CA Identity Manager™

Guia de Administração

12.6.5

Referências a produtos da CA Technologies

Este documento faz referência aos seguintes produtos da CA Technologies:

- CA CloudMinder™ Identity Management
- Diretório do CA
- CA Identity Manager ™
- CA Identity Governance (anteriormente CA GovernanceMinder)
- CA SiteMinder®
- Relatórios de atividades de usuários da CA
- CA AuthMinder ™

Entrar em contato com o Suporte técnico

Para assistência técnica online e uma lista completa dos locais, principais horários de atendimento e números de telefone, entre em contato com o Suporte técnico pelo endereço http://www.ca.com/worldwide.

Índice

Capítulo 1: Planejamento da função

Para planejar as funções, você decide que tipo de função sua empresa ou organização necessita e como delegará o gerenciamento dos usuários e o acesso de seus aplicativos. Com base nessas decisões, é possível determinar as características de cada função.

Para usar as funções de maneira eficiente, considere os seguintes tipos de pergunta sobre as necessidades dos usuários e as responsabilidades do administrador:

- Em que departamentos e organizações os usuários precisam ser gerenciados?
- Em terminais gerenciados, de quais contas adicionais os usuários precisarão?
- Quais usuários devem ser administradores de outros usuários?
- Quem deve gerenciar os administradores?
- Quais tarefas administrativas e de acesso são necessárias em cada função?
- Quem deve criar funções e tarefas?
- Como posso usar funções para delegar trabalho?

  A última pergunta refere-se ao compartilhamento do trabalho de gerenciar usuários e à concessão de acesso a aplicativos. Mais informações sobre o modelo de delegação podem ser encontradas em Administração delegada.

De acordo com as respostas a essas perguntas, você pode decidir quantas funções são necessárias e de que tipo.

Esta seção contém os seguintes tópicos:

Funções para gerenciamento de acesso e identidades

Para ativar o gerenciamento de identidades de usuário e do respectivo acesso a outras contas, o CA CloudMinder fornece os seguintes tipos de função:

Tipo de função	Finalidade
Função administrativa	Contém tarefas administrativas de forma que, quando um usuário recebe essa função, ele pode trabalhar no CA CloudMinder, executando tarefas como alterar a senha de um usuário ou associação de grupo. As funções administrativas também podem incluir qualquer tarefa que aparecer no console de usuário.
Função de provisionamento	Contém modelos de conta que definem contas existentes em terminais gerenciados, como um sistema de email. Os modelos de conta também definem como os atributos do usuário são mapeados para contas.
Função de acesso	As funções de acesso fornecem uma maneira adicional de fornecer direitos no CA Identity Manager ou outro aplicativo. Por exemplo, você pode usar as funções de acesso para executar as seguintes ações: ■ Fornecer acesso indireto a um atributo de usuário. ■ Criar expressões complexas. ■ Definir um atributo de perfil que outro aplicativo pode usar para determinar direitos.

Características da função

Quando você cria uma função, define as características mostradas na tabela a seguir:

Características	Definição
Perfil da função	Características gerais da função.
Tarefas	Tarefas para uma função administrativa.
Modelos de conta	Modelos que definem contas em terminais gerenciados para uma função de provisionamento.
Regras de integrantes, Políticas de integrantes	Uma regra de integrante define as condições para que um usuário seja um integrante de uma função administrativa ou de uma função de acesso. Um política de integrante combina uma regra de integrante com regras de escopo. **Observação:** as funções de provisionamento não possuem regras nem políticas de integrantes. Para tornar um usuário um integrante, use a opção Modificar integrantes/administradores da função de provisionamento.

Características	Definição
Regras administrativas, Políticas administrativas	■ Uma regra administrativa define as condições para que um usuário seja um administrador de funções. ■ Uma política administrativa combina uma regra administrativa com uma regra de escopo e privilégios de administrador para atribuir a função.
Regras de proprietário	Condições para que um usuário seja um proprietário da função.
Regras de escopo	Limita quais objetos podem ser gerenciados pela função.
Ações de adição, Ações de remoção	Altera para um perfil de usuário quando um usuário é adicionado ou removido como integrante ou administrador da função.

Perfil da função

O perfil da função mostra o nome e a descrição da função, bem como indica se a função está ou não ativada. Se ativada, a função está disponível para ser usada assim que ela é criada.

Tarefas da função

Para uma função administrativa, você pode escolher uma ou mais tarefas administrativas, incluindo tarefas externas, de uma ou mais categorias.

Modelos de conta

Cada função de provisionamento contém modelos de conta. Eles definem as contas existentes nos terminais gerenciados. Por exemplo, um terminal para uma conta do Exchange pode definir o tamanho da caixa de correio. Os modelos de conta também definem como os atributos do usuário são mapeados para contas.

É possível escolher um ou mais terminais para cada tipo de terminal. Um usuário com uma função atribuída recebe uma conta no terminal.

Regras para integrante, administrador e proprietário

Cada função inclui regras sobre quem pode ser um integrante, administrador ou proprietário da função. Portanto, um usuário pode ser integrante de uma função, várias funções ou nenhuma função.

As regras para integrante, administrador e proprietário usam as condições da tabela a seguir:

Condição da regra	Exemplo	Sintaxe da regra
O usuário deve corresponder a um valor de atributo.	Usuários cujos cargos começam com sênior	com <filtro-de-usuário>
O usuário deve corresponder a vários valores de atributo.	Usuários com cargo=gerente e localidade=leste	com <filtro-de-usuário>
O usuário deve pertencer a organizações nomeadas.	Usuários na organização de vendas e inferior	em <regra-de-org>
O usuário deve pertencer a organizações que atendam a uma condição especificada pelos atributos da organização.	Usuários em organizações onde Tipo de negócios=gold ou platinnum	em organizações com <filtro-de-org>
O usuário deve pertencer a organizações específicas e corresponder a atributos de usuário específicos.	Usuários com cargo=gerente e localidade=leste e que estão no departamento de vendas ou marketing da organização	com <filtro-de-usuário> e que estiver em <regra-de-org>
O usuário deve pertencer a um grupo específico.	Usuários que são integrantes do grupo 401K	que são os integrantes de grupo <grupo>
O usuário deve ser integrante de uma função.	Usuários que são integrantes da função de central de atendimento	que são os integrantes de <regra-de-função>
O usuário deve ser administrador de uma função.	Usuários que são administradores da função de Gerente de vendas	que são os administradores de <regra-de-função>
O usuário deve ser proprietário de uma função.	Usuários que são proprietários da função de Gerenciador de usuários	que são os proprietários de <regra-de-função>
O usuário deve pertencer a um grupo que atenda a uma condição especificada pelos atributos do grupo.	Usuários que são integrantes de grupos com proprietário=CIO	que são os integrantes de grupo <filtro-de-grupo>

Condição da regra	Exemplo	Sintaxe da regra
O usuário deverá atender a uma condição com base em uma consulta LDAP.	(Use um diretório LDAP nas situações em que uma consulta criada no Console de usuário do CA Identity Manager é insuficiente)	usuário retornado pela consulta ldap_query

Algumas regras podem envolver a comparação de um valor com um atributo de valor múltiplo. Para que a regra se aplique, pelo menos um valor em um atributo de valor múltiplo deve atender à regra. Por exemplo, se a regra for Atributo A IGUAL a 1, e o valor do atributo A for 1, 2, 3 para o usuário X, isso significa que esse usuário atende aos critérios.

O usuário que cria a função talvez não possa modificá-la. Para que ele possa modificar a função, esse usuário deverá atender às condições nas regras de proprietário.

Observação: em grandes implementações, a avaliação das regras para integrante, administrador e proprietário pode levar bastante tempo. Para reduzir o tempo de avaliação para regras que incluem atributos de usuário, você pode ativar a opção de avaliação em memória. Para obter mais informações, consulte o *Guia de Configuração*.

Regras de escopo

É possível combinar regras de integrante e administrativas com regras de escopo. As *regras de escopo* limitam objetos nos quais a função pode ser usada.

- Para um integrante da função, as regras de escopo controlam quais objetos podem ser gerenciados com a função.
- Para um administrador da função, as regras de escopo controlam quais usuários podem se tornar integrantes de função e administradores.

O escopo se aplica ao objeto principal da tarefa. Por exemplo, o usuário é o objeto principal da tarefa Criar usuário. No entanto, o escopo não se aplica aos grupos desse usuário, porque o grupo é um objeto secundário.

Para a maioria dos tipos de objeto, é possível especificar os tipos de regras de escopo na tabela a seguir.

Condição da regra	Exemplo	Sintaxe da regra
Tudo	Integrantes da função podem gerenciar todos os objetos	Tudo
O objeto deve corresponder a um ou mais valores de atributo.	Usuários cujos **cargos** começam com **sênior**	com <filter>

Quando você seleciona a opção de filtro, o CA Identity Manager exibe dois tipos de filtro:

<atributo> <comparador><valor>

Um atributo no perfil do objeto deve corresponder a um valor específico.

<atributo> <comparador> <atributo de usuário> do administrador

Um atributo no perfil do objeto deve corresponder a um atributo no perfil do administrador. Por exemplo: os usuários em que gerente = ID de usuário do administrador.

Opções adicionais, que são descritas nas próximas tabelas, estão disponíveis para objetos de usuário, grupo e organização.

Observação: as regras de escopo do usuário a seguir são exemplos. É possível criar outras regras para controlar diferentes relacionamentos entre o administrador e os usuários que o administrador pode gerenciar.

Condição da regra	Exemplo	Sintaxe da regra
O usuário deve corresponder a um valor de atributo.	Usuários em que o integrante do grupo de vendas ou o telefone celular não sejam iguais a nulo	com <filtro-de-usuário>
O usuário deve corresponder a vários valores de atributo.	Usuários com cargo=gerente e localidade=EUA	com <filtro-de-usuário>
O usuário deve pertencer a organizações nomeadas.	Os usuários na organização Austrália ou Nova Zelândia **Observação:** a regra de escopo da organização se aplica a suborganizações da organização que atende à regra. Por exemplo, se a regra de organização for "na Organização1", a regra de escopo se aplicará à Organization1.1 e Organization1.2, mas não se aplicará à Organização1.	em <regra-de-org>
O usuário deve pertencer a organizações que atendam a uma condição especificada pelos atributos da organização.	Usuários em organizações onde Tipo de negócios=gold ou platinnum	em organizações com <filtro-de-org>
O usuário deve pertencer a organizações específicas e corresponder a atributos de usuário específicos.	Usuários com cargo=gerente e localidade=leste e que estão no departamento de vendas ou marketing da organização	com <filtro-de-usuário> e que estiver em <regra-de-org>

Condição da regra	Exemplo	Sintaxe da regra
O atributo em um perfil de usuário deve corresponder a um atributo no perfil do administrador.	Usuários com gerente = ID de usuário do administrador	com <atributo-de-usuário> <comparador> <atributo-de-usuário> do administrador **Observação:** não use o comparador Não é igual com um atributo de valor múltiplo.
O usuário está na mesma organização que o administrador.	Os usuários na organização, onde Jeff (administrador) é integrante	da organização do administrador.
O usuário está em uma organização que está listada no atributo do administrador.	Usuários em vendas ou marketing	organização que é um valor no <atrib-admin> do administrador

Observação: as regras de escopo do grupo a seguir são apenas exemplos. É possível criar outras regras para controlar diferentes relacionamentos entre o administrador e os grupos que o administrador pode gerenciar.

Condição da regra	Exemplo	Sintaxe da regra
O grupo deve corresponder a um valor de atributo.	O nome do grupo com Nome do grupo = 401K	com <filtro-de-grupo>
Os grupos devem pertencer a organizações nomeadas.	Grupos no departamento de contabilidade da organização ou abaixo	em <regra-de-org>
O grupo deve corresponder a um valor de atributo e pertencer a organizações nomeadas.	Grupos com Tipo de negócios=Finanças e que estão no departamento de vendas ou abaixo na organização.	com <filtro-de-grupo> e que estiverem em <regra-de-org>
O grupo deve ser listado em um atributo do administrador.	Grupos com Descrição = Engenharia	com <atributo-de-grupo> <comparador> <atributo-de-usuário> do administrador **Observação:** não use o comparador Não é igual com um atributo de valor múltiplo.

Observação: as regras de escopo de organização a seguir são apenas exemplos. É possível criar outras regras para controlar diferentes relacionamentos entre o administrador e as organizações que o administrador pode gerenciar.

Condição da regra	Exemplo	Sintaxe da regra
A organização deve corresponder a um valor de atributo.	organizações com Nome da organização = finanças	com <filtro-de-org>
A organização deve pertencer à organização nomeada.	organizações em no departamento de finanças e abaixo	em <regra-de-org>
A organização deve corresponder a um valor de atributo e pertencer à organização nomeada.	organizações com Nome=finanças e estão em finanças ou abaixo	com <filtro-de-org> e estão em <filtro-de-org>

Avaliação de operadores

Ao criar regras para uma função, você pode incluir os operadores >=, <=, < e >. No entanto, esses operadores são avaliados como sequências de caracteres pelo diretório LDAP ou banco de dados relacional. A maioria dos repositórios de usuários compara sequências de caracteres com base no alfabeto. Desse modo, na comparação de 500 com 1.100, o repositório de usuários pode determinar que 500 é maior porque 5 é maior que 1.

Você pode alterar como as sequências de caracteres são comparadas no repositório de usuários. Consulte a documentação do serviço de diretório LDAP ou do software de banco de dados relacional.

O CA Identity Manager processa instruções OR antes das instruções AND. Veja o exemplo a seguir:

```
where(company=CA and city=Boston or city=Framingham)
```

Nesse exemplo, o CA Identity Manager processa (Boston ou Framingham) primeiro e, em seguida, executa a lógica AND com company=CA.

Regras não diferenciam letras maiúsculas de minúsculas

Ao criar funções administrativas ou de acesso, as regras que você cria podem ser avaliadas de maneira que diferencie ou não letras maiúsculas de minúsculas, de acordo com o repositório de usuários.

No entanto, no fim de uma operação de criação ou modificação, as regras são avaliadas internamente de maneira que não diferencie letras maiúsculas de minúsculas antes de confirmar as alterações no repositório de usuários. Por exemplo, se uma regra tiver uma condição onde cargo=gerente, a regra corresponderá ao objeto de repositório de usuários se tiver um valor de cargo de gerente ou Gerente.

