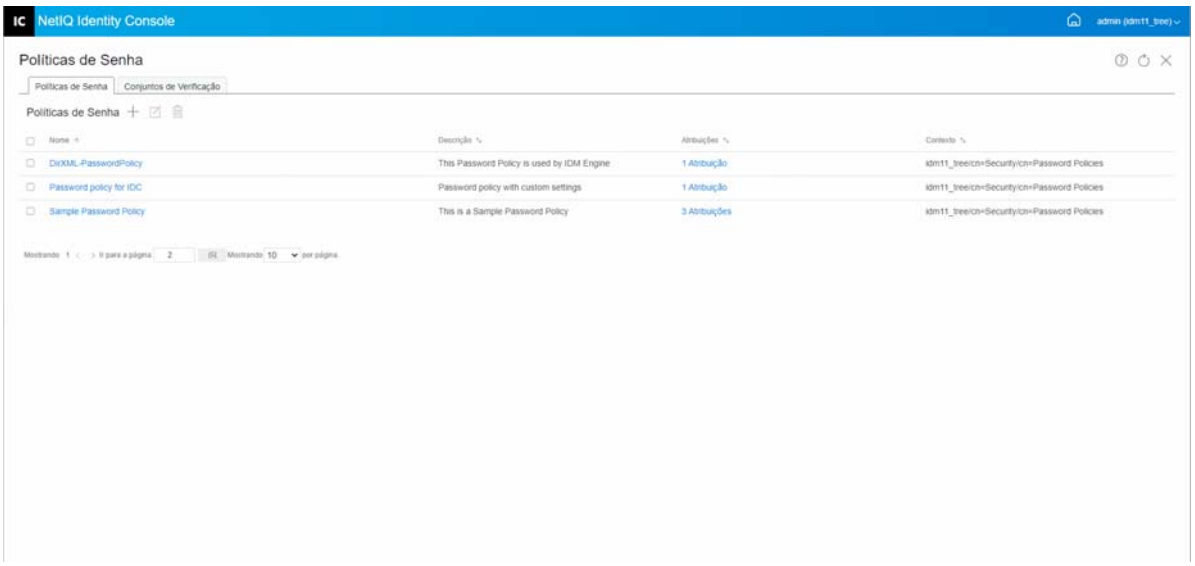


Apagando políticas de senha

Para apagar as políticas de senha, execute as seguintes etapas:

1. Clique nas opções **Gerenciamento de Autenticação** > **Políticas de Senha** da landing page do Identity Console.
2. Selecione as políticas de senha apropriadas na lista e clique no ícone .
3. Na próxima tela de aviso, clique em **OK**.
4. Uma mensagem de confirmação aparece, indicando que as políticas de senha foram apagadas.

Figura 18-12 *Apagando uma política de senha*



Gerenciando conjuntos de verificação

Um conjunto de verificação é composto de uma ou mais perguntas que um usuário responde para validar a própria identidade. Um conjunto de verificação faz parte do Autoatendimento de senha.

Quando um usuário tem problemas para lembrar ou usar a própria senha, ele pode usar o Autoatendimento de senha em vez de ligar para o suporte técnico. Um conjunto de verificação permite que um usuário valide a identidade e, em seguida, receba uma dica ou senha em um e-mail, ou que redefina uma senha usando um browser da Web.

Você pode permitir que os usuários criem e respondam suas próprias perguntas, ou exigir que os usuários respondam a perguntas que você cria.

A página Conjuntos de verificação permite que você pesquise os conjuntos de verificação existentes, crie um novo conjunto de verificação e edite conjuntos de verificação existentes.

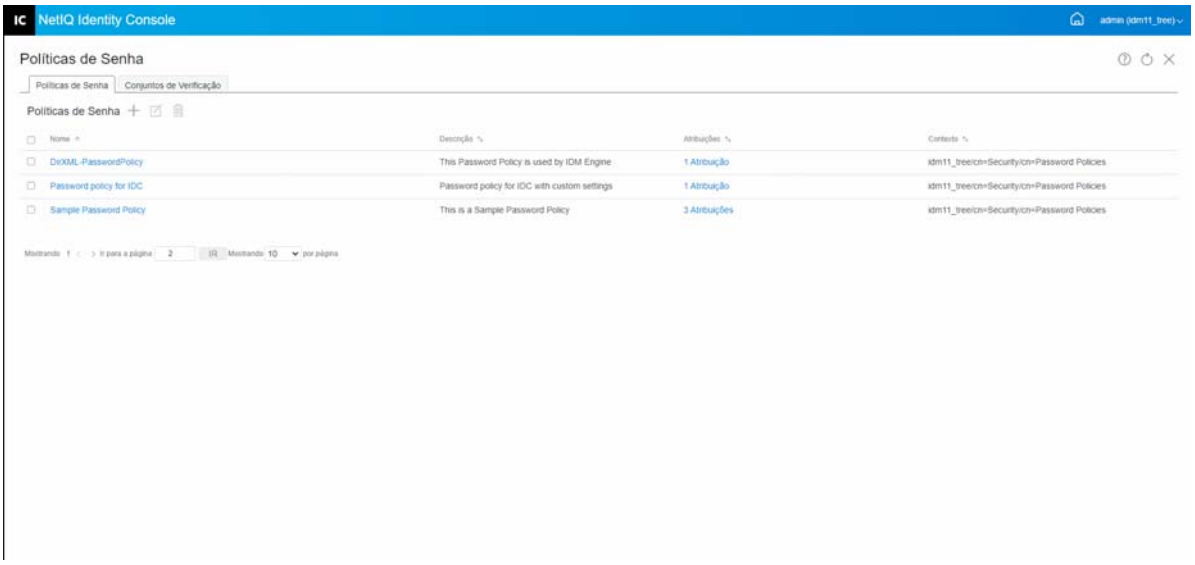
- “Criando um novo conjunto de verificação” na página 123
- “Modificando um conjunto de verificação” na página 124
- “Apagando conjunto(s) de verificação” na página 125

Criando um novo conjunto de verificação

Para criar um novo conjunto de verificação, siga estas etapas:

1. Clique nas opções **Gerenciamento de Autenticação** > **Políticas de Senha** > **Conjuntos de Verificação** na landing page do Identity Console.
2. Clique no ícone + para criar um novo conjunto de verificação.
3. Especifique um nome para o objeto conjunto de verificação e selecione o container ou subcontainer no qual o conjunto de verificação deve ser criado.
4. Crie um novo conjunto de perguntas a serem solicitadas para recuperar a senha do usuário. Você também pode selecionar do conjunto de perguntas aleatórias existente.
5. Defina o número de perguntas a serem feitas e clique em **Criar**.
6. Uma mensagem de confirmação aparece, indicando que o conjunto de verificação foi criado com sucesso.

Figura 18-13 *Criando um conjunto de verificação*

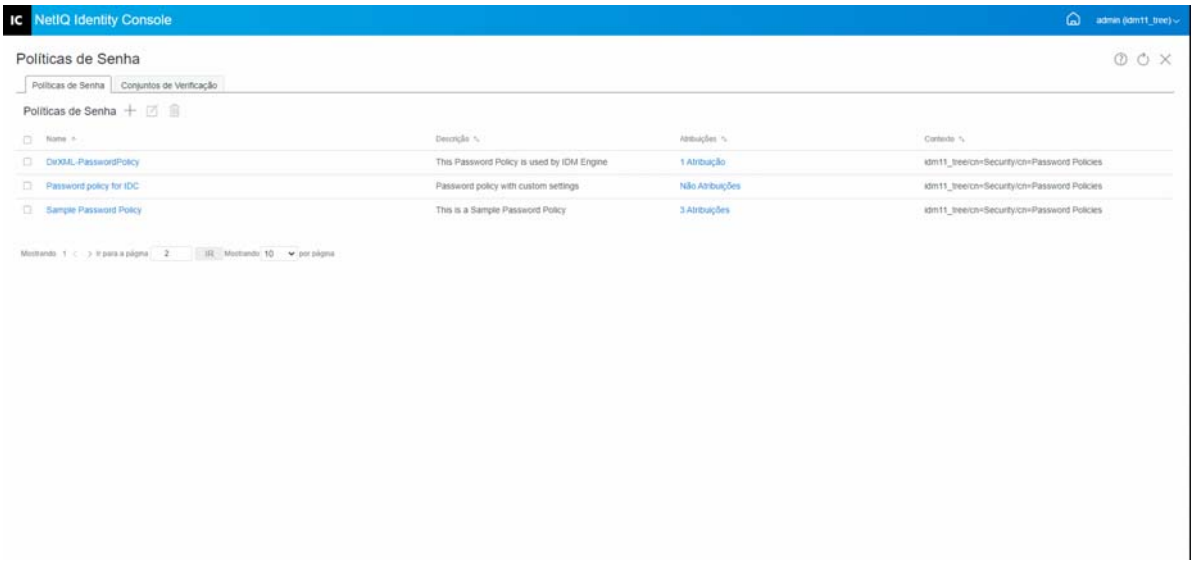


Modificando um conjunto de verificação

Para modificar um conjunto de verificação existente, execute as seguintes etapas:

1. Clique nas opções **Gerenciamento de Autenticação** > **Políticas de Senha** > **Conjuntos de Verificação** na landing page do Identity Console.
2. Selecione o conjunto de verificação apropriado na lista e clique no ícone ☑.
3. Faça as mudanças necessárias na página Modificar o conjunto de verificação e clique em **Gravar**.
4. Uma mensagem de confirmação aparece, indicando que o conjunto de verificação foi modificado com sucesso.

Figura 18-14 *Modificando um conjunto de verificação*

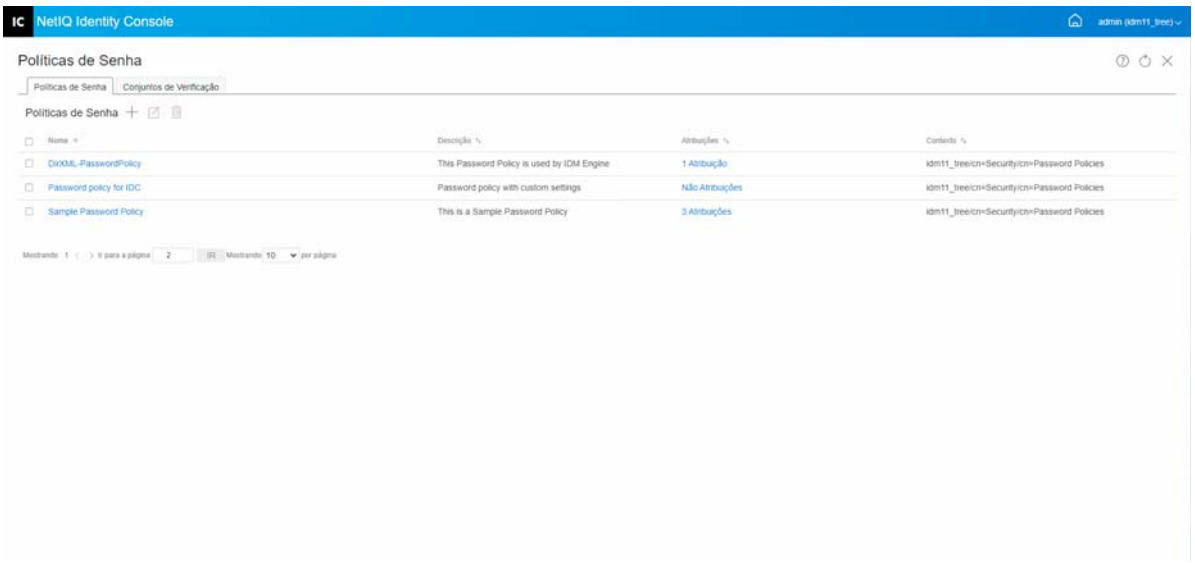


Apagando conjunto(s) de verificação

Para apagar conjunto(s) de verificação, execute as seguintes etapas:

1. Clique nas opções **Gerenciamento de Autenticação** > **Políticas de Senha** > **Conjuntos de Verificação** na landing page do Identity Console.
2. Selecione o conjunto de verificação necessário na lista e clique no ícone .
3. Clique em **OK** na tela de confirmação.
4. Uma mensagem de confirmação aparece, indicando que o conjunto de verificação foi apagado com sucesso.

Figura 18-15 *Apagando um conjunto de verificação*



19 Gerenciando objetos grupo SNMP

O SNMP (Simple Network Management Protocol) é o protocolo padrão de operação e manutenção para a Internet no intercâmbio de informações de gerenciamento entre aplicativos de console de gerenciamento e dispositivos gerenciados.

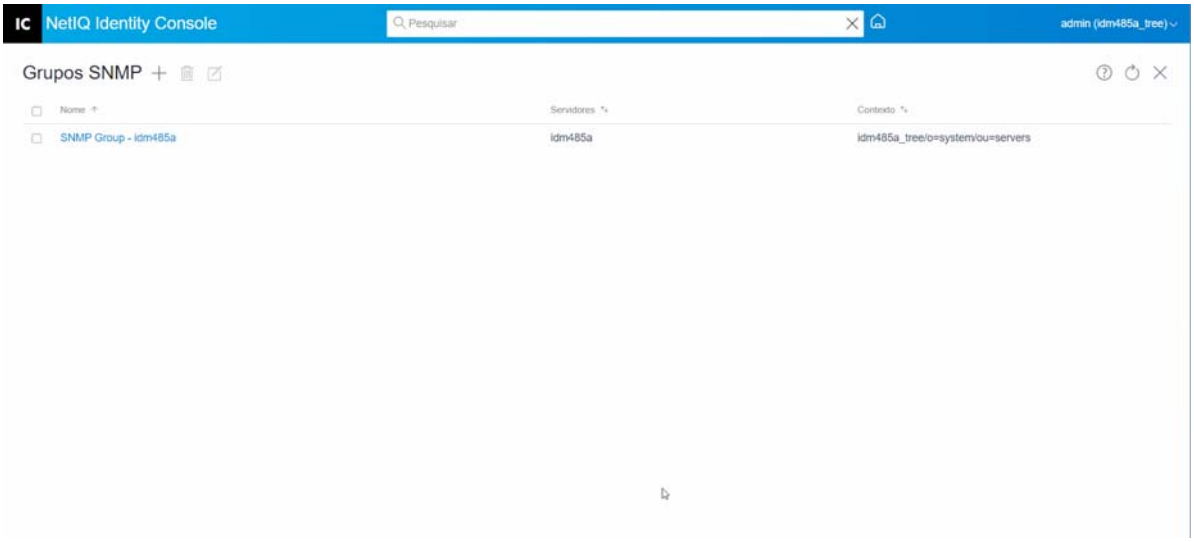
Ao utilizar o módulo SNMP, você pode executar as seguintes tarefas:

Criando objetos grupo SNMP

Para criar objetos grupo SNMP, execute as seguintes etapas:

1. Clique no módulo **SNMP** na landing page do Identity Console.
2. Clique no ícone + para criar um novo objeto grupo SNMP.
3. Especifique o nome e selecione o contexto para criar um novo objeto grupo SNMP.
4. Clique no botão **Criar**.
5. Uma mensagem aparece na tela, confirmando que o objeto grupo SNMP foi criado com sucesso.

Figura 19-1 *Criando objetos grupo SNMP*

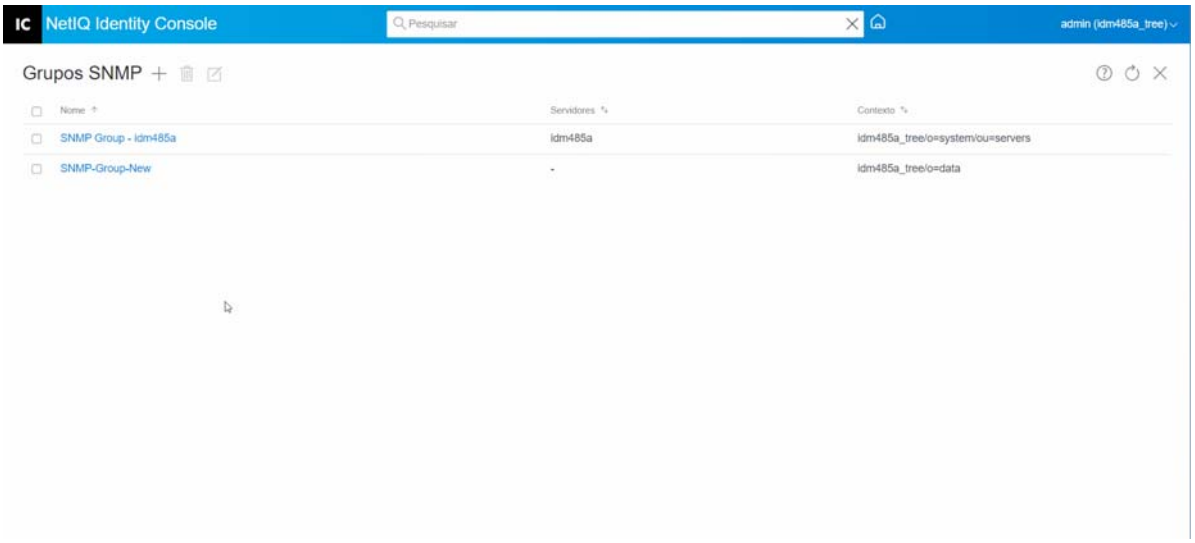


Modificando objetos grupo SNMP

Para modificar objetos grupo SNMP, execute as seguintes etapas:

1. Clique no módulo **SNMP** na landing page do Identity Console.
2. Selecione o objeto grupo SNMP que você deseja modificar e clique no ícone .
3. Modifique os parâmetros configuráveis na página **Geral**/**Detecções**.
4. Quando concluir esse procedimento, clique no botão **Gravar**.
5. Uma mensagem aparece na tela, confirmando que o objeto grupo SNMP foi modificado com sucesso.

Figura 19-2 *Modificando objetos grupo SNMP*

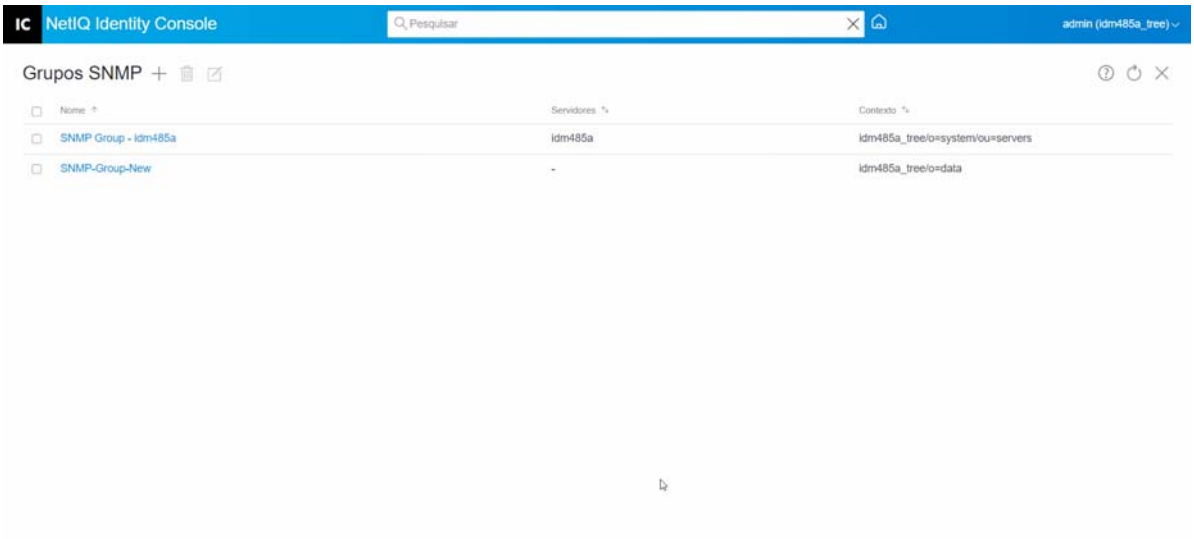


Apagando objetos grupo SNMP

Para apagar objetos grupo SNMP, execute as seguintes etapas:

1. Clique no módulo **SNMP** na landing page do Identity Console.
2. Selecione o objeto grupo SNMP que você deseja modificar e clique no ícone .
3. Clique em **OK** na próxima tela.
4. Uma mensagem aparece na tela, confirmando que o objeto grupo SNMP foi apagado com sucesso.

Figura 19-3 *Apagando objetos grupo SNMP*



20 Gerenciando a autenticação em segundo plano aprimorada

Para acessar o eDirectory por meio do plug-in EBA do Identity Console, você precisa ter um servidor habilitado para EBA em sua árvore com um arquivo eba.p12 válido. Para obter mais informações sobre como habilitar o EBA na árvore do eDirectory, consulte Enabling EBA on an eDirectory Tree (Habilitar o EBA em uma árvore do eDirectory) no *NetIQ eDirectory Administration Guide* (Guia de Administração do eDirectory do NetIQ).

Observação: Se quiser usar o módulo EBA com o Identity Console, você deverá fazer upgrade do seu servidor do eDirectory para 9.2.4 HF2.

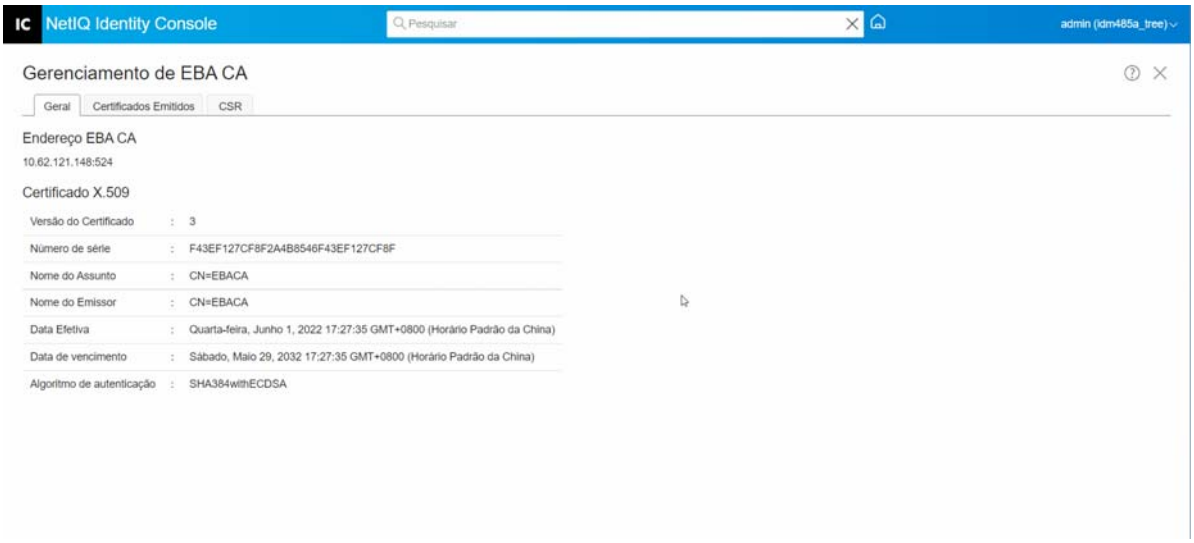
Para abrir a página de gerenciamento do EBA CA, efetue login no portal do Identity Console e clique no módulo **EBA**.

A página de gerenciamento do EBA CA inclui as seguintes guias para gerenciar diferentes aspectos do EBA CA:

- **Geral:** Exibe o endereço IP da EBA CA e seu certificado.
- **Certificados emitidos:** Exibe os certificados NCP CA juntamente com seu endereço IP e porta.

  Para revogar um certificado, selecione-o e clique em ⊘. Use essa opção apenas em situações extremas, pois o servidor que possui o certificado de CA do NCP ficará não funcional quando você revogar o certificado dele. Normalmente, a revogação do certificado torna-se necessária quando um servidor é comprometido.
- **CSR:** Lista as solicitações de autenticação de certificados pendentes para aprovação do administrador. Para aprovar uma solicitação de autenticação de certificado, selecione o certificado da lista e clique em **Aprovar**.

Figura 20-1 *Gerenciando a autenticação em segundo plano aprimorada*



II Gerenciando o Identity Manager usando o Identity Console

Esta seção descreve várias tarefas que você pode executar para gerenciar o(s) seu(s) servidor(es) do Identity Manager usando o portal Identity Console.

21 Gerenciando drivers e conjuntos de drivers

Um conjunto de drivers é um container que mantém os drivers do Identity Manager. Apenas um conjunto de drivers pode estar ativo em um servidor por vez. Como resultado, todos os drivers ativos precisam ser agrupados no mesmo conjunto de drivers. O conjunto de drivers pode ser criado usando a ferramenta Designer. Para obter mais informações, confira Configuring Driver Sets (Configurando conjuntos de drivers) no *NetIQ Designer for Identity Manager Administration Guide* (Guia de administração do NetIQ Designer for Identity Manager).

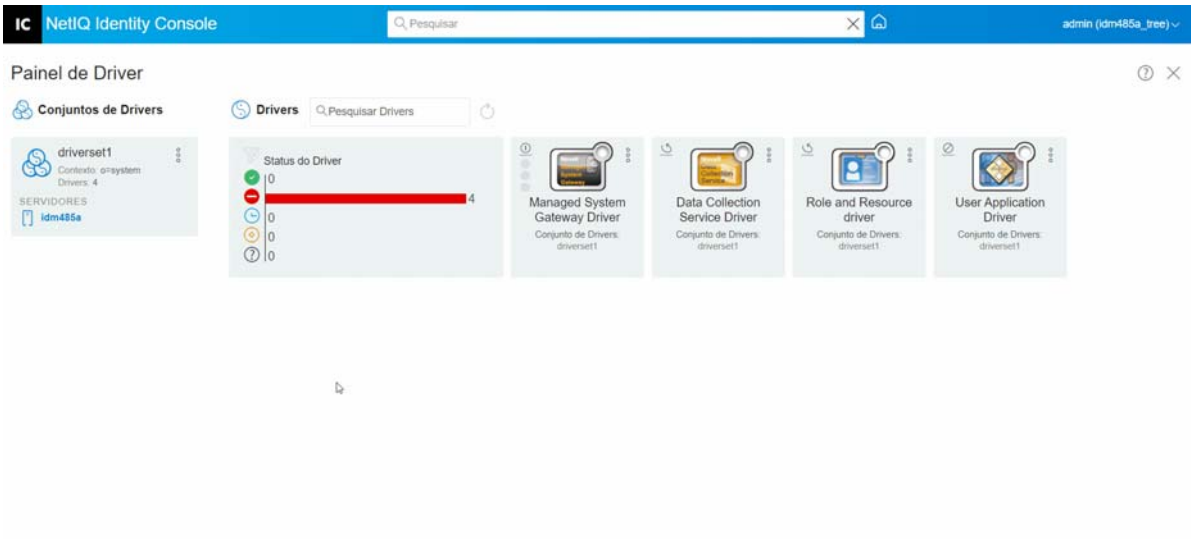
Adicionando ou apagando servidores

Um conjunto de drivers pode ser associado a um ou vários servidores por vez. No entanto, com base no seu requisito, você pode associar um objeto conjunto de drivers diferente ao servidor disponível.

Para adicionar um novo servidor, clique no ícone no objeto conjunto de drivers específico > selecione **Adicionar Servidores** e selecione o servidor apropriado no browser de contexto.

Para apagar um servidor existente, selecione a opção **Remover Servidor**.

Figura 21-1 *Adicionando o servidor ao conjunto de drivers*



Ativando conjuntos de drivers usando a chave de ativação do produto

Antes de usar qualquer conjunto de drivers e os drivers dentro dele, você precisa ativá-lo usando o código de ativação recebido em seu ID de e-mail. Depois de comprar uma licença, você receberá a sua chave de ativação da NetIQ. Execute as seguintes etapas para ativar o conjunto de drivers usando a sua chave de ativação:

1. Clique na guia **Administração IDM** na tela inicial do Identity Console.

2. Clique no ícone de Ações ⋮ na caixa do conjunto de drivers específico que você deseja ativar e clique em **Instalação de ativação**.

   Ao aplicar a Ativação, cada guia de conjunto de drivers no bloco Administração IDM mostra as informações de ativação de todos os servidores associados a esse conjunto de drivers. Essas informações ajudam a identificar quando a ativação expirará.

3. Se você tiver o arquivo de ativação baixado no seu computador, selecione a caixa de seleção para **Selecionar um arquivo contendo credenciais**.