Ações de adição e remoção

É necessário especificar uma ação de adição e remoção para o que o CA Identity Manager gerencie corretamente a associação de uma função quando um administrador concede ou revoga a função.

- A ação de adição deve fazer com que o usuário atenda aos critérios em uma das regras de integrante da função. Por exemplo, se a regra de integrante para a função Gerenciador de usuários determinar que os integrantes da função têm "Gerenciador de usuários" como um valor do atributo Funções administrativas, a ação de adição deverá adicionar "Gerenciador de usuários" ao atributo Funções administrativas.
- A ação de remoção deve alterar o perfil de um usuário para que este não atenda mais à regra de integrante quando esta for revogada.

Cada função pode ter duas *ações de adição* e duas *ações de remoção*.

Se os administradores podem adicionar e remover integrantes da função, você define as ações de adição e remoção. Caso contrário, o usuário tem a função ao atender à regra de integrante, assim como ao pertencer ao grupo RoleAdmins. Por exemplo:

- A Função A pode ser atribuída por um administrador, de modo que as ações de adição ou remoção serão definidas.
- A Função B tem uma regra em que todos os integrantes do grupo "finanças" têm a função. Essa função não pode ser atribuída, de modo que não possui ação de adição ou remoção.

Ao definir ações de adição e remoção, considere o uso do atributo Função administrativa, que o CA Identity Manager pode usar para armazenar uma lista de funções do usuário. Por exemplo, você pode configurar uma ação de adição que inclui o funcionário em um atributo Função administrativa do usuário quando esse usuário é adicionado como integrante da função Funcionário. Quando um administrador atribui a função Funcionário a um gerente que já possui as funções Autoadministrador e Gerenciador de usuários, o atributo Função administrativa do gerenciador pode conter os seguintes valores: Autoadministrador, Gerenciador de usuários, Funcionário.

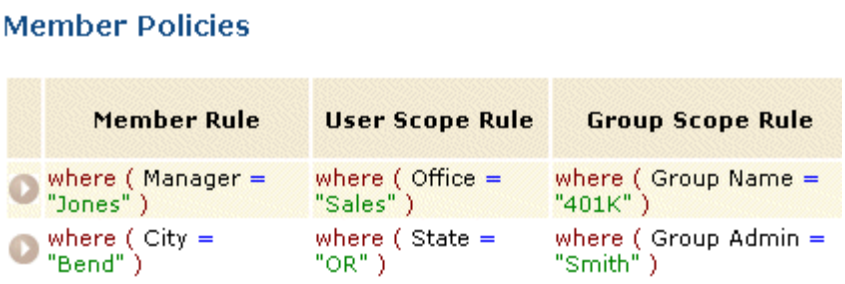
Para usar o atributo Função administrativa, o conhecido atributo %ADMIN_ROLE_CONSTRAINT% deve ser mapeado para um atributo de valor múltiplo em perfis de usuário. Para obter mais informações, consulte o *Guia de Configuração do CA Identity Manager*.

Importante: ao definir uma ação de adição, evite configurar uma regra que se refira à função que você está definindo. Por exemplo, não defina uma ação de adição que torna um usuário integrante da Função A se ele for um integrante da Função A. Isso criará um erro repetitivo que fará com que o servidor de políticas seja reiniciado.

Políticas de integrantes

Uma *política de integrante* indica que, se um usuário atender à regra de integrante, significa que ele tem o escopo definido nessa política. A figura a seguir mostra uma função que possui duas políticas de integrante.

- A primeira política indica que, se um integrante da função tiver o gerente Jones, esse integrante poderá usar a função em usuários no escritório de vendas e gerenciá-los como integrantes do grupo 401k.
- A segunda política indica que, se um integrante da função estiver na cidade de Bend, esse integrante poderá usar a função em usuários no estado do Oregon e gerenciá-los como integrantes dos grupos que possuem o administrador de grupos Smith.

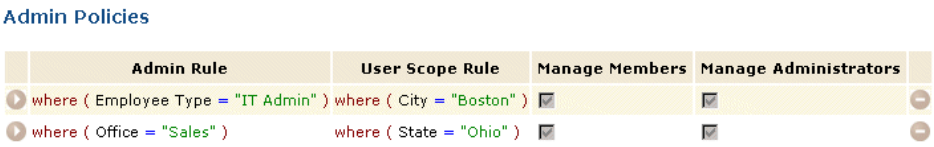


Políticas administrativas

Uma *política administrativa* indica que, se um usuário atender à regra administrativa, esse usuário tem os privilégios de administrador e o escopo do usuário definidos nessa política. O escopo do usuário define onde a função é usada. Os privilégios de administrador determinam se o administrador da função pode gerenciar integrantes ou administradores da função.

A figura a seguir mostra uma função que tem duas políticas administrativas, que são definidas como segue:

- Para a primeira política, um administrador de TI pode adicionar e remover integrantes e administradores da função dos usuários na cidade de Boston.
- Para a segunda política, um administrador em Vendas pode adicionar e remover integrantes no estado de Ohio.



Lista de verificação de planejamento de função

Antes de criar uma função, use esta lista de verificação de características da função.

Característica da função	Detalhes
Perfil da função	Defina um nome e uma descrição para a função, bem como o status Ativado.
Tarefas	Inclua tarefas administrativas e de acesso.
Modelos de conta	Inclua modelos de conta que definem contas que existem nos terminais (somente funções de provisionamento).
Políticas de integrantes	Para cada política de integrante, defina: ■ Regras de integrantes - quem pode usar a função ■ Regras de escopo - quais objetos um integrante da função pode gerenciar ■ Ação de adição - o que acontece com o perfil de um usuário que se torna um integrante ■ Ação de remoção - o que acontece com o perfil de um usuário que é removido como um integrante

Característica da função	Detalhes
Políticas administrativas	Para cada política administrativa: ■ Regras administrativas - quem pode gerenciar os usuários como integrantes ou administradores ■ Regras de escopo - quais usuários o administrador pode gerenciar como integrantes ou administradores ■ Ação de adição - o que acontece com o perfil de um usuário que se torna um administrador ■ Ação de remoção - o que acontece com o perfil de um usuário que é removido como um administrador
Regras de proprietário	Defina quem pode modificar a função.

Capítulo 2: Funções administrativas

Esta seção contém os seguintes tópicos:

Funções administrativas e tarefas administrativas

Você pode criar funções que contêm tarefas de gerenciamento de objetos que estão de acordo com suas necessidades de negócios individuais. Por exemplo, você cria diversas funções com tarefas que gerenciam usuários e outras funções com tarefas que gerenciam as funções que você criar.

Como alternativa, você pode criar funções separadas com:

- Tarefas para que os administradores gerenciem usuários
- Tarefas que gerenciam os administradores
- Tarefas para gerenciar funções administrativas
- Tarefas para gerenciar funções de acesso

Observação: também é possível usar as funções administrativas padrão fornecidas com o CA Identity Manager. Essas funções possuem tarefas que são agrupadas em categorias semelhantes à lista anterior.

Funções administrativas e ambientes do CA Identity Manager

Ao efetuar logon em um ambiente do CA Identity Manager, a conta de usuário tem uma ou mais funções administrativas. Cada função administrativa contém tarefas, como Criar usuário, que você usa nesse ambiente do CA Identity Manager.

Por exemplo, no ambiente *central* do CA Identity Manager, uma função administrativa, *central de atendimento*, tem tarefas para redefinir senhas. A função possui uma regra de integrante de que o usuário deve ser um funcionário de TI. Quando funcionários de TI efetuam logon no ambiente *central* do CA Identity Manager, eles têm a função de *central de atendimento* e podem redefinir as senhas dos usuários nesse ambiente do CA Identity Manager.

Funções administrativas e o console de usuário

Um ambiente do CA Identity Manager é exibido por meio do console de usuário. Suas funções administrativas atribuídas determinam o que você consegue ver nesse console, conforme mostrado na tabela a seguir:

Funções atribuídas	Formato do console de usuário
Função de Gerente do sistema	A lista de categorias para todos os objetos e todas as tarefas administrativas padrão para o gerenciamento desses objetos
Funções para gerenciar mais de um tipo de objeto	A lista de categorias com um item para cada tipo de objeto que você pode gerenciar
Funções para gerenciar um tipo de objeto, como Usuários	As tarefas para esse objeto (como Modificar usuário) *sem* uma lista de categorias
Uma função de aprovação	A tela de lista de tarefas É exibida se o administrador tiver tarefas com aprovação pendente (por exemplo, os usuários autorregistrados precisam de aprovação)

Se você puder gerenciar mais de um objeto, a lista de categorias é exibida e mostra os objetos que podem ser modificados, como Usuários e Grupos como guias na parte superior da tela. Selecione uma guia para exibir as tarefas em suas funções atribuídas.

Observação: se seu navegador da internet não oferecer suporte a CSS (Cascading Style Sheet - Folha de Estilos em Cascata), o console de usuário usará um formato diferente. Para controlar esse formato, consulte o *Guia de Configuração*.

Criar uma função administrativa

Você pode criar uma função administrativa quando souber quais são os requisitos da função. Esses requisitos estão relacionados às seguintes questões:

- Os usuários que precisam dessa função
- Os objetos que essa função gerencia
- O ambiente com os objetos para gerenciar

Iniciar a criação da função administrativa

Para criar uma função administrativa no console de usuário.

Para criar uma função administrativa

1. Efetue logon em uma conta do CA Identity Manager que tenha uma função com tarefas para a criação de funções administrativas.

   Por exemplo, o primeiro usuário de um ambiente tem a função de Gerente do sistema, que tem a tarefa Criar função administrativa.

2. Selecione Funções e tarefas, Funções administrativas e Criar função administrativa.

3. Decida se deseja criar ou copiar uma função.

   A guia Perfil é exibida, onde você começa a definir a função administrativa.

4. Defina o perfil da função administrativa.

Definir o perfil da função administrativa

Na guia Perfil, você define as características básicas da função.

Para definir o perfil:

1. Digite um nome e uma descrição e preencha qualquer outro atributo personalizado que for definido para a função.

   Observação: é possível especificar atributos personalizados na guia Perfil que especificam informações adicionais sobre as funções administrativas. Você pode usar essas informações adicionais para facilitar as pesquisas de funções em ambientes que incluem um número significativo de funções.

2. Selecione Ativado se estiver pronto para tornar a função disponível para uso assim que criá-la.

3. Selecione tarefas administrativas para a função (na página 32).

Selecionar tarefas administrativas para a função

Na guia Tarefas, selecione as tarefas administrativas para incluir na função. Você pode incluir tarefas de diferentes categorias ou copiar tarefas usadas em outra função.

Para selecionar as tarefas administrativas:

1. Selecione a categoria no campo Filtrar por categoria.

   Para exibir a lista de categorias de tarefa disponíveis, clique no ícone com a seta para baixo.

2. Selecione a tarefa a ser incluída na função no campo Adicionar tarefa.

   O CA Identity Manager adiciona a tarefa à lista de tarefas da função.

3. Adicione outras repetindo as etapas 1 e 2.

4. Remova uma tarefa da função com um clique no ícone de sinal de menos () da tarefa.

5. Defina políticas de integrante para uma função administrativa (na página 33).

Definir políticas de integrante para uma função administrativa

Na guia Integrantes, você pode criar políticas de integrantes, que determinam quem pode ser um integrante da função.

Para definir políticas de integrantes:

1. Clique em Adicionar para definir políticas de integrantes. Uma política de integrante contém estas regras:

   - Uma regra de integrante que define os requisitos para que um usuário seja um integrante da função.

     Observação: os seguintes operadores tratam os números como caracteres em regras de integrante:

     - Menor que (<)
     - Menor que ou igual a (<=)
     - Maior que (>)
     - Maior que ou igual a (=>)

     Por exemplo, 10 virá após 1, mas antes de 2.

   - As regras de escopo que limitam os objetos principais e secundários disponíveis para as tarefas da função.

     Por exemplo, a função contém uma tarefa que modifica os usuários ao atribuí-los aos grupos. Como resultado, a regra de escopo do usuário limita os usuários (objeto principal) que podem ser encontrados, e a regra de escopo do grupo limita os grupos (objeto secundário) que podem ser atribuídos.

   Observação: certifique-se de inserir uma resposta para, pelo menos, uma pergunta de escopo. As regras de escopo limitam os objetos principais e secundários disponíveis para as tarefas da função. Por exemplo, a função contém uma tarefa que modifica os usuários ao atribuí-los aos grupos. Como resultado, a regra de escopo do usuário limita os usuários (objeto principal) que podem ser encontrados, e a regra de escopo do grupo limita os grupos (objeto secundário) que podem ser atribuídos.

2. Verifique se a Política de integrante é exibida na guia Integrantes.

   - Para editar uma política, clique no símbolo de seta para a direita à esquerda.
   - Para removê-la, clique no ícone do sinal de menos.

3. Na guia Integrantes, como opção, é possível marcar a caixa de seleção intitulada Os administradores podem adicionar e remover integrantes desta função. Se essa caixa de seleção estiver desmarcada, os usuários se tornam integrantes se cumprirem uma regra de integrante.

   Quando esse recurso é ativado, a tela se expande.

4. Na área expandida, defina a Ação de adição e a Ação de remoção (na página 25) para quando um usuário for adicionado ou removido como um integrante da função.

   Importante: Para a ação de adição, evite configurar uma regra que se refere à função que você estiver definindo. Por exemplo, não defina uma ação de adição que torna um usuário integrante da Função A se ele for um integrante da Função A.

5. Defina políticas administrativas para uma função administrativa (na página 34).

Definir políticas administrativas para uma função administrativa

Na guia Administradores, você define quem pode adicionar ou remover usuários como integrantes e administradores dessa função.

Para definir políticas administrativas:

1. Se desejar tornar a opção Gerenciar administradores disponível, marque a caixa de seleção Os administradores podem adicionar e remover administradores desta função.

   Quando esse recurso é ativado, a tela se expande.

2. Na área expandida, defina a Ação de adição e a Ação de remoção para quando um usuário for adicionado ou removido como um administrador da função.

3. Defina as políticas administrativas, que contêm regras administrativas e de escopo, e pelo menos um privilégio de administrador (Gerenciar integrantes ou Gerenciar administradores).

   Observação: você pode adicionar várias políticas administrativas com regras e privilégios diferentes para administradores que atendam à regra.

4. Para editar uma política, clique no símbolo de seta à esquerda. Para removê-la, clique no ícone do sinal de menos.

5. Defina regras de proprietário para uma função administrativa (na página 34).

Definir regras de proprietário para uma função administrativa

Na guia Proprietários, defina regras sobre quem pode ser um proprietário da função, que é um usuário que pode modificar a função.

Para definir as regras de proprietário:

1. Defina as regras de proprietário, que determinam os usuários que podem modificar a função.

2. Clique em Enviar.

   Uma mensagem é exibida, indicando que a tarefa foi enviada. Um atraso momentâneo ocorre antes que um usuário possa usar a função.

A função está disponível para ser usada. Agora, um usuário que atende às condições da regra de integrante pode efetuar logon no ambiente e usar as tarefas da função.

Verificar uma função administrativa

Siga estas etapas:

1. Escolha Funções administrativas.
2. Escolha Exibir função administrativa.
3. Selecione o nome da função.

Como alternativa, você pode escolher Sistema, Exibir tarefas enviadas para verificar se a tarefa de criação da função foi concluída.

Permitir que os usuários atribuam funções a si mesmos

Os usuários podem atribuir determinadas funções a si mesmos. Por exemplo, você pode permitir que os usuários se inscrevam para a função de Gerenciador de delegação para que possam delegar o itens de trabalho de um usuário a outro.

Para controlar as funções que os usuários podem atribuir a si mesmos, você configura os critérios na tarefa Funções autogerenciáveis.

Siga estas etapas:

1. Modifique a tarefa Funções autogerenciáveis da seguinte maneira:
   a. Selecione Funções e tarefas, Modificar tarefa administrativa e pesquise a tarefa Funções autogerenciáveis.
   b. Selecione a guia Guias.

      O CA Identity Manager exibe a lista de guias que se aplicam à tarefa.

   c. Selecione o ícone em forma de seta para a direita ao lado da guia Autogerenciador de funções para editá-la.

d. Preencha os seguintes campos:

Mostrar apenas as funções administrativas em conformidade com as regras abaixo

Especifica os critérios que o CA Identity Manager usa para determinar que funções os usuários têm permissão de atribuir a si mesmos.

Para adicionar outras regras, clique no ícone do sinal de mais (+).

Usuário a ser utilizado como administrador da função administrativa

Especifica o administrador para funções que os usuários podem atribuir a si mesmos.

As funções que os usuários podem atribuir a si mesmos devem ter o usuário que você selecionar nesse campo como administrador *e* atender aos critérios especificados no campo Mostrar apenas as funções administrativas em conformidade com as regras abaixo.

Tela de lista

Especifica as colunas e o formato para a lista de funções que um usuário pode selecionar para atribuir uma função a si mesmo.

e. Clique em OK e, em seguida, clique em Enviar.

2. Adicione a tarefa Funções autogerenciáveis a uma função e atribua essa função aos usuários que devem ter esse recurso.

Capítulo 3: Tarefas administrativas

Esta seção contém os seguintes tópicos:

Planejamento de tarefa administrativa

As funções administrativas consistem em tarefas administrativas, que representam recursos granulares para o gerenciamento de objetos. Por exemplo, você pode gerenciar um objeto de usuário usando estas tarefas administrativas:

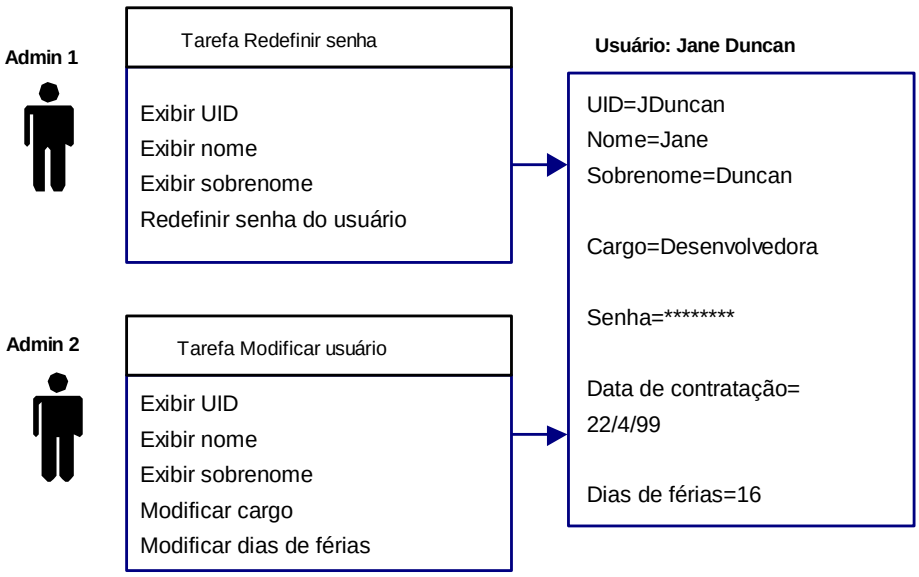
- Criar usuário
- Exibir usuário
- Modificar usuário
- Redefinir senha de usuário

Você cria ou modifica cada tarefa para corresponder exatamente às suas necessidades. Em seguida, você combina as tarefas administrativas apropriadas em funções administrativas, que atribui aos administradores. Com essas funções, os administradores terão exatamente os que precisam para gerenciar objetos.

Para planejar a criação de uma tarefa administrativa, decida quais objetos precisa gerenciar (usuário, grupo, organização, função ou tarefa) e quais os administradores usarão essas tarefas. Por exemplo:

- Para gerenciar os usuários, os administradores da central de atendimento precisam de tarefas que gerenciem os atributos do usuário, como ID ou cargo de usuário.
- Para gerenciar o acesso de usuários aos aplicativos, outros administradores precisam de tarefas que tornem os usuários integrantes das funções de acesso.
- Para gerenciar as funções usadas por administradores da central de atendimento, os administradores de nível superior precisam de tarefas que gerenciem as funções administrativas.

Para um tipo de objeto, como usuários, é possível criar tarefas, de modo que diferentes administradores gerenciem atributos diferentes. Por exemplo, a figura a seguir mostra um usuário que é gerenciado por dois administradores.



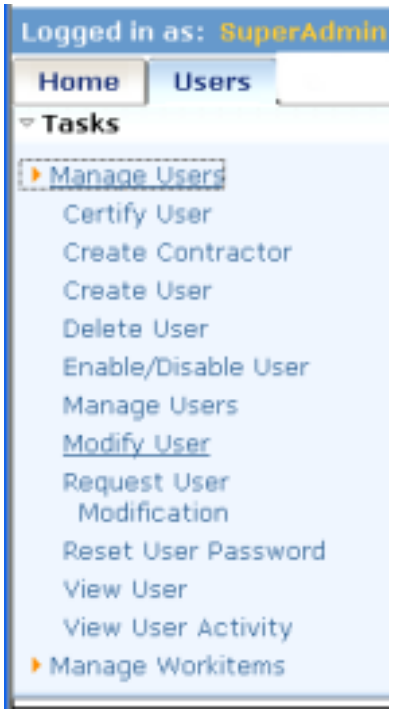
- O administrador 1 tem a tarefa Redefinir senha de usuário; esse administrador pode exibir a ID de usuário e o nome do funcionário ou redefinir sua senha.
- O administrador 2 tem a tarefa Modificar usuário; esse administrador pode exibir a ID de usuário e o nome do funcionário ou modificar seu cargo e os dias de férias.

Um exemplo de tarefa administrativa

Ao criar uma tarefa administrativa, você define o conteúdo e o layout das telas na tarefa, incluindo:

- O nome da tarefa
- A categoria na qual a tarefa é exibida
- As guias e os campos a serem usados na tarefa, bem como as propriedades de exibição do campo
- Os campos que um administrador pode usar em uma consulta de pesquisa e os campos exibidos nos resultados da pesquisa

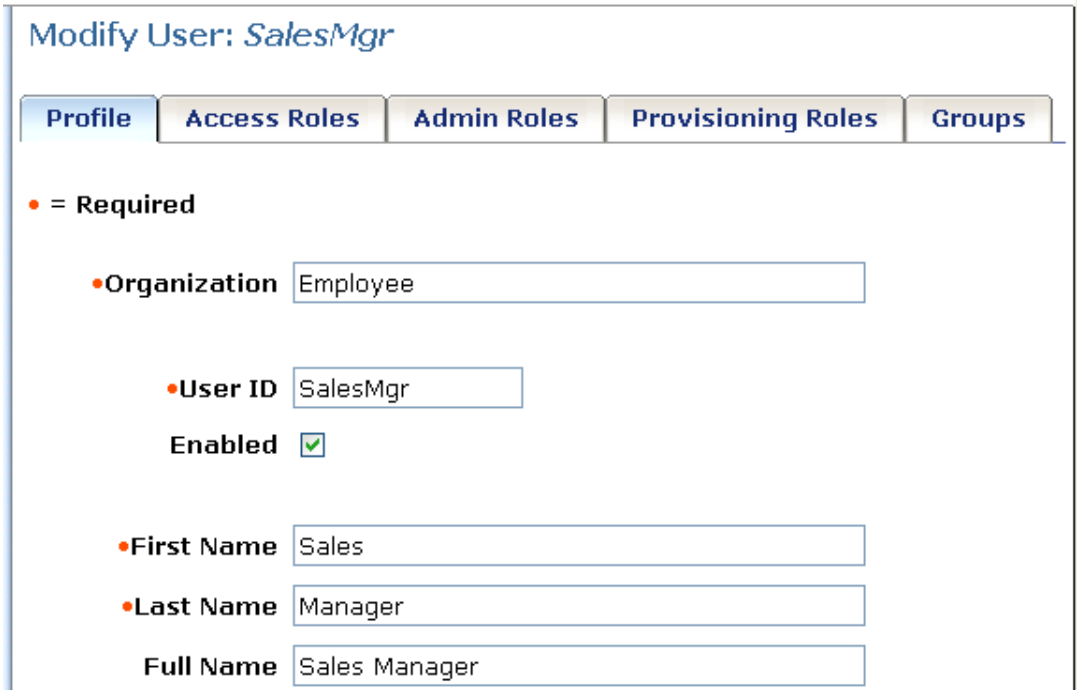
Para compreender os elementos de uma tarefa, considere a tarefa Modificar usuário. Nesse caso, Usuários é a categoria, Gerenciar usuários é uma subcategoria e Modificar usuário é a tarefa. Você cria os nomes da categoria e da tarefa quando cria uma tarefa.



Quando você seleciona Modificar usuário, uma tela de pesquisa é exibida. Uma *tela de pesquisa* contém opções para localizar o objeto a ser exibido ou modificado. Cada opção é chamada de *filtro*, que é um limite para os objetos encontrados pela pesquisa.

Após preencher a tela de pesquisa, uma tela com guias será exibida. Por exemplo, a figura a seguir mostra as guias para a tarefa Modificar usuário. A guia Perfil é exibida primeiro e mostra os atributos do usuário; as outras guias mostram a função e os privilégios de grupo do usuário.

Para a tarefa criada, você decide quais guias incluir e determina a ordem e o conteúdo de cada uma delas.

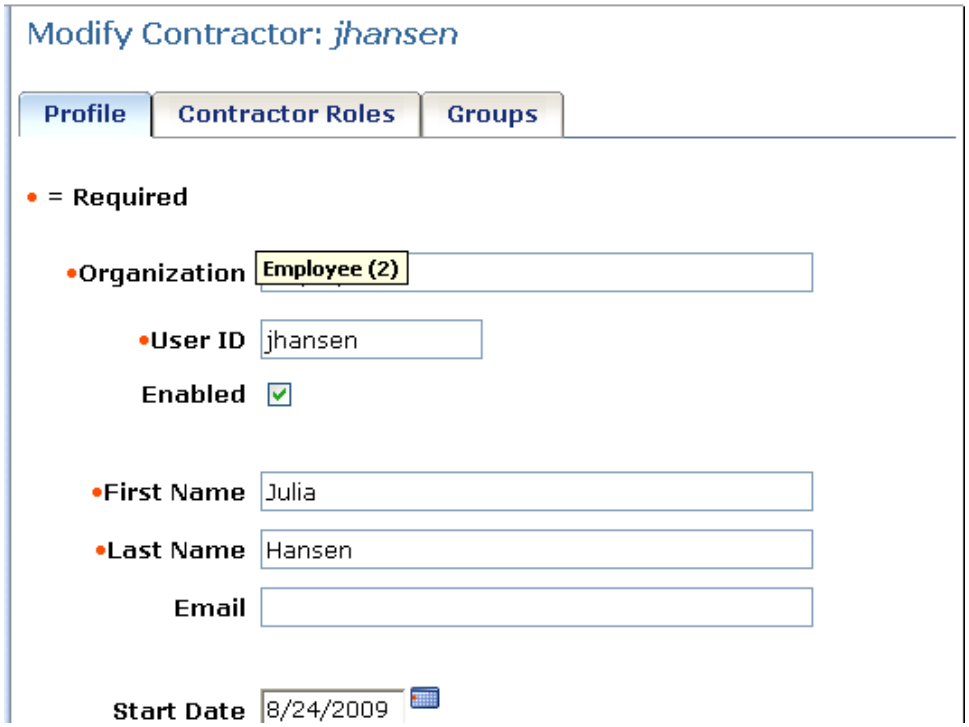


Por exemplo, usando a tarefa Modificar usuário como um modelo, você pode criar uma tarefa Modificar contratante cujas alterações foram feitas:

- Nos campos da guia Perfil
- Nas guias a serem incluídas na tarefa e seu conteúdo
- Na categoria sob a qual a tarefa é exibida

  Você pode criar essa tarefa sob uma nova categoria: Contratante.

A tarefa Modificar contratante inclui alguns dos campos da guia Perfil na tarefa Modificar usuário, além de outros campos, como a data de início do contrato e a empresa do contratante. Os administradores podem procurar um contratante pesquisando por nome do contratante, empresa e data de início.



A nova tarefa também inclui a guia Funções do contratante, onde é possível adicionar funções para contratantes.

Opções de utilização de tarefa administrativa

O CA Identity Manager oferece duas maneiras de usar as tarefas administrativas:

- **Selecionar a tarefa**

  Você seleciona uma categoria e a tarefa e, em seguida, pesquisa o objeto ao qual a tarefa se aplica.

  Por exemplo, para modificar um perfil de usuário, selecione a categoria Usuários e, em seguida, selecione a tarefa Modificar usuário. Em seguida, é possível procurar o usuário a ser modificado.