4. Procure o arquivo de ativação, selecione-o e clique em **Enviar**.

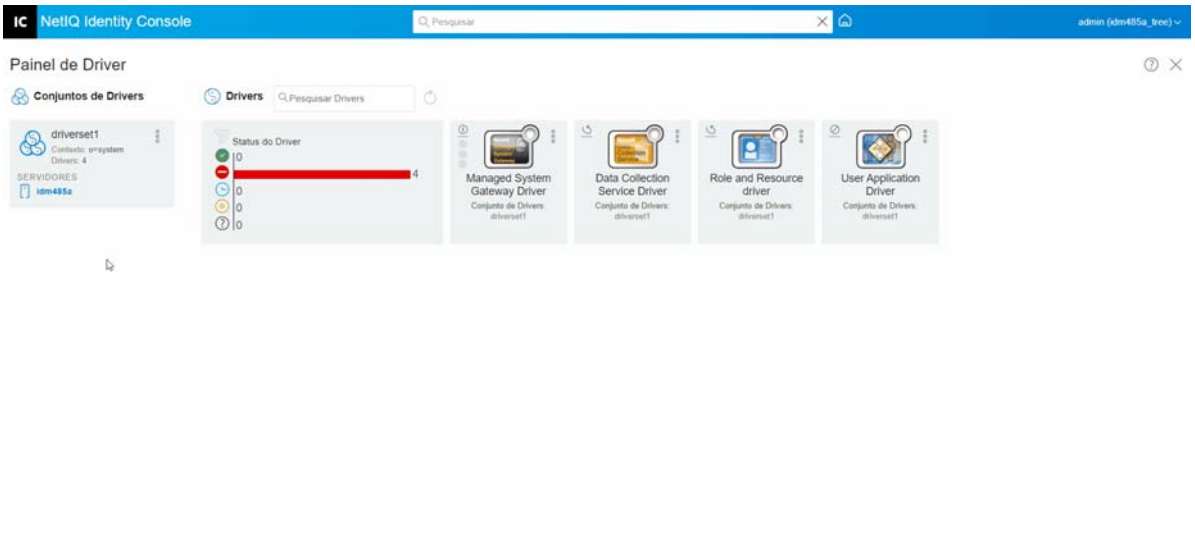
5. Alternativamente, você pode ativar o conjunto de drivers usando o conteúdo do arquivo de ativação. Selecione a caixa de seleção de **Digite as credenciais**.

   5a Abra o arquivo de Credencial de ativação de produto e copie o conteúdo da Credencial de ativação de produto na sua área de transferência.

   5b Se você optou por copiar o conteúdo, não inclua linhas nem espaços extras. Você deve começar a copiar a partir do primeiro traço (-) da credencial (----INÍCIO DA CREDENCIAL DE ATIVAÇÃO DE PRODUTO) até o último traço (-) da credencial (TÉRMINO DA CREDENCIAL DE ATIVAÇÃO DE PRODUTO-----) e clicar em **Terminar**.

6. Uma mensagem de confirmação aparece, indicando que o conjunto de drivers foi ativado com sucesso.

Figura 21-2 *Ativando conjuntos de drivers*

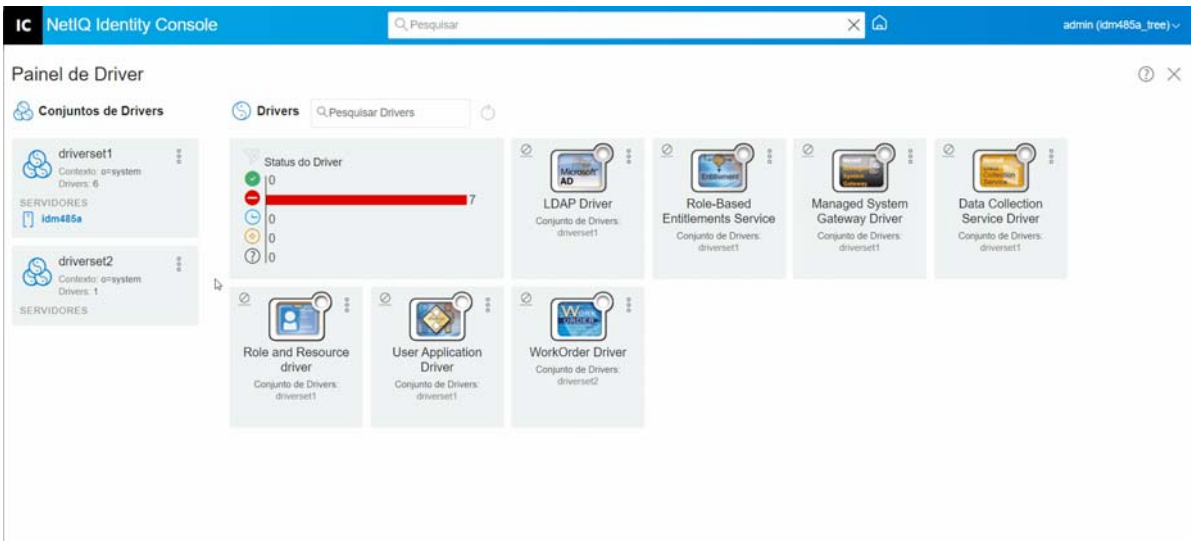


Visualizando informações de ativação de conjuntos de drivers

Depois de ativar o conjunto de drivers, você precisa verificar se ele foi ativado com sucesso. Para verificar, execute as seguintes etapas:

1. Clique na guia **Administração IDM** na tela inicial do Identity Console.
2. Clique no ícone de Ações ⋮ no objeto específico do conjunto de drivers para o qual você deseja verificar as informações de ativação e clique em **Informações de ativação**.
3. A janela de informações relacionada à ativação aparece no seu computador. Você pode verificar os detalhes de ativação do conjunto de drivers específico nessa página.

Figura 21-3 *Visualizando informações de ativação de conjuntos de drivers*

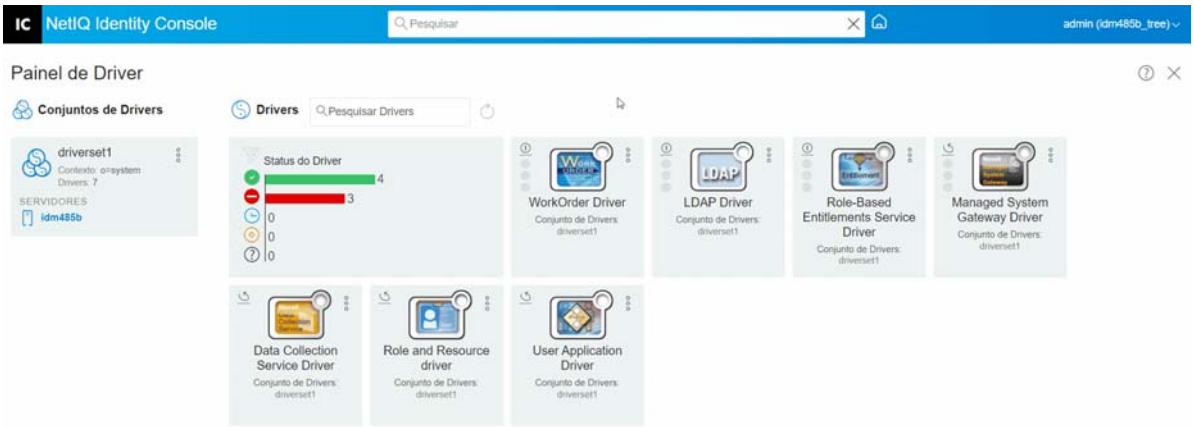


Iniciando e parando drivers

Quando um driver é criado, ele é parado por padrão. Para fazer o driver funcionar, você precisa iniciá-lo. O Identity Manager é um sistema orientado por eventos, por isso, depois que o driver é iniciado, ele permanece ocioso até que um evento ocorra. Execute as seguintes etapas para iniciar/parar o(s) driver(s).

1. Clique na guia **Administração IDM** na tela inicial do Identity Console.
2. Clique no objeto específico do conjunto de drivers definido no lado direito da tela do computador para exibir todos os drivers associados a ele.
3. Clique no ícone de Ações ⋮ no driver específico e selecione **Iniciar Driver**.
4. Se quiser parar um objeto driver, clique no ícone de Ações ⋮ no driver específico e selecione **Parar Driver**.
5. (Opcional) Alternativamente, você pode iniciar ou parar todos os drivers que residem simultaneamente no mesmo objeto conjunto de drivers. Clique no ícone de Ações ⋮ no objeto conjunto de drivers e selecione **Iniciar Todos os Drivers** ou **Parar Todos os Drivers**.

Figura 21-4 *Iniciando e parando drivers*

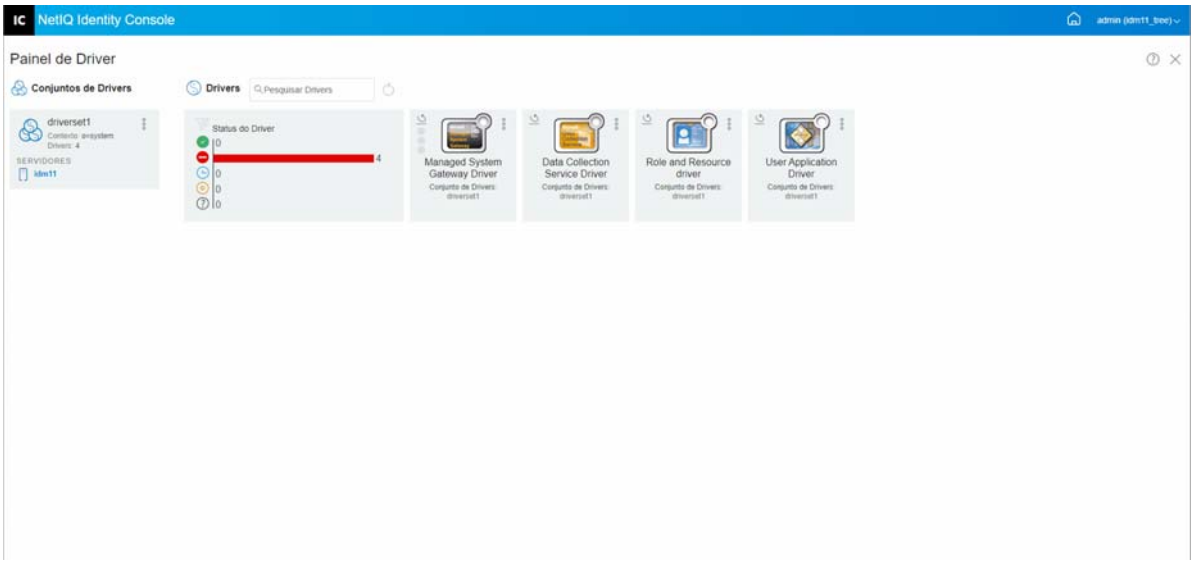


Pesquisando por drivers

O Identity Console oferece a opção de pesquisar um driver específico em seu servidor. Para pesquisar um driver, execute as seguintes etapas:

1. Clique na guia **Administração IDM** na tela inicial do Identity Console.
2. Especifique o nome do driver na caixa **Pesquisar**. O objeto Driver específico aparecerá na tela do computador. Você também pode atualizar a lista de drivers clicando no ícone ↻.

Figura 21-5 *Pesquisando por drivers*



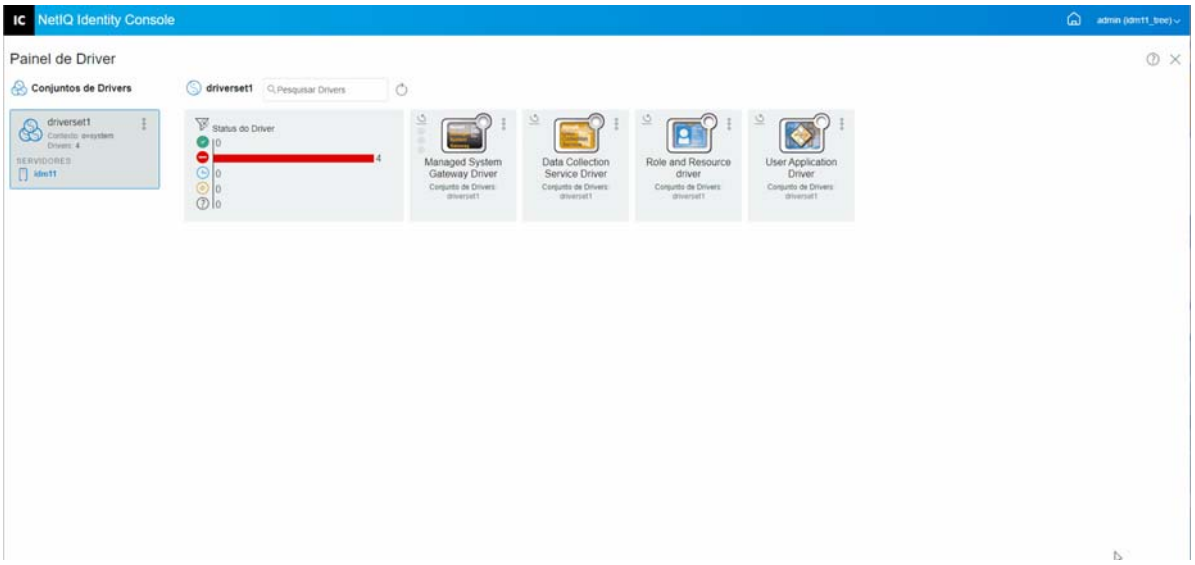
Filtrando os drivers e conjuntos de drivers

Os drivers podem ser filtrados com base no status deles na página de **Administração IDM**. Para filtrar drivers:

1. Clique na guia **Administração IDM** na tela inicial do Identity Console.
2. Clique nos seguintes ícones na guia **Driver's Status**(Status do Driver) para filtrar os drivers com base no status deles:
   - Clique no ícone para filtrar todos os drivers em execução em seu servidor.
   - Clique no ícone para filtrar todos os drivers parados em seu servidor.
   - Clique no ícone para filtrar todos os drivers que estão iniciando.
   - Clique no ícone para filtrar todos os drivers que estão parando.
   - Clique no ícone para filtrar os drivers que não têm um status associado a eles. Quando um conjunto de drivers não tiver um servidor associado a ele, os drivers residentes no conjunto de drivers exibirão o status **Desconhecido**.

   Para limpar qualquer filtro que tenha sido aplicado aos drivers, clique no ícone visível na guia **Driver's Status**(Status do Driver).
3. Os conjuntos de driver também podem ser filtrados usando o portal Identity Console. Por padrão, o portal Identity Console exibirá todos os drivers associados a todos os conjuntos de drivers em seu servidor. Se você quiser ver drivers em um conjunto de drivers específico, deverá selecionar aquele conjunto de drivers apropriado na lista de conjuntos de driver no lado esquerdo do portal Identity Console. Para limpar a seleção do conjunto de drivers, clique no conjunto de drivers selecionado mais uma vez.

Figura 21-6 *Filtrando drivers e conjuntos de drivers*



Apagando o conjunto de drivers

Para apagar um conjunto de drivers, execute as seguintes etapas:

1. Clique na guia **Administração IDM** na tela inicial do Identity Console.
2. Clique no botão de ações ⋮ no conjunto de drivers apropriado que deseja apagar.
3. Selecione **Apagar**.

Ações do driver

As seguintes ações são suportadas clicando no ícone de ações ⋮ na guia do driver individual:

- **Iniciar Driver**: Para iniciar um driver
- **Parar Driver**: Para parar um driver
- **Reiniciar Driver**: Para reiniciar um driver parado
- **Apagar Driver**: Para apagar um driver
- **Estatísticas**: Para ver as estatísticas de desempenho do driver
- **Copiar Dados**: Para copiar os dados do driver de um servidor para outro. Essa opção só está disponível para ambiente de vários servidores.

22 Gerenciando propriedades de conjunto de drivers

Esta seção fornece informações sobre as propriedades comuns a todos os conjuntos de drivers. Isso inclui todas as propriedades (Senha nomeada, Nível de registro, Inspetor de conjunto de drivers e assim por diante).

Esta seção se divide nas seguintes categorias:

Configurando de conjuntos de driver

Para modificar a configuração do conjunto de drivers, execute as seguintes etapas:

1. Clique em **Administração IDM** > **Clique no menu de contexto (reticências) do conjunto de drivers apropriado** > **Propriedades do conjunto de drivers**.
2. Por padrão, a página **Configuração do conjunto de drivers** é exibida. As opções de Configuração do conjunto de drivers são divididas nas seguintes categorias:

Senha nomeada

O Identity Manager permite que você armazene com segurança várias senhas para um conjunto de drivers. Essa funcionalidade é referida como senhas nomeadas. Cada senha diferente é acessada por uma chave ou nome.

Você pode adicionar senhas nomeadas a um conjunto de drivers ou a drivers individuais. Senhas nomeadas para um conjunto de drivers estão disponíveis para todos os drivers no conjunto.

Para usar uma senha nomeada em uma política de driver, você se refere a ela pelo nome da senha, em vez de usar a senha real, e o mecanismo do Identity Manager envia a senha para o driver. O método descrito nesta seção para armazenar e recuperar senhas nomeadas pode ser usado com qualquer driver, sem a necessidade mudanças no shim do driver.

A senha nomeada pode ser acessada selecionando **Administração IDM** > **Clique no menu de contexto (reticências) do conjunto de drivers apropriado** > **Propriedades do Conjunto de Drivers** > **Senha Nomeada** em **Configuração do Conjunto de Drivers**.

Para adicionar uma nova senha nomeada, clique no ícone +. Para remover uma senha nomeada existente, selecione a senha apropriada e clique no ícone  .

Valores de configuração globais

Exibe uma lista ordenada de objetos configuração global. Os objetos contêm definições de valores de configuração globais de extensão para o driver que o Identity Manager carrega quando o driver é iniciado. Você pode adicionar ou remover os objetos configuração global e mudar a ordem em que os objetos são executados. Clique no ícone  para gravar os valores de configuração globais. Para atualizar a lista de valores de configuração globais, clique no ícone  .

Configurando os parâmetros do ambiente Java

Para configurar os parâmetros do ambiente Java, execute as seguintes etapas:

1. No Identity Console, selecione **Administração IDM** > **Clique no menu de contexto (reticências) do conjunto de drivers apropriado** > **Propriedades do conjunto de drivers**.
2. Clique em **Parâmetros de ambiente Java** em **Configuração do conjunto de drivers** para exibir a página de propriedades que contém os parâmetros do ambiente Java.
3. Modifique as seguintes configurações, conforme desejado:

   Adições de classpath: Especifique caminhos adicionais para que a JVM pesquise arquivos de pacote (`.jar`) e de classe (`.class`). Usar esse parâmetro é o mesmo que usar o comando `java -classpath`. Ao entrar em vários caminhos de classe, separe-os com um ponto-e-vírgula (;) para uma JVM do Windows e com dois pontos (:) para uma JVM do UNIX ou Linux.

   Opções de JVM: Especifique opções adicionais a serem usadas com a JVM. Consulte a sua documentação da JVM para obter opções válidas.

   DHOST_JVM_OPTIONS é a variável de ambiente correspondente. Ela especifica os argumentos para a JVM 1.2. Por exemplo:

   ```
   -Xnoagent -Xdebug -Xrunjdwp: transport=dt_socket,server=y, address=8000
   ```

   Cada string de opções é separada por um espaço em branco. Se uma string de opções contiver um espaço em branco, ela deverá ser colocada entre aspas duplas.

   A opção de atributo de conjunto de drivers tem precedência sobre a variável de ambiente DHOST_JVM_OPTIONS. Esta variável de ambiente é abordada no final da opção de atributo de conjunto de drivers.

   Tamanho inicial do heap: Especifique o tamanho inicial (mínimo) do heap disponível para a JVM. O aumento do tamanho inicial do heap pode melhorar o tempo de inicialização e o desempenho de throughput. Use um valor numérico seguido por G, M ou K. Se nenhum tamanho de letra for especificado, o tamanho usará bytes por padrão. O uso desse parâmetro é o mesmo que usar o comando `java -Xms`.

DHOST_JVM_INITIAL_HEAP é a variável de ambiente correspondente. Ela especifica o tamanho inicial do heap da JVM no número decimal de bytes. Ela tem precedência sobre a opção de atributo de conjunto de drivers.

Consulte a documentação da JVM para obter informações sobre o tamanho padrão do heap inicial da JVM.

Tamanho máximo do heap: Especifique o tamanho máximo do heap disponível para a JVM. Use um valor numérico seguido por G, M ou K. Se nenhum tamanho de letra for especificado, o tamanho usará bytes por padrão. Usar este parâmetro é o mesmo que usar o comando `java -Xmx`.

DHOST_JVM_MAX_HEAP é a variável de ambiente correspondente. Ela especifica o tamanho máximo do heap da JVM no número decimal de bytes. Ela tem precedência sobre a opção de atributo de conjunto de drivers.

Consulte a documentação da JVM para obter informações sobre o tamanho máximo padrão do heap da JVM.

4 Clique em para gravar as mudanças.

5 Reinicie o cofre de identidade para aplicar as mudanças.

Gerenciando a lista de atributos avaliados

Para adicionar atributos à lista de atributos avaliados para um conjunto de drivers específico, execute as seguintes etapas:

1 No Identity Console, selecione o módulo **Gerenciamento de Objetos**.

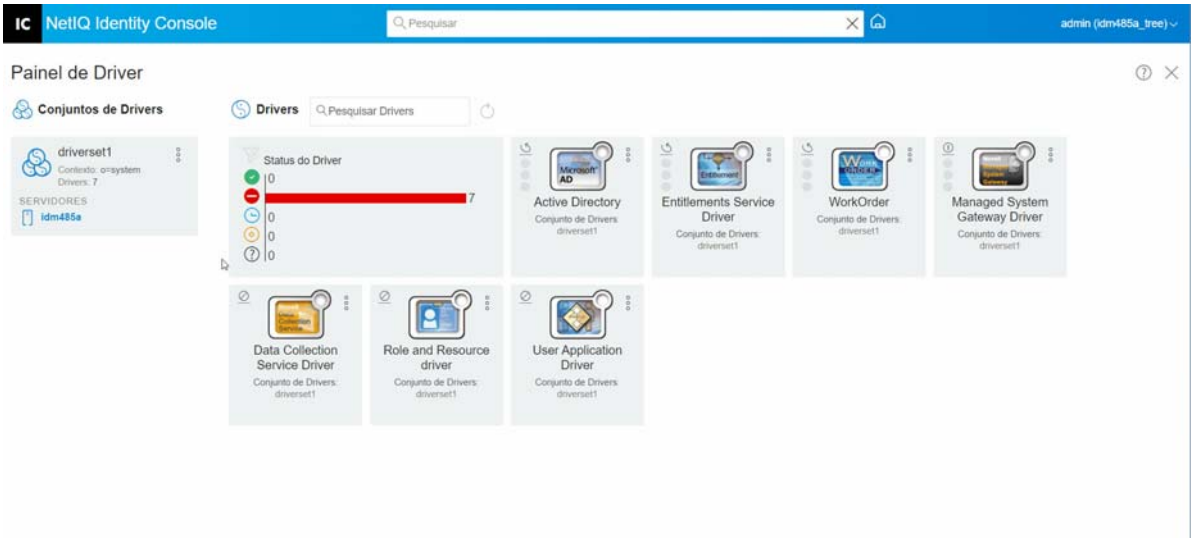
2 Selecione o tipo **DirXML-DriverSet** da lista suspensa e clique no botão Pesquisar.

3 Clique no conjunto de drivers apropriado na lista de pesquisa.

4 Para adicionar atributos não avaliados à lista de atributos, clique no ícone ao lado dos **Atributos Avaliados** e selecione os atributos não avaliados na lista.

5 Depois de concluir o procedimento, clique em **OK**.

Figura 22-1 *Gerenciamento de parâmetros de configuração do conjunto de drivers*



Gerenciando tarefas para conjuntos de drivers

O Identity Console permite que você programe eventos usando a opção Tarefas para todos os drivers residentes no respectivo conjunto de drivers.

A página Programador de tarefas contém o nome da tarefa, se a tarefa está habilitada ou desabilitada, quando ela está programada para ser executada e a descrição da tarefa. Clique no nome da tarefa para ativar a página Tarefas. Clique no ícone habilitar/desabilitar na coluna Habilitado para habilitar ou desabilitar a tarefa. Clique na descrição da tarefa para ver a descrição completa da tarefa.

A página Tarefas é acessada selecionando **Administração IDM** > **Clique no menu de contexto (reticências) do conjunto de drivers apropriado** > **Propriedades do conjunto de drivers** > guia **Avançado** da página principal do Identity Console. A guia Tarefas contém uma tabela que mostra os objetos tarefa existentes para o driver selecionado, que está listado com o seu Nome exclusivo na entrada do Driver.

A página Programador de Tarefas permite que você execute as seguintes tarefas:

- **Criar a Tarefa**: Clique no ícone  para criar uma nova tarefa.

  No pop-up **Nova Tarefa**, para criar uma nova tarefa, realize as seguintes etapas:

  1. Especifique o nome da tarefa.
  2. Selecione o tipo da tarefa.
  3. Clique no ícone  e, na lista disponível de servidores, selecione o servidor no qual deseja executar a tarefa. Caso contrário, especifique um nome do servidor e selecione o servidor.
  4. Clique no botão **Criar**.
- **Iniciar a Tarefa**: Selecione uma tarefa clicando na caixa à esquerda da tarefa e clique no ícone .
- **Parar a Tarefa**: Selecione uma tarefa clicando na caixa à esquerda da tarefa e clique no ícone .
- **Habilitar a Tarefa**: Selecione uma tarefa clicando na caixa à esquerda da tarefa e clique no ícone .
- **Desabilitar a Tarefa**: Selecione uma tarefa clicando na caixa à esquerda da tarefa e clique no ícone .
- **Obter Status**: Selecione uma tarefa clicando na caixa à esquerda da tarefa e clique no ícone .
- **Apagar a Tarefa**: Selecione uma tarefa clicando na caixa à esquerda da tarefa e clique no ícone .

Clique em uma tarefa para acessar a página **Job Property** (Propriedade da Tarefa). Aqui você pode configurar como você quer que a tarefa seja executada.

Geral: Mostra o nome da classe Java da tarefa. Use esta página para habilitar ou desabilitar a tarefa, apague-a após a execução dela, selecione o servidor ou servidores em que essa tarefa deve ser executada, especifique o servidor de e-mail e dê à tarefa um nome de exibição e uma descrição diferentes.

Programação: Permite definir quando executar a tarefa. Especifique Iniciar a tarefa em para definir o horário e se executar a tarefa diariamente, semanalmente, mensalmente, anualmente. Você também pode personalizar quando quer executar a tarefa ou pode optar por habilitar o botão de alternância para executar a tarefa manualmente.

Escopo: Permite que você defina os objetos aos quais essa tarefa se aplica. Um objeto pode ser um container, um grupo dinâmico, um grupo ou um objeto Folha. Clique em Adicionar para selecionar o objeto ao qual você deseja que essa tarefa se aplique. Use o botão Procurar para selecionar um objeto e, em seguida, clique em OK. Para remover um objeto da lista de escopo, selecione um objeto de escopo clicando na caixa à esquerda do objeto DN e clique em Remover.

Quando um objeto for adicionado, selecione-o para exibir mais opções. Se você selecionar um objeto de grupo, terá a opção de aplicar a tarefa apenas aos membros do grupo ou apenas ao grupo. Se você selecionar um objeto Container, terá a opção de aplicar a tarefa a todos os descendentes no container, a todos os filhos no container ou apenas ao container.

Parâmetros: Permite adicionar parâmetros adicionais à tarefa e ver os parâmetros da forma como estão configurados atualmente. Esses parâmetros mudam, dependendo do tipo de tarefa selecionada.

Resultados: Permite definir o que você quer fazer com os resultados da tarefa. A página Resultados é dividida em duas partes: Resultado Intermediário e Resultado Final, com os seguintes resultados sendo permitidos: Sucesso, Aviso, Erro e Interrompido. À direita da coluna Resultados está a coluna Ação. Clicar na coluna Ação permite definir como você deseja receber notificações para cada resultado. As ações incluem o envio de um resultado de auditoria ou o envio de um e-mail quando o resultado for concluído. Se você não selecionar uma opção, nenhuma ação será tomada para o resultado.

Na guia **Rastrear**, você pode configurar o rastreamento de um driver específico. Para obter mais informações, consulte “Configurando o nível de rastreamento” na página 175

Gerenciando bibliotecas para um conjunto de drivers específico

Os objetos biblioteca armazenam várias políticas e outros recursos que são compartilhados por um ou mais drivers. Um objeto biblioteca pode ser criado em um objeto conjunto de drivers ou em qualquer container do eDirectory. Várias bibliotecas podem existir em uma árvore do eDirectory. Os drivers podem se referir a qualquer biblioteca na árvore, desde que o servidor que esteja executando o driver mantenha uma réplica de Leitura/Gravação ou Master do objeto biblioteca.

Folhas de estilo, políticas, regras e outros objetos recurso podem ser armazenados em uma biblioteca e ser referenciados por um ou mais drivers.

Ao utilizar o módulo Gerenciamento de Bibliotecas, você pode executar as seguintes tarefas:

- “Visualizando e apagando uma biblioteca existente” na página 146
- “Visualizando e apagando objetos biblioteca” na página 146

Visualizando e apagando uma biblioteca existente

Para ver e apagar uma biblioteca existente, execute as seguintes etapas:

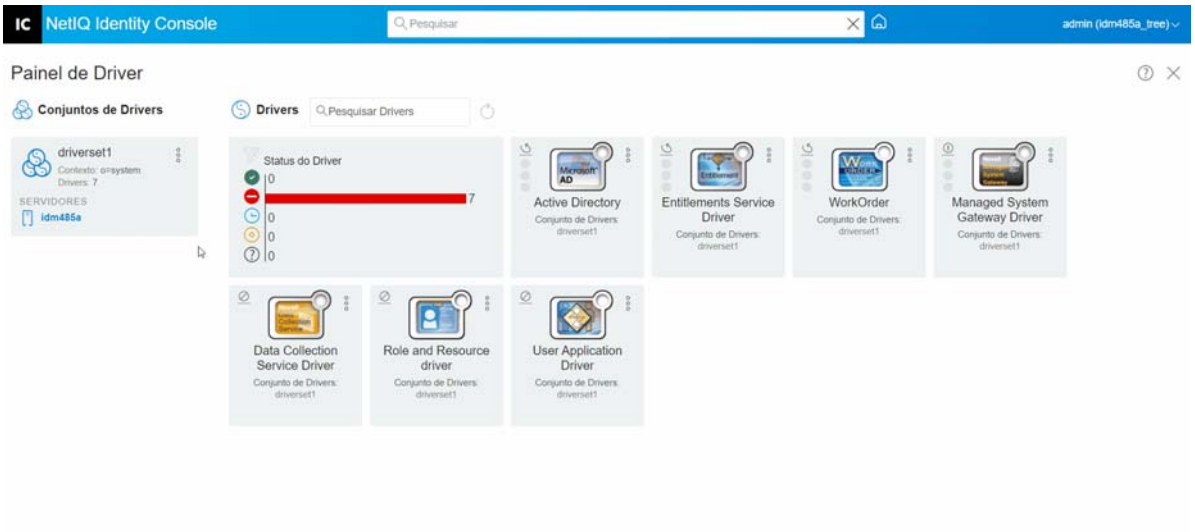
1. No Identity Console, selecione **Administração IDM** > **Clique no menu de contexto (reticências) do conjunto de drivers apropriado** > **Propriedades do conjunto de drivers** > **Avançado** > **Bibliotecas**.
2. Selecione a biblioteca apropriada na lista.
3. Clique no ícone . Clique em **OK** para confirmar.

Visualizando e apagando objetos biblioteca

Você pode ver e apagar políticas e mapear tabelas de objetos biblioteca. Para apagar objetos, execute as seguintes etapas:

1. No Identity Console, selecione **Administração IDM** > **Clique no menu de contexto (reticências) do conjunto de drivers apropriado** > **Propriedades do conjunto de drivers** > **Avançado** > **Bibliotecas**.
2. Clique na biblioteca apropriada na lista.
3. Para apagar políticas, selecione a guia **Políticas**.
4. Selecione a política apropriada na lista e clique no ícone .
5. Para apagar tabelas de mapeamento, selecione a guia **Tabelas de mapeamento**.
6. Selecione a tabela de mapeamento apropriada na lista e clique no ícone .
7. Clique em **OK** para confirmar.

Figura 22-2 *Gerenciando tarefas e bibliotecas para conjuntos de drivers*



Configurando os níveis de registro e rastreamento dos conjuntos de driver

Para configurar o registro e o rastreamento dos conjuntos de driver, selecione **Administração IDM** > **Clique no menu de contexto (reticências) do conjunto de drivers apropriado** > **Propriedades do conjunto de drivers** > guia **Configuração de registro e rastreamento** da página principal do Identity Console. Esta seção se divide nas seguintes categorias:

Configurando o nível de registro

Cada conjunto de drivers tem um campo de nível de registro, no qual você pode definir o nível de erros que devem ser rastreados. O nível indicado aqui determina quais mensagens estão disponíveis para os registros. Por padrão, o nível de registro é definido para monitorar mensagens de erro. (Isso também inclui mensagens fatais.) Para monitorar tipos de mensagens adicionais, mude o nível de registro. Para configurar o nível de registro, no Identity Console, selecione **Administração IDM** > **Clique no menu de contexto (reticências) do conjunto de drivers apropriado** > **Propriedades do conjunto de drivers** > **Configuração de registro e de rastreamento** > **Nível de registro**. A tabela a seguir descreve as configurações do nível de registro:

Opção	Descrição
Desligue o registro para registros do conjunto de drivers, do Subscritor e do Editor	Desliga todo o registro para todos os drivers no objeto conjunto de drivers, no canal do Subscritor e no canal do Editor.
Número máximo de entradas no registro (50-500)	Número de entradas no registro. O valor padrão é 50.

Níveis de registro	Os seguintes níveis de registro estão disponíveis para seleção:
	◆ **Erros de Registro**: Registra apenas erros
	◆ Erros e avisos de registro: Registra erros e avisos
	◆ **Eventos específicos de registro**: Registra os eventos selecionados. A seleção dessa opção permite a seguinte lista de eventos:
	  ◆ **Eventos do mecanismo de metadiretório**
	  ◆ **Eventos de status**
	  ◆ **Eventos de operação**
	  ◆ **Eventos de transformação**
	  ◆ **Eventos de aprovisionamento de credenciais**
	◆ **Apenas atualizar o horário do último registro**: Atualiza o horário do último registro.
	◆ **Registro desligado**: Desliga o registro para o driver.

Configurando o nível de rastreamento

Você pode configurar o rastreamento de um conjunto de drivers específico. Dependendo do nível de rastreamento especificado para um conjunto de drivers, o rastreamento exibe eventos relacionados ao driver quando o mecanismo processa os eventos. O nível de rastreamento do driver afeta apenas o driver ou conjunto de drivers em que o rastreamento está definido. Se você estiver usando o Carregador Remoto, o arquivo de rastreamento do Carregador Remoto será definido diretamente no Carregador Remoto e conterá apenas o rastreamento de shim do driver.

Para configurar o rastreamento de um conjunto de drivers, selecione **Administração IDM** > **Clique no menu de contexto (reticências) do conjunto de drivers apropriado** > **Propriedades do conjunto de drivers** > **Configuração de registro e de rastreamento** > guia **Rastrear**. A tabela a seguir descreve as configurações de rastreamento:

Parâmetro	Driver
Nível de rastreamento	À medida que o nível de rastreamento do driver aumenta, o mesmo ocorre com a quantidade de informações exibidas no rastreamento. O nível de rastreamento um mostra erros, mas não a causa dos erros. Se você quiser ver informações de sincronização de senha, defina o nível de rastreamento para cinco. Se você selecionar **Usar a configuração do conjunto de drivers** o valor será retirado do conjunto de drivers.
Nível de rastreamento XSL	O rastreamento exibe eventos XSL. Defina esse nível de rastreamento somente ao solucionar problemas nas folhas de estilo XSL. Se você não quiser ver as informações do XSL, defina o nível como zero.
Porta de depuração do Java	Permite que os desenvolvedores anexem um depurador Java. Reinicie o cofre de identidade depois de anexar o depurador Java.
Arquivo de rastreamento	Especifique o nome do arquivo e a localização de onde as informações do Identity Manager estão escritas para o driver selecionado. Se você selecionar **Usar a configuração do conjunto de drivers**, o valor será retirado do conjunto de drivers.
Codificação de arquivo de rastreamento	O arquivo de rastreamento usa a codificação padrão do sistema. Você poderá especificar outra codificação, se desejar. Se você selecionar **Usar a configuração do Conjunto de Drivers**, o valor será retirado do conjunto de drivers.

Parâmetro	Driver
Limite de tamanho do arquivo de rastreamento	Permite definir um limite para o arquivo de rastreamento Java. Se você definir o tamanho do arquivo como ilimitado, o tamanho do arquivo aumentará até que não haja mais espaço em disco. **Observação:** Se o limite de tamanho do arquivo for especificado, o arquivo de rastreamento será criado em vários arquivos. O Identity Manager divide automaticamente o tamanho máximo do arquivo em dez e cria dez arquivos separados. O tamanho combinado desses arquivos é igual ao tamanho máximo do arquivo de rastreamento. Se você selecionar **Usar a configuração do conjunto de drivers**, o valor será retirado do conjunto de drivers.

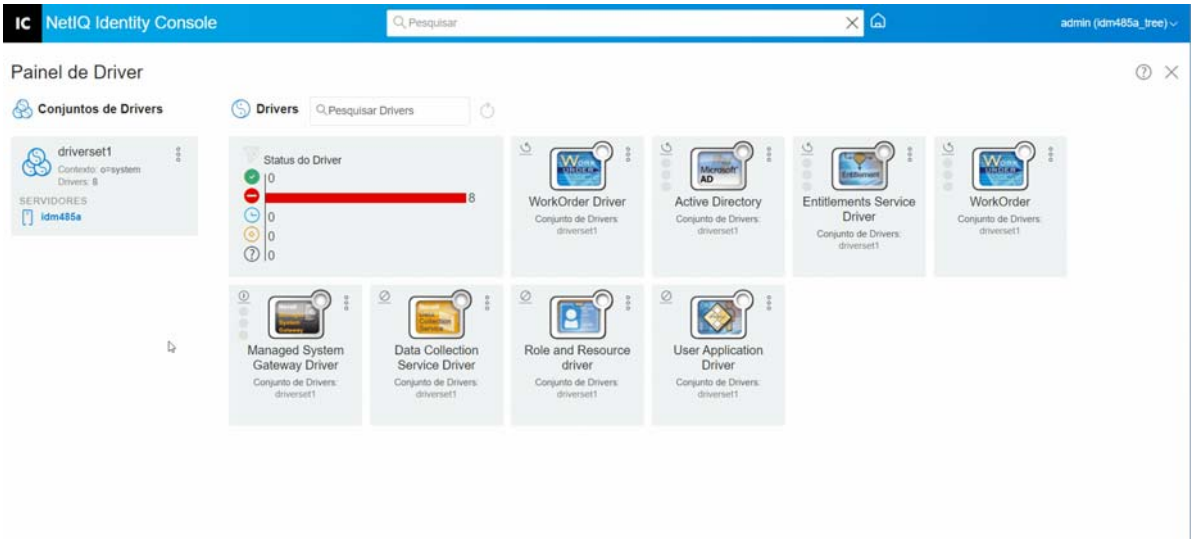
Rastreando scripts DirXML

A opção Rastreamento de Scripts DirXML permite selecionar um nível de rastreamento para um conjunto de drivers. A seleção é aplicada a todas as políticas no conjunto de drivers. As seguintes opções de rastreamento de script DirXML estão disponíveis para seleção:

- Todos os rastreamentos de script DirXML ligados
- Todos os rastreamentos de script DirXML desligados
- Rastreamento de regras de script DirXML ligado
- Rastreamento de regras de script DirXML desligado

Clique em para gravar as mudanças.

Figura 22-3 *Gerenciando os níveis de registro e rastreamento dos conjuntos de drivers*



Gerenciando as estatísticas e o Inspetor do conjunto de drivers

Você pode usar o Inspetor do conjunto de drivers para ver informações detalhadas sobre os objetos associados a um conjunto de drivers. Esta seção se divide nas seguintes categorias:

Visualizando estatísticas do conjunto de drivers

Você pode usar o portal Identity Console para ver uma variedade de estatísticas para um driver individual ou para um conjunto de drivers inteiro. Isso inclui estatísticas como o tamanho do arquivo de cache, o tamanho das transações não processadas no arquivo de cache, as transações mais antigas e mais recentes e o número total de transações não processadas por categoria (adicionar, remover, modificar e assim por diante). Para ver as estatísticas do conjunto de drivers:

1. No Identity Console, selecione **Administração de IDM** > **Clique no menu de contexto (reticências) do conjunto de drivers apropriado** > **Propriedades do conjunto de drivers** > **Inspetor e estatísticas** > **Estatísticas**.
2. Selecione o servidor apropriado na lista suspensa.

   É mostrada uma página que permite ver as estatísticas de todos os drivers contidos no conjunto de drivers.

   - Para atualizar as estatísticas, clique no ícone .
   - Para fechar as estatísticas de um driver, clique no botão no canto superior direito da janela de estatísticas do driver.
   - Para abrir as estatísticas para todos os drivers, clique em **Ações** > **Mostrar Tudo**.
   - Para recolher a lista de transações não processadas de um driver, clique no botão localizado acima da lista. Para recolher a lista de transações não processadas para todos os drivers, clique em **Ações** > **Recolher todas as transações**.
   - Para expandir a lista de transações, clique no botão . Para expandir a lista de transações não processadas para todos os drivers, clique em **Ações** > **Expandir todas as transações**.
   - Para fechar o painel de estatísticas de drivers desabilitados, clique em **Ações** e selecione **Fechar drivers desabilitados**.

Vendo informações de versão

O mecanismo do Identity Manager, os shims do driver e os arquivos de configuração do driver contêm um número de versão separado. A opção Descoberta de versão no Identity Console ajuda você a encontrar as versões do mecanismo do Identity Manager e as versões dos shims do driver. Os arquivos de configuração do driver contêm uma convenção de nomeação própria. Para ver as informações da versão:

1. No Identity Console, selecione **Administração de IDM** > **Clique no menu de contexto (reticências) do conjunto de drivers apropriado** > **Propriedades do conjunto de drivers** > **Inspetor e estatísticas** > **Descoberta de versão**.
2. Ver uma exibição de nível superior das informações de versão:
   - A árvore do eDirectory à qual você está autenticado

     Observação: O eDirectory é chamado de Cofre de Identidade quando usado no ambiente do Identity Manager.
   - O conjunto de drivers que você selecionou
   - Servidores associados ao conjunto de drivers

     Se o conjunto de drivers estiver associado a dois ou mais servidores, você poderá ver informações do Identity Manager em cada servidor.
   - Drivers
3. Clique no ícone **Ver** para exibir uma representação textual das mesmas informações contidas na visualização de nível superior.
4. Clique no botão Exportar para exportar e gravar o texto em um arquivo em sua unidade local ou de rede.

Vendo estatísticas de associação

Usando o recurso de Estatísticas de associação do Identity Manager, você pode encontrar mais informações sobre a associação das identidades gerenciadas pelo Identity Manager. O Identity Manager utiliza as estatísticas de associação para obter a contagem de associações para os drivers do Identity Manager.

Para obter os objetos ativos, inativos e gerenciados pelo sistema para um driver, execute a tarefa de estatísticas de associação. Você pode programar a tarefa de estatísticas de associação em uma base diária, semanal, mensal ou anual. Por padrão, a tarefa está programada para ser executada toda semana.

O painel de Estatísticas de associação exibe mais informações sobre a associação. Alternativamente, você pode ver mais informações exportando as associações para um arquivo.

Observação

- A contagem de associações para os drivers é por servidor. Se um objeto estiver associado a mais de um driver, a contagem de associações será calculada exclusivamente para cada driver.
- Se você tem mais de 200 mil associações, recomendamos que você defina o tamanho máximo do heap do conjunto de drivers para 2 GB ou mais. Para obter informações sobre como definir o tamanho do heap, consulte "Configurando os parâmetros do ambiente Java" na página 142.

Para ver as estatísticas de associação:

1. No Identity Console, selecione **Administração de IDM** > **Clique no menu de contexto (reticências) do conjunto de drivers apropriado** > **Propriedades do conjunto de drivers** > **Inspetor e estatísticas** > **Estatísticas de associação**.
2. Selecione o servidor para o qual você deseja executar as estatísticas de associação.
3. A contagem de associações exibe o resultado previamente computado.

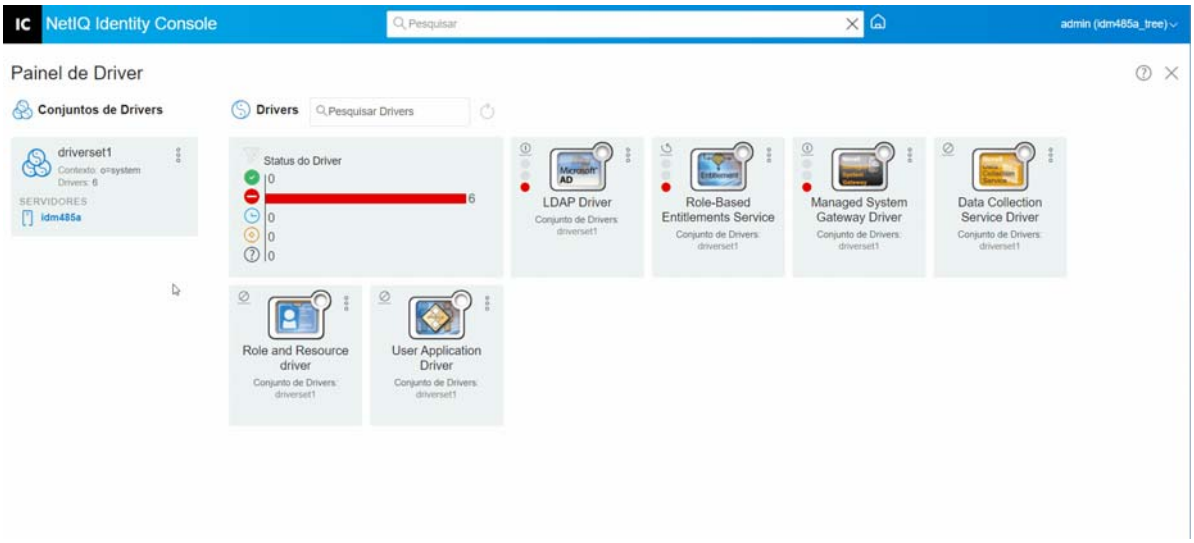
   O Identity Console exibe a contagem de associações para objetos ativos, inativos e gerenciados pelo sistema para todos os drivers associados ao conjunto de drivers.

   O Identity Console considera grupos e unidades de organização como objetos gerenciados pelo sistema. O Identity Console considerará um objeto como inativo se o atributo `Login desabilitado` no objeto for definido como verdadeiro e o objeto não tiver sido modificado nos últimos 120 dias. Todos os objetos restantes são considerados objetos gerenciados ativos.
4. Clique no ícone para obter os resultados atualizados.

   Quando um driver é desabilitado no servidor, o Identity Console não exibe o driver no painel.
5. Clique no ícone para exportar os detalhes do sistema e os detalhes da contagem de associações para os drivers associados ao servidor.
6. Para exportar os objetos associados a um driver específico, clique em ao lado dos objetos necessários e grave o arquivo.

   Observação: No caso de drivers Fan-Out, apenas objetos exclusivos são exportados. Se um objeto estiver associado a várias instâncias de um driver de Fan-Out, o Identity Console exibirá todas as contagens de associações no painel. No entanto, se você optar por exportar os objetos em um arquivo, o Identity Console exportará apenas os objetos exclusivos.
7. Clique em **Ações** e selecione a opção necessária para organizar o painel de contagem de associações.

Figura 22-4 *Gerenciando Estatísticas do Conjunto de Drivers*



23 Gerenciando propriedades do driver

Esta seção fornece informações sobre as propriedades comuns a todos os drivers. Isso inclui todas as propriedades (Senha Nomeada, Valores de Controle de Mecanismo, Nível de Registro e assim por diante).

As informações de ativação de um driver são exibidas, o que lembra uma ação para você ativar o driver de expiração.

Para modificar a configuração do driver, execute as seguintes etapas:

1. Clique na guia **Drivers** na tela inicial do Identity Console.
2. Clique na guia do respectivo driver para ver a página de configuração do driver.

   Por padrão, a página **Parâmetros de conexão** é exibida. As opções de configuração do driver são divididas nas seguintes categorias:

Parâmetros de conexão

Os parâmetros de conexão controlam se o driver deve estar em execução localmente ou remotamente.

- **Java:** Use essa opção para especificar o nome da classe Java que é instanciada para o componente shim do driver. Ela pode estar no diretório classes como um arquivo de classe ou no diretório `lib` em um arquivo `.jar`. Selecione essa opção para executar o driver localmente. Você também precisa especificar a Senha do objeto driver e o limite do cache de driver. Você pode definir uma nova senha clicando no link **Definir Senha**.

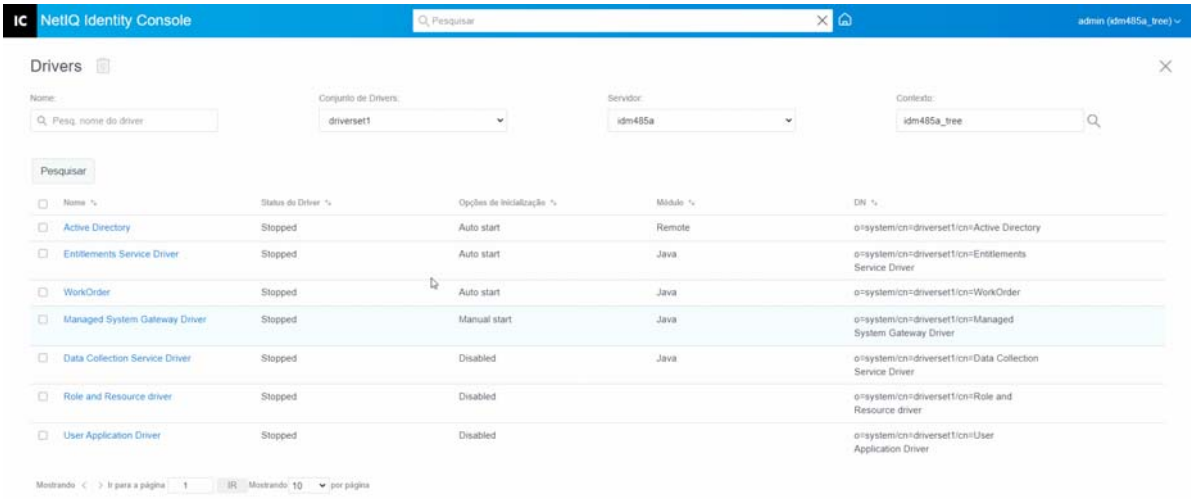
  Por exemplo, `com.microfocus.nds.dirxml.driver.scim.SCIMDriverShim`
- **Nativo:** Essa opção é usada para especificar o nome do `.dll` que é desenvolvido em uma linguagem nativa (como C++) para o driver. Você também precisa especificar a Senha do objeto driver e o limite do cache de driver. Você pode definir uma nova senha clicando no link **Definir Senha**.

  Por exemplo, `addriver.dll`

- **Conectar-se ao Carregador Remoto:** Essa opção é usada quando o driver está se conectando remotamente ao sistema conectado. Se essa opção for selecionada, você precisará especificar as seguintes subopções:
  - **Parâmetros de conexão de carregador remoto**: Inclui informações dos detalhes do ambiente do Carregador Remoto, tais como Nome de host, Porta de conexão etc.
  - **Senha do Carregador Remoto**: A senha do Carregador Remoto.
  - **Senha do objeto driver**: Especifica uma senha para o objeto driver. Se você estiver usando o Carregador Remoto, precisará digitar uma senha nesta página. O Carregador Remoto usa essa senha para autenticar-se ao shim do driver remoto.
- **Autenticação**: Os parâmetros de autenticação são usados para autenticar os servidores do Mecanismo do Identity Manager e do Carregador Remoto. Especifique os seguintes parâmetros:
  - **ID de Autenticação**: Especifique um ID do aplicativo de usuário. Esse ID é usado para passar informações de assinatura do cofre de identidade para o aplicativo.
  - **Contexto de autenticação**: Especifique o endereço IP ou o nome do servidor com o qual o shim do aplicativo deve se comunicar.
  - **Senha do aplicativo**: Opção para definir a senha de autenticação de aplicativo.

Uma vez concluído, clique no ícone para gravar a configuração.

Figura 23-1 *Gerenciando parâmetros de conexão*



Configuração do driver

A seção de configuração do driver permite configurar os parâmetros específicos do driver, valores de controle de mecanismo, valores de configuração global etc. Quando você muda os parâmetros do driver, você sintoniza o comportamento do driver para se alinhar ao ambiente de rede. Esta seção se divide nas seguintes categorias:

Parâmetros do driver

Os parâmetros do driver são divididos em Configurações de driver, Configurações do subscritor e Configurações do editor. Essas configurações serão preenchidas com base na configuração do seu driver. Para obter mais informações sobre os parâmetros do driver, consulte o guia específico do driver na Documentação de drivers do Identity Manager.

Uma vez concluído o procedimento, você poderá gravar os parâmetros clicando em  . Se você quiser definir os parâmetros para o valor padrão, clique no ícone  . Para modificar a configuração do driver usando o arquivo xml, clique no ícone  .

Valores de configuração globais

Exibe uma lista ordenada de objetos configuração global. Os objetos contêm definições de valores de configuração globais de extensão para o driver que o Identity Manager carrega no momento da inicialização do driver. Você pode ver ou modificar os objetos na guia **Valores de configuração globais** usando o editor XML. Clique no ícone  para gravar os valores de configuração globais. Para atualizar a lista de valores de configuração globais, clique no ícone  . Para apagar valores de configuração globais, selecione o objeto valor de configuração global apropriado e clique no ícone  .

Valores de controle de mecanismo

Os valores de controle de mecanismo são uma maneira de possibilitar a mudança de certos comportamentos padrão do mecanismo do Identity Manager. Os valores só poderão ser acessados se um servidor estiver associado ao objeto conjunto de drivers.

Opção	Descrição
Intervalo entre tentativas do canal do subscritor em segundos	O intervalo entre tentativas do canal do subscritor controla a frequência com que o mecanismo do Identity Manager tenta novamente realizar o processamento de uma transação em cache depois que o objeto subscritor do shim do aplicativo retorna um status de repetição.
Formulário qualificado para valores de atributo de sintaxe DN	A especificação qualificada para valores de atributo de sintaxe DN controla se os valores de atributo de sintaxe DN são apresentados em forma de barra não qualificada ou forma de barra qualificada. Uma configuração Verdadeiro significa que os valores são apresentados em forma qualificada.
Forma qualificada a partir de eventos de renomeação	O formulário qualificado para eventos de renomeação controla se a parte do nome novo dos eventos de renomeação provenientes do Cofre de Identidade é apresentada ao canal do Subscritor com qualificadores de tipo. Por exemplo, CN=. Uma configuração Verdadeiro significa que os nomes são apresentados em forma qualificada.
Tempo máximo de espera de replicação do eDirectory em segundos	Essa configuração controla o tempo máximo que o mecanismo do Identity Manager espera para que uma determinada mudança se replique entre a réplica local e uma réplica remota. Isso afeta apenas as operações em que o mecanismo do Identity Manager é obrigado a entrar em contato com um servidor remoto do eDirectory na mesma árvore para executar uma operação e pode precisar esperar até que alguma mudança tenha sido replicada para ou do servidor remoto antes que a operação possa ser concluída (por exemplo, movimentações de objeto quando o servidor do Identity Manager não mantém a réplica master do objeto movido; operações de direitos do sistema de arquivos para usuários criados por meio de um gabarito.)
Use o modo retrocompatível fora de conformidade para o XSLT	Esse controle define o processador XSLT usado pelo mecanismo do Identity Manager para um modo retrocompatível. O modo retrocompatível faz com que o processador XSLT use um ou mais comportamentos que não são compatíveis com os padrões XPath 1.0 e XSLT 1.0. Isso é feito para compatibilidade retroativa com folhas de estilo DirXML existentes que dependem dos comportamentos não padrão. Por exemplo, o comportamento do operador XPath “!=” operador quando um operando é um conjunto de nós e o outro operando é diferente de um conjunto de nós está incorreto em versões do DirXML até (e incluindo) o Identity Manager 2.0. Esse comportamento foi corrigido; no entanto, o comportamento corrigido é desabilitado por padrão através deste controle em favor da compatibilidade retroativa com as folhas de estilo do DirXML existentes.
Máximo de objetos aplicativo a serem migrados de uma só vez	Esse controle é usado para limitar o número de objetos aplicativo que o mecanismo do Identity Manager solicita de um aplicativo durante uma consulta individual que é realizada como parte de uma operação Migrar Objetos de um Aplicativo. Se erros java.lang.OutOfMemoryError forem encontrados durante uma operação Migrar de um Aplicativo, esse número deverá ser definido abaixo do padrão. O padrão é 50. **Observação:** Esse controle não limita o número de objetos aplicativo que podem ser migrados; ele limita apenas o tamanho do lote.