- **Selecionar o objeto**

  Você utiliza as tarefas Gerenciar, como Gerenciar usuários ou Gerenciar grupos, para procurar um objeto. Depois de selecionar o objeto, poderá exibir uma lista de tarefas que podem ser usadas para gerenciar esse objeto. Esse método é chamado *navegação em tarefas-objeto*.

  Por exemplo, para modificar um usuário usando esse método, você seleciona a categoria Usuário e, em seguida, a tarefa Gerenciar usuários. É possível pesquisar e selecionar o usuário que deseja gerenciar. Nos resultados da pesquisa, clique em um ícone para exibir uma lista de tarefas que podem ser usadas para gerenciar o usuário selecionado. Nessa lista, é possível selecionar Modificar usuário ou qualquer outra tarefa apropriada.

  Você também pode configurar listas de tarefas diferentes de Gerenciar. Por exemplo, você pode adicionar uma lista de tarefas à guia Associação. Nesse caso, uma lista de tarefas fica disponível para cada integrante que aparece na guia Associação.

  Observação: apenas as tarefas que o administrador atual pode usar são exibidas na lista de tarefas para um objeto.

Tarefas administrativas padrão

O CA Identity Manager inclui um conjunto de tarefas e funções administrativas padrão, que são adicionadas ao CA Identity Manager importando um arquivo de definições de função no Management Console. Quando você cria um ambiente no Management Console e opta por criar as funções padrão, o CA Identity Manager importa automaticamente um arquivo de definições de função.

Observação: para oferecer suporte a algumas funcionalidades, como o gerenciamento de contas para determinados tipos de terminal, talvez você precise importar mais arquivos de definições de função para criar as funções e tarefas que você precisa.

Na maioria dos casos, você poderá usar as tarefas padrão instaladas. No entanto, talvez você precise modificar a guia Perfil nas tarefas de usuário padrão, como Criar usuário, Modificar usuário e Exibir usuário. A guia Perfil contém todos os campos que estão definidos para o objeto de usuário no arquivo de configuração do diretório. É possível limitar o número de campos que aparecem na guia, ou alterar as propriedades de exibição do campo.

Observação: é recomendável criar uma cópia de uma tarefa padrão para modificar, em vez de modificar a tarefa padrão diretamente.

Como criar uma tarefa administrativa personalizada

Uma *tarefa administrativa* é uma função administrativa que um usuário pode executar no CA Identity Manager. Exemplos de tarefas administrativas incluem Criar usuário, Modificar grupo e View Role Membership.

O CA Identity Manager inclui tarefas administrativas padrão que você pode modificar para atender às suas necessidades de negócios.

Ao criar uma tarefa administrativa personalizada, execute as seguintes etapas:

Observação: a seção Pré-requisitos do Active Directory (na página 63) inclui considerações adicionais quando o CA Identity Manager gerencia um repositório de usuários do Active Directory.

1. No console de usuário do CA Identity Manager, selecione Funções e tarefas, Tarefa administrativa, Criar tarefa administrativa.

   O CA Identity Manager perguntará se deseja criar uma tarefa ou criar uma tarefa com base em uma tarefa existente.

   Por exemplo, selecione a tarefa Modificar usuário como a base da nova tarefa.

2. Selecione Create a Copy of an Existing Task e procure a tarefa a ser copiada.

   Observação: é recomendável modificar a cópia de uma tarefa padrão, em vez de modificar a tarefa padrão diretamente.

3. Após selecionar OK, você verá uma tela com as seis guias a seguir:

Guia	Finalidade	Consulte o tópico
Perfil	Definir o perfil da tarefa que está sendo criada	Definir o perfil da tarefa (na página 44)
Pesquisar	Limitar o intervalo de objetos gerenciados pela tarefa	Definir o escopo da tarefa (na página 49)
Guias	Escolher e projetar as guias para a tarefa	Escolher guias para a tarefa (na página 58)
Campos	Mostrar os campos usados em todas as guias	Exibir os campos na tarefa (na página 62)
Eventos	Selecionar um processo de fluxo de trabalho para cada evento se o ambiente do CA Identity Manager e a tarefa usar fluxo de trabalho	Atribuir processos de fluxo de trabalho para eventos (na página 62)
Uso de função	Exibir as funções que incluem a tarefa que você está modificando ou visualizando	Exibir uso de função (na página 62)

Observação: para obter mais informações sobre a criação de tarefas administrativas personalizadas, consulte o *Guia de Design do Console de Usuário*.

Definir o perfil da tarefa

A guia Perfil contém configurações gerais para a tarefa.

Observação: para obter mais informações sobre as configurações do perfil de tarefa administrativa, consulte o *Guia de Design do Console de Usuário*.

Para definir o perfil da tarefa

1. Escolha o tipo de objeto para a tarefa, que é chamado de objeto principal, e a ação a ser executada nele.
2. Preencha os campos necessários e marque as caixas de seleção apropriadas, conforme necessário, para a tarefa.

   Observação: se você estiver criando uma tarefa que tenha configurações de perfil semelhantes às de uma tarefa existente, clique em Copiar o perfil de outra tarefa. Esta opção preenche as configurações de perfil para a tarefa que está sendo criada com as configurações de perfil de qualquer tarefa existente que você selecionar. Em seguida, você adiciona um nome e uma descrição para a nova tarefa.
3. (Opcional) Associar um manipulador de tarefas de lógica de negócios à tarefa.
4. Depois de preencher essa guia, vá para a próxima etapa, Definir o escopo da tarefa (na página 49).

Guia Admin Task Profile

A guia Admin Task Profile permite definir as configurações gerais para uma tarefa administrativa.

Essa guia contém os seguintes campos:

- **Nome**

  Define o nome da tarefa.
- **Qualificador**

  Define um identificador exclusivo para a tarefa. É usado em URLs, serviços web ou arquivos de propriedades. O qualificador pode conter caracteres ASCII (a-z, A-Z), números (0-9) ou caracteres de sublinhado, começando com uma letra ou sublinhado.
- **Descrição**

  Especifica uma observação opcional sobre a finalidade da tarefa.

- **Ordem das tarefas**

  Especifica a ordem de exibição para a tarefa. Se nenhuma ordem for especificada, as tarefas são exibidas em ordem alfabética.

- **Categoria**

  Especifica uma categoria para a tarefa. As categorias são exibidas como guias na parte superior da tela.

- **Ordem da categoria**

  Especifica a ordem em que a guia de categoria é exibida. Por exemplo, se você configurar a ordem da categoria como 3, a categoria especificada será exibida como a terceira guia.

- **Categoria 2**

  Especifica a categoria de segundo nível, que é exibida como um link abaixo da lista de guias de categoria. A categoria de segundo nível é exibida apenas quando a guia para a categoria de primeiro nível estiver selecionada. Por exemplo, se você criou uma tarefa com a categoria de primeiro nível de Employee e uma categoria de segundo nível de Employee Management, a categoria Employee Management será exibida somente depois de selecionar a guia Employee.

- **Ordem da categoria 2**

  Especifica a ordem em que a categoria de segundo nível aparece, se mais de uma categoria de segundo nível existir em uma categoria principal.

- **Categoria 3**

  Especifica a categoria de terceiro nível, que aparece no painel de navegação esquerdo. As tarefas são listadas na categoria de terceiro nível. Por exemplo, em um ambiente padrão, um usuário com a função Gerente do sistema ou Gerenciador de usuários verá a opção Gerenciar usuários da categoria de terceiro nível quando selecionar a guia Usuários.

- **Ordem da categoria 3**

  Especifica a ordem em que a categoria de terceiro nível é exibida.

- **Objeto principal**

  Especifica o objeto no qual a tarefa opera.

- **Ação**

  Especifica a operação a ser executada no objeto.

- **Sincronização de usuário**

  Especifica se a tarefa sincroniza os usuários com políticas de identidade. É possível selecionar uma das seguintes opções:

  - **Desativado** (padrão)

    Especifica que a tarefa não aciona a sincronização de usuário.

  - **Ao concluir a tarefa**

    Especifica que o CA Identity Manager inicia o processo de sincronização de usuário após a conclusão de todos os eventos em uma tarefa. Essa configuração é a opção de sincronização padrão para as tarefas Criar usuário, Modificar usuário e Excluir usuário. A configuração padrão para todas as outras tarefas é Desativado.

    Observação: se você selecionar a opção Ao concluir a tarefa de uma tarefa que inclui vários eventos, o CA Identity Manager não sincronizará os usuários até que todos os eventos da tarefa sejam concluídos. Se um ou mais desses eventos exigirem uma aprovação de fluxo de trabalho, esse procedimento pode levar vários dias. Para evitar que o CA Identity Manager espere para aplicar as políticas de identidade após a conclusão de todos os eventos, selecione a opção Em cada evento.

  - **Em cada evento**

    Especifica que o CA Identity Manager inicia o processo de sincronização de usuário (na página 462) quando cada evento em uma tarefa for concluído.

    Para tarefas com um evento principal e um secundário para o mesmo usuário, a configuração da sincronização de usuário como Em cada evento pode resultar na aplicação de mais políticas de identidade para um usuário do que na opção Ao concluir a tarefa.

- **Sincronização de conta**

  Sincroniza as contas existentes no servidor de provisionamento, se você tiver ativado o provisionamento.

  - **Desativado** (padrão)

    Especifica que a tarefa não aciona a sincronização de conta.

  - **Ao concluir a tarefa**

    Especifica que o CA Identity Manager inicia o processo de sincronização de conta após a conclusão de todos os eventos em uma tarefa.

- **Em cada evento**

  Especifica que o CA Identity Manager inicia o processo de sincronização de conta quando cada evento em uma tarefa for concluído.

  Observação: para obter um melhor desempenho, selecione Ao concluir a tarefa. No entanto, se você selecionar a opção Ao concluir a tarefa de uma tarefa que inclui vários eventos, o CA Identity Manager não sincronizará as contas até que todos os eventos da tarefa sejam concluídos. Se um ou mais desses eventos exigirem uma aprovação de fluxo de trabalho, esse procedimento pode levar vários dias. Para evitar que o CA Identity Manager espere para sincronizar as contas após a conclusão de todos os eventos, selecione a opção Em cada evento.

- **Ocultar nos menus**

  Impede que a tarefa seja exibida nos menus. Ative este controle se a tarefa for chamada apenas por um URL ou por outra tarefa.

- **Tarefa pública**

  Torna a tarefa disponível para usuários que não fizeram logon no CA Identity Manager. As tarefas públicas padrão são senha esquecida e autorregistro.

- **Ativar a auditoria**

  Registra as informações sobre a tarefa em um banco de dados de auditoria. As informações de auditoria podem ser usadas para gerar relatórios. Consulte o *Guia de Configuração*.

- **Ativar fluxo de trabalho**

  Permite que os eventos do CA Identity Manager associados à tarefa acionem processos de fluxo de trabalho, se você possuir o mecanismo de fluxo de trabalho instalado. Por exemplo, os eventos associados à tarefa Excluir grupo podem acionar um processo de fluxo de trabalho que inclui uma etapa de aprovação.

- **Ativar serviços web**

  Marca a tarefa como um item para o qual a saída da WSDL (Web Services Description Language) pode ser gerada a partir do Management Console. Ative este controle se desejar usar o envio remoto de tarefa. Para obter mais informações, consulte o *Guia de Programação do Java*.

- **Processo de fluxo de trabalho**

  Permite a configuração para fluxo de trabalho em nível de tarefa. Clique no ícone em forma de lápis para configurar o fluxo de trabalho com base em políticas ou sem base em políticas.

- **Prioridade da tarefa**

  Determina a ordem em que o CA Identity Manager executa as tarefas. As tarefas com uma prioridade alta são executadas antes de tarefas com uma prioridade média ou baixa. A prioridade padrão para uma tarefa é média.

  Observação: é possível usar a tarefa Exibir tarefas enviadas para pesquisar tarefas com uma prioridade específica e, em seguida, exibir seus status.

- **Manipuladores de tarefas de lógica de negócios**

  Associa um manipulador de tarefas de lógica de negócios (na página 67) à tarefa.

- **Botões de ação do fluxo de trabalho**

  Adiciona botões de ação personalizados às tarefas de aprovação de fluxo de trabalho.

- **Copiar o perfil de outra tarefa**

  Copia os dados da guia Perfil de outra tarefa.

  Por exemplo, você pode copiar as configurações da guia Perfil da tarefa Modificar usuário e, em seguida, adicionar um nome e descrição.

Propriedades da configuração da tarefa

As propriedades da configuração da tarefa controlam as propriedades de exibição e determinados comportamentos da tarefa.

Caminho do ícone da tarefa

Especifica o URL que um gráfico usa como ícone para essa tarefa em listas de tarefas.

Visualização do ícone da tarefa

Exibe o ícone da tarefa, como ele é exibido em listas de tarefas.

Remover a navegação em tarefas

Quando marcada, oculta a navegação de nível superior e a lista de tarefas, uma vez que um usuário seleciona uma tarefa. Impede os usuários de sair da tarefa atual até que concluam as ações necessárias ou cancelem a tarefa.

Janela de destino

Ao fornecer um valor nesse campo, o CA Identity Manager abre essa tarefa em uma nova janela do navegador. Use esse campo para abrir uma nova janela do navegador para uma tarefa externa que redireciona os usuários para outro site.

Você pode especificar qualquer nome para a janela.

Observação: não use esse campo para abrir tarefas administrativas do CA Identity Manager em uma janela separada do navegador. O CA Identity Manager não oferece suporte a várias janelas do navegador para uma única sessão de usuário do CA Identity Manager.

Definir o escopo da tarefa

Na guia Pesquisar, você define o escopo da tarefa, que limita os objetos disponíveis para a tarefa. Por exemplo, se o objeto de uma tarefa forem usuários, você pode definir o escopo como usuários que são prestadores de serviço.

Observação: se a tarefa não possuir um objeto principal, ou se a ação for modificada, exibida ou aprovada automaticamente, a guia Pesquisar não será exibida.

É possível definir as seguintes configurações na guia Pesquisar:

Tela de pesquisa

A tela de pesquisa limita o escopo da tarefa com base em filtros. Clique em Procurar para ver as opções de tela de pesquisa disponíveis.

Observação: é possível criar sua própria tela de pesquisa (na página 50). Para criar uma versão modificada de uma tela de pesquisa existente, selecione a tela de pesquisa e clique em Copiar. Em seguida, você pode modificar a tela de pesquisa sem alterar a definição da tela de pesquisa original. Para criar uma tela de pesquisa, clique em Novo.

Opções de pesquisa

As opções de pesquisa são exibidas somente quando o objeto for uma função ou um grupo.

- A primeira opção limita a pesquisa com base nos campos que são definidos na tela de pesquisa. Com esses limites, a pesquisa localiza todos os grupos ou funções no escopo do administrador.
- Outras opções limitam a pesquisa conforme indicado.

Observe o seguinte:

- Por padrão, o grupo pesquisa telas com suporte à filtragem. Isso significa que os administradores podem especificar critérios para limitar o escopo das pesquisas de grupo. Para remover o recurso de filtragem, crie uma tela de pesquisa que não contenha campos a serem incluídos em uma consulta de pesquisa.
- *Sem suporte à filtragem*, que é exibido na guia Pesquisar quando o objeto é uma função, significa que a tarefa exibe as funções que atendem aos critérios da opção selecionada. Os campos de pesquisa que são configurados na tela de pesquisa são ignorados.

Os objetos modificados devem permanecer no escopo do administrador

Quando essa caixa de seleção for marcada, o CA Identity Manager exibirá um erro se alterações na tarefa fizerem o administrador perder o escopo sobre o objeto principal. Por exemplo, um administrador pode usar Modificar usuário para alterar um atributo Tipo de funcionário de um usuário para Gerente. Essa alteração poderá colocar o usuário fora do escopo do administrador.

Configuração da tela de pesquisa

Configure uma tela de pesquisa para limitar o escopo da tarefa e controlar os campos nos quais os usuários podem pesquisar. Telas de pesquisa se aplicam a dois tipos de objeto:

- Um *objeto principal* — O objeto a ser modificado ou exibido pela tarefa.
- Um *objeto secundário* — O objeto que está relacionado ao objeto principal.

  Por exemplo, se você incluir uma guia de grupo em uma tarefa de criação de usuários, o usuário será o objeto principal e o grupo será o objeto secundário. A guia de grupo precisa de uma tela de pesquisa de grupos.

  Observação: depois de configurar uma tela de pesquisa, você pode usá-la para qualquer tarefa para procurar um objeto principal ou secundário.

Filtros de pesquisa

Os filtros de pesquisa limitam quais objetos a pesquisa retorna. Por exemplo, se o objeto forem usuários, é possível limitar a pesquisa para localizar apenas prestadores de serviço. Você pode configurar um filtro para encontrar os usuários com Tipo de funcionário definido como prestador de serviço.

É possível configurar os campos a seguir para realizar pesquisas:

Mostrar apenas os objetos em conformidade com as regras abaixo

Define os critérios adicionais a serem combinados com o filtro definido pelo usuário para limitar a pesquisa.

Observe o seguinte ao usar este campo**:**

- Devido às limitações das pesquisas de funções de provisionamento, esses critérios substituem os campos de filtro pelo mesmo nome inserido pelo usuário.
- Os atributos usados quando você configurar este campo não devem ser adicionados como campos de pesquisa disponíveis na tela de pesquisa.

  Por exemplo, se você configurar a tela de pesquisa para exibir somente as funções em que o atributo Ativado é definido como Sim, remova o atributo Ativado da lista de atributos que os usuários podem especificar nos critérios de pesquisa.

  Caso contrário, os critérios inseridos pelo usuário serão ignorados.

Filtro de pesquisa padrão

Define um filtro que, por padrão, é exibido quando um administrador usa a tela de pesquisa. Por exemplo, se estiver configurando uma tela de pesquisa para a tarefa Modify Contractor e souber que os administradores geralmente pesquisam prestadores de serviço com base no nome da empresa de contrato, você poderá definir o filtro padrão como Contract Firm = *. Os administradores podem substituir o filtro padrão, especificando critérios de pesquisa diferentes. A definição de um filtro padrão melhora o desempenho ao limitar o número de resultados retornados se um administrador não especificar um filtro antes de iniciar uma pesquisa.

Selecionar automaticamente todos os resultados de pesquisa quando usados com tarefas de seleção múltipla

Especifica que todos os resultados de pesquisa são selecionados por padrão. Se você marcar essa caixa de seleção, todos os objetos na lista de resultados da pesquisa serão exibidos com uma caixa de seleção ao lado do nome do objeto.

Executar pesquisa automaticamente

Especifica que um campo de pesquisa é exibido com os resultados da pesquisa.

Definir automaticamente a entidade da tarefa quando houver apenas um único resultado de pesquisa

Define o objeto principal da tarefa automaticamente quando somente um objeto corresponde ao filtro de pesquisa.

Por exemplo, suponha que se essa opção seja selecionada para uma tela de pesquisa de usuário que está associada à tarefa Modificar usuário. Quando um administrador abre a tarefa Modificar usuário e digita um filtro de pesquisa que retorna apenas um usuário, o CA Identity Manager abre a tarefa Modificar usuário para esse usuário. O administrador não precisa selecionar o usuário para abrir a tarefa Modificar usuário.

Observação: para que essa configuração seja aplicada, Executar pesquisa automaticamente também deverá ser selecionada.

Salvar filtro de pesquisa

Especifica que o filtro de pesquisa para a tarefa está salvo para o usuário na sessão atual. Na próxima vez que esse usuário pesquisar na tarefa, o filtro de pesquisa salvo será exibido.

Observação: o CA Identity Manager salva o filtro de pesquisa para a duração da sessão do usuário. Quando o usuário efetua logoff, o filtro de pesquisa é desmarcado.

Pesquisar na organização

Exibe um filtro de organização na tela de pesquisa. Se essa caixa de seleção for marcada, os administradores poderão especificar um filtro que limita as organizações nas quais o CA Identity Manager pesquisará um objeto. Você pode especificar valores padrão para o filtro de pesquisa de organização, especificando uma tela de pesquisa no campo Pesquisa de organização.

Salvar a organização da pesquisa

Especifica que a organização para a tarefa é salva se uma organização tiver sido estabelecida para a pesquisa. Na próxima vez em que um usuário pesquisar na tarefa, a organização será exibida.

Pesquisa de organização

Especifica a tela de pesquisa que o CA Identity Manager usa para permitir que os administradores pesquisem uma organização.

Escopo da pesquisa de organização padrão

Especifica o escopo da pesquisa de organização padrão que é exibido quando um administrador usa uma tela de pesquisa. O escopo da pesquisa determina os níveis em uma árvore da organização que são incluídos na pesquisa. Os administradores podem substituir o escopo da pesquisa de organização padrão, especificando critérios de pesquisa diferentes na tela de pesquisa.

Por exemplo, se você configurar uma tela de pesquisa para uma tarefa personalizada Modify Contractor em um ambiente que armazena as informações do prestador de serviço em vários níveis da árvore da organização, é possível definir o escopo da pesquisa de organização padrão como e inferior.

Pesquisa de expressão simples

Define o tipo de filtro de pesquisa que é exibido na tela de pesquisa. Quando essa caixa de seleção for marcada, os usuários poderão especificar um único filtro de pesquisa, como <attribute><comparator><value>. Quando você desmarcar essa caixa de seleção, os usuários poderão especificar vários filtros de pesquisa. Por exemplo, <attribute1><comparator><value1> AND <attribute2><comparator> <value2>. Os objetos que atendem às condições em todos os filtros são retornados nos resultados da pesquisa. No exemplo anterior, objetos que incluem <value1> e <value2> seriam retornados como resultados da pesquisa.

Igual apenas à pesquisa

Proíbe que os administradores usem operadores de pesquisa que não sejam iguais.

Exibir número de resultados

Exibe o número de resultados da pesquisa correspondentes. Quando essa caixa de seleção for marcada, todas as pesquisas retornarão a mensagem "Há X resultados".

Adicionar botão de tarefa para <nome da tarefa>

Adiciona um link para outra tarefa na tela de pesquisa. O link é exibido como um botão.
Esse campo geralmente é usado para adicionar um Criar tarefa a uma tela de pesquisa que esteja configurada para navegação em tarefas-objeto.

Rótulo opcional

Especifica um rótulo para a tarefa selecionada no campo anterior. Esse rótulo aparece no botão para a tarefa.

Adicionar botão de exclusão múltipla para <nome da tarefa>

Adiciona um link para uma tarefa que permite aos administradores selecionar vários objetos a serem excluídos. O link é exibido como um botão.
Esse campo geralmente tem navegação em tarefas-objeto.

Campos de pesquisa e resultados da pesquisa

Em outra parte da tela de pesquisa, você deve selecionar campos que um administrador pode usar em uma consulta de pesquisa e os campos que serão exibidos nos resultados da pesquisa.

Selecione os campos em que um usuário pode pesquisar

Selecione os campos que um administrador pode usar para criar uma consulta de pesquisa.

Para adicionar outros campos, selecione os campos na caixa de listagem abaixo da tabela de campos de pesquisa.

Depois de selecionar os campos, você pode alterar a ordem em que eles aparecem usando os ícones em forma de seta para cima e para baixo, à direita do campo.

Observação: se você não especificar os campos nos quais um administrador pode pesquisar, o CA Identity Manager iniciará a pesquisa automaticamente.

Selecione os campos que são exibidos nos resultados da pesquisa

Selecione os campos que o CA Identity Manager exibe nos resultados da pesquisa. É possível selecionar campos que não estão disponíveis na consulta de pesquisa.

Para adicionar outros campos, selecione os campos na caixa de listagem abaixo da tabela de campos de pesquisa.

Estilo

Ao selecionar um campo a ser exibido nos resultados da pesquisa, você poderá selecionar uma das seguintes opções de estilo:

- **Nome booleano para exibição**

  Exibe o nome do campo para todos os resultados que forem verdadeiros. Por exemplo, se você digitar Ativado como o nome do atributo que indica um status da conta de usuário, "Ativado" será exibido nos resultados da pesquisa para todas as contas de usuário ativas.

- **Marca de seleção**

  Exibe o valor como uma marca de verificação selecionada, com base no valor do atributo. Por exemplo, se você selecionar o estilo da marca de verificação para representar o estado Ativado/Desativado de contas de usuário, o CA Identity Manager exibirá uma marca de verificação selecionada para todas as contas ativas.

- **Sequência de caracteres com vários valores**

  Exibe os valores em um atributo de vários valores em linhas separadas. Os valores são listados em ordem alfabética.

- **Caixa de seleção somente leitura**

  Exibe o valor como uma caixa de seleção de somente leitura.

- **Sequência**

  Exibe o valor como uma sequência de caracteres de texto.

- **Tarefa**

  Adiciona uma lista de tarefas a um campo. Os usuários clicam em um ícone em forma de seta para visualizar uma lista das tarefas que podem ser executadas no objeto associado ao campo de pesquisa. Por exemplo, se você adicionar uma lista de tarefas a um campo Sobrenome nos resultados da pesquisa, os usuários poderão clicar no ícone em forma de seta desse campo para ver uma lista das tarefas que podem ser executadas no usuário selecionado.

  Essa configuração também pode ser usada para fazer com que um valor de atributo seja exibido como um link para uma tarefa.

  Se você selecionar o estilo Tarefa, um ícone em forma de seta para a direita será exibido ao lado da coluna Estilo. Clique na seta para abrir uma caixa de diálogo Propriedades do campo. Use essa caixa de diálogo para configurar uma lista de tarefas.

- **Lista de tarefas**

  Adiciona mais tarefas que os usuários podem executar nos objetos em telas de pesquisa e de lista. Por exemplo, é possível configurar a tela de pesquisa na tarefa Modificar usuário para permitir que os usuários executem uma tarefa, como desativar um usuário, na lista de usuários retornados pela pesquisa.

  Ao selecionar essa opção, é possível determinar se os usuários acessam a tarefa clicando em um ícone ou em um vínculo de texto.

- **Menu de tarefas**

  Adiciona mais tarefas (similar ao estilo Lista de Tarefas) como itens de menu pop-up.

  Ao selecionar essa opção, um botão de ação aparece ao lado de cada objeto em uma tela de pesquisa ou de lista. Os usuários clicam no botão de ação para visualizar a lista de tarefas que podem ser executadas para esse objeto.

Observação: para ver as opções de estilo Lista de tarefas e Menu de tarefas, selecione (Separador) quando adicionar um campo à tabela de resultados da pesquisa. Para obter mais informações sobre como adicionar outras tarefas a telas de pesquisa e de lista, consulte o *Guia de Design do Console de Usuário*.

Classificável

Marque esta caixa de seleção para permitir que os administradores classifiquem os resultados da pesquisa por campo ou campos.

Defina a ordem de classificação padrão para os resultados da pesquisa

Especifica a ordem em que os resultados da pesquisa são exibidos. Os resultados da pesquisa são classificados inicialmente pelo primeiro campo na lista e, em seguida, por cada campo adicional na ordem em que aparecem. Marque a caixa de seleção Decrescente para classificar os resultados em ordem decrescente.

Selecionar objetos com alterações no campo *nome*

Especifica que os objetos nos quais o campo especificado foi alterado são selecionados quando o usuário clica no botão Selecionar.

Retornar *N* resultados por página

Selecione o número de resultados a serem exibidos por página. Quando os resultados da pesquisa excedem o número especificado, o CA Identity Manager exibe um link para cada página de resultados.

Ajuda definida pelo usuário nas telas de pesquisa

Se desejar adicionar texto personalizado à tela de pesquisa, é possível definir o texto na caixa de texto HTML correspondente. É possível adicionar texto nas seguintes áreas:

- Início ou no fim da página
- Antes ou depois da criação
- Antes ou depois dos resultados

Tipos de tela de pesquisa

O CA Identity Manager inclui estas telas de pesquisa pré-configuradas.

Tela de pesquisa de função de acesso

A tela de pesquisa de função de acesso permite configurar filtros de pesquisa para encontrar as funções de acesso que correspondem a determinados critérios.

Tela de pesquisa de tarefa de acesso

A tela de pesquisa de tarefa de acesso permite configurar filtros de pesquisa para encontrar as tarefas de acesso que correspondem a determinados critérios. Essa tela de pesquisa é usada para localizar uma tarefa de acesso para exibir ou modificar, ou para adicionar uma tarefa a uma função de acesso.

Tela de pesquisa de função administrativa

A tela de pesquisa de função administrativa permite configurar filtros de pesquisa para encontrar as funções administrativas que correspondem a determinados critérios.

Tela de pesquisa de tarefa administrativa

A tela de pesquisa de tarefa administrativa permite configurar filtros de pesquisa para encontrar as tarefas administrativas que correspondem a determinados critérios. Essa tela de pesquisa é usada para localizar uma tarefa administrativa para exibir ou modificar, ou para adicionar uma tarefa a uma função administrativa.