Opção	Descrição
Definir creatorsName em objetos criados no cofre de identidade	Esse controle é usado pelo mecanismo do Identity Manager para determinar se o atributo creatorsName deve ser definido para o DN deste driver em todos os objetos criados no cofre de identidade por este driver. A definição do atributo creatorsName permite identificar facilmente objetos criados por este driver, mas também resulta em uma redução de desempenho. Se não for definido, o atributo creatorsName usará por padrão o valor do DN do objeto Servidor NCP que está hospedando o driver.
Gravar associações pendentes	Este controle determina se o mecanismo do Identity Manager grava uma associação pendente em um objeto durante o processamento do canal do Subscritor. A gravação de uma associação pendente oferece pouco ou nenhum benefício, mas resulta em uma perda de desempenho. No entanto, existe a opção de ligá-la para compatibilidade retroativa.
Usar valores de eventos de senha	Este controle determina a fonte do valor relatado para o atributo nspmDistributionPassword para eventos Adicionar e Modificar do canal do Subscritor. Definir o controle para Falso significa que o valor atual da nspmDistributionPassword é obtido e relatado como o valor do evento de atributo. Isso significa que apenas o valor atual da senha está disponível. Esse é o comportamento padrão. Definir o controle para Verdadeiro significa que o valor registrado com o evento do eDirectory é descriptografado e é relatado como o valor do evento de atributo. Isso significa que tanto o valor da senha antiga (se existir) quanto o valor da senha de substituição no momento do evento estão disponíveis. Isso é útil para sincronizar senhas com determinados aplicativos que requerem a senha antiga para habilitar a configuração de uma nova senha.
Repetir ventos fora de banda	Este controle determina se os eventos de sincronização fora de banda deverão ou não ser tentados novamente se o status de **repetição** para o evento de sincronização fora de banda for recebido. Se o controle for definido como Falso, a sincronização fora de banda não será tentada novamente. Se for definido como verdadeiro, a sincronização fora de banda será tentada novamente até ter sucesso.
Usar o mecanismo Rhino ECMAScript	Determina se o mecanismo do Identity Manager usa o mecanismo Rhino ECMAScript. O mecanismo usa o Rhino como o mecanismo de ECMAScript padrão. Esse controle é **verdadeiro** por padrão. Se você definir esse controle como **Falso**, o mecanismo usará o script Nashorm.

Opção	Descrição
Habilitar canal de serviço do subscritor	Determina se o mecanismo do Identity Manager processa as consultas fora de banda no canal de Serviço do Subscritor do driver. Alguns exemplos comuns dessas consultas são a atualização de mapa de código, a coleta de dados e as consultas desencadeadas por meio de dxcmd. Quando esse controle é definido como verdadeiro, o canal processa separadamente essas consultas sem interromper o processamento normal dos eventos. Atualmente, esse controle só está disponível para uso com o driver de Fan-Out JDBC (habilitado por padrão).
Habilitar o relatório de status da sincronização de senhas	Este controle determina se o mecanismo do Identity Manager relata o status dos eventos de mudança de senha do canal do Subscritor. Relatar o status dos eventos de mudança de senha do canal do Subscritor permite que aplicativos como o Aplicativo de Usuário do Identity Manager monitorem o progresso de sincronização de uma mudança de senha que deve ser sincronizada com o aplicativo conectado.
Combinar valores do objeto gabarito com os da operação adicionar	Esse valor determina se o mecanismo do Identity Manager combina valores semelhantes de um gabarito de criação e uma operação adicionar ao executar essa operação. A definição do valor para Verdadeiro faz com que os valores de atributo multivalor do gabarito sejam usados, além dos valores para o mesmo atributo especificado na operação adicionar. A definição do valor para Falso faz com que os valores do gabarito sejam ignorados caso haja valores para o mesmo atributo especificado na operação Adicionar.
Permitir loopback de eventos do canal do editor para o canal do subscritor	Esse valor determina se o mecanismo do Identity Manager permite que um evento faça um loop do canal do Editor do driver para o canal do Subscritor. A definição desse valor para Falso faz com que o mecanismo do Identity Manager não permita o loopback dos eventos. A definição desse valor para Verdadeiro faz com que o mecanismo do Identity Manager permita o loopback dos eventos do canal do Editor para o canal do Subscritor.

Opção	Descrição
Reverter para o comportamento do valor de participação calculado	Esse valor determina o método utilizado pelo mecanismo do Identity Manager ao realizar ações de leitura e pesquisa relacionadas à participação no grupo. A definição desse valor para Falso (a configuração padrão) faz com que o mecanismo do Identity Manager, ao ler ou pesquisar os atributos de Membro e de Membro do Grupo dos objetos Cofre de Identidade, devolva apenas os valores que são valores “estáticos”. Os valores estáticos são objetos que receberam participação no grupo por designação direta ao grupo, em vez de designação herdada através de um grupo aninhado. A definição desse valor para Verdadeiro faz com que o mecanismo do Identity Manager reverta para o método usado antes do Identity Manager 3.6. Nas versões anteriores à 3.6, a pesquisa do mecanismo do Identity Manager dos atributos Membro e Membro do Grupo recuperou todos os valores “calculados”. Os valores calculados incluem objetos que são 1) participação atribuída estaticamente ou então 2) participação atribuída dinamicamente em virtude dos cálculos de hierarquia de grupo aninhados usados pelo eDirectory. Uma pesquisa do atributo Membro do Grupo retorna todos os objetos que foram diretamente atribuídos ao grupo ou aos quais a participação foi atribuída por um grupo aninhado.
Tempo máximo para esperar o desligamento do driver em segundos	Esta configuração controla o tempo máximo que o mecanismo do Identity Manager aguarda pelo encerramento do canal do Editor do driver. Se o driver não for encerrado dentro do intervalo de tempo especificado, o mecanismo do Identity Manager encerrará o driver.
Meta-caracteres de escape de expressão regular	Este controle determina os meta-caracteres que serão escapados enquanto expandem a variável local quando usados em um contexto de expressão regular. Todos os caracteres que precisam ser escapados devem ser adicionados como uma lista separada por vírgula para este valor de controle. Se um metacaractere não estiver presente no valor de controle, ele não será escapado durante a expansão da variável local contendo uma expressão regular. Ao usar esse controle, verifique o seguinte: ◆ Que o valor não é deixado vazio. Por padrão, ele é preenchido com ***$***. Esse caractere é necessário para a expansão de uma variável local. ◆ O valor deverá ser uma lista válida separada por vírgula (,), caso contrário, você encontrará erros durante a avaliação da política. ◆ Para escapar todos os metacaracteres, especifique "\,$,^,.,?,*,+,[,],(,),|" como um valor. ◆ Se um metacaractere não precisar ser escapado, remova esse caractere do valor. ◆ Para escapar qualquer meta-caractere, especifique o metacaractere seguido por uma barra invertida (\).

Opção	Descrição
Ignorar as mudanças de direitos de outros drivers	Este controle determina se o mecanismo do Identity Manager ignora ou processa mudanças de direitos de outros drivers. O valor padrão é Verdadeiro. Isso significa que o driver ignora automaticamente as mudanças de direitos de outros drivers. Se esse controle for definido como Falso, as mudanças de direitos de outros drivers serão armazenadas em cache e processadas por este driver.
Permitir loopback de evento de direito do CPRS para o canal do Subscritor	Este controle determina se o mecanismo do Identity Manager permite que um evento de direito gerado por uma designação CPRS faça loopback para o canal do Subscritor do driver. O valor padrão é Falso. Isso significa que o evento não faz loopback para o canal do Subscritor. Se esse controle for definido como Verdadeiro, o evento fluirá para o canal do Subscritor do driver.

Opções de inicialização

As Opções de inicialização permitem definir o estado do driver quando o servidor do Identity Manager é iniciado.

- **Início automático**: O driver é iniciado toda vez que o servidor do Identity Manager é iniciado.
- **Manual**: O driver não é iniciado quando o servidor do Identity Manager é iniciado. O driver precisa ser iniciado usando o portal Identity Console.
- **Desabilitado**: O driver tem um arquivo de cache que armazena todos os eventos. Quando o driver é definido como Desabilitado, esse arquivo é apagado e nenhum novo evento é armazenado no arquivo até que o estado do driver mude para Manual ou Início automático.

Depois de definir a sua opção de inicialização preferencial, clique no ícone  para gravar. Para redefinir a opção de inicialização, clique no ícone  .

Senha nomeada

O Identity Manager permite que você armazene com segurança várias senhas para um driver. Essa funcionalidade é referida como senhas nomeadas. Cada senha diferente é acessada por uma chave ou nome.

Você pode adicionar senhas nomeadas a um conjunto de drivers ou a drivers individuais. Senhas nomeadas para um conjunto de drivers estão disponíveis para todos os drivers no conjunto. Senhas nomeadas para um driver individual estão disponíveis apenas para esse driver.

Para usar uma senha nomeada em uma política de driver, você se refere a ela pelo nome da senha, em vez de usar a senha real, e o mecanismo do Identity Manager envia a senha para o driver. O método descrito nesta seção para armazenar e recuperar senhas nomeadas pode ser usado com qualquer driver, sem a necessidade mudanças no shim do driver.

Para adicionar uma nova senha nomeada, clique no ícone  . Para remover uma senha nomeada existente, clique no ícone  . Para gravar a sua lista, clique no ícone  .

Igualdade de segurança

Utilize a página Equivalente de Segurança para ver ou mudar a lista de objetos para os quais o driver tem um equivalente de segurança explícito. Esse objeto tem efetivamente todos os direitos dos objetos listados.

Você pode adicionar um novo objeto na lista de Igualdade de Segurança clicando no ícone +. Se você adicionar ou apagar um objeto nessa lista, o sistema automaticamente adicionará ou removerá esse objeto da propriedade “Segurança Equivalente a” desse objeto. Não é preciso adicionar o trustee [Público] ou os containers pai desse objeto à lista, porque esse objeto já tem uma equivalência de segurança implícita a eles.

Para remover um objeto existente dessa lista, clique no ícone  . Para gravar a sua lista, clique no ícone  .

Objetos excluídos

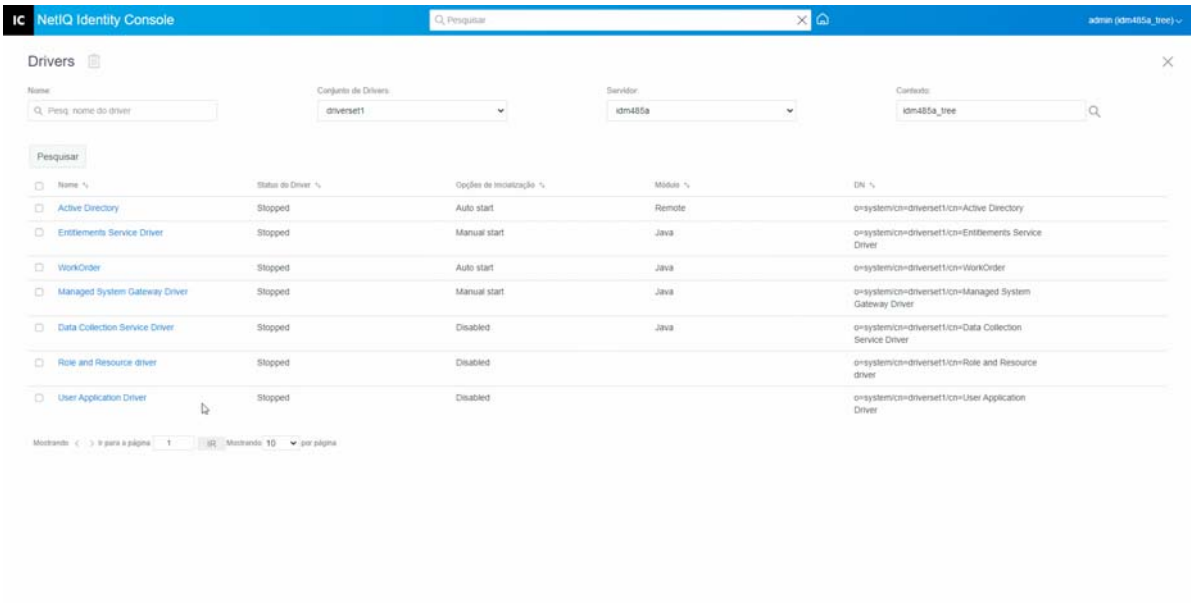
Use essa opção para criar uma lista de objetos que não serão replicados no aplicativo. Recomendamos adicionar nesta lista todos os objetos que representam uma função administrativa (por exemplo, o objeto Admin). Você pode adicionar um novo objeto nessa lista clicando no ícone +. Para remover um objeto existente dessa lista, clique no ícone  . Para gravar a sua lista, clique no ícone  .

Gerenciando a lista de atributos avaliados

Para adicionar atributos à lista de atributos avaliados para um driver específico, execute as seguintes etapas:

1. No Identity Console, selecione o módulo **Gerenciamento de Objetos**.
2. Selecione o tipo **Dir-XML-Driver** na lista suspensa e clique no botão Pesquisar.
3. Clique no driver apropriado na lista de pesquisa.
4. Para adicionar atributos não avaliados à lista de atributos, clique no ícone + ao lado dos **Atributos Avaliados** e selecione os atributos não avaliados na lista.
5. Depois de concluir o procedimento, clique em **OK**.

Figura 23-2 *Gerenciando a configuração de drivers*



Transformação e sincronização de dados

Esta seção se divide nas seguintes categorias:

- “Exibição de sincronização de dados” na página 164
- “Filtros de atributo de classe” na página 167
- “Script ECMA” na página 168
- “Mapeamento de atributo recíproco” na página 168

Exibição de sincronização de dados

A página visão geral do driver é dividida nas seguintes categorias:

- “Filtro” na página 165
- “Todas as políticas” na página 165
- “Migrar dados para o cofre de identidade” na página 165
- “Migrar dados do cofre de identidade” na página 166
- “Sincronizar objetos” na página 166
- “Rastreando scripts DirXML” na página 166

Filtro

Os filtros existentes no driver permitem que você especifique quais classes e atributos um aplicativo pode enviar e receber do Cofre de Identidade. Se você quiser que uma classe específica seja passada para o mecanismo de metadiretório para ser processada, deverá adicionar a classe ao filtro no canal apropriado. Você também pode filtrar objetos por um valor de atributo específico que você define.

Para adicionar classes e atributos que você deseja que sejam incluídos para sincronização e modificar o filtro do driver, clique em **Filtrar** no canal do Editor ou do Subscritor.

Observação: A representação gráfica da Visão Geral mostra dois objetos separados para o filtro do driver nos canais do Editor e do Subscritor. Embora existam dois objetos mostrados, o mesmo filtro é usado para ambos os canais.

Todas as políticas

Por padrão, a página Todas as políticas é exibida. Você pode importar uma política existente no container clicando no ícone  . Você também pode remover qualquer política que não seja necessária. Para selecionar um nível de rastreamento para o driver, clique no ícone  . Você pode mover as políticas para cima e para baixo na lista usando os ícones  e  .

Observação: A adição e a implantação de novas políticas para drivers não são suportadas pelo Identity Console. Recomendamos que você use iManager e Identity Designer para adicionar e implantar novas políticas.

Migrar dados para o cofre de identidade

Ao utilizar essa tarefa, você pode definir os critérios que o Identity Manager usa para migrar objetos de um aplicativo para o cofre de identidade. Quando você migra um objeto, o mecanismo de metadiretório aplica todas as políticas de Correspondência, Colocação e Criação, bem como o filtro Editor, ao objeto. Os objetos são migrados para o cofre de identidade usando a ordem especificada na lista Classe. Você pode executar as seguintes tarefas usando essa opção:

1. **Adicionar classe e atributos**: Para adicionar ou remover classes e atributos que você deseja migrar, clique no ícone  . Em seguida, selecione a classe e os respectivos atributos que você deseja adicionar. Depois de selecionar a classe e os atributos, clique em **Adicionar** para gravar as suas mudanças.
2. **Editar valor do atributo**: Para mudar o valor do atributo de migração especificado ao editar a lista, clique no ícone de Editar Atributo.
3. **Reordenar a lista de classes**: Use os botões e para mudar a ordem das classes na lista. Os objetos são migrados para o cofre de identidade usando a ordem especificada na lista Classe.
4. **Atualizar:** Clique no ícone  para atualizar a lista.

Migrar dados do cofre de identidade

Ao utilizar a guia **Exportar**, você pode selecionar containers ou objetos que deseja migrar do cofre de identidade para um aplicativo. Quando você migra um objeto, o mecanismo de metadiretório aplica todas as políticas de Correspondência, Criação e Colocação, bem como o filtro do Subscritor, ao objeto.

Para migrar objetos ou containers do Cofre de Identidade para outro aplicativo, clique no ícone  . Procure o objeto que você deseja migrar, selecione-o e clique em **OK** para adicionar o objeto à lista de migração. Para remover objetos da lista de migração, clique no ícone  .

Após terminar de selecionar os objetos que deseja migrar, clique em  para iniciar a migração. O progresso da migração será exibido na tela. Se quiser parar a migração, clique no botão  .

Sincronizar objetos

A operação de sincronização procura objetos que foram modificados e os sincroniza. Ou você pode selecionar **Examinar todos os objetos** para iniciar a sincronização imediatamente. Alternativamente, você pode definir uma data/hora para iniciar a sincronização.

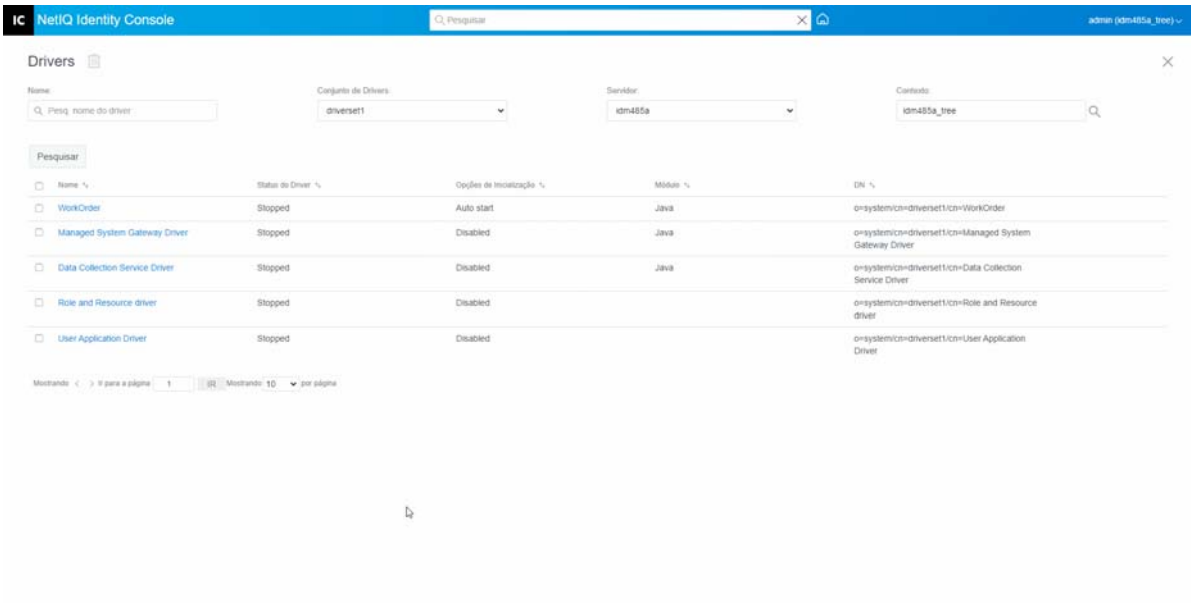
Rastreando scripts DirXML

A opção Rastreando scripts DirXML permite selecionar um nível de rastreamento para um driver. Ela também aplica configurações de rastreamento a todos os Canais do Editor e do Subscritor. As seguintes opções de rastreamento de script DirXML estão disponíveis para seleção:

- Todos os rastreamentos de script DirXML ligados
- Todos os rastreamentos de script DirXML desligados
- Rastreamento de regras de script DirXML ligado
- Rastreamento de regras de script DirXML desligado

Clique em  para gravar as mudanças.

Figura 23-3 *Gerenciando a sincronização de dados de drivers*



Filtros de atributo de classe

Os filtros de atributo de classe permitem que você especifique quais classes e atributos um aplicativo pode enviar e receber do cofre de identidade. Se você quiser que uma classe específica seja passada para o mecanismo de metadiretório para ser processada, você deverá adicionar a classe ao filtro no canal apropriado. Você também tem a capacidade de filtrar objetos por um valor de atributo específico que você define. Ao utilizar essa opção, você pode executar as seguintes ações:

- **Definir gabarito**: Use essa opção para definir as opções padrão para todos os atributos adicionados ao filtro. Clique no ícone ao lado do rótulo Filtro de Atributo de Classe.
- **Adicionar uma nova classe**: Adicione uma nova classe clicando no ícone .
- **Adicionar Um Novo Atributo**: Adicione um novo atributo clicando no ícone .
- **Copiar Filtro De**: Esta opção permite copiar um filtro de outro driver. Clique no ícone para copiar o filtro.
- **Editar XML**: Edite as configurações do filtro de classe e de atributo usando o ícone de Editar arquivo XML.
- **Apagar classe ou atributos**: Apague qualquer classe ou atributo clicando no ícone ao lado da respectiva classe ou atributo.

Você pode definir as seguintes opções para um valor de classe e atributo nos canais do Subscritor e do Editor:

- Sincronizar
- Ignorar

- Notificar
- Redefinir

Autoridade de fusão

Se um atributo não estiver sincronizado em nenhum dos canais, nenhuma mesclagem ocorrerá.

Se um atributo estiver sendo sincronizado em um canal e não no outro, então todos os valores existentes no destino desse canal serão removidos e substituídos pelos valores da origem desse canal. Se a origem tiver vários valores e o destino só puder acomodar um valor, apenas um dos valores será usado no lado do destino.

Se um atributo estiver sendo sincronizado em ambos os canais e ambos os lados puderem acomodar apenas um valor, o aplicativo conectado adquirirá os valores armazenados no cofre de identidade, a menos que não haja valor no cofre de identidade. Nesse cenário, o cofre de identidade adquire os valores do aplicativo conectado.

Se um atributo estiver sendo sincronizado em ambos os canais e apenas um lado puder acomodar vários valores, o valor do canal de valor único será adicionado ao canal multivalor se ele ainda não estiver lá. Se não houver valor no lado único, você poderá escolher o valor a ser adicionado ao lado único. Você pode definir as seguintes opções para a Autoridade de Fusão:

- Padrão
- Cofre de identidade
- Aplicativo
- Nenhum

Clique em  para gravar as mudanças.

Script ECMA

Exibe uma lista ordenada de arquivos de recursos ECMAScript. Os arquivos contêm as funções de extensão para o driver que o Identity Manager carrega no momento da inicialização do driver. Você pode importar arquivos adicionais clicando em  , remover arquivos existentes clicando em  ou mudar a ordem dos arquivos executados. Você também pode mover os scripts para cima e para baixo na lista. Você pode gravar a lista de scripts do ECMA clicando no ícone  .

Mapeamento de atributo recíproco

Mapeamentos de atributo recíproco permitem criar e gerenciar os backlinks ou as referências entre objetos. Por exemplo, o objeto Grupo inclui um atributo Membros que faz referência a todos os objetos Usuário que pertencem a esse grupo. Da mesma forma, cada objeto Usuário inclui um atributo Participação no Grupo que faz referência aos objetos Grupo dos quais esse usuário é um membro. Para que o mecanismo de metadiretório mantenha o Group object (objeto Grupo) > Members attribute synchronized with the User object (atributo Membros sincronizado com o objeto Usuário) > Group Membership attribute for all Group objects and User objects (atributo Participação

no Grupo para todos os objetos Grupo e objetos Usuário) no cofre de identidade, esses atributos precisam ser vinculados. Os links entre atributos de objeto são conhecidos como mapeamentos de atributo recíproco.

Ao utilizar esse módulo, você pode executar as seguintes ações:

Criando mapeamentos de atributo recíproco personalizados

Esta seção só se aplica se a página de mapeamento de atributo recíproco exibe o prompt **O driver não contém mapeamentos de atributo recíproco personalizados. Clique no ícone '+' acima para criar mapeamentos de atributo recíproco básicos**.

1. Clique no ícone + para criar uma nova lista de mapeamentos de atributos recíprocos personalizados.
2. Os mapeamentos de atributo padrão do driver são exibidos. Agora você pode adicionar mapeamentos, modificar os mapeamentos existentes ou apagar mapeamentos.

Adicionando um novo mapeamento de atributo recíproco

Quando você cria um mapeamento de atributo recíproco, você deve primeiro adicionar um dos atributos à lista de mapeamentos recíprocos.

1. Clique no ícone + ao lado do menu suspenso Ações.
2. Na nova entrada de atributo, selecione o atributo desejado na lista suspensa.
3. Especifique os detalhes do mapeamento recíproco:
   - 3a **Classe de origem**: Especifica o nome da classe à qual o atributo na lista de mapeamentos está associado. Por exemplo, se você tiver colocado o atributo Participação de grupo na lista de mapeamentos recíprocos, a Classe de origem associada será Usuário.
   - 3b **Classe de destino**: Especifica o nome da classe associado ao atributo para o qual você deseja criar um mapeamento recíproco. Por exemplo, se você tiver colocado o atributo Participação de grupo na lista de mapeamentos recíprocos, a Classe de destino associada será Grupo.
   - 3c **Atributo recíproco**: Especifica o nome do atributo para o qual você deseja criar um mapeamento recíproco.

4 Se você quiser mapear o atributo para outro atributo recíproco, clique no ícone  à direita do nome do atributo.

   Uma nova seção para o atributo é adicionada no final da lista de atributos. Selecione a classe de origem, a classe de destino e o atributo recíproco.

Removendo um mapeamento de atributo recíproco

Para remover um mapeamento de atributo recíproco:

1 Selecione a caixa de seleção para o mapeamento de atributo recíproco que você deseja apagar em frente à **Classe de origem**.

2 Clique no ícone  ao lado da lista suspensa de atributos.

Removendo um atributo da lista de mapeamentos recíprocos

Para remover um atributo da lista de mapeamentos recíprocos:

1 Selecione o atributo que você deseja remover selecionando a caixa de seleção na frente do atributo.

2 Clique no ícone  ao lado da lista suspensa **Ações**.

Reordenando atributos mapeados

Os mapeamentos de atributo são resolvidos na ordem listada, de cima para baixo. Você pode mover os atributos mapeados para cima ou para baixo na lista para garantir que eles sejam resolvidos na ordem correta. Em geral, você deve listar mapeamentos específicos primeiro, seguidos por mapeamentos mais gerais. Por exemplo, um mapeamento do atributo Membro em um objeto Grupo deve ser listado antes de um mapeamento para o atributo Membro em quaisquer objetos (a opção <Qualquer classe>).

Selecione a caixa de seleção na frente do atributo mapeado que você deseja mover e clique em  para mover o atributo para cima ou clique em  para movê-lo para baixo.

Removendo o mapeamento de atributo recíproco personalizados

Você pode apagar os mapeamentos de atributo personalizados que você criou. Isso resulta no mecanismo de metadiretório usando os mapeamentos de atributo padrão para o driver.

Para remover um mapeamento de atributo recíproco personalizado, clique no ícone  na parte superior da tela.

Edição de XML de atributo recíproco

Se desejar, você poderá editar diretamente o XML de um atributo recíproco. Para isso, clique no ícone  Editar XML na página de mapeamento de atributo recíproco personalizado. Isso abre um editor XML básico que permite modificar o XML. Quando terminar, clique em OK ou Cancelar para fechar o editor XML.