Tela de pesquisa de aprovação

A tela de pesquisa de aprovação permite configurar a exibição que aparece na parte superior de uma tarefa de aprovação.

Tela de pesquisa de usuário com certificação inicial

A tela de pesquisa de usuário com certificação inicial permite configurar filtros de pesquisa para localizar usuários e defini-los para exigir certificação. Os usuários selecionados terão seu status de certificação configurado para *exigindo a certificação*.

Tela de pesquisa de certificação de usuário

A tela de pesquisa de certificação de usuário permite configurar os filtros de pesquisa para localizar usuários que exigem certificação.

Tela de pesquisa de delegação

A tela de pesquisa de delegação permite configurar os filtros de pesquisa para localizar outros usuários para adicionar como representantes. Um representante é outro usuário ao qual você poderá conceder temporariamente permissão para exibir e resolver os itens de trabalho do fluxo de trabalho.

Tela de pesquisa Ativar/desativar usuário

A tela de pesquisa Ativar/desativar usuário permite configurar filtros de pesquisa para ativar/desativar os usuários que correspondem a determinados critérios.

Tela de pesquisa de usuário com certificação final

A tela de pesquisa de usuário com certificação final permite configurar filtros de pesquisa para identificar usuários cujo ciclo de certificação deve ser concluído.

Tela da pesquisa de Contrato de Licença de Usuário Final

A tela da pesquisa de Contrato de Licença de Usuário Final permite configurar a tarefa Autorregistro com uma página específica do seu aplicativo com base em identidades.

Pesquisa para a opção Explorar e correlacionar

A tela de pesquisa para a opção Explorar e correlacionar permite configurar filtros de pesquisa para explorar e correlacionar as definições que corresponderem a determinados critérios.

Pesquisa de upload de arquivo do alimentador

A tela de pesquisa de upload de arquivo do alimentador permite procurar pelo arquivo do alimentador para fazer upload. Um arquivo do alimentador é usado para automatizar ações repetidas realizadas em um grande número de objetos gerenciados.

Tela de pesquisa de senha esquecida/Tela de pesquisa de ID de usuário esquecida

A tela de pesquisa de senha esquecida permite configurar a tarefa Senha esquecida para solicitar aos usuários informações que verificam sua identidade.

Tela de pesquisa de grupo

A tela de pesquisa de grupo permite configurar filtros de pesquisa para grupos, como grupos dentro da organização financeira.

Tela de pesquisa de conjunto de políticas de identidade

A tela de pesquisa de conjunto de políticas de identidade permite configurar filtros de pesquisa para localizar conjuntos de políticas de identidade que corresponderem a determinados critérios.

Tela de pesquisa de manipulador de atributos lógicos

A tela de pesquisa de manipulador de atributos lógicos permite configurar filtros de pesquisa para localizar manipuladores de atributos lógicos. Essa tela de pesquisa é usada para localizar um manipulador de atributos lógicos para exibir ou modificar suas configurações.

Tela de pesquisa Gerenciar relatórios

A tela de pesquisa Gerenciar relatórios permite configurar filtros de pesquisa para localizar um relatório para exibir ou excluir.

Tela de pesquisa de usuário não certificado

A tela de pesquisa de usuário não certificado permite configurar filtros de pesquisa para localizar os usuários que não foram certificados até o final do período de certificação.

Tela de pesquisa de organização

A tela de pesquisa de organização permite configurar filtros de pesquisa para limitar a escolha de organizações para determinadas suborganizações.

Tela de pesquisa de função de provisionamento

A tela de pesquisa de função de provisionamento permite configurar os filtros de pesquisa para recuperar funções de provisionamento.

Tela de pesquisa de modelo de conta

A tela de pesquisa de modelo de conta permite configurar os filtros de pesquisa para recuperar modelos de contas.

Tela de pesquisa de política de senha

A tela de pesquisa de política de senha permite configurar os filtros de pesquisa para localizar políticas de senha que correspondem a determinados critérios.

Tela de pesquisa de definição de instantâneo

A tela de pesquisa de definição de instantâneo permite configurar os filtros de pesquisa para localizar uma definição de instantâneo para exibir, modificar ou excluir.

Tela de pesquisa padrão

A tela de pesquisa padrão permite configurar filtros para localizar objetos gerenciados personalizados.

Tela de pesquisa de usuário

A tela de pesquisa de usuário permite configurar filtros de pesquisa para localizar usuários que correspondem a determinados critérios. Por exemplo, é possível procurar por usuários que são prestadores de serviço.

Depois de preencher a guia Pesquisar, vá para Escolher guias para a tarefa.

Escolher guias para a tarefa

Na guia Guias, nomeie e configure as guias. Cada uma delas é um conjunto de campos que você inclui na tarefa. Você pode incluir guias padrão ou criar guias. Por exemplo, a tarefa Modificar usuário inclui as seguintes guias:

- Perfil
- Funções de acesso
- Funções administrativas
- Grupos
- Delegar itens de trabalho

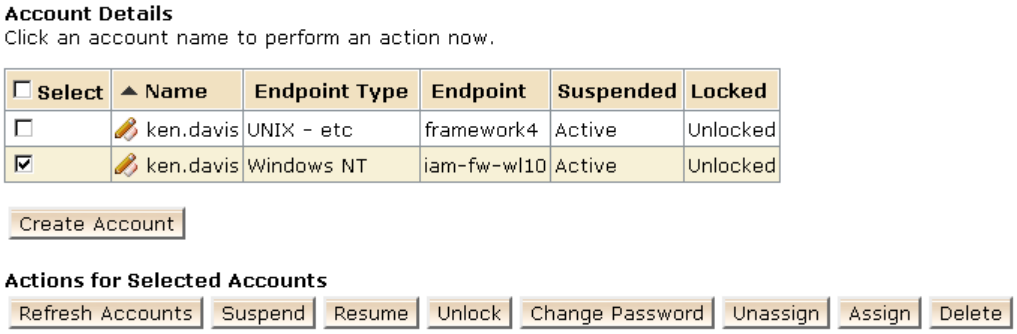
Para editar a definição de uma guia, clique no ícone de edição () ao lado do nome da guia.

Mais informações:

Guias da conta (na página 59)
Guia Programação (na página 61)

Guias da conta

Em geral, a guia Contas é adicionada às tarefas que permitem exibir ou modificar um usuário.



Quando a guia Contas é adicionada a uma tarefa Modificar usuário, os administradores podem executar outras ações nas contas do usuário. Por exemplo:

- Suspender ou retomar uma conta.
- Desbloquear uma conta que tenha sido bloqueada automaticamente devido a um acesso incorreto ou inadequado. Por exemplo, uma conta pode ser bloqueada quando um usuário excede o número aceitável de tentativas de logon sem êxito definido em uma política de senha do CA Identity Manager.
- Alterar a senha do usuário em uma ou mais contas.
- Atribuir e remover a atribuição de contas para um usuário.

Para obter detalhes sobre as outras opções que você pode fornecer na guia Contas, consulte a ajuda do console de usuário para a configuração da guia Contas.

Pré-requisito para usar a guia Contas

Para usar a guia Contas, o CA Identity Manager deve ser configurado com suporte a provisionamento, e o ambiente do CA Identity Manager deve incluir um diretório de provisionamento.

Observação: para configurar o suporte a provisionamento de um ambiente, consulte o *Guia de Configuração*.

Campos na guia Contas

A guia Contas exibe detalhes sobre as contas do usuário nos sistemas do terminal.

Alguns dos campos mais significativos são os seguintes:

- Nome — O nome de logon, nome de email ou outro nome para a conta.
- Tipo de terminal — O tipo de terminal, como um diretório LDAP, que é associado à conta.
- Terminal — O terminal específico que é associado à conta.
- Suspenso — Um dos três estados.
  - Ativo será exibido se a conta estiver ativada.
  - Suspenso será exibido se a conta estiver desativada.
  - Ativação pendente (manual) será exibido se ela não puder ser retomada ou suspensa. Efetue logon no sistema do terminal para retomar ou suspender a conta.
  - Indisponível será exibido se o estado não puder ser recuperado porque não há comunicação com o terminal.
- Bloqueado — Mostra se a conta está bloqueada. O bloqueio ocorre quando um usuário faz várias tentativas de efetuar logon na conta com a senha errada. Indisponível será exibido se o estado não puder ser recuperado porque não há comunicação com o terminal.

Funções adicionais na guia Contas

Quando a guia Contas é incluída em uma tarefa que modifica um usuário, os administradores podem usar essa tarefa para executar funções nas contas do usuário. As funções disponíveis são determinadas pela configuração da guia.

Você pode selecionar quais funções estarão disponíveis usando a opção Modificar tarefa administrativa em uma tarefa que contém a guia Contas. Edite a guia Contas para determinar se funções como Atribuir contas e Remover atribuição de contas estão disponíveis na guia.

Observação: consulte a ajuda online de configuração da guia Contas para obter mais informações.

Guia Programação

A programação permite automatizar a execução de uma tarefa em uma data posterior. Se você programar uma tarefa que esteja associada a um fluxo de trabalho, o CA Identity Manager executará todas as tarefas conforme definido nesse fluxo de trabalho. O status das tarefas programadas pode ser exibido na página Exibir tarefas enviadas.

Uma tarefa programada que ainda não foi executada pelo CA Identity Manager pode ser cancelada na página Exibir tarefas enviadas.

Observação: se uma tarefa programada for cancelada e você reenviar essa tarefa, ela será executada imediatamente, independentemente da hora programada para execução.

O CA Identity Manager fornece o agendador como uma guia especial. Para acessar o agendador, é necessário configurar uma tarefa com a guia Programação.

Adicionar a guia Programação a uma tarefa administrativa

O CA Identity Manager permite programar tarefas para execução em uma data e hora específicas. Para programar uma tarefa, você deve adicionar a guia Programação a uma tarefa administrativa.

Observação: não é possível adicionar uma guia Programação a todas as tarefas administrativas no CA Identity Manager. Se a tarefa não puder ser programada, a guia Programação não estará disponível na tela Modificar tarefa administrativa.

Para adicionar a guia Programação a uma tarefa administrativa:

1. Clique em Funções e tarefas, Tarefa administrativa, Modificar tarefa administrativa.

   A página Selecionar tarefa administrativa é exibida.

2. Selecione Nome ou Categoria no campo de onde e, em seguida, digite a sequência de caracteres para pesquisa e clique em Pesquisar.

   O CA Identity Manager exibe as tarefas administrativas que atendem aos critérios de pesquisa.

3. Escolha uma tarefa administrativa e clique em Selecionar.

   O CA Identity Manager exibe os detalhes da tarefa para a tarefa administrativa selecionada.

4. Clique em Guias.

   As guias configuradas para a tarefa administrativa selecionada são exibidas.

5. Selecione Programação na lista suspensa Quais guias devem aparecer nesta tarefa?

   e clique em  .

   A guia Programação é adicionada à lista de guias que serão exibidas na tarefa administrativa selecionada.

6. Clique em Enviar.

   A guia Programação é adicionada à tarefa administrativa selecionada.

Exibir os campos na tarefa

Na guia Campos, você exibe os campos que se aplicam a essa tarefa. Esses campos são aqueles criados nas guias para essa tarefa. Para alterar os campos usados, retorne à guia Guias e selecione a guia que exige a alteração.

Depois de preencher essa guia, vá para a próxima etapa, Atribuir processos de fluxo de trabalho para eventos (na página 62).

No entanto, se esse ambiente do CA Identity Manager não usar o fluxo de trabalho, você pode clicar em Enviar. Uma mensagem é exibida, indicando se a tarefa foi executada com êxito. Se for bem-sucedida, você poderá adicionar a tarefa a uma função, de forma que os integrantes da função possam começar a usar a tarefa.

Exibir uso de função

Na guia Uso de função, você pode visualizar as funções que incluem a tarefa que estiver sendo exibida ou modificada.

Os proprietários de funções podem adicionar e remover tarefas das funções.

Observação: a opção Funções administrativas padrão fornece uma lista de tarefas nas funções administrativas que estão instaladas no CA Identity Manager por padrão.

Atribuir processos de fluxo de trabalho para eventos

Se você tiver ativado o fluxo de trabalho para esse ambiente do CA Identity Manager, use a guia Eventos para selecionar um processo de fluxo de trabalho para cada evento que a tarefa iniciar. O processo de fluxo de trabalho que você selecionou substitui aquele selecionado por padrão no Management Console do CA Identity Manager.

Para obter mais detalhes sobre os mapeamentos padrão de fluxo de trabalho, consulte o capítulo sobre configurações avançadas do *Guia de Configuração*.

Para concluir a criação dessa tarefa, clique em Enviar. Uma mensagem é exibida, indicando se a tarefa foi executada com êxito. Se for bem-sucedida, você poderá adicionar a tarefa a uma função, de forma que os integrantes da função possam começar a usar a tarefa.

Gerenciar um armazenamento de usuários do Active Directory

Se o Active Directory for o repositório de usuários, antes de criar tarefas administrativas, talvez seja necessário configurar determinados recursos do Active Directory.

O atributo sAMAccountName

O atributo sAMAccountName se aplica a usuários e grupos. Esse atributo é obrigatório e deve ser incluído nas telas de tarefas usadas para criar usuários e grupos.

Observação: ao criar usuários, o valor do atributo sAMAccountName não pode exceder 20 caracteres. Essa restrição não se aplica a grupos.

Você pode criar um manipulador de atributos lógicos personalizado que gera um sAMAccountName exclusivo automaticamente quando um usuário ou um grupo é criado. Nesse caso, você pode incluir o atributo sAMAccountName como um campo oculto nas telas Criar usuário e Criar grupo.

Consulte o capítulo sobre atributos lógicos no *Guia de Programação do Java* para obter mais informações.

Tipo e escopo do grupo

No Active Directory, há dois tipos de grupo:

- Segurança - Listado nas ACLs (Access Control Lists - Listas de Controle de Acessos), que definem permissões para recursos e objetos.
- Distribuição - Usado para agrupar objetos, como usuários e grupos. Grupos de distribuição não podem ser usados para conceder privilégios no Active Directory.

Cada tipo de grupo possui um escopo que determina o seguinte:

- Local de integrantes - Onde os possíveis integrantes podem residir
- Permissões - Onde o grupo pode ser usado para privilégios de acesso (se o grupo for um grupo de segurança)
- Associação do grupo a outros grupos - O local dos grupos aos quais esse grupo pode pertencer

Cada tipo de grupo pode ter um dos seguintes escopos:

Escopo	Local de integrantes	Permissões	Associação do grupo a outros grupos
Universal	Os integrantes do grupo podem ser grupos universais, grupos globais e usuários de qualquer domínio da floresta.	Podem ser usadas para conceder acesso de qualquer domínio em uma floresta.	Podem ser integrantes de grupos de local de domínio e de grupos universais de qualquer domínio da floresta.
Global	Os integrantes do grupo podem ser grupos globais e usuários localizados no mesmo domínio que o grupo.	Podem ser usadas para conceder acesso de qualquer domínio em uma floresta.	Podem ser integrantes de grupos globais, de local de domínio e de grupos universais de qualquer domínio da floresta.
Local de domínio	Os integrantes do grupo podem ser grupos universais, grupos globais e usuários de qualquer domínio da floresta. Os integrantes também podem ser grupos locais de domínio no mesmo domínio.	Podem ser usadas apenas para conceder acesso ao domínio no qual o grupo está localizado.	Só pode ser integrante de outros grupos locais de domínio no domínio.

Tipo e escopo do grupo não são atributos obrigatórios; no entanto, se você não especificar o tipo e o escopo do grupo, o Active Directory criará um grupo de segurança com escopo global.

Para criar grupos de um tipo diferente, você pode criar um manipulador de atributos lógicos personalizado. Consulte o capítulo sobre atributos lógicos no *Guia de Programação do Java*.

Após configurar esses recursos do Active Directory, vá para a próxima etapa: Criar uma tarefa administrativa.

Tarefas externas para funções de aplicativo

Uma tarefa externa faz o seguinte:

- Permite que um administrador execute uma função em um aplicativo que não seja o CA Identity Manager no console de usuário.
- Como opção, passa informações para o aplicativo para gerar tarefas específicas de usuário, grupo ou organização.

Por exemplo, uma tarefa externa pode passar informações sobre uma organização a um aplicativo que gera pedidos de compra. O administrador que está executando a tarefa pode exibir os pedidos de compra em aberto para a organização no console de usuário.

É possível exibir tarefas externas ao abrir o aplicativo em uma nova janela do navegador, ou mostrá-las como guias em uma tarefa administrativa do CA Identity Manager.

Duas guias estão disponíveis para tarefas externas. Elas são configuradas da mesma maneira; no entanto, funcionam de forma diferente.

- A Guia externa é uma guia visual, o que significa que a tarefa exibe o conteúdo do URL dentro de uma guia.
- O URL externo é uma guia não visual, o que significa que a tarefa redireciona para o URL digitado.

A Guia externa

Uma guia externa pode ser adicionada a qualquer tarefa Criar, Exibir ou Modificar para torná-la uma tarefa externa. Por exemplo, se você adicionar uma Guia externa a uma tarefa Criar usuário, a guia aparecerá nessa tarefa.

Para uma guia externa:

- Nenhum evento é gerado para uma tarefa externa.
- É possível, como opção, usar objetos gerenciados.

- No campo URL externo, você pode especificar o endereço do aplicativo como:
  - Um endereço completo, incluindo o nome de domínio totalmente qualificado, por exemplo:

    http://server1.mycompany.org/report/viewUserReport
  - Um caminho relativo, por exemplo:

    /report/viewUserReport

    Se você especificar o caminho relativo, o CA Identity Manager acrescentará automaticamente o nome de domínio totalmente qualificado do servidor em que o CA Identity Manager está instalado.
- É possível configurar os atributos a serem transmitidos ao aplicativo na guia Perfil.
- É possível incluir ou excluir o DN de administrador ou o nome da tarefa no URL.

A guia URL externo

Você pode adicionar uma guia URL externo a uma tarefa de exibição, por exemplo, Exibir usuário. Ao usar a tarefa Exibir usuário, você será redirecionado para o site identificado pelo URL. Nenhuma outra guia ficará visível.

Para uma guia URL externo:

- A guia URL externo deve ser a única guia na tarefa. Se houver outras guias associadas à mesma tarefa, a guia externa não redirecionará os usuários para o URL especificado.
- A tarefa pode gerar eventos que podem ser auditados.
- No campo URL externo, você pode especificar o endereço do aplicativo como:
  - Um endereço completo, incluindo o nome de domínio totalmente qualificado, por exemplo:

    http://server1.mycompany.org/report/viewUserReport
  - Um caminho relativo, por exemplo:

    /report/viewUserReport

    Se você especificar o caminho relativo, o CA Identity Manager acrescentará automaticamente o nome de domínio totalmente qualificado do servidor em que o CA Identity Manager está instalado.
- É possível, como opção, usar objetos gerenciados.
- Você pode configurar os atributos a serem passados para o URL.

  Forneça um URL para o aplicativo que deseja iniciar e inclua os atributos que devem ser passados para o aplicativo.
- É possível incluir ou excluir o DN de administrador ou o nome da tarefa no URL.

Componentes avançados de tarefas

Os componentes avançados de tarefas permitem especificar um processamento personalizado para uma tarefa:

- A validação em nível de tarefa valida um valor de atributo com base em outros atributos da tarefa. Por exemplo, você pode validar se o código de área de um número de telefone fornecido pelo usuário é apropriado para a cidade e o estado desse usuário.
- Os manipuladores de tarefas de lógica de negócios (na página 67) executam lógicas de negócios personalizadas antes que uma tarefa do CA Identity Manager seja submetida para processamento. Normalmente, a lógica de negócios personalizada valida os dados. Por exemplo, um manipulador de tarefas de lógica de negócios pode verificar o limite de associação a um grupo antes que o CA Identity Manager adicione um novo integrante ao grupo. Se o limite de associação ao grupo for atingido, o manipulador de tarefas de lógica de negócios exibirá uma mensagem informando o administrador do grupo de que o novo integrante não pôde ser adicionado.

Criar manipuladores de tarefas de lógica de negócios

Um nome de classe totalmente qualificado de um manipulador de tarefas de lógica de negócios é definido da seguinte maneira:

1. Crie ou modifique uma tarefa administrativa.
2. Na guia Admin Profile, clique em Manipuladores de tarefas de lógica de negócios.

   A tela Manipuladores de tarefas de lógica de negócios é exibida. Essa tela lista os manipuladores de tarefas de lógica de negócios existentes e atribuídos à tarefa. O CA Identity Manager executa os manipuladores na ordem em que aparecem na lista.
3. Clique em Adicionar.

   A tela Detalhes do manipulador de tarefas de lógica de negócios é exibida.

Use a tela Detalhes do manipulador de tarefas de lógica de negócios para definir as seguintes informações para o manipulador de tarefas de lógica de negócios que estiver atribuindo à tarefa:

Nome

O nome que está sendo atribuído ao manipulador de tarefas de lógica de negócios.

Descrição

Uma descrição opcional do manipulador de tarefas de lógica de negócios.

Classe Java

Se o manipulador de tarefas de lógica de negócios for implementado em Java, o nome de classe totalmente qualificado desse manipulador de tarefas de lógica de negócios, por exemplo:

com.mycompany.MyJavaBLTH

O CA Identity Manager espera que o arquivo da classe esteja localizado no diretório raiz designado para arquivos de classe Java personalizados. Para obter informações sobre a implantação de arquivos de classe Java, consulte o *Guia de Programação do Java*.

Nome de arquivo do JavaScript

Se o manipulador de tarefas de lógica de negócios for implementado no JavaScript e o código JavaScript estiver contido em um arquivo, especifique o nome do arquivo nesse campo. Por exemplo, talvez você deseje colocar o JavaScript em um arquivo, se o manipulador de tarefas de lógica de negócios for ser usado por várias telas de tarefas.

O CA Identity Manager espera que o arquivo esteja localizado no diretório raiz designado para arquivos JavaScript personalizados. Para obter informações sobre a implantação de arquivos JavaScript, consulte o *Guia de Programação do Java*.

Se você armazenar o arquivo em um subdiretório da raiz, inclua o nome do subdiretório quando especificar o nome do arquivo JavaScript - por exemplo:

JavaScriptSubDir\MyJavaScriptBLTH.js

As barras devem ser apropriadas para a plataforma onde o arquivo JavaScript está implantado.

JavaScript

Você pode implementar um manipulador de tarefas de lógica de negócios JavaScript digitando o código JavaScript inteiro nesse campo, em vez de em um arquivo. Por exemplo, talvez você deseje colocar o JavaScript nesse campo se o script for muito curto ou se não for ser usado com outras telas de tarefas.

Propriedade e valor

Com implementações Java, esses campos são pares de nome/valor opcionais de dados que são passados para o método init() do manipulador de tarefas de lógica de negócios Java, para serem usados de acordo com a necessidade da lógica de negócios do manipulador.

Para adicionar uma propriedade definida pelo usuário, especifique um nome de propriedade e valor, e, em seguida, clique em Adicionar.

Observação: se você adicionar um manipulador de tarefas de lógica de negócios Java, o servidor do aplicativo deve ser reiniciado para que o manipulador seja carregado.

Tarefas administrativas e eventos

As tarefas administrativas incluem *eventos*, ações que o CA Identity Manager executa para concluir a tarefa. Uma tarefa pode incluir vários eventos. Por exemplo, a tarefa Criar usuário pode incluir eventos que criam o perfil do usuário, adicionam o usuário a um grupo e atribuem funções.

O CA Identity Manager auditora eventos, aplica regras de negócios específicas para clientes que são associadas aos eventos e, quando os eventos são mapeados para os processos de fluxo de trabalho, exige aprovação para eventos.

Se vários eventos forem gerados para uma tarefa, e os eventos forem mapeados para os processos de fluxo de trabalho, todos os processos de fluxo de trabalho deverão ser concluídos antes que o CA Identity Manager possa concluir a tarefa.

Eventos principais e secundários

Geralmente, os eventos são independentes de outros eventos. Entretanto, algumas tarefas são associadas a um evento principal e a um ou mais eventos secundários:

- Uma falha de um evento principal resulta na rejeição automática de todos os seus eventos secundários. Por exemplo, se CreateUserEvent falhar, não há necessidade de AddToGroupEvent ocorrer para o usuário. Também resulta no cancelamento da tarefa associada.
- Uma falha de um evento secundário não afeta o êxito ou a falha de quaisquer outros eventos executados para a tarefa ou a execução da própria tarefa. Por exemplo, em uma tarefa Criar usuário, AddToGroupEvent pode ser recusado, o que significa que o novo usuário não poderá ser adicionado a um grupo específico. O usuário ainda pode ser criado (CreateUserEvent), atribuído a funções de provisionamento (AssignProvisioningRoleEvent) e até mesmo adicionado a outros grupos.

Exibir os eventos de uma tarefa

É possível exibir os eventos que estão associados a uma tarefa no console de usuário do CA Identity Manager.

Para exibir os eventos de uma tarefa

1. Selecione Funções e tarefas e Exibir tarefa administrativa no console de usuário.
2. Procure e selecione a tarefa apropriada.
3. Selecione a guia Eventos.

   O CA Identity Manager exibe os eventos que estão associados à tarefa atual.

Eventos gerados para perfis não modificados

Cada objeto de usuário, grupo e organização contém um conjunto de atributos físicos que são armazenados no diretório do usuário. Se um atributo físico de um desses objetos for alterado em uma guia do perfil, o CA Identity Manager gerará um evento Modify depois que o usuário enviar a tarefa. Por exemplo, se um atributo *Cargo* for alterado na guia Perfil do usuário, o CA Identity Manager gerará o evento ModifyUserEvent.

Se um objeto de usuário, grupo ou organização for representado em uma guia do perfil, mas nenhum atributo físico tiver sido alterado quando o usuário clicar em Enviar, o CA Identity Manager não gerará um evento Modify. Em vez disso, o respectivo evento View será gerado, da seguinte maneira:

- ViewUserEvent é gerado em vez de ModifyUserEvent
- ViewGroupEvent é gerado em vez de ModifyGroupEvent
- ViewOrganizationEvent é gerado em vez de ModifyOrganizationEvent

Processamento de tarefas administrativas

O tempo necessário para processar uma tarefa depende das etapas envolvidas. Quando uma tarefa é enviada para processamento, o CA Identity Manager executa as seguintes etapas:

1. O CA Identity Manager valida os dados que estão sendo enviados.

   Isso é chamado de *fase síncrona*.

2. Se a tarefa exigir aprovação, o CA Identity Manager envia a tarefa para o mecanismo de fluxo de trabalho.

   a. O mecanismo de fluxo de trabalho determina os aprovadores e coloca a tarefa de aprovação nas listas de tarefas desses aprovadores.

   b. Como opção, o CA Identity Manager envia um email notificando os aprovadores sobre o item de trabalho pendente.

   c. Um aprovador reserva o item de trabalho (o que remove o item das listas de tarefas de outros aprovadores) e aprova ou recusa esse item.

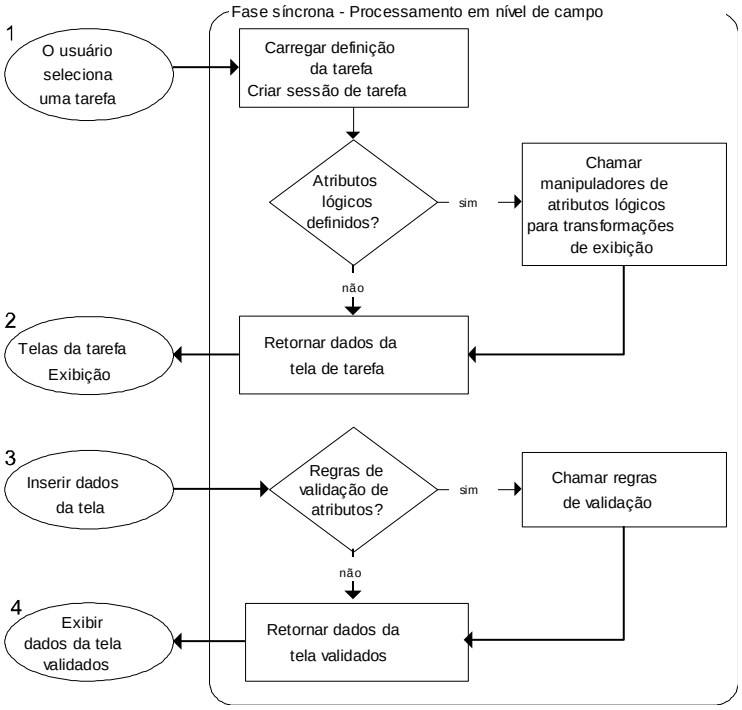
   d. Como opção, o CA Identity Manager envia um email notificando os usuários envolvidos sobre o status da tarefa.