Configurações avançadas

As configurações avançadas são divididas nas seguintes categorias:

Gerenciando direitos

A página Direitos contém uma tabela que mostra todos os direitos definidos atualmente no driver selecionado (listado com o respectivo nome totalmente exclusivo). As seguintes ações são permitidas nesta página:

- **Editar em XML**: Para editar os direitos no arquivo XML, selecione o direito da lista e clique no ícone  . Em seguida, marque a caixa **Habilitar Edição de XML**.
- **Apagar**: Para apagar um direito, clique na caixa à esquerda do nome de direito e clique no ícone  . Você vê uma mensagem afirmando que a operação não pode ser desfeita e perguntando se você tem certeza de que deseja apagar o direito selecionado. Clique em **OK** para apagar o direito ou clique em **Cancelar** para parar a operação. Você pode clicar em várias caixas para apagar vários direitos ou clicar na caixa superior esquerda para apagar todos os direitos.

Gerenciando uma tabela de mapeamento de objetos

As políticas do Identity Manager usam tabelas de mapeamento para mapear um conjunto de valores para outro conjunto de valores correspondentes. Quando você instala o pacote de direitos, as políticas deste pacote são adicionadas ao conjunto de políticas de inicialização do driver. O driver executa essas apólices apenas uma vez quando o driver é iniciado. Para obter mais informações, consulte Objetos de tabela de mapeamento no *Guia de Administração de Driver do Identity Manager da NetIQ*.

Ao utilizar a Tabela de Mapeamento de Objetos, você pode executar as seguintes ações:

- **Modificar um mapeamento existente:** Para modificar uma tabela de mapeamento de objetos existente, clique no mapeamento na lista e execute as seguintes ações na próxima tela:
  - Adicione uma nova coluna.

    Especifique um valor para a coluna e selecione se o valor diferencia ou não maiúsculas e minúsculas ou se é numérico.
  - Adicione uma nova linha e especifique um valor para a linha.
  - Clique no ícone  .
- **Apagar mapeamento**: Para remover um mapeamento da lista, selecione o mapeamento apropriado da lista e clique no ícone  .
- **Editar no XML**: Para editar um mapeamento no arquivo XML, clique no mapeamento na lista e selecione o ícone  . Em seguida, marque a caixa **Habilitar Edição de XML**.

Gerenciando tarefas para drivers

O Identity Console permite que você programe eventos usando a opção Tarefas para todos os drivers individuais.

A página Programador de tarefas contém o nome da tarefa, se a tarefa está habilitada ou desabilitada, quando ela está programada para ser executada e a descrição da tarefa. Clique no nome da tarefa para ativar a página Tarefa. Clique no ícone habilitar/desabilitar na coluna Habilitado para habilitar ou desabilitar a tarefa. Clique na descrição da tarefa para ver a descrição completa da tarefa.

A guia Tarefas contém uma tabela que mostra os objetos tarefa existentes para o driver selecionado, que está listado com o seu Nome exclusivo na entrada do driver.

A página Programador de Tarefas permite que você execute as seguintes tarefas:

- **Criar a Tarefa**: Clique no ícone  para criar uma nova tarefa.

  No pop-up **Nova Tarefa**, para criar uma nova tarefa, realize as seguintes etapas:

  1. Especifique o nome da tarefa.
  2. Selecione o tipo da tarefa.
  3. Clique no ícone  e, na lista disponível de servidores, selecione o servidor no qual deseja executar a tarefa. Caso contrário, especifique um nome do servidor e selecione o servidor.
  4. Clique no botão **Criar**.
- **Iniciar a Tarefa**: Selecione uma tarefa clicando na caixa à esquerda da tarefa e clique no ícone .
- **Parar a Tarefa**: Selecione uma tarefa clicando na caixa à esquerda da tarefa e clique no ícone .
- **Habilitar a Tarefa**: Selecione uma tarefa clicando na caixa à esquerda da tarefa e clique no ícone .
- **Desabilitar a Tarefa**: Selecione uma tarefa clicando na caixa à esquerda da tarefa e clique no ícone .
- **Obter Status**: Selecione uma tarefa clicando na caixa à esquerda da tarefa e clique no ícone .
- **Apagar a Tarefa**: Selecione uma tarefa clicando na caixa à esquerda da tarefa e clique no ícone  .

Clique em uma tarefa para acessar a página **Job Property** (Propriedade da Tarefa). Aqui você pode configurar como você quer que a tarefa seja executada.

Geral: Mostra o nome da classe Java da tarefa. Use esta página para habilitar ou desabilitar a tarefa, apague-a após a execução dela, selecione o servidor ou servidores em que essa tarefa deve ser executada, especifique o servidor de e-mail e dê à tarefa um nome de exibição e uma descrição diferentes.

Programação: Permite definir quando executar a tarefa. Especifique Iniciar a tarefa em para definir o horário e se executar a tarefa diariamente, semanalmente, mensalmente, anualmente. Você também pode personalizar quando quer executar a tarefa ou pode optar por habilitar o botão de alternância para executar a tarefa manualmente.

Escopo: Permite que você defina os objetos aos quais essa tarefa se aplica. Um objeto pode ser um container, um grupo dinâmico, um grupo ou um objeto Folha. Clique em Adicionar para selecionar o objeto ao qual você deseja que essa tarefa se aplique. Use o botão Procurar para selecionar um objeto e, em seguida, clique em OK. Para remover um objeto da lista de escopo, selecione um objeto de escopo clicando na caixa à esquerda do objeto DN e clique em Remover.

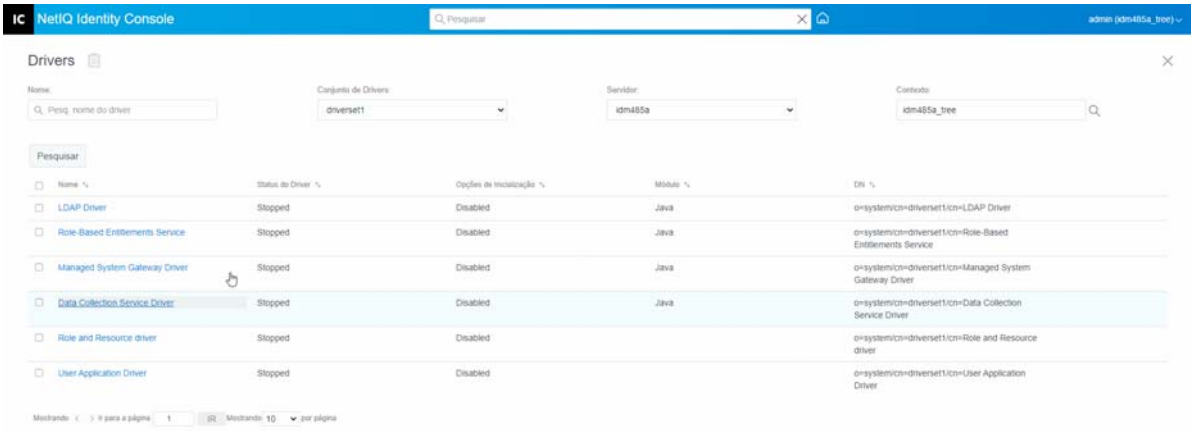
Quando um objeto for adicionado, selecione-o para exibir mais opções. Se você selecionar um objeto de grupo, terá a opção de aplicar a tarefa apenas aos membros do grupo ou apenas ao grupo. Se você selecionar um objeto Container, terá a opção de aplicar a tarefa a todos os descendentes no container, a todos os filhos no container ou apenas ao container.

Parâmetros: Permite adicionar parâmetros adicionais à tarefa e ver os parâmetros da forma como estão configurados atualmente. Esses parâmetros mudam, dependendo do tipo de tarefa selecionada.

Resultados: Permite definir o que você quer fazer com os resultados da tarefa. A página Resultados é dividida em duas partes: Resultado Intermediário e Resultado Final, com os seguintes resultados sendo permitidos: Sucesso, Aviso, Erro e Interrompido. À direita da coluna Resultados está a coluna Ação. Clicar na coluna Ação permite definir como você deseja receber notificações para cada resultado. As ações incluem o envio de um resultado de auditoria ou o envio de um e-mail quando o resultado for concluído. Se você não selecionar uma opção, nenhuma ação será tomada para o resultado.

Na guia **Rastrear**, você pode configurar o rastreamento de um driver específico. Para obter mais informações, consulte “Configurando o nível de rastreamento” na página 175

Figura 23-4 *Gerenciando configurações avançadas*



Configurando os níveis de registro e rastreamento dos drivers

Para configurar o registro e o rastreamento para os seus drivers, selecione a guia **Drivers** > **Configuração de Registro e Rastreamento** na página principal do Identity Console. Esta seção se divide nas seguintes categorias:

Configurando o nível de registro

Cada driver tem um campo de nível de registro, no qual você pode definir o nível de erros que devem ser rastreados. O nível indicado aqui determina quais mensagens estão disponíveis para os registros. Por padrão, o nível de registro é definido para monitorar mensagens de erro. (Isso também inclui mensagens fatais.) Para monitorar tipos de mensagens adicionais, mude o nível de registro. Para configurar o nível de registro, selecione a guia **Configuração de Registro e Rastreamento** > **Nível de Registro**. A tabela a seguir descreve as configurações do nível de registro:

Opção	Descrição
Usar as configurações de registro do conjunto de drivers	Se isso for selecionado, o driver registrará eventos com base nas configurações de registro do objeto Conjunto de Drivers.
Desligue o registro para registros do Conjunto de Drivers, do Subscritor e do Editor	Desliga todo o registro para este driver no objeto Conjunto de Drivers, no canal do Subscritor e no canal do Editor.
Número máximo de entradas no registro (50-500)	Número de entradas no registro. O valor padrão é 50.

Níveis de registro	Os seguintes níveis de registro estão disponíveis para seleção:
	◆ **Erros de Registro**: Registra apenas erros
	◆ Erros e avisos de registro: Registra erros e avisos
	◆ **Eventos específicos de registro**: Registra os eventos selecionados. A seleção dessa opção permite a seguinte lista de eventos:
	  ◆ **Eventos do mecanismo de metadiretório**
	  ◆ **Eventos de status**
	  ◆ **Eventos de operação**
	  ◆ **Eventos de transformação**
	  ◆ **Eventos de aprovisionamento de credenciais**
	◆ **Apenas atualizar o horário do último registro**: Atualiza o horário do último registro.
	◆ **Registro desligado**: Desliga o registro para o driver.

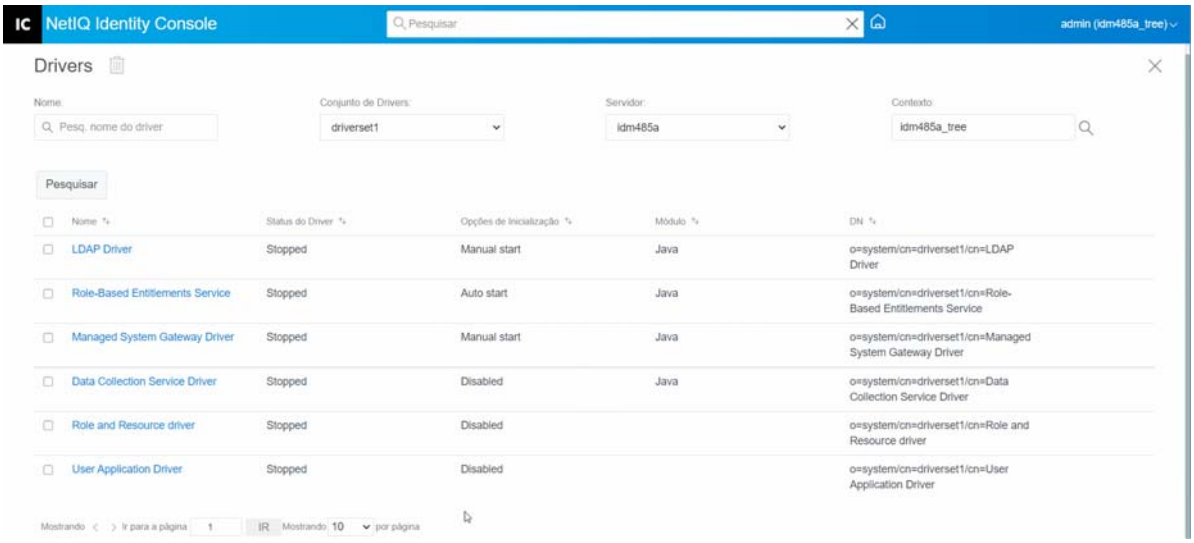
Configurando o nível de rastreamento

Você pode configurar o rastreamento para um driver específico. Dependendo do nível de rastreamento especificado para um driver, o rastreamento exibe eventos relacionados ao driver quando o mecanismo processa os eventos. O nível de rastreamento do driver afeta apenas o driver ou conjunto de drivers em que o rastreamento está definido. Se você estiver usando o Carregador Remoto, o arquivo de rastreamento do Carregador Remoto será definido diretamente no Carregador Remoto e conterá apenas o rastreamento de shim do driver.

Para configurar o rastreamento para um driver, selecione a guia **Configuração de registro e rastreamento** > **Rastreamento**. A tabela a seguir descreve as configurações de rastreamento:

Parâmetro	Driver
Nível de rastreamento	À medida que o nível de rastreamento do driver aumenta, o mesmo ocorre com a quantidade de informações exibidas no rastreamento. O nível de rastreamento um mostra erros, mas não a causa dos erros. Se você quiser ver informações de sincronização de senha, defina o nível de rastreamento para cinco. Se você selecionar **Usar a configuração do conjunto de drivers**, o valor será retirado do conjunto de drivers.
Arquivo de rastreamento	Especifique o nome do arquivo e a localização de onde as informações do Identity Manager estão escritas para o driver selecionado. Se você selecionar **Usar a configuração do conjunto de drivers**, o valor será retirado do conjunto de drivers.
Nome de rastreamento	As mensagens de rastreamento do driver são pré-gravadas com o valor inserido em vez do nome do driver. Use se o nome do driver for muito longo.
Codificação de arquivo de rastreamento	O arquivo de rastreamento usa a codificação padrão do sistema. Você poderá especificar outra codificação, se desejar.
Limite de tamanho do arquivo de rastreamento	Permite definir um limite para o arquivo de rastreamento Java. Se você definir o tamanho do arquivo como ilimitado, o tamanho do arquivo aumentará até que não haja mais espaço em disco. **Observação:** Se o limite de tamanho do arquivo for especificado, o arquivo de rastreamento será criado em vários arquivos. O Identity Manager divide automaticamente o tamanho máximo do arquivo em dez e cria dez arquivos separados. O tamanho combinado desses arquivos é igual ao tamanho máximo do arquivo de rastreamento. Se você selecionar **Usar a configuração do conjunto de drivers**, o valor será retirado do conjunto de drivers.

Figura 23-5 *Gerenciando os níveis de registro e rastreamento dos drivers*



Inspecionando drivers

Você pode usar o Inspetor de Driver para ver informações detalhadas sobre os objetos associados a um driver. Esta seção se divide nas seguintes categorias:

- “Inspetor de Driver” na página 176
- “Inspetor de cache de driver” na página 177
- “Inspetor de cache de sincronização fora de banda” na página 178
- “Declarações sobre o driver” na página 179
- “Monitorando a saúde do driver” na página 179

Inspetor de Driver

Para ver os objetos associados a um driver:

1. No Identity Console, selecione a guia **Drivers** > **Inspetor** > **Inspetor de Drivers**.
2. No campo **Driver**, especifique o nome totalmente exclusivo do driver que você deseja inspecionar ou clique no ícone de procura para procurar o driver desejado e selecioná-lo.
3. Depois de selecionar o driver a ser inspecionado, clique em **OK** para exibir a página Inspetor de Driver.

   A página exibe informações sobre os objetos associados ao driver selecionado. É possível executar qualquer uma das seguintes ações:

   - **Apagar:** Remove a associação entre o driver e um objeto. Selecione a caixa de seleção na frente do objeto que você não deseja mais que seja associado ao driver, clique no ícone e clique em **OK** para confirmar o apagamento.
   - **Atualizar:** Selecione o ícone de atualização para reler todos os objetos associados ao driver e atualizar as informações.

- **Mostrar:** Selecione o número de associações para exibir por página. Você pode selecionar um número predefinido (25, 50 ou 100) ou especificar outro número de sua escolha. O padrão é de 10 associações por página. Se houver mais associações do que o número exibido, você poderá usar os botões de seta para exibir as páginas de associações seguintes e anteriores.
- **Ações:** Realizar ações nos objetos associados ao driver. Clique em **Ações** e selecione uma das seguintes opções:
  - **Mostrar todas as associações:** Exibe todos os objetos associados ao driver.
  - **Filtro para associações desabilitadas:** Exibe todos os objetos associados ao driver que têm um estado Desabilitado.
  - **Filtrar associações manuais:** Exibe todos os objetos associados ao driver que têm um estado Manual.
  - **Filtrar associações de migração:** Exibe todos os objetos associados ao driver que têm um estado Migrar.
  - **Filtrar associações pendentes:** Exibe todos os objetos associados ao driver que têm um estado Pendente.
  - **Filtrar associações processadas:** Exibe todos os objetos associados ao driver que têm um estado Processado.
  - **Filtrar associações indefinidas:** Exibe todos os objetos associados ao driver que têm um estado Indefinido.
  - **Resumo da associação:** Exibe o estado de todos os objetos associados ao driver.
- **DN do objeto:** Exibe o DN dos objetos associados.
- **Estado:** Exibe o estado de associação do objeto.
- **ID de objeto:** Mostra o valor da associação.

Inspetor de cache de driver

Você pode ver as transações no arquivo de cache de um driver usando o Identity Console. O **Inspetor de cache de driver** exibe informações sobre o arquivo de cache, incluindo uma lista dos eventos a serem processados pelo driver.

1. No Identity Console, selecione a guia **Drivers** > **Inspetor** > **Inspetor de cache de driver**.
2. No campo **Driver**, especifique o nome exclusivo do driver cujo cache você deseja inspecionar ou clique no ícone de procura para procurar o driver desejado e selecioná-lo, então clique em **OK** para exibir a página Inspetor de cache de driver.

   O arquivo de cache de um driver só pode ser lido quando o driver não estiver em execução. Se o driver estiver parado, a página Inspetor de cache de driver exibirá o cache. Se o driver estiver em execução, a página exibirá a nota `O driver não está parado, o cache não pode ser lido` em vez das entradas de cache. Para parar o driver, clique no botão  , fazendo com que o cache seja lido e exibido.

   - **Cache do driver no servidor:** Lista o servidor que contém esta instância do arquivo de cache. Se o driver estiver sendo executado em vários servidores, você poderá selecionar outro servidor na lista para exibir o arquivo de cache do driver para esse servidor.
   - **Ícones de iniciar/parar driver:** Exibe o estado atual do driver e permite que você inicie ou pare o driver. O cache só pode ser lido enquanto o driver está parado.

- **Apagar:** Selecione entradas no cache e clique no ícone  para removê-las do arquivo de cache.
- **Ações:** Permite que você execute ações nas entradas no arquivo de cache. Clique em **Ações** para expandir o menu e selecione uma das seguintes opções:
  - **Limpar todos os eventos armazenados em cache:** Permite que você limpe todos os eventos em cache.
  - **Resumo do cache:** Resume todos os eventos armazenados no arquivo de cache.

Visualizando os Detalhes do Sistema Conectado para Drivers

Para visualizar os detalhes do sistema conectado para um driver específico, execute as seguintes ações:

1. No Identity Console, clique no módulo **Inspetor de Objetos**.
2. Procure o objeto Driver específico para o qual deseja exibir os sistemas conectados e selecione-o.
3. Todos os detalhes do sistema conectado para o objeto Driver selecionado serão exibidos no computador.

Inspetor de cache de sincronização fora de banda

Para ver eventos no cache de sincronização fora de banda:

1. No Identity Console, Selecione **Drivers** > **Inspetor** > guia **Inspetor do cache de sincronização fora de banda**.
2. No campo **Driver**, especifique o nome exclusivo do driver cujo cache você deseja inspecionar ou clique no ícone de procura para procurar o driver desejado e selecioná-lo, depois clique em **OK**.

   O arquivo de cache de um driver só pode ser lido quando o driver não estiver em execução. Se o driver estiver parado, a página Inspetor de cache de driver exibirá o cache. Se o driver estiver em execução, a página exibirá a nota `O driver não está parado, o cache não pode ser lido` em vez das entradas de cache. Para parar o driver, clique no botão  , fazendo com que o cache seja lido e exibido.
   - **Nome de arquivo de cache:** Exibe o nome de arquivo do cache.
   - **Cache do driver no servidor:** Lista o servidor que contém esta instância do arquivo de cache. Se o driver estiver sendo executado em vários servidores, você poderá selecionar outro servidor na lista para exibir o arquivo de cache do driver para esse servidor.
   - **Ícones de iniciar/parar driver:** Exibe o estado atual do driver e permite que você inicie ou pare o driver. O cache só pode ser lido enquanto o driver está parado.
   - **Apagar:** Selecione entradas no cache e clique no ícone  para removê-las do arquivo de cache.
   - **Ações:** Permite que você execute ações nas entradas no arquivo de cache. Clique em **Ações** para expandir o menu e selecione uma das seguintes opções:
     - **Resumo do cache:** Resume todos os eventos armazenados no arquivo de cache.
     - **Limpar todos os eventos armazenados em cache:** Permite que você limpe todos os eventos em cache.

Declarações sobre o driver

As declarações sobre o driver são como uma ficha do driver. Elas declaram o que o driver suporta e incluem algumas configurações. As declarações sobre o driver devem ser fornecidas pelo respectivo desenvolvedor. Um administrador de rede geralmente não precisa editar as declarações sobre o driver. Caso o administrador queira editar as declarações sobre o driver, poderá fazê-lo selecionando a opção **Drivers** > **Inspetor** > **Declarações sobre o driver** > **Habilitar edição de XML**.

Monitorando a saúde do driver

O monitoramento de saúde do driver permite que você veja o estado atual de saúde do driver como verde, amarelo ou vermelho, e defina as ações a serem desempenhadas em resposta a cada um desses estados de saúde.

Você cria as condições (critérios) que determinam cada um dos estados de saúde e define as ações a serem realizadas sempre que o estado de saúde do driver mudar. Por exemplo, se a saúde do driver mudar de um estado verde para um estado amarelo, você poderá realizar ações como reiniciar o driver, encerrar o driver e enviar um e-mail para a pessoa designada para resolver problemas relacionados ao driver.

Ao utilizar esse módulo, você pode executar as seguintes tarefas:

- “Modificando as Condições de Saúde do Driver” na página 179
- “Modificando as ações de saúde do driver” na página 182
- “Criando um Estado Personalizado” na página 183
- “Modificando um estado personalizado” na página 184

Modificando as Condições de Saúde do Driver

Você controla as condições que determinam cada estado de saúde. O estado verde destina-se a representar um driver íntegro, enquanto um estado vermelho pretende representar um driver não íntegro.

As condições para o estado verde são avaliadas primeiro. Se o driver não atender às condições verdes, as condições amarelas serão avaliadas. Se o driver não atender às condições amarelas, um estado de saúde vermelho será automaticamente atribuído ao driver.

Para modificar as condições de um estado:

1. No Identity Console, abra a página Configuração de saúde do driver para um driver cujas condições você deseja modificar:
   - **1a** Abra a home page do Identity Console.
   - **1b** Selecione **Drivers** > **Clique no driver apropriado na lista** > **Inspetor** > **Configuração de saúde do driver**.
2. Clique na guia para o estado (Verde ou Amarelo) que você deseja modificar.

   A guia apresenta as condições atuais para o estado de saúde. As condições são organizadas em grupos, e os operadores lógicos, sejam eles AND ou OR, são usados para combinar cada condição e cada grupo. Considere o seguinte exemplo para o estado verde:

```
GROUP1
Condition1 and
Condition2
Or
GROUP2
Condition1 and
Condition2 and
Condition3
```

No exemplo, um estado verde será atribuído ao driver se as condições de GRUPO1 ou as condições de GRUPO2 forem avaliadas como verdadeiras. Se nenhum dos dois grupos de condições for verdadeiro, então as condições para o estado amarelo serão avaliadas.

As condições que podem ser avaliadas são:

- **Estado do Driver:** Em execução, parado, iniciando, encerrando ou não executando. Por exemplo, uma das condições padrão para o estado de saúde verde é que o driver esteja em execução.
- **Driver em overflow de cache:** O estado do cache usado para conter transações de driver. Se o driver está em overflow de cache, todo o cache disponível foi usado. Por exemplo, a condição padrão para o estado de saúde verde é que a condição de Driver no Overflow de Cache é falsa e a condição padrão para o estado de saúde amarelo é que a condição de Driver no Overflow de Cache é verdadeira.
- **Mais Recente:** A idade da transação mais recente no cache.
- **Mais Antigo:** A idade da transação mais antiga no cache.
- **Tamanho total:** O tamanho do cache.
- **Tamanho não processado:** O tamanho de todas as transações não processadas no cache.
- **Transações não processadas:** O número de transações não processadas no cache. Você pode especificar todos os tipos de transações ou tipos de transações específicos (como adições, remoções ou renomeações).
- **Histórico de Transações:** O número de transações processadas em vários pontos do canal do Subscritor ou do Editor durante um determinado período de tempo. Essa condição usa vários elementos no seguinte formato:

  <*tipo de transação*> <*local e período de tempo da transação*> <*operador relacional*> <*número da transação*>.

  - <*tipo de transação*>: Especifica o tipo da transação que está sendo avaliada. Pode ser todas as transações, adiciona, remove, renomeia e assim por diante.
  - <*local e período de tempo da transação*>: Especifica o local no canal do Subscritor ou do Editor e o período de tempo que está sendo avaliado. Por exemplo, você pode avaliar o número total de transações processadas como eventos relatados pelo Editor nas últimas 48 horas. Por padrão, os dados do histórico de transações são mantidos por duas semanas, o que significa que você não pode especificar um período de tempo maior que duas semanas, a menos que você mude a configuração padrão de duração dos dados de transação.
  - <*operador relacional*>: Especifica que as transações identificadas devem ser iguais a, diferentes de, inferiores a, inferiores ou iguais a, maiores que ou maiores ou iguais ao <número de transações>.
  - <*número de transações*>: Especifica o número de transações que estão sendo utilizadas na avaliação.

A seguir, um exemplo de uma condição de Histórico de Transações é fornecido:

```
<número de adições> <como comandos do editor> <nos últimos 10
minutos> <é menor que> <1000>
```

- **Histórico Disponível:** A quantidade de dados do histórico de transações que está disponível para avaliação. O objetivo principal para essa condição é garantir que uma condição de Histórico de Transações não faça com que o estado atual falhe porque não tem dados suficientes de histórico de transações coletados para o período de tempo que está sendo avaliado.

  Por exemplo, suponha que você deseja usar a condição de Histórico de Transações para avaliar o número de adições como comandos do editor nas últimas 48 horas (o exemplo mostrado na seção Histórico de Transações acima). No entanto, você não quer que a condição falhe se ainda não houver o equivalente a 48 horas de dados, o que poderá ser o caso após a configuração inicial da saúde do driver ou se o servidor do driver for reiniciado (porque os dados do histórico de transações são mantidos na memória). Portanto, você cria grupos de condições semelhantes aos seguintes:

  ```
  Grupo1 Histórico Disponível <é menor que> <48 horas> ou Grupo2
  Histórico Disponível <é maior ou igual a> <48 horas> e Histórico de
  Transações <número de adições> <como comandos do editor> <nas
  últimas 48 horas> <é menor que> <1000>
  ```

  O estado é avaliado como verdadeiro se qualquer grupo de condições é verdadeiro, o que significa que a) há menos de 48 horas de dados ou b) há pelo menos 48 horas de dados e o número de adições como comandos do editor nas últimas 48 horas é inferior a 1000.

  O estado é avaliado como falso se ambas as condições são avaliadas como falsas, o que significa que a) há pelo menos 48 horas de dados e b) o número de adições como comandos de editor nas últimas 48 horas é superior a 1000.

3 Modifique os critérios da forma que desejar.

- Para adicionar um novo grupo, clique no ícone + ao lado dos **Grupos de Condição**.
- Para adicionar uma condição, clique no ícone + ao lado dos operadores lógicos (AND/OR). Alternativamente, você também pode clicar no link **Adicionar nova condição**.
- Para reordenar grupos de condições ou condições individuais, selecione a caixa de seleção ao lado do grupo ou condição que deseja mover e clique nos botões de seta para movê-lo para cima e para baixo. Você também pode usar os botões de seta para mover uma condição de um grupo para outro.

4 Quando concluir esse procedimento, grave as suas mudanças clicando no botão **Gravar**.

5 Se você quiser mudar as ações associadas às condições que você definiu, continue com "Modificando as ações de saúde do driver" na página 182.

Modificando as ações de saúde do driver

Você pode determinar as ações que deseja que sejam realizadas quando o estado de saúde do driver mudar. Por exemplo, se o estado mudar de verde para amarelo, você poderá encerrar ou reiniciar o driver, gerar um evento ou iniciar um workflow. Ou, se o estado mudar de amarelo para verde, quaisquer ações associadas ao estado verde serão realizadas.

As ações de um estado de saúde são realizadas apenas uma vez cada vez que as condições são atendidas; enquanto o estado permanecer verdadeiro, as ações não se repetirão. Se o estado mudar porque as respectivas condições não estão mais sendo atendidas, as ações serão executadas novamente na próxima vez que as condições forem atendidas.

1. No Identity Console, abra a página configuração de saúde do driver para um driver cujas ações você deseja modificar:
   1a. Abra a home page do Identity Console.
   1b. Selecione **Drivers** > **Clique no driver apropriado na lista** > **Inspetor** > **Configuração de saúde do driver**.
2. Clique na guia **Amarelo**, **Verde** ou **Vermelho** para o estado cujas ações você deseja modificar.
3. Clique no ícone mais (+) ao lado do título **Ações** para adicionar uma ação e selecione o tipo de ação desejada:
   - **Iniciar Driver:** Inicia o driver.
   - **Parar Driver:** Para o driver.
   - **Reiniciar driver:** Para e depois inicia o driver.
   - **Limpar o cache de driver:** Remove todas as transações, incluindo transações não processadas, do cache.
   - **Enviar E-mail:** Envia um e-mail para um ou mais destinatários. O gabarito que você deseja usar no corpo da mensagem do e-mail já deve existir. Para incluir o nome do driver, o nome do servidor e as informações atuais do estado de saúde no e-mail, adicione os tokens `$Driver$`, `$Server$` e `$HealthState$` ao gabarito de e-mail e, em seguida, inclua os tokens no texto da mensagem. Por exemplo:

     ```
     The current health state of the $Driver$ driver running on $Server$
     is $HealthState$.
     ```

     Importante: Para enviar e-mails para vários usuários, separe cada endereço de e-mail apenas com uma vírgula (,). Não use ponto-e-vírgula em vez de vírgula.
   - **Gravar mensagem de rastreamento:** Gravará uma mensagem para o arquivo de registro da tarefa de Saúde do Driver ou no arquivo de registro do conjunto de drivers se o arquivo de rastreamento não estiver configurado na tarefa de Saúde do Driver.
   - **Gerar evento:** Gera um evento que pode ser usado pelo Audit e pelo Sentinel.
   - **Executar o ECMAScript:** Executa um ECMAScript existente.

     Para obter informações sobre como construir scripts ECMA, consulte Usando o ECMAScript em Políticas em *NetIQ Identity Manager - Usando o Designer para criar políticas*.
   - **Iniciar o workflow:** Inicia um workflow de aprovisionamento.

- **Em caso de erro:** Se uma ação falhar, instruirá o que fazer com as demais ações, o estado de saúde atual e a tarefa de Saúde do Driver.
  - **Afetar ações por:** Você pode continuar a executar as ações restantes, parar a execução das ações restantes ou usar a configuração atual por padrão. A configuração atual só se aplicará se você tiver várias ações Em caso de erro e definir as ações Afetar por opção em uma das ações Em caso de erro anteriores.
  - **Afetar o estado por:** Você pode gravar o estado atual, rejeitar o estado atual ou padrão para a configuração atual. A gravação do estado faz com que as condições de estado continuem a ser avaliadas como verdadeiras. A rejeição do estado faz com que as condições de estado sejam avaliadas como falsas. A configuração atual só se aplicará se você tiver várias ações Em caso de erro e definir o estado Afetar por opção em uma das ações Em caso de erro anteriores.
  - **Afetar a tarefa de saúde do driver por:** Você pode continuar a executar a tarefa, interrompê-la e desabilitá-la ou usar a configuração atual por padrão. Se você continuar a executar a tarefa, isso fará com que ela termine de avaliar as condições para determinar o estado de saúde do driver e realize quaisquer ações associadas ao estado. Interromper e desabilitar a tarefa para a atividade atual dela a encerra; a tarefa não é executada novamente até você habilitá-la. A configuração atual só se aplicará se você tiver várias ações Em caso de erro e definir o estado Afetar Tarefa de Saúde do Driver por configuração em uma das ações Em caso de erro anteriores.

4 Quando concluir esse procedimento, grave as suas mudanças clicando no botão **Gravar**.

Criando um Estado Personalizado

Você pode criar um ou mais estados personalizados para realizar ações independentes do estado de saúde atual do driver (verde, amarelo, vermelho). Se as condições de um estado personalizado forem atendidas, suas ações serão realizadas independentemente do estado de saúde atual.

Assim como nos estados de saúde verde, amarelo e vermelho, as ações de um estado personalizado são realizadas apenas cada vez que as condições são atendidas; enquanto o estado permanecer verdadeiro, as ações não se repetirão. Se o estado mudar porque as respectivas condições não estão mais sendo atendidas, as ações serão executadas novamente na próxima vez que as condições forem atendidas.

1 No Identity Console, abra a página Configuração de saúde do driver para um driver para o qual você deseja criar um estado personalizado:

  1a Abra a home page do Identity Console.

  1b Selecione **Drivers** > **Clique no driver apropriado na lista** > **Inspetor** > **Configuração de saúde do driver**.

2 Clique no ícone + ao lado dos ícones de status de saúde do driver (verde, amarelo e vermelho)

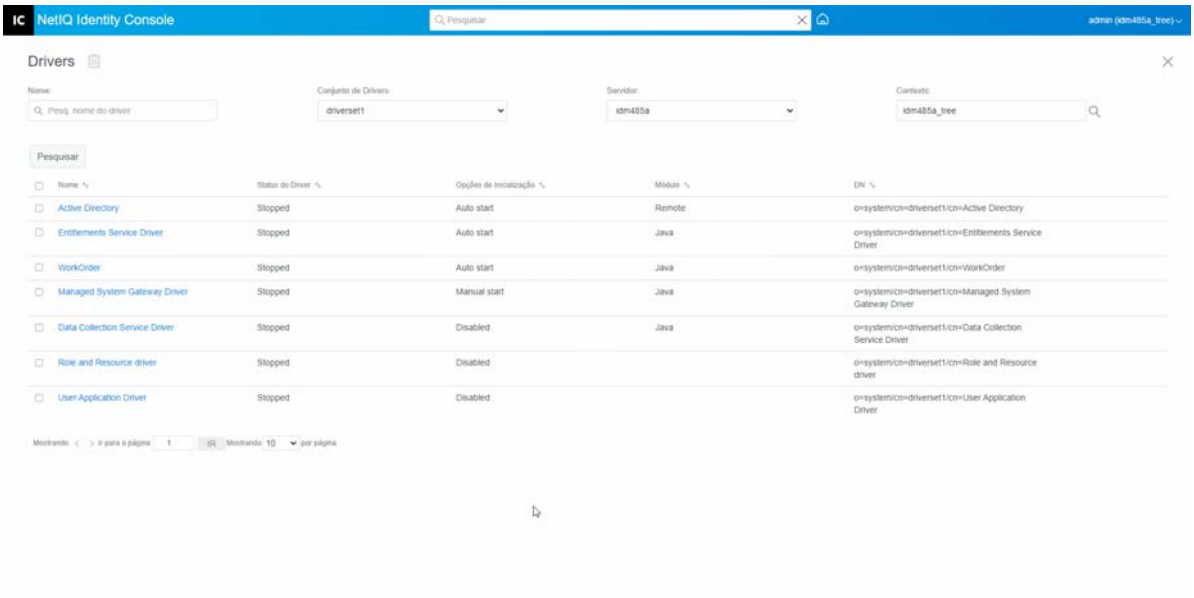
3 Siga as instruções em "Modificando as Condições de Saúde do Driver" na página 179 e "Modificando as ações de saúde do driver" na página 182 para definir as condições e ações do estado personalizado.

Modificando um estado personalizado

Para modificar estados personalizados, execute as seguintes etapas:

1. No Identity Console, abra a página Configuração de saúde do driver para um driver para o qual você deseja criar um estado personalizado:
   - **1a** Abra a home page do Identity Console.
   - **1b** Selecione **Drivers** > **Clique no driver apropriado na lista** > **Inspetor** > **Configuração de saúde do driver**.
2. Clique no ícone ao lado dos ícones de status de saúde do driver (verde, amarelo e vermelho)
3. Siga as instruções em "Modificando as Condições de Saúde do Driver" na página 179 e "Modificando as ações de saúde do driver" na página 182 para definir as condições e ações do estado personalizado.

Figura 23-6 *Gerenciando inspetores de drivers*



24 Gerenciando estatísticas do conjunto de drivers

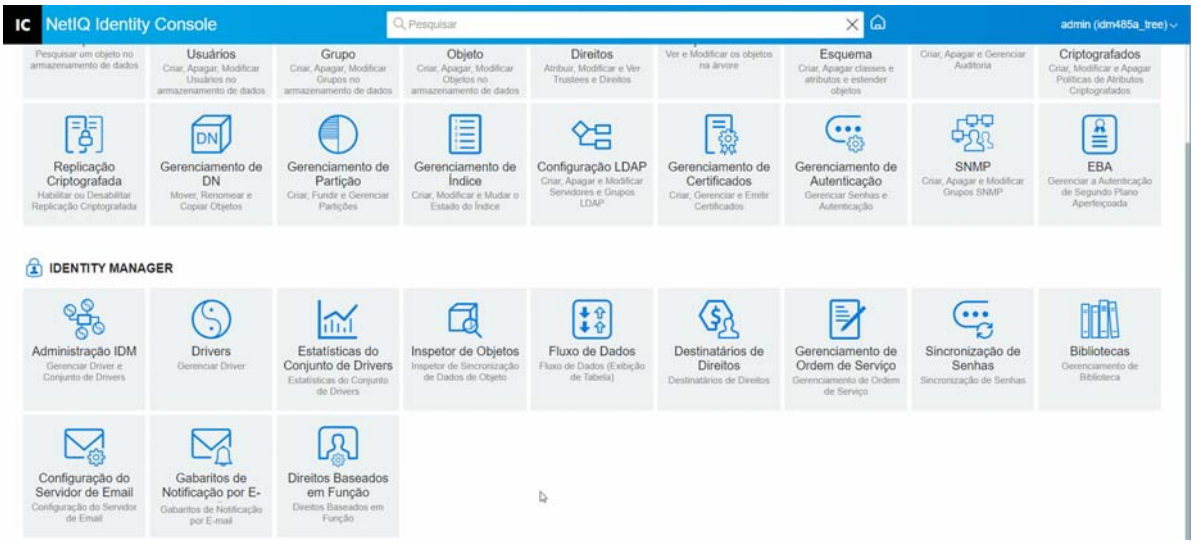
Você pode usar o portal Identity Console para ver uma variedade de estatísticas para um driver individual ou para um conjunto de drivers inteiro. Isso inclui estatísticas como o tamanho do arquivo de cache, o tamanho das transações não processadas no arquivo de cache, as transações mais antigas e mais recentes e o número total de transações não processadas por categoria (adicionar, remover, modificar e assim por diante). Para ver as estatísticas do conjunto de drivers:

1. No Identity Console, abra a página **Estatísticas do conjunto de drivers**.
2. Selecione o servidor apropriado na lista suspensa.

   É mostrada uma página que permite ver as estatísticas de todos os drivers contidos no conjunto de drivers.

   - Para atualizar as estatísticas, clique no ícone .
   - Para fechar as estatísticas de um driver, clique no botão no canto superior direito da janela de estatísticas do driver.
   - Para abrir as estatísticas para todos os drivers, clique em **Ações** > **Mostrar Tudo**.
   - Para recolher a lista de transações não processadas de um driver, clique no botão localizado acima da lista. Para recolher a lista de transações não processadas para todos os drivers, clique em **Ações** > **Recolher todas as transações**.
   - Para expandir a lista de transações, clique no botão . Para expandir a lista de transações não processadas para todos os drivers, clique em **Ações** > **Expandir todas as transações**.
   - Para fechar o painel de estatísticas de drivers desabilitados, clique em **Ações** e selecione **Fechar drivers desabilitados**.

Figura 24-1 *Gerenciando Estatísticas do Conjunto de Drivers*



25 Inspecionando objetos do Identity Manager

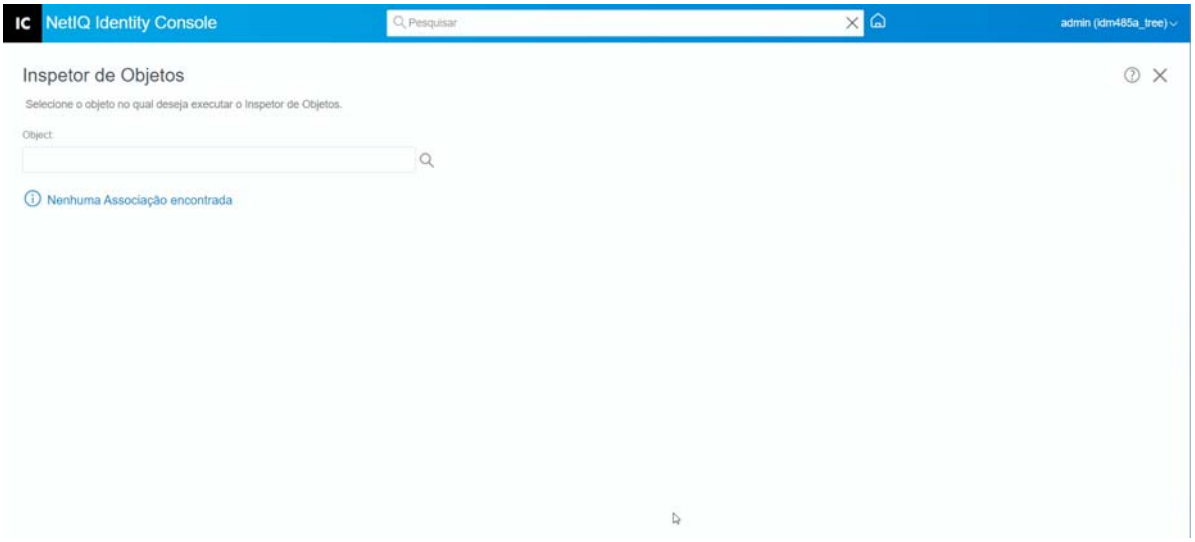
Você pode usar o Inspetor de Objetos para ver informações detalhadas sobre como um objeto participa das relações do Identity Manager. Essas relações incluem os sistemas conectados que estão associados ao objeto, o modo como os dados fluem entre o cofre de identidade e os sistemas conectados, os valores de atributo que estão atualmente armazenados no cofre de identidade e nos sistemas conectados, as configurações do driver do sistema conectado e assim por diante.

Para inspecionar os objetos do Identity Manager, clique na opção **Inspetor de Objetos** na página principal do Identity Console. Especifique o nome totalmente exclusivo do objeto que você deseja inspecionar ou clique no ícone de procura para procurar o objeto desejado e selecioná-lo.

A seção Sistemas Conectados lista cada um dos sistemas conectados com os quais o objeto está associado. Ao utilizar a página **Inspetor de Objetos**, você pode executar as seguintes ações:

- **Adicionando uma Associação**: Para adicionar uma nova associação com um sistema conectado, clique no ícone +. Pesquise pelo **Objeto Driver de Integração**, selecione-o e especifique o **ID de Objeto Associado**.
- **Apagando uma associação**: Para apagar uma associação com um sistema conectado, selecione a caixa de seleção à esquerda da associação e clique no ícone 🗑. Para apagar todas as associações, selecione a caixa de seleção abaixo da coluna Apagar e clique no ícone 🗑.

Figura 25-1 *Inspecionando Objetos do Identity Manager*



26 Gerenciando o fluxo de dados

O fluxo de dados ilustra os canais do Editor e do Subscritor para vários drivers em apenas uma exibição. Você pode ver e atualizar a propriedade de dados para todos os drivers que usam essa opção.

Para acessar a exibição de tabela do fluxo de dados, clique no módulo **Fluxo de Dados (Exibição de Tabela)** da página principal do Identity Console. Em seguida, procurar o container apropriado e selecione-o para exibir a lista dos drivers.

Para gerenciar a propriedade de dados de drivers individuais, execute as seguintes etapas:

1 Cada driver tem dois botões para gerenciar o fluxo de dados através dos canais do Editor e do Subscritor. O botão do lado esquerdo gerencia o fluxo de dados sobre o canal do Editor e o botão do lado direito gerencia o fluxo de dados sobre o canal do Subscritor.

   1a **Sincronizar**: Selecione essa opção para sincronizar o atributo específico. O ícone será mudado para ↑ no canal do editor e para ↓ no canal do subscritor após a seleção dessa opção.

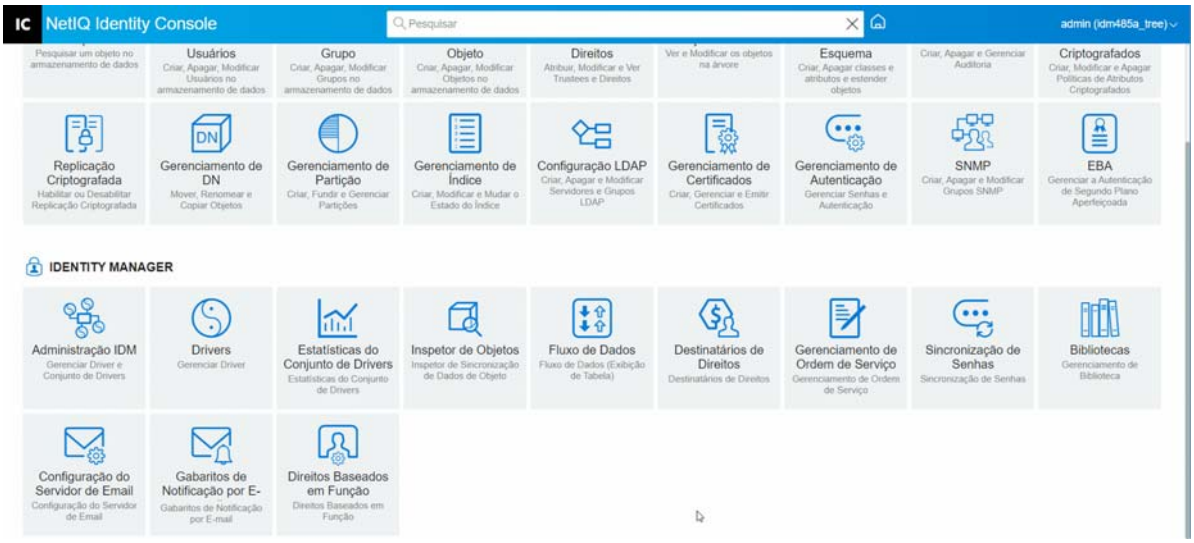
   1b **Ignorar**: Selecione essa opção para parar a sincronização do atributo específico. O ícone será mudado para ⊘ depois que essa opção for selecionada.

   1c **Notificar**: Selecione essa opção para receber notificações sobre mudanças feitas em um atributo específico. Mas a mudança não será sincronizada automaticamente. O ícone será mudado para 🔔 depois que essa opção for selecionada.

   1d **Redefinir**: Selecione essa opção para redefinir o valor do atributo para o valor especificado pelo outro canal. O ícone será mudado para ↻ depois que essa opção for selecionada.

   Observação: Você pode definir esse valor tanto no canal do Editor quanto no canal do Subscritor. Você não pode definir esse valor em ambos os canais simultaneamente.

Figura 26-1 *Gerenciando o Fluxo de Dados*



27 Gerenciando destinatários de direitos

As referências e os resultados de direitos são mantidos em objetos que tiveram um direito concedido a eles ou revogados deles. Referências e resultados de direitos contêm informações sobre se o direito está atualmente concedido ao objeto em questão ou revogado dele. Os destinatários de direitos são quaisquer objetos que contenham referências a um direito.

Referências de direitos

Para ver as referências e resultados de direitos, clique na opção **Destinatários de Direitos** na página principal do Identity Console e selecione Referência de Direito. Em seguida, preencha o nome totalmente exclusivo do objeto que é um `DirXML-EntitlementRecipient`. Você pode clicar no botão  de seletor de objetos para selecionar o objeto.

Resultados de direitos

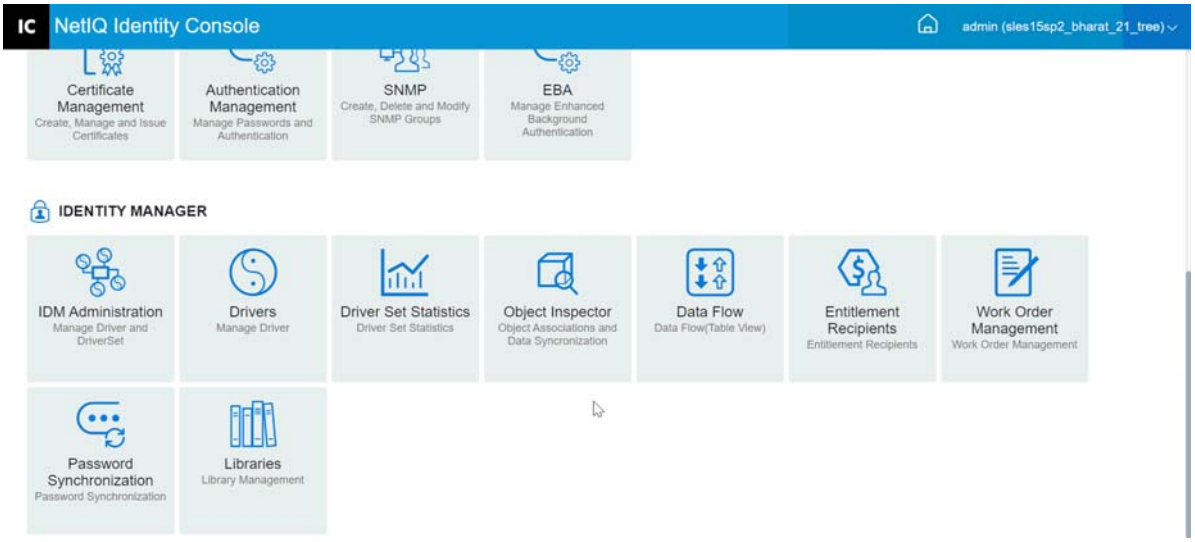
A tabela Resultados de Direito do Identity Console lista os resultados de direito associados ao objeto selecionado. Para visualizar o direito associado, selecione o DN de Direito. Para visualizar os resultados de direito no formato XML, selecione o ID de Resultado correspondente.

- **Títulos da Coluna Resultados de Direito**: Os títulos da coluna incluem o nome totalmente exclusivo do direito, o estado atual de ser concedido ou revogado, de onde os resultados vieram (fonte), o status do resultado, as mensagens que vieram com o resultado, a marcação de horário do resultado e a identificação do resultado.
  - **DN do Direito**: Clique no nome totalmente exclusivo do direito do objeto para ativar a página Modificar Objeto. Esta página permite que você visualize como os atributos do eDirectory foram atribuídos ao objeto. Você também pode usar esta página para modificar os atributos do objeto. O número de categorias mostradas na página Modificar Objeto depende do objeto selecionado.
  - **Estado**: Mostra se o direito foi concedido ou revogado. Se o plug-in encontrar qualquer outro valor no fluxo XML, ele exibirá esse valor diretamente.
  - **Mensagem**: Mensagens que o shim DirXML associou ao status dos resultados. As informações armazenadas na parte <msg></msg> do arquivo de resultados XML. Clique na entrada do ID dos Resultados para ver os detalhes completos do resultado em uma página do Visualizador XML.

- **Marcação de Horário**: o momento em que o mecanismo de direito processou e gravou o resultado. Clique na entrada do ID dos Resultados para ver os detalhes completos do resultado em uma página do Visualizador XML.
- **ID do Resultado**: Clique na entrada do ID do Resultado para ver os detalhes completos do resultado em uma página do Visualizador XML. Quando terminar de ver os resultados, clique em Fechar.

Para apagar uma entrada de resultados de direito, clique na caixa de seleção à esquerda da entrada de resultados de direito e selecione **Apagar**.

Figura 27-1 *Gerenciando destinatários de direitos*



28 Gerenciando ordens de serviço

Os drivers do Identity Manager podem criar ordens de serviço como resultado de eventos processados pelos drivers. Por exemplo, se você usar um driver de Recursos Humanos (SAP HR, PeopleSoft e assim por diante), poderá fazer com que o driver gere uma ordem de serviço sempre que um novo usuário for adicionado.

Você pode usar o Identity Console para criar e gerenciar ordens de serviço criadas para vários drivers que suportem essa funcionalidade específica.

Criando uma nova ordem de serviço

Para criar uma nova ordem de serviço, siga estas etapas:

1. Clique na opção **Ordem de Serviço** na landing page do Identity Console.
2. Clique no ícone + para criar uma nova ordem de serviço.
3. Especifique um nome para a ordem de serviço e clique em **OK**.

   O nome é usado para o nome do objeto Ordem de serviço no cofre de identidade.
4. Preencha os campos a seguir:

   Status: O status de uma nova ordem de serviço pode ser **Pendente** ou **Em Pausa**. Normalmente, o status da ordem de serviço é **Pendente**. Você pode parar uma ordem de serviço selecionando **Em Pausa**. Depois que uma ordem de serviço foi processada, o status resultante da ordem de serviço aparece neste campo.

   Data de Vencimento: Você pode optar por fazer com que o driver execute a ordem de serviço imediatamente ou programe-a. Para programar uma data de vencimento, clique no ícone do calendário. Use o calendário para escolher a data. Use as setas para selecionar o mês, o ano e a hora.

   Repetir ordem de serviço: Selecione essa opção para que a ordem de serviço seja processada várias vezes. Especifique o intervalo de tempo escolhendo o número de semanas, dias, horas ou minutos antes que a ordem de serviço seja repetida. A ordem de serviço para de repetir na data do apagamento, a menos que seja apagada ou editada manualmente, ou que o driver envie uma mensagem de erro.

   Data do apagamento: Use o controle do calendário para selecionar uma data para apagar ordens de trabalho configuradas. As ordens de serviço com um status de erro não são apagadas, a menos que você selecione **Apagar ordem de serviço mesmo que a ordem de serviço tenha um erro**.

Ordens de serviço dependentes: Quando você cria uma nova ordem de serviço, é possível torná-la dependente de uma ou mais ordens de serviço. Clique em  para procurar ordens de serviço dependentes e selecioná-las. Para remover uma ordem de serviço da lista, selecione-a e clique em  .

Tipo: Use este campo para especificar um tipo de ordem de serviço. O driver não muda esse atributo. O atributo é passado para o objeto WorkToDo quando a ordem de serviço é processada.

Número da ordem de serviço: Um número exclusivo de ordem de serviço. Esse valor pode ser atribuído por um sistema de ordem de serviço corporativo que não seja o NetIQ eDirectory, como um banco de dados de ordens de serviço.

Informações de contato: Informações de contato para o responsável pela ordem de serviço.

Registro de processamento de ordens de serviço: Após o processamento de uma ordem de serviço, o driver registra os resultados da ordem de serviço, incluindo o status, nesse campo. Isso permite verificar o status atual da ordem de serviço e identificar quaisquer problemas que o driver encontrou ao tentar configurá-la.

O atributo de status da ordem de serviço permanece pendente até que ela seja processada. A ordem de serviço será processada quando a data de vencimento tiver expirado. O driver informa os resultados do processamento definindo o atributo de status para Configuração, Aviso ou Erro. Se a ordem de serviço está Em Pausa, ela ignora a ordem de serviço.

- **Pendente:** O driver aguarda a data de vencimento para completar a ordem de serviço.
- **Configurado:** A ordem de serviço foi processada com sucesso.
- **Erro:** O driver não pôde cumprir a ordem de serviço.
- **Aviso:** Há um aviso sobre a ordem de serviço. Por exemplo, se a ordem de serviço tiver uma ordem de serviço dependente com uma data de vencimento posterior, o driver enviará um aviso.

Descrição: A descrição da ordem de serviço.

Conteúdo da ordem de serviço: Os dados nesse campo são usados pelas regras do driver para processar a ordem de serviço. Por exemplo, pode ser o XML que a transformação de comandos usa para processar a ordem de serviço.

Apagando uma ordem de serviço existente

Para apagar uma ordem de serviço existente, execute as seguintes etapas:

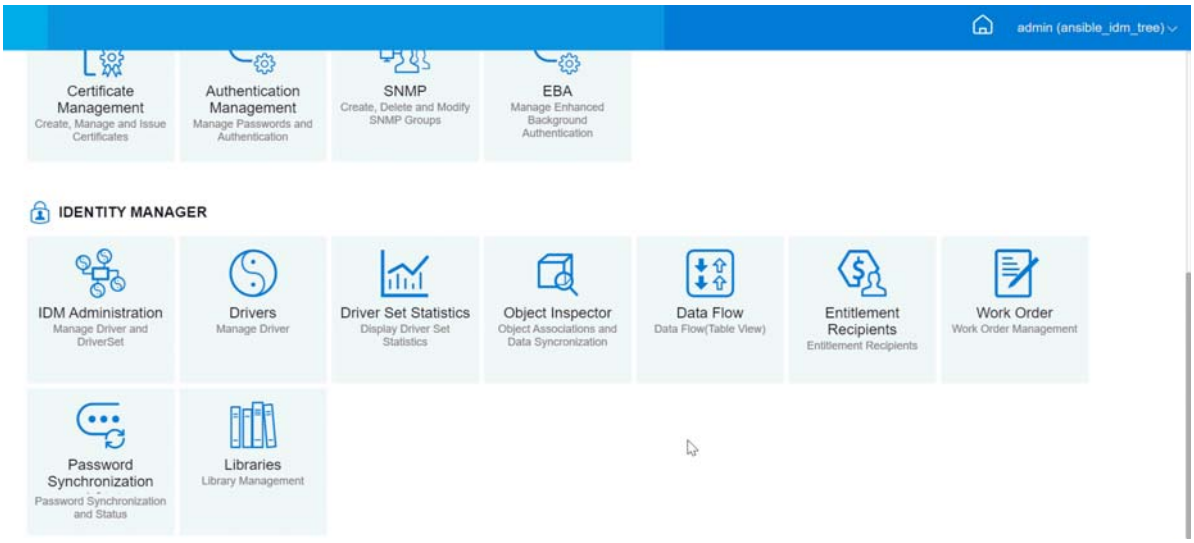
1. Clique na opção **Ordem de Serviço** na landing page do Identity Console.
2. Selecione a ordem de serviço que deseja apagar.
3. Clique no ícone  .

Filtrando a lista de ordens de serviço

Para filtrar a lista de ordens de serviço, execute as seguintes etapas:

1. Clique na opção **Ordem de Serviço** na landing page do Identity Console.
2. Clique em **Ações** em Gerenciamento de ordens de serviço.
3. No menu suspenso, selecione o tipo de filtro:
   - **Mostrar todos:** Todas as ordens de serviço associadas ao driver são listadas.
   - **Configurado:** Apenas as ordens de trabalho configuradas associadas ao driver são listadas.
   - **Erro:** Apenas ordens de serviço com status de erro são listadas.
   - **Em Pausa:** As ordens de serviço que foram colocadas manualmente em pausa são listadas.
   - **Pendente:** As ordens de trabalho que ainda não estão vencidas são listadas.

Figura 28-1 *Gerenciando Ordens de Serviço*



29 Gerenciando status e sincronização de senhas

Você pode verificar a sincronização de senhas e o status da senha de drivers individuais usando o portal Identity Console. Para verificar, selecione o módulo **Sincronização de Senhas** na página principal do Identity Console.

Você pode executar as seguintes ações usando esse módulo:

- "Verificando o status da sincronização de senhas" na página 197
- "Verificando as configurações de sincronização de senhas" na página 198

Verificando o status da sincronização de senhas

Você pode determinar se a senha de distribuição de um usuário específico é a mesma que a senha no sistema conectado. Execute as seguintes etapas para verificar o status da sincronização de senhas:

1. No Identity Console, selecione **Sincronização de senhas** > **Status de senha**.
2. Procure um usuário cujo status da senha você deseja verificar e selecione-o.
3. Os seguintes status de senha podem ser vistos:
   - As senhas estão sincronizadas.
   - As senhas NÃO estão sincronizadas.
   - O status da senha é desconhecido, pois o sistema conectado não pode ser contatado para solicitar uma verificação de senha.
   - Ocorreu um erro.

Observação: Para ver mais detalhes sobre cada um dos status acima, você deve passar o mouse sobre o status na coluna **Status da senha**.

A tarefa Status da senha faz com que o driver execute uma ação Verificar a senha do objeto. Nem todos os drivers suportam a verificação de senha. Aqueles que suportam precisam conter um recurso de verificação de senha nas declarações sobre o driver. O Identity Console não permite que as operações de verificação de senha sejam enviadas para drivers que não contenham esse recurso nas declarações.

A ação Verificar a senha do objeto verifica a senha de distribuição. Se a senha de distribuição não estiver sendo atualizada, a ação Verificar a senha do objeto poderá informar que as senhas não estão sincronizadas.

A senha de distribuição não será atualizada se qualquer uma das seguintes situações ocorrer:

- Você está usando o método de sincronização usando a senha do NDS para sincronizar ou usando a senha universal para sincronizar. Para obter mais informações, consulte "Criando uma política de senha com configurações personalizadas" na página 118.

Observação: A ação Status de senha verifica a senha do NDS em vez da senha universal para o cofre de identidade. Portanto, se a política de senha do usuário não especificar a sincronização da senha do NDS com a senha Universal, as senhas serão sempre relatadas como não sincronizadas. Na verdade, a senha de distribuição e a senha no sistema conectado podem estar em sincronia, mas o resultado da ação Verificar o Status da Senha não será preciso, a menos que a senha do NDS e a senha de distribuição estejam sincronizadas com a senha Universal.

Verificando as configurações de sincronização de senhas

A sincronização de senhas permite sincronizar senhas em sistemas conectados usando o Identity Manager. Para ver as configurações de sincronização de senhas para sistemas conectados, selecione o conjunto de drivers apropriado na lista suspensa.

Usando a sincronização de senhas, você pode configurar sistemas conectados para fazer o seguinte:

- Publicar senhas para o Identity Manager.
- Assinar senhas do Identity Manager ou de outros sistemas conectados.
- Assegurar o uso obrigatório de políticas de senha em sistemas conectados.
- Enviar e-mails de notificação.

Execute as seguintes etapas para verificar as configurações de sincronização de senhas:

1. No Identity Console, selecione **Sincronização de Senhas** > **Sincronização de Senhas** na página principal.
2. Selecione o conjunto de drivers que contém o driver cujas configurações você deseja verificar.
3. Clique no nome do driver da lista.

   Observação: As configurações habilitadas e desabilitadas variam, dependendo do driver. Apenas as configurações para recursos suportados pelo driver estão disponíveis.

   ---

4. Verifique se as configurações estão definidas corretamente.

   O Identity Manager aceita senhas (canal do editor): Se essa opção estiver habilitada, o Identity Manager permitirá que as senhas fluam do sistema conectado para o cofre de identidade. A desabilitação dessa opção significa que o fluxo de nenhum elemento <password> é permitido para o Identity Manager. Eles são retirados do XML por uma política de sincronização de senhas no canal do editor.

   Essa configuração se aplica às senhas de usuário fornecidas pelo próprio sistema conectado e aos valores de senha que são criados por uma política no canal do editor.

   Se essa opção estiver habilitada, mas a opção Senha de distribuição abaixo dela estiver desabilitada, um valor de <password> proveniente do sistema conectado será gravado diretamente na senha Universal no cofre de identidade. Se a política de senha do usuário não habilitar a Senha universal, a senha será gravada na senha do NDS.

Use a Senha de distribuição para a sincronização de senhas: Essa configuração só estará disponível se a configuração **O Identity Manager aceita senhas (canal do editor)** estiver habilitada.

Se essa opção estiver habilitada, um valor de senha proveniente do sistema conectado será gravado na Senha de distribuição. A Senha de Distribuição é reversível, o que significa que ela pode ser recuperada no armazenamento de dados do Identity Vault para sincronização de senhas. Ela é usada pelo Identity Manager para sincronização bidirecional de senhas com sistemas conectados. Para que o Identity Manager distribua senhas deste sistema para outros sistemas, essa opção precisa ser habilitada.

Aceite a senha somente se ela estiver em conformidade com a política de senha do usuário:

Essa configuração só estará disponível se a configuração **Usar senha de distribuição para sincronização de senhas** estiver habilitada.

Se essa opção for selecionada, o Identity Manager não gravará uma senha deste sistema conectado na senha de distribuição no cofre de identidade nem a publicará em sistemas conectados, a menos que a senha esteja em conformidade com a política de senha do usuário.

Se uma senha não estiver em conformidade, habilite a configuração **Redefinir a senha do usuário para a senha de distribuição** para redefinir a senha do usuário no sistema conectado. Isso permite que você assegure o uso obrigatório da política de senha no sistema conectado, bem como no cofre de identidade. Se você não selecionar essa opção, as senhas de usuário poderão ficar fora de sincronismo em sistemas conectados. No entanto, você precisa considerar as políticas de senha do sistema conectado ao decidir se deve usar essa opção. Alguns sistemas conectados podem não permitir a redefinição por não permitirem que você repita senhas.

Ao usar a configuração **Notificar o usuário sobre a falha de sincronização de senha por e-mail**, você pode informar os usuários quando há falha na definição ou redefinição de uma senha. A notificação é especialmente útil para essa opção. Se o usuário mudar para uma senha que é permitida pelo sistema conectado, mas rejeitada pelo Identity Manager por causa da política de senha, o usuário não saberá que a senha foi redefinida até que o usuário receba uma notificação ou tente efetuar login com a senha antiga no sistema conectado.

Sempre aceitar senha, ignorar políticas de senha: Essa configuração só estará disponível se a configuração **Usar senha de distribuição para sincronização de senhas** estiver habilitada.

Se você selecionar essa opção, o Identity Manager não assegurará o uso obrigatório da política de senha do usuário a este sistema conectado. O Identity Manager grava a senha deste sistema conectado na senha de distribuição no cofre de identidade e a distribui para outros sistemas conectados, independentemente da conformidade com a política de senha.

O aplicativo aceita senhas (Canal do Subscritor): Se você habilitar essa opção, o driver enviará senhas do cofre de identidade para este sistema conectado. Isso também significa que, se um usuário mudar a senha em um sistema conectado diferente que está publicando senhas para a senha de distribuição no cofre de identidade, a senha será mudada nesse sistema conectado.

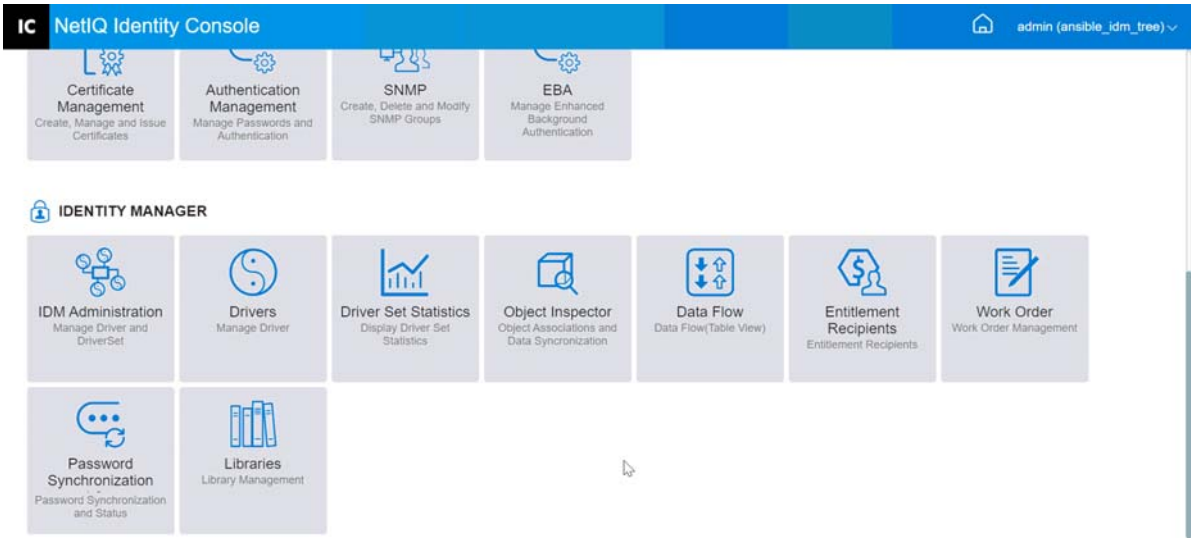
Por padrão, a senha de distribuição é a mesma que a senha universal no cofre de identidade, de modo que as mudanças na senha universal feitas no cofre de identidade também são enviadas para o sistema conectado.

Notificar o usuário da falha na sincronização de senhas por e-mail: Se você habilitar essa opção, o e-mail será enviado ao usuário se uma senha não for sincronizada, definida ou redefinida. O e-mail enviado ao usuário é baseado em um gabarito de e-mail. Esse gabarito é fornecido pelo aplicativo de sincronização de senhas. No entanto, para que o gabarito funcione,

você deve personalizá-lo e especificar um servidor de e-mail para enviar as mensagens de notificação. Para obter instruções, consulte Configuring E-Mail Notification (Configurando a notificação por e-mail) no *Guia de gerenciamento de senhas do NetIQ Identity Manager*.

5 Quando terminar, clique em **Gravar** para gravar as suas mudanças. As configurações são gravadas como valores de configuração globais.

Figura 29-1 *Gerenciando a sincronização de senhas*



30 Gerenciando bibliotecas

Os objetos biblioteca armazenam várias políticas e outros recursos que são compartilhados por um ou mais drivers. Um objeto biblioteca pode ser criado em um objeto conjunto de drivers ou em qualquer container do eDirectory. Várias bibliotecas podem existir em uma árvore do eDirectory. Os drivers podem se referir a qualquer biblioteca na árvore, desde que o servidor que esteja executando o driver mantenha uma réplica de Leitura/Gravação ou Master do objeto biblioteca.

Folhas de estilo, políticas, regras e outros objetos recurso podem ser armazenados em uma biblioteca e ser referenciados por um ou mais drivers.

Ao utilizar o módulo Gerenciamento de Bibliotecas, você pode executar as seguintes tarefas:

- "Visualizando e apagando uma biblioteca existente" na página 201
- "Visualizando e apagando objetos biblioteca" na página 201

Visualizando e apagando uma biblioteca existente

Para ver e apagar uma biblioteca existente, execute as seguintes etapas:

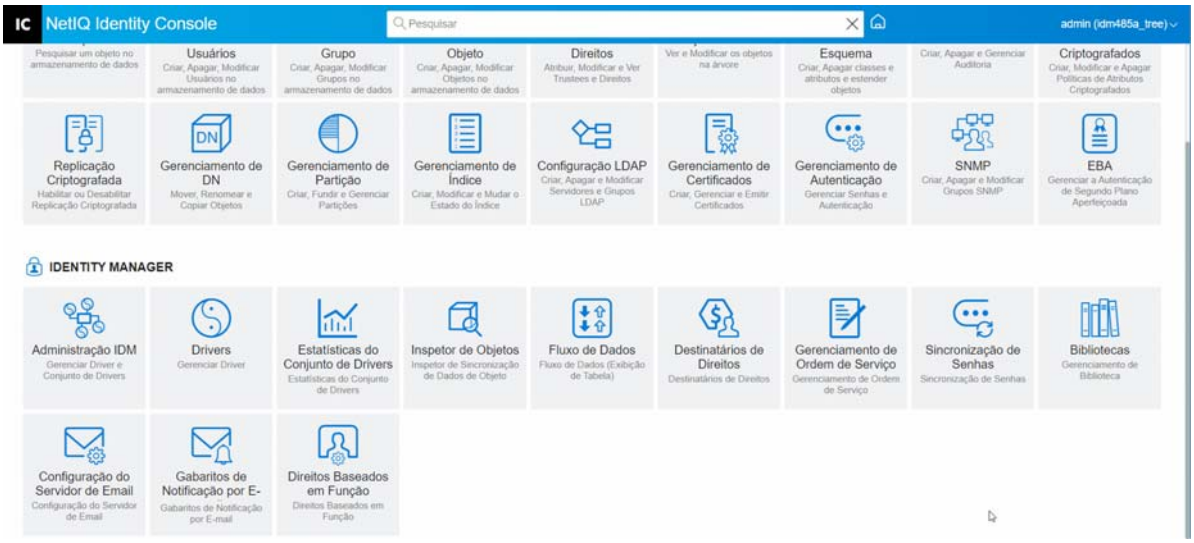
1. No Identity Console, selecione o módulo **Bibliotecas** na home page.
2. Selecione a biblioteca apropriada na lista.
3. Clique no ícone  . Clique em **OK** para confirmar.

Visualizando e apagando objetos biblioteca

Você pode ver e apagar políticas e mapear tabelas de objetos biblioteca. Para apagar objetos, execute as seguintes etapas:

1. No Identity Console, selecione o módulo **Bibliotecas** na home page.
2. Clique na biblioteca apropriada na lista.
3. Para apagar políticas, selecione a guia **Políticas**.
4. Selecione a política apropriada na lista e clique no ícone  .
5. Para apagar tabelas de mapeamento, selecione a guia **Tabelas de mapeamento**.
6. Selecione a tabela de mapeamento apropriada na lista e clique no ícone  .
7. Clique em **OK** para confirmar.

Figura 30-1 *Gerenciando Bibliotecas*



31 Gerenciando opções de servidor de e-mail

Você pode usar as Opções do Servidor de E-mail para especificar as configurações do servidor de e-mail SMTP.

Nome de Host

O nome de host do servidor de e-mail SMTP. Também pode ser um endereço IP. Você também pode especificar uma porta personalizada seguida pelo nome de host ou endereço IP.

Importante: Use dois pontos (:) como um separador entre o nome do host ou endereço IP e a porta.

De

Você pode especificar um endereço de e-mail válido que é exibido como um campo do cabeçalho de e-mail.

Valor do tempo de espera

A opção de tempo de espera permite definir o limite de tempo (em segundos) para enviar e-mails de notificação.

Habilitar SSL

Você pode optar por habilitar a opção SSL, se necessário.

Autenticar no servidor usando credenciais

Use para um servidor SMTP seguro. Se o servidor exigir autenticação antes de enviar e-mails, especifique o nome do usuário e a senha aqui.

Apesar de as informações de autenticação serem especificadas aqui, você pode ainda precisar especificá-las separadamente para o aplicativo que está enviando e-mails de notificação.

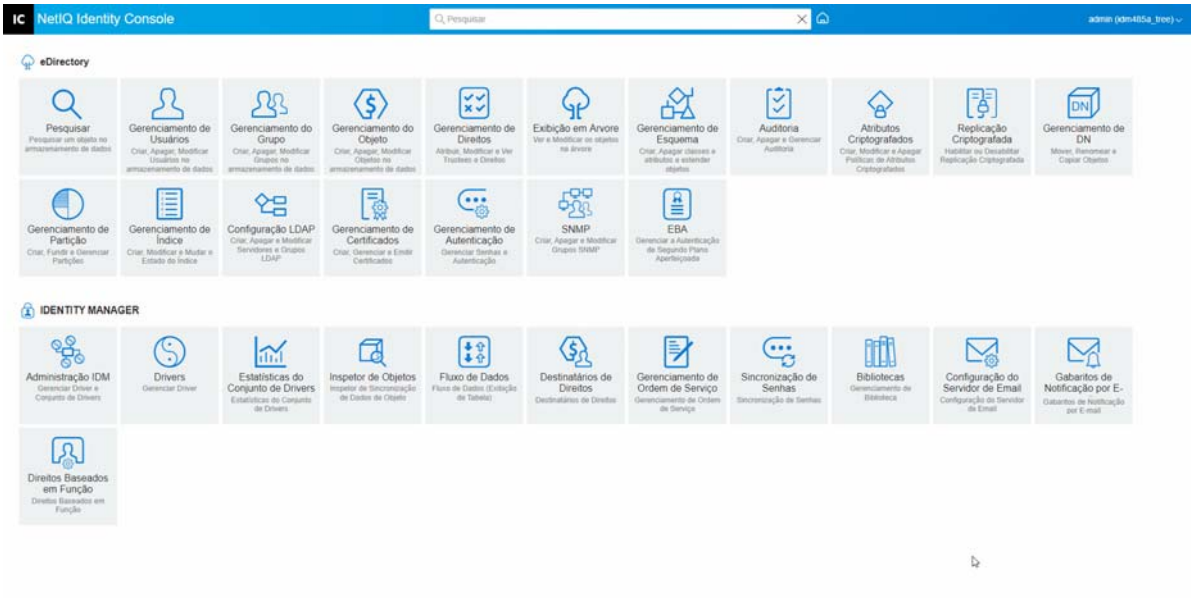
Por exemplo, você pode usar as informações de autenticação que você especifica aqui para enviar notificações de e-mail de Senha Esquecida. No entanto, a sincronização de senhas do Identity Manager usa a política de driver para enviar e-mails de notificação. Talvez você também precise fornecer as informações de autenticação nessa política de driver.

Para autenticar o servidor, execute as seguintes etapas:

1. Selecione a opção **Autenticar-se com o servidor usando credenciais**.
2. Especifique **Nome de Usuário** e **Senha**.
3. Clique em **Testar Conexão com o Servidor** para verificar a conectividade.
4. Clique em **Gravar**.

Observação: Depois de salvar os detalhes de credenciais, a opção **Testar a Conexão do Servidor** é desabilitada.

Figura 31-1 *Configuração do servidor de e-mail*



32 Gerenciando gabaritos de e-mail

Esta lista mostra os gabaritos de notificação disponíveis. Você usa esses gabaritos para enviar uma mensagem de e-mail aos usuários nesta árvore. Você pode personalizar esses gabaritos com seu próprio texto.

Alguns aplicativos fornecem gabaritos próprios. Esses objetos Gabarito estão localizados no container de Segurança, geralmente encontrado na raiz de sua árvore.

Você pode classificar a lista por nome, data ou assunto.

Assunto

O texto que um usuário visualiza no Título do assunto de um e-mail. Para editar um gabarito, clique no Título do assunto do gabarito. Usando a interface Editar Gabarito de Notificação por E-mail, você pode modificar o gabarito e seus detalhes.

Nome do Gabarito

Cada gabarito tem um nome único. O aplicativo que envia o e-mail faz referência a esse nome.

Modificado em

A data e o horário em que o gabarito foi modificado pela última vez.

Novo

Permite que você crie um novo gabarito de e-mail.

1. Clique no ícone +.
2. Especifique um nome para o novo gabarito (por exemplo, Aprovação) e clique em **OK**.

Se tiver desabilitado os pop-ups, você retornará ao pop-up Editar Gabarito de Notificação por E-mail. O nome do novo gabarito aparece na coluna Nome, mas [No Subject] ([Nenhum Assunto]) aparece na coluna Título do assunto. Neste caso, clique em [No Subject] ([Nenhum Assunto]) para que você possa fornecer detalhes no novo gabarito.

Editar Gabarito de Notificação por E-mail

A página Editar Gabarito de Notificação por E-mail permite modificar o gabarito de e-mail. Você pode personalizar o gabarito com seu próprio texto.

Nome do Gabarito

Exibe o nome do gabarito.

Assunto

O texto que um usuário visualiza no Título do assunto de um e-mail. Você pode mudar o texto da linha do assunto; o nome real do gabarito permanecerá o mesmo.

Enviar Como

O formato que o servidor SMTP usa para enviar o e-mail: Texto ou HTML.

Tokens ou tags de substituição

As tags de substituição ajudam você a personalizar a mensagem para o usuário. Você pode copiar tags de substituição da lista de tags disponíveis e colá-las na mensagem.

Cada gabarito inclui tokens ou tags de substituição padrão, que são variáveis necessárias para personalizar o e-mail para o usuário. Por exemplo, o gabarito de e-mail de Senha Esquecida para enviar uma senha ao usuário inclui o token ou a tag de substituição padrão chamada "CurrentPassword".

Adicionar: Você pode definir outros tokens ou tags de substituição para usar no corpo da mensagem.

Para adicionar um token ou tag de substituição, execute as seguintes etapas:

1. Clique no ícone  .
2. Especifique o **Nome** e a **Descrição** na janela **Adicionar Tag de Substituição**.
3. Clique em **Ok**.
4. O novo token ou tag de substituição são listados na coluna Tags de Substituição.

Copiar Tag: Clique em  para copiar a tag selecionada para o buffer do sistema e, em seguida, você pode clicar no mouse para colá-la e utilizá-la na linha de assunto ou no corpo da mensagem.

Apagar: Selecione um token ou tag de substituição na lista e clique em  para apagar a tag da lista. Não remova tags necessárias para o corpo da mensagem.

Corpo da mensagem

O texto da mensagem de e-mail.

Clique em **Atualizar** depois de especificar todas as modificações do gabarito de notificação por e-mail.

Apagar

Remove (Cofre de Identidade) gabaritos que você criou. Não é possível apagar gabaritos padrão que são enviados com aplicativos como o Identity Manager.

1. Selecione o gabarito que você deseja apagar.

   Se você clicar no Título do assunto do gabarito, o Identity Console fornecerá a caixa de diálogo Edit Email Templates (Editar Gabaritos de E-mail).
2. Clique no ícone Apagar.
3. Clique em **OK**.

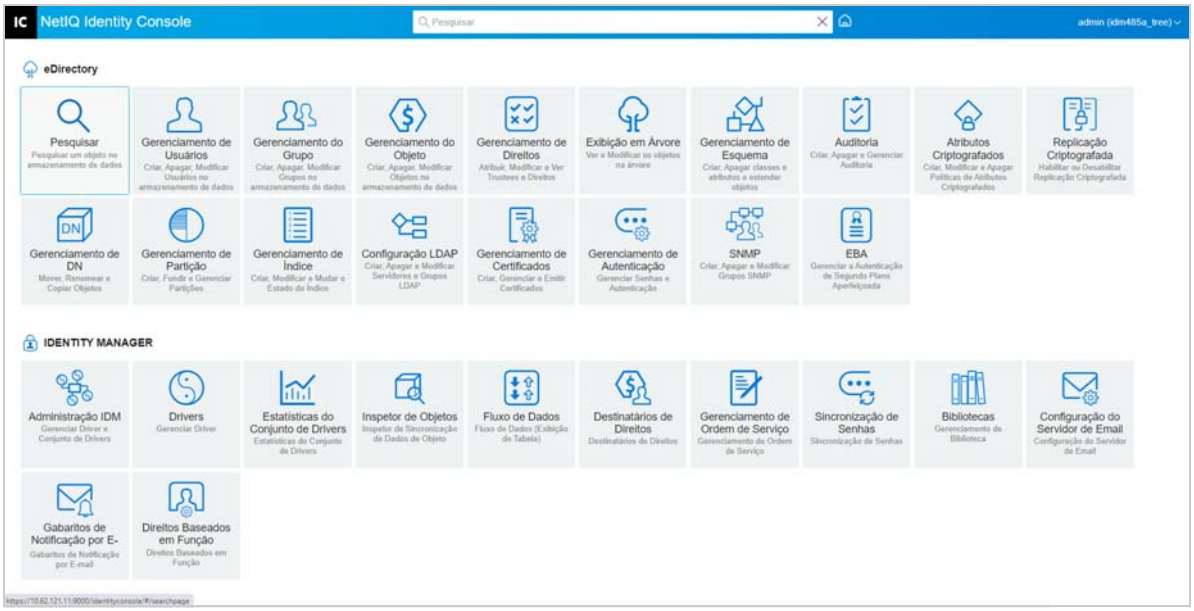
Gabaritos de Filtro

Permite filtrar qual gabarito de e-mail você deseja exibir. Apenas os gabaritos selecionados serão exibidos. A opção Filter by all (Filtrar por todos) exibe todos os gabaritos.

Atualizar Gabaritos

Clique no ícone para atualizar e remover quaisquer gabaritos de filtro aplicados.

Figura 32-1 *Gabaritos de notificação por e-mail*



33 Gerenciando direitos com base em função

O RBE permite que você conceda direitos em sistemas conectados a um grupo de usuários do NetIQ® Identity Console. Através de políticas de RBE, você pode simplificar a gestão das políticas comerciais e reduzir a necessidade de configurar seus drivers do Identity Manager.

O módulo Role-based Entitlement (Direito com base em função) tem o seguinte:

Role-based Entitlement (Direito com base em função)

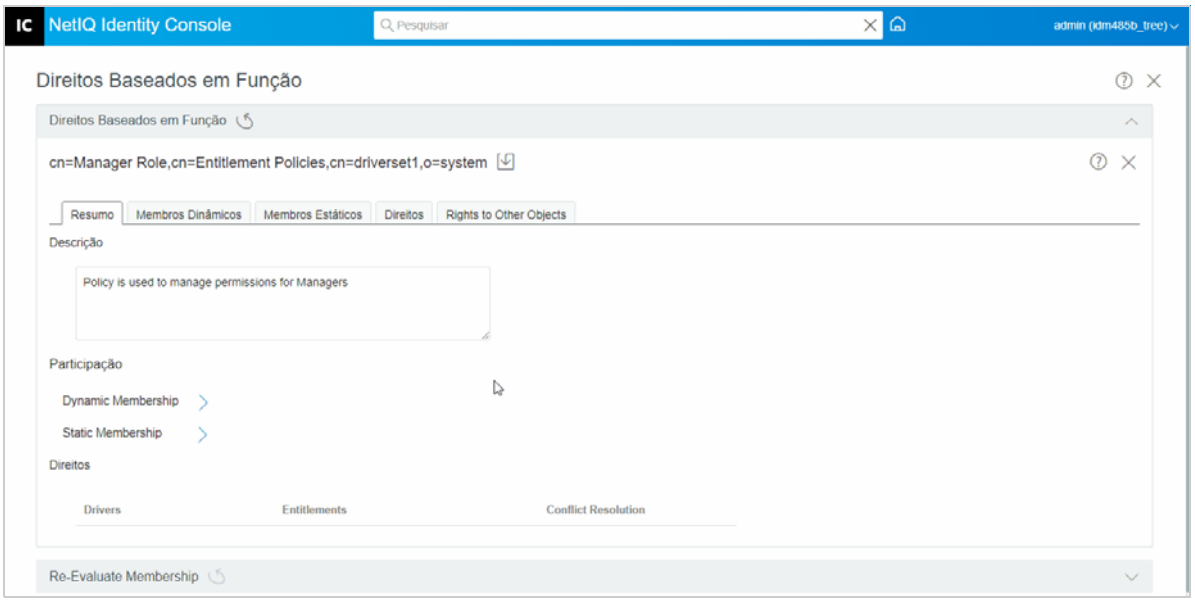
Uma política de RBE é um objeto de grupo dinâmico do Identity Console com recursos adicionais adicionados para permitir que você conceda RBEs em sistemas conectados. Quando você cria uma política de RBE, você define a participação na política e os direitos que devem ser concedidos aos membros da política de RBE. Cada política de RBE está associada a apenas um objeto Conjunto de Drivers atribuído a um servidor específico. Como um driver do Identity Manager, cada política de direitos pode gerenciar apenas objetos que estão em uma réplica master ou de leitura/gravação no servidor ao qual ela é atribuída.

As seguintes seções explicam em detalhes sobre o direito com base em função:

Resumo

Esta página resume uma exibição de alto nível dos critérios de participação e dos direitos para a política de direitos.

Figura 33-1 *Página de Resumo*



Participação:

Os critérios especificados para a participação dinâmica são exibidos na sintaxe de um filtro LDAP. A Identidade de Pesquisa indica quais direitos do objeto são usados na consulta para participação dinâmica, e o Escopo e o DN de Base indicam qual parte da árvore está incluída na consulta.

Você pode visualizar as inclusões e exclusões de participação estática marcando a caixa de seleção.

A lista combinada de todos os membros não é exibida na página Resumo porque a lista pode ser longa. Para ver uma lista combinada de todos os membros dinâmicos e estáticos da política de direitos, use a guia Membership > View Membership (Participação > Visualizar Participação).

Direitos:

Os direitos sobre sistemas conectados que são concedidos aos membros da política de direitos. Tenha em mente que há consistência imprecisa entre os direitos com base em função e os sistemas conectados. Isso significa que o status de um direito em um sistema conectado não é exibido na interface da política de direitos. Se você conceder um direito a uma política de direitos e, posteriormente, esse direito não estiver mais disponível no sistema conectado, o direito ainda estará listado na política de direitos até você o remover manualmente da lista.

Conflict Resolution (Resolução de Conflitos):

Para RBEs que têm valores, este método será usado para determinar quais valores serão concedidos a um usuário se duas ou mais políticas de RBE concederem valores diferentes a esse usuário. Um exemplo de direito que tem valores é a participação em listas de distribuição de e-mails, em que os valores são os nomes das listas de distribuição.

O método de resolução de conflitos é definido separadamente para cada direito individual em cada objeto driver. Se um direito for usado em múltiplas políticas de RBE, o método de resolução de conflitos será o mesmo em todas as políticas de RBE. Para alterar o método de resolução de conflitos para um direito, altere a configuração para esse direito nas declarações sobre o driver em questão.

- **Unrecognized** (Não reconhecido): A política de RBE não foi concluída no assistente ou a configuração foi digitada incorretamente nas declarações sobre o driver.
- **Merge** (Fundir): A configuração padrão é Merge (Fundir) (`union` nas declarações sobre o driver). Isso significa que um usuário recebe todos os valores para este direito de todas as políticas de RBE das quais é membro.

  Ao usar a configuração padrão Merge (Fundir), a ordem de prioridade da lista de políticas não é importante para este direito específico.

  Por exemplo, um usuário passa a participar de listas de distribuição de e-mails para o GroupWise® Driver A por duas políticas de RBE diferentes, a política Gerentes e a política Membros da Equipe. Na Política 1, o usuário passa a participar da lista de distribuição de e-mails intitulada Gerentes e, na Política 2, o usuário passa a participar da lista de distribuição de e-mails Membros da Equipe. Com uma configuração Merge (Fundir), o usuário passa a participar de ambas as listas de distribuição de e-mails.
- **Priority** (Prioridade): Esta configuração significa que, se várias políticas de RBE concederem a um usuário valores diferentes para o mesmo direito do mesmo objeto driver, o usuário receberá apenas os valores especificados na política de RBE que é a mais alta na lista.

  Ao utilizar a configuração Priority (Prioridade), a ordem de prioridade da lista de políticas é importante para este direito específico.

  Por exemplo, um usuário passa a participar de listas de distribuição de e-mails para o GroupWise Driver A por duas políticas de RBE diferentes, a política Gerentes e a política Membros da Equipe. Na política Gerentes, o usuário passa a participar da lista de distribuição de e-mails Gerentes e, na política de Membros da Equipe, o usuário passa a participar da lista de distribuição de e-mails de Membros da Equipe. A política Gerentes está listada mais alto na lista de políticas do que a política Membros da Equipe. Com uma configuração Priority (Prioridade), o usuário passa a participar apenas da lista de distribuição de e-mails dos gerentes.

  O uso da prioridade para resolução de conflitos poderá ser útil se, por exemplo, um atributo no sistema conectado permitir apenas um valor. Se duas políticas de RBE diferentes concederem um valor para esse atributo ao mesmo usuário, o usuário receberá o valor que é concedido pela política de RBE alta na lista.

Observação: Não está prevista nenhuma configuração de resolução de conflitos para direitos que não têm valores, como uma conta. Direitos que não têm valores são sempre concedidos aos membros da política de RBE, independentemente da prioridade das políticas na lista.

Membros Dinâmicos

Os critérios especificados para a participação dinâmica são exibidos na sintaxe de um filtro LDAP. A Identidade de Pesquisa indica quais direitos do objeto são usados na consulta para participação dinâmica, e o Escopo e o DN de Base indicam qual parte da árvore está incluída na consulta.

Filtro de participação

Você pode definir critérios para a participação, como localização na árvore e atributos do objeto. Por exemplo, a participação pode depender se o usuário está no container Ativo ou se o cargo inclui a palavra Gerente. Os usuários que atendem aos critérios especificados passam a fazer parte da política de RBE automaticamente, sem que você precise adicioná-los a ela. A participação dinâmica é o mesmo que um objeto Grupo Dinâmico.

Se um objeto mudar e deixar de atender aos critérios de participação dinâmica, os direitos serão automaticamente revogados na próxima vez que o usuário for reavaliado.

Definir parâmetros de pesquisa

Especifique a localização dos usuários que você deseja que a política de direitos gerencie. Escolha o container que contém os usuários (DN de Base) e o quanto você quer que a pesquisa se distancie do container (Escopo de Pesquisa). Para que a política de direitos gerencie os usuários nos containers especificados, os usuários precisam estar em uma réplica master ou de leitura/gravação no servidor.

As seguintes opções são fornecidas para Escopo de Pesquisa:

- Este container e os respectivos subcontainers: Os usuários abaixo deste container na árvore serão membros da política de direitos se atenderem aos critérios especificados para a participação dinâmica. Os usuários dentro de subcontainers também serão membros se atenderem aos critérios.
- Somente neste container: Os usuários dentro deste container serão membros da política de direitos somente se atenderem aos critérios especificados para a participação dinâmica. Os usuários dentro de subcontainers abaixo deste container não são membros, mesmo que atendam aos critérios.

Definir Critérios de Filtro

Especifique as características que determinam quais usuários são membros da política de direitos.

Na página Resumo para uma política de direitos, os critérios de participação dinâmica especificados são exibidos na sintaxe de um filtro LDAP.

Por padrão, a participação dinâmica está definida para incluir todos os objetos da classe Usuário (e objetos de classes derivadas da classe Usuário) dentro do escopo da pesquisa como membros da política de direitos.

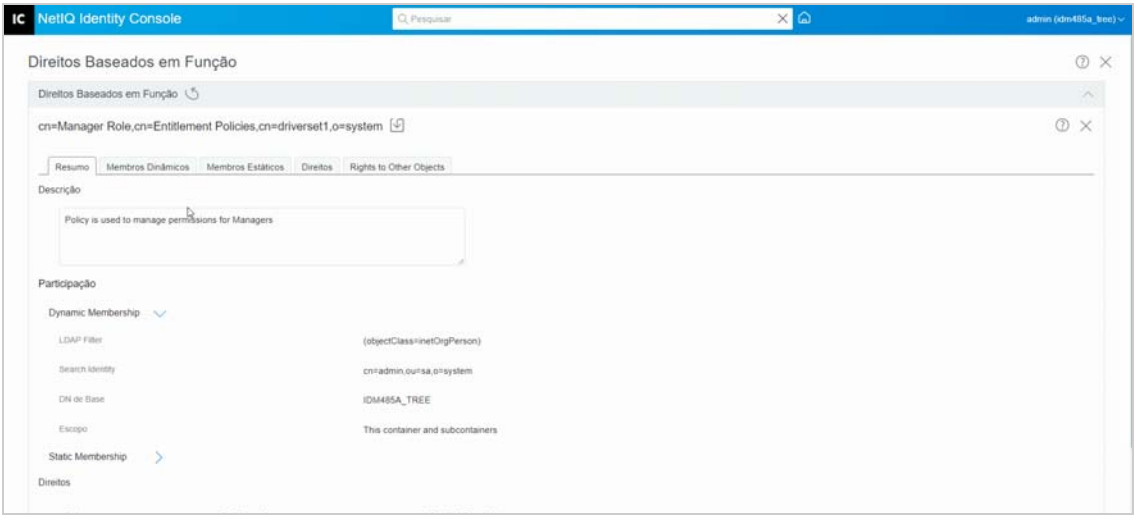
Observação: Se você criar uma nova classe de objeto derivada de Usuário, uma política de direitos existente não tomará conhecimento dessa classe até você fazer uma modificação na política de direitos. Isso impede a concessão acidental de direitos a usuários de uma nova classe. Quando qualquer modificação é feita na política de direitos, a lista de classes derivadas do usuário para essa política é atualizada.

Criando Participação Dinâmica

Na guia Membros Dinâmicos, execute o seguinte:

1. Clique na guia **Membros Dinâmicos**.
2. Use os filtros **Identidade da Pesquisa**, **Iniciar a Pesquisa em** e **Escopo da Pesquisa** conforme desejar.
3. Clique no **Criar Grupo** específico para criar uma nova condição ou uma linha e, em seguida, forneça os critérios ou condições de pesquisa necessários.

Figura 33-2 *Membros Dinâmicos*



Escopo da Pesquisa: O Escopo da Pesquisa indica o conjunto de entradas no DN ou abaixo do DN de base que podem ser consideradas possíveis correspondências para uma operação de pesquisa.

Critérios de Pesquisa: Você pode limitar uma pesquisa para facilitar a localização de um registro específico ou um grupo de registros dentre um grande número de registros.

DN de Base: O DN de Base é o ponto de onde um servidor vai pesquisar usuários.

Grupo LDAP: É uma organização hierárquica de Usuários, Grupos e Unidades Organizacionais que são containers para usuários e grupos.

Observação: O usuário pode criar grupos únicos ou múltiplos com condições. As condições consistem em atributos, operadores e valor. Por padrão, **Object Class** > **is equal** > **User** (Classe de Objeto > é igual a > Usuário) está preenchido.

Membros Estáticos

Membros Estáticos são a classe de membros declarados usando palavras-chave estáticas. Um membro estático tem certos acessos limitados.

Na guia Membros Estáticos, as seguintes operações podem ser realizadas:

Incluir Membros:

Adicione membros estaticamente que não estão incluídos pelo filtro de participação dinâmica.

Excluir Membros:

Exclua os membros que atendam aos critérios do filtro, mas não devem ser incluídos na política de direitos.

Direitos

O RBE permite que você conceda direitos em sistemas conectados e direitos no Identity Manager. Os direitos podem ser qualquer um dos seguintes:

- Contas em sistemas conectados.
- Participação em listas de distribuição de e-mails em sistemas conectados.
- Participação em grupos em sistemas conectados.
- Atributos para os objetos correspondentes em sistemas conectados, preenchidos com valores especificados por você.

Observação: A funcionalidade Direitos faz parte do Identity Manager, portanto você precisa ter drivers do Identity Manager instalados e configurados para suportar direitos antes de poder conceder direitos em sistemas conectados.

Criar direito

Na guia Direitos, execute o seguinte:

1. Clique na guia **Direitos**.
2. Clique em + para **Add Drivers** (Adicionar Drivers) e para fornecer direitos em sistemas conectados.

   A tela **Adicionar Driver** é exibida.
3. Selecione o driver do menu suspenso.
4. Clique em **Adicionar**.

   A tela **Add Entitlements** (Adicionar Direitos) é exibida.
5. No menu suspenso **Select an Entitlement** (Selecionar um direito), selecione o grupo que você deseja adicionar.
6. Selecione o **Query Type** (Tipo de Consulta):
   - **Cached** (Em Cache): Quando as consultas foram executadas anteriormente.
   - **External Query** (Consulta Externa): Quando as consultas são novas.

   A tela **Add Group Entitlement** (Adicionar Direito de Grupo) é exibida.
7. Selecione o direito de grupo no menu suspenso e clique em **Selecionar**.

Rights to other Objects (Direitos a outros objetos)

Use esta página para dar direitos de trustee de política de direitos a um objeto eDirectory. Cada membro da política de direitos torna-se um trustee do objeto.

Além de atribuir direitos a todos os atributos, você pode clicar em Add Property (Adicionar Propriedade) para atribuir direitos a propriedades específicas.

A caixa de seleção Herdar determina se os direitos fluem para baixo na árvore. Por exemplo, se você está atribuindo direitos a um objeto container e deseja que a política de direitos tenha os mesmos direitos dos objetos e subcontainers que estão abaixo desse container, selecione a caixa de seleção Herdar.

Os direitos a objetos no eDirectory serão concedidos aos membros da política de direitos depois que você concluir suas mudanças nesta página. Em contrapartida, os direitos em sistemas conectados serão concedidos a cada membro da política de direitos na próxima vez que um atributo usado para a participação dinâmica for modificado para esse usuário ou o usuário for movido ou renomeado. (O mesmo acontece quando direitos são revogados.) Use a tarefa Reavaliar a Participação para forçar uma atualização.

Criar direitos a outros objetos

Para criar direitos:

1 Clique na guia **Rights to Other Objects** (Direitos a Outros Objetos)

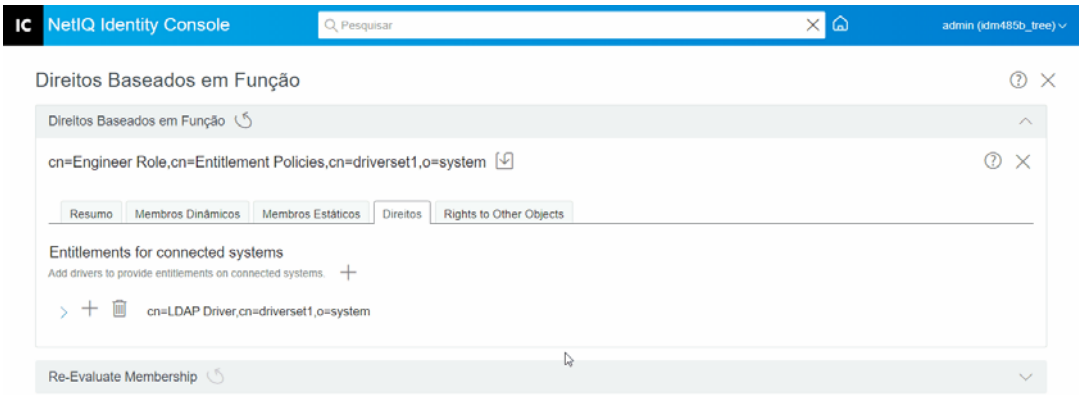
Aqui você pode adicionar um novo objeto e procurar por aqueles objetos para os quais você deseja que esta política de direitos seja um trustee.

1a Para adicionar um objeto, clique no botão +.

A página **BROWSER DE CONTEXTO** é exibida. A página é composta por `Objetos`.

1b Expanda os `Objetos` e selecione Grupos ou Usuários individuais de acordo com os seus requisitos e atribua direitos a eles.

Figura 33-3 *Rights to other Objects (Direitos a outros objetos)*

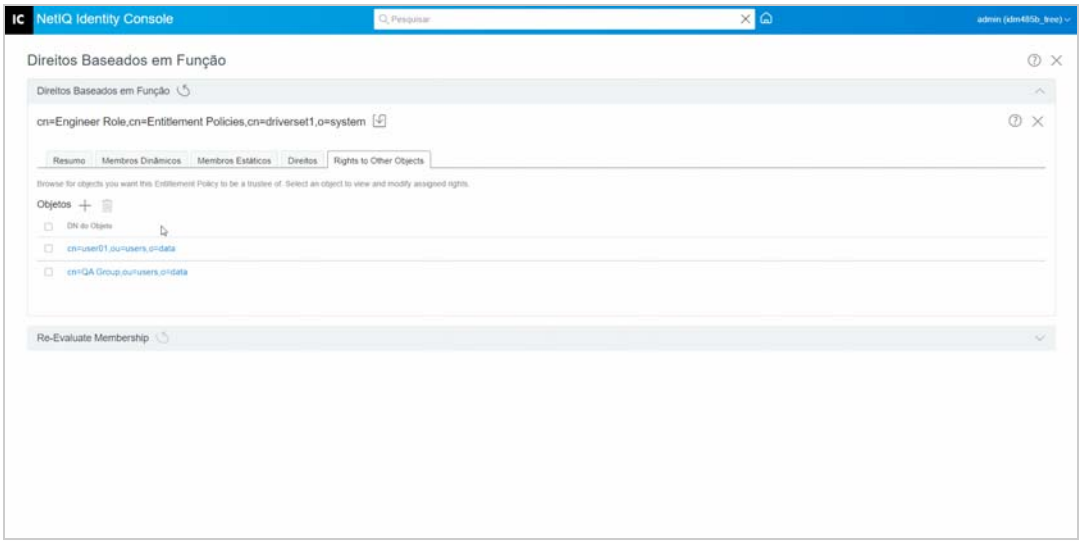


1c Para adicionar mais propriedades, clique em +.

A página **SELECT PROPERTIES** (SELECIONAR PROPRIEDADES) é exibida. Esta página tem a lista de propriedades que um objeto pode ter.

1d Clique em **Concluído**.

Figura 33-4 *Selecione Propriedades*



2 (Opcional) O uso das setas **Para Cima** e **Para Baixo** prioriza as políticas de RBE.

Priorizar a política é resolver conflitos de direitos entre múltiplas políticas. A política mais alta tem a maior prioridade. Para obter mais informações, consulte: "Priorizar políticas de RBE" na página 216

Priorizar políticas de RBE

Quando você cria políticas de RBE, é possível que as políticas que afetam um determinado usuário possam entrar em conflito.

A ordem das políticas de RBE na lista representa prioridade. Você pode alterar a ordem da lista usando os botões de seta para cima e para baixo.

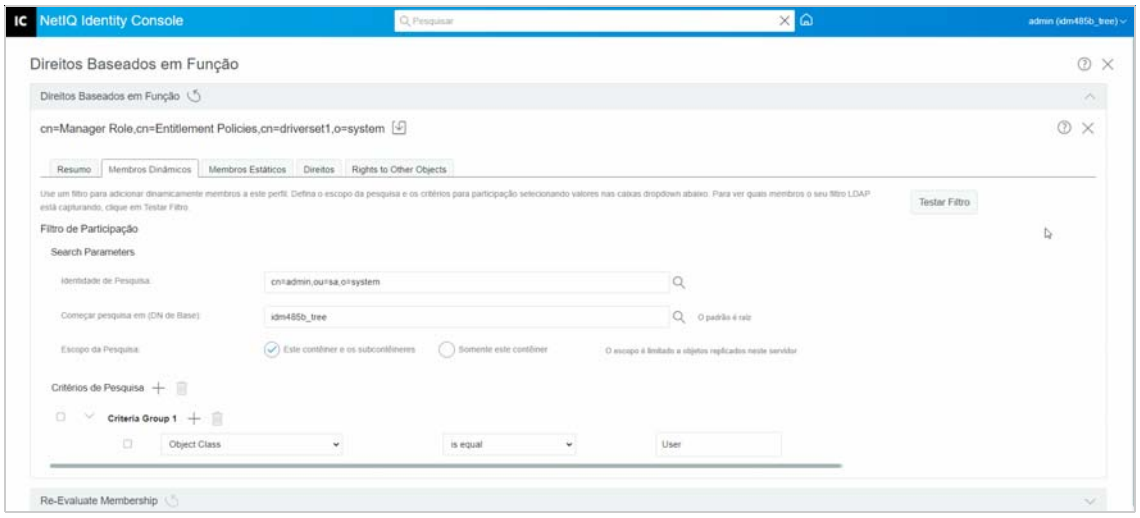
- Essa configuração poderá ser útil se, por exemplo, um atributo no sistema conectado permitir apenas um valor. Se duas políticas de RBE diferentes concederem um valor para esse atributo ao mesmo usuário, o usuário receberá o valor que é concedido pela política de RBE mais alta da lista. Como outro exemplo, talvez você tenha configurado seu ambiente para usar Direitos a fim de colocar usuários em uma estrutura hierárquica em outro sistema. Você gostaria que o usuário fosse colocado em um local ou em outro, não em dois locais ao mesmo tempo.
- Tenha em mente que a configuração é independente para cada direito oferecido por cada driver.
- Como regra geral, você deve colocar políticas de administrador ou gerente mais alto na lista do que políticas para usuários finais ou contribuintes individuais. Você deve colocar grupos com participação mais restrita em uma posição mais alta do que grupos com participação mais ampla.

Para priorizar políticas de RBE:

1 Selecione a política de direitos cuja prioridade você deseja aumentar ou diminuir.

2 Usar as setas **Para Cima** ou **Para Baixo** prioriza as políticas de RBE.

Figura 33-5 *Priorizando as políticas*

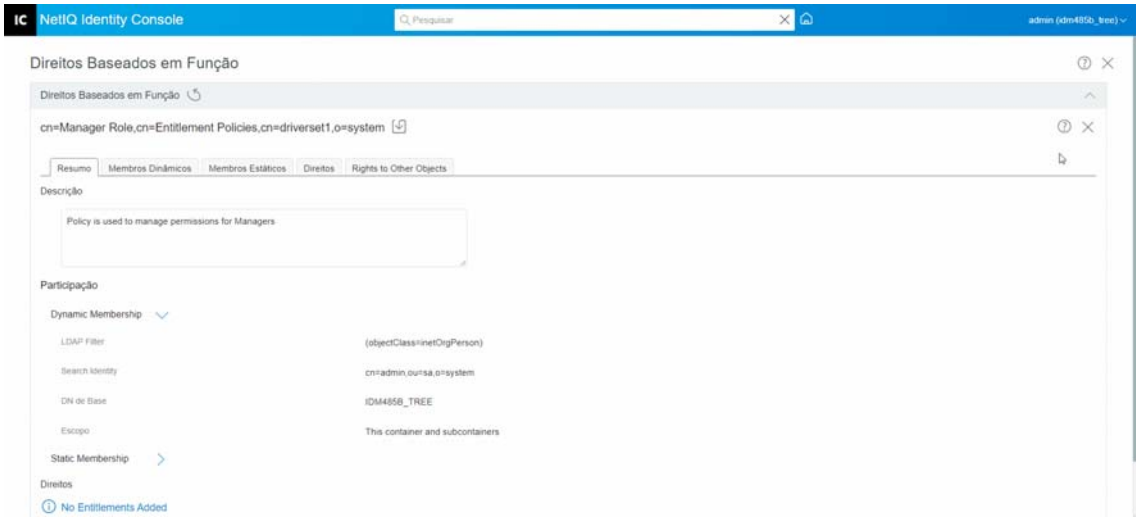


3 Clique no botão Gravar .

O resumo dos detalhes da participação na política é exibido na guia **Resumo**.

4 Reinicie o driver.

Figura 33-6 *Fechar e reiniciar*



Observação: Você precisa reiniciar o driver para que as mudanças entrem em vigor.

Reavaliar a participação

O recurso **Direitos Baseados em Função** permite que você conceda direitos em sistemas conectados a um grupo de usuários.

Quando você cria ou edita uma política de RBE, a participação de cada usuário precisa ser reavaliada para determinar se os direitos em sistemas conectados precisam ser concedidos, mudados ou revogados. Por padrão, a reavaliação ocorre para um usuário de cada vez, da próxima vez que um atributo que afeta a participação é mudado para cada usuário ou quando um usuário é movido ou renomeado. Esse comportamento padrão minimiza o uso de recursos do sistema, mas significa que pode haver um atraso significativo entre o momento em que a política de RBE é mudada e o tempo de concessão, mudança ou revogação de direitos para um determinado usuário.

Você pode garantir que os direitos do usuário sejam atualizados de uma só vez usando a tarefa "Reavaliar políticas de RBE" na página 218 para especificar usuários que precisam ser reavaliados imediatamente. Recomendamos que você faça isso cada vez que criar ou editar uma política de RBE.

Antes do Identity Manager 3.6, a reavaliação da participação foi realizada para todas as políticas de RBE em um conjunto de drivers, não para uma política de direitos individual. No entanto, o Identity Manager 3.6 permite que você **avalie** uma política de RBE e **adicione** os membros dela à **Objects List** (Lista de Objetos) selecionada. Se você tiver definido uma política de direitos e criado uma lista de associados, verá o cabeçalho de texto **Avalie uma Política de Direitos para adicionar os membros dela à lista** ao lado da entrada Objetos selecionada. Selecione a política e clique no ícone + para adicionar os membros da política à **Objects List** (Lista de Objetos) selecionada. Você pode adicionar ou remover membros ou objetos da **Lista de Objetos** selecionada.

Para aproveitar melhor os recursos do sistema, você deve fazer todas as suas mudanças nas políticas de RBE em um determinado conjunto de drivers antes de usar a opção "Reavaliar políticas de RBE" na página 218.

Observação: A reavaliação dos direitos é necessária apenas para direitos em sistemas conectados. Quando os direitos do Identity Console são mudados para uma política de RBE, as alterações entram em vigor imediatamente para cada usuário. Você precisa ter o driver de Serviço de Direitos em execução para que as reavaliações de participação sejam realizadas.

Reavaliar políticas de RBE

Para reavaliar a participação:

1. Clique em **Reavaliar a Participação** > **Selecionar o Conjunto de Drivers**.

   Uma lista das políticas criadas aparecerá.

2. Selecione a política que precisa ser avaliada e clique em **Avaliar** Evaluate.

   Na guia **Objetos**, os usuários que fazem parte do grupo aparecerão.

3. (Opcional) Para adicionar um usuário específico, clique em +.

   Quando os usuários estão faltando na lista e você deseja adicionar usuários específicos, só então você pode usar este recurso **Adicionar** +.

4. (Opcional) Para remover o usuário específico, clique em 🗑.

Quando usuários específicos precisam ser removidos da lista, só então você pode usar o recurso **Apagar** .

5 Clique no botão Reavaliar a participação .

Figura 33-7 *Reavaliar a participação*