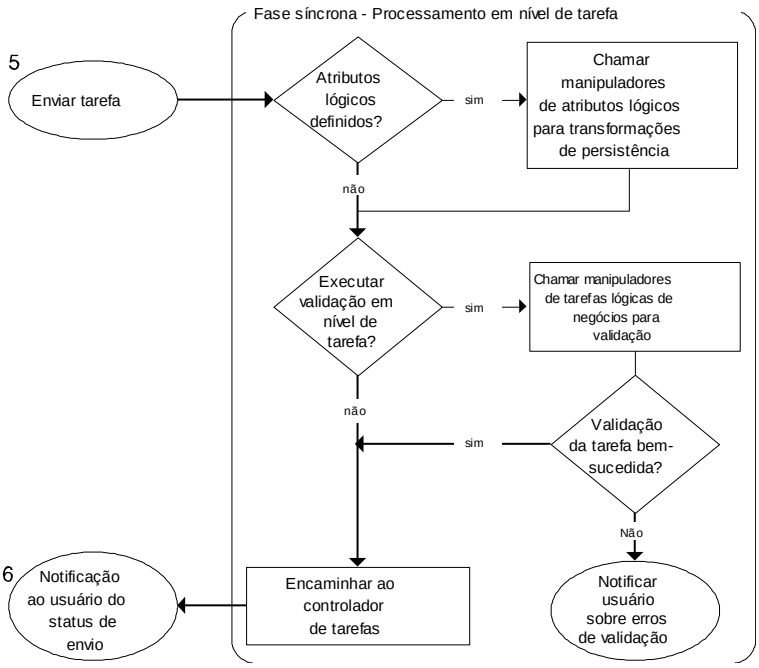
   Isso é chamado de *fase assíncrona*.

3. O CA Identity Manager executa a tarefa, se ela não tiver sido recusada.

Processamento da fase síncrona

Durante a fase síncrona, o CA Identity Manager pode transformar e validar os dados que os usuários inserem nas telas de tarefas, além de aplicar lógica de negócios nesses dados antes que a tarefa seja enviada para processamento. O diagrama a seguir fornece uma descrição de alto nível do que ocorre durante essa fase.

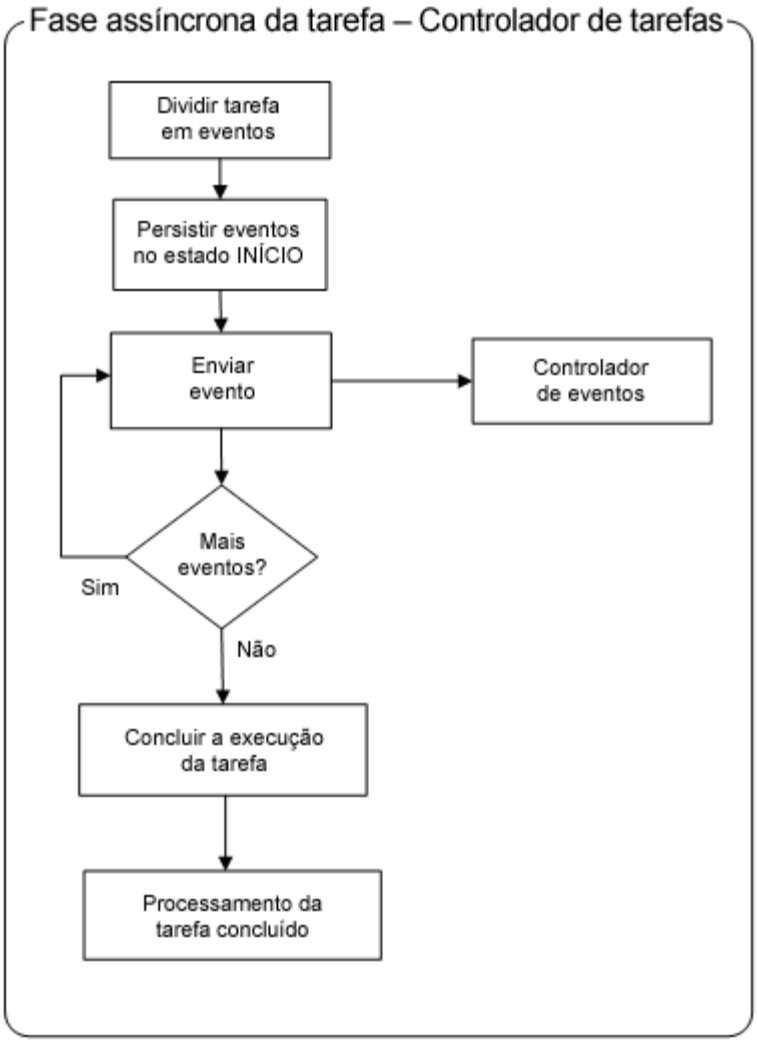




Processamento da fase assíncrona

Após a conclusão da fase síncrona, a tarefa entra na fase assíncrona para execução. Durante essa fase, uma tarefa gera um ou mais eventos. Esses eventos podem ser definidos pelo usuário, como criar um perfil de usuário ou adicionar um usuário a um grupo, ou gerados pelo sistema, como gravar informações no log de auditoria.

O controlador de tarefas, um componente do CA Identity Manager Server, é responsável pelo ciclo de vida de uma tarefa e de seus eventos, conforme mostrado na ilustração a seguir:



Para a maioria dos eventos, o ciclo de vida, a execução e as ações são independentes de qualquer outro evento. (As tarefas de criação exigem que o evento de criação do objeto principal seja executado antes de quaisquer eventos secundários.)

Normalmente, um evento passa pelos seguintes estados:

- Início
- Pendente
- Aprovado
- Executar
- Concluído
- Enviar

Observação: o CA Identity Manager fornece ganchos, chamados EventListeners, que "escutam" um determinado evento ou grupo de eventos. Quando o evento ocorre, o ouvinte de eventos executa uma lógica de negócios personalizada que é apropriada para o evento e para o estado do evento atual. Você pode usar a API do ouvinte de eventos para criar ouvintes de eventos personalizados. Consulte o *Guia de Programação do Java* para obter mais informações.

Imagens para tarefas administrativas

Você pode criar imagens para usar em tarefas administrativas que coloca na página inicial.

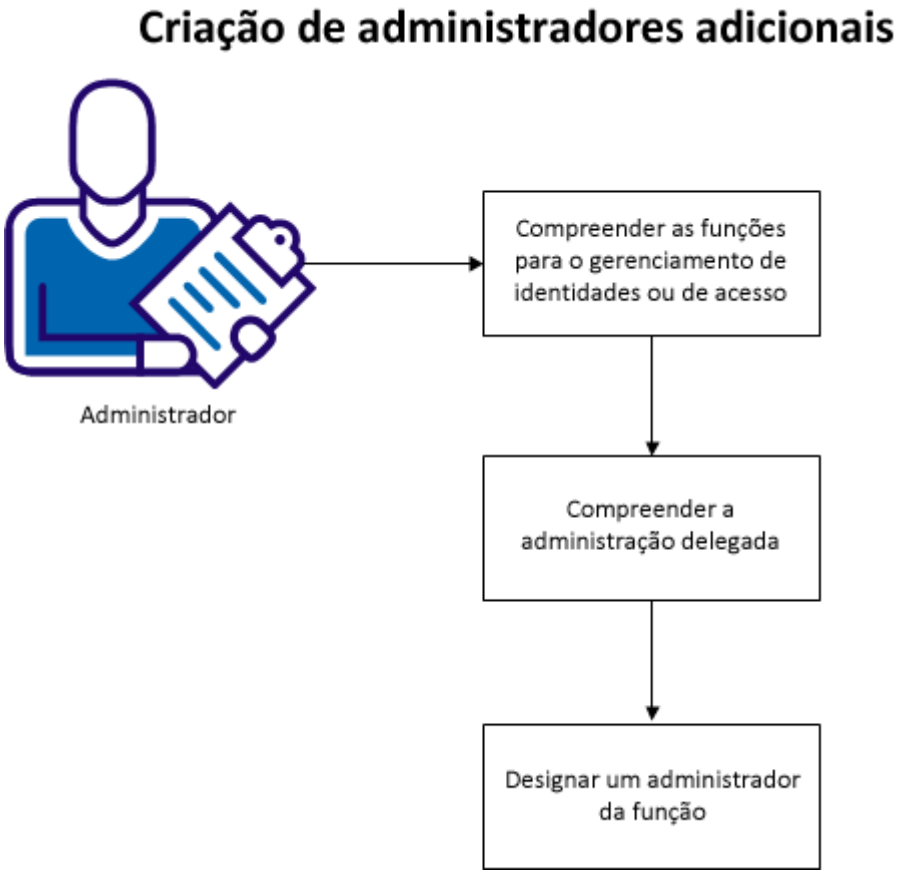
Capítulo 4: Administradores e usuários

Esta seção contém os seguintes tópicos:

Criando administradores

Você pode ser o único responsável por conceder todas as funções aos usuários em seu sistema. Também é possível compartilhar o trabalho de concessão de funções de usuário ao designar administradores adicionais. Essa abordagem é chamada de *administração delegada*.

O diagrama a seguir mostra as informações que precisam ser entendidas, e as etapas a serem executadas, na criação de administradores adicionais.



Os tópicos a seguir explicam como criar administradores adicionais:

- Funções para gerenciamento de acesso e identidades (na página 18)
- Administração delegada (na página 76)
- Designar um administrador de função (na página 77)

Funções para gerenciamento de acesso e identidades

Para ativar o gerenciamento de identidades de usuário e do respectivo acesso a outras contas, o CA CloudMinder fornece os seguintes tipos de função:

Tipo de função	Finalidade
Função administrativa	Contém tarefas administrativas de forma que, quando um usuário recebe essa função, ele pode trabalhar no CA CloudMinder, executando tarefas como alterar a senha de um usuário ou associação de grupo. As funções administrativas também podem incluir qualquer tarefa que aparecer no console de usuário.
Função de provisionamento	Contém modelos de conta que definem contas existentes em terminais gerenciados, como um sistema de email. Os modelos de conta também definem como os atributos do usuário são mapeados para contas.
Função de acesso	As funções de acesso fornecem uma maneira adicional de fornecer direitos no CA Identity Manager ou outro aplicativo. Por exemplo, você pode usar as funções de acesso para executar as seguintes ações: ■ Fornecer acesso indireto a um atributo de usuário. ■ Criar expressões complexas. ■ Definir um atributo de perfil que outro aplicativo pode usar para determinar direitos.

Administração delegada

A administração delegada é o uso de funções para compartilhar o trabalho de gerenciar usuários e conceder acesso ao aplicativo.

Para cada função no sistema, um usuário pode atender a uma ou mais das seguintes funções:

Função	Definição
Proprietário da função	Modifica a função.
Administrador da função	Atribui a função aos usuários e a outros administradores de função.

Função	Definição
Integrante da função	Usa a função para executar tarefas administrativas ou de acesso ou para usar uma conta do terminal.

Ao dividir essas funções entre usuários, você pode compartilhar o trabalho de gerenciar uma função. Por exemplo, é possível que os administradores de nível inferior gerenciem a associação de função e os administradores de nível superior modifiquem a função.

É possível implementar a administração delegada das seguintes maneiras:

- Designe diretamente um usuário como um administrador de uma determinada função.
- Configure *regras administrativas* para uma função. As regras administrativas definem quais usuários podem ser administradores de uma função. O sistema cria administradores adicionais automaticamente quando os usuários atendem aos critérios especificados nas regras.

  Observação: apenas um administrador com privilégios para modificar uma função pode configurar regras administrativas para essa função. Normalmente, os administradores de sistema executam essa atividade. Para configurar regras administrativas que deleguem automaticamente a administração para uma função, consulte a seção intitulada Funções administrativas na seção Informações de referência da Ajuda online.

Designar um administrador de função

Você pode designar um usuário como administrador de uma função. O administrador pode então atribuir a função a outros usuários.

Siga estas etapas:

1. Efetue logon no Console de usuário como um usuário com tarefas de gerenciamento de função.
2. Selecione Tarefas, Funções e tarefas.
3. Selecione uma das seguintes tarefas:
   - Funções administrativas, Modificar integrantes/administradores da função administrativa
   - Funções de provisionamento, Modificar integrantes/administradores da função de provisionamento
   - Funções de acesso, Modificar integrantes/administradores da função de acesso

Uma tela de pesquisa é exibida.

4. Selecione a função que pretende atribuir ao usuário.
5. Clique na guia Administradores.

   Uma lista de administradores de função atuais é exibida.

6. Clique em Adicionar um usuário.

   Uma tela de pesquisa é exibida.

7. Procure o usuário que deseja adicionar como um administrador e clique em Selecionar.

   Uma lista atualizada de administradores de função é exibida.

8. Clique em Enviar.

   O usuário se torna um administrador da função. Essa etapa conclui o processo de delegação da administração de uma função de provisionamento. Agora o administrador pode atribuir a função a outros usuários, concedendo acesso a contas de terminal associadas.

Etapas de delegação

A administração delegada ocorre da seguinte forma:

1. Um administrador cria a função com regras para quem é um proprietário, administrador ou integrante da função.
2. Um proprietário da função modifica a função, quando alterações são necessárias.
3. Um administrador de função:
   - Atribui mais administradores de função (opcional).
   - Atribui mais integrantes da função (opcional).

   Alguns usuários já são administradores ou integrantes da função ao atender às regras definidas na função.

4. Um integrante da função usa a função:
   - Um integrante da função administrativa gerencia usuários e outros objetos no ambiente do CA Identity Manager.
   - Um integrante da função de acesso executa funções em aplicativos corporativos.
   - Um integrante da função de provisionamento usa as contas definidas pelas políticas na função.

Exemplo de delegação

Você pode criar uma função com regras para quem pode ser um integrante ou administrador. Em seguida, você pode atribuir a função, de modo que outros usuários (que ainda não atendam às regras) possam se tornar um integrante ou administrador da função.

Considere o exemplo a seguir de administradores que gerenciam os direitos de aplicativo corporativo de usuários finais:

- Jeff é o proprietário da função Contador; assim, quando a função requer alterações, Jeff a modifica.
- David e Lisa são administradores dessa função. Eles atribuem usuários regionais como integrantes da função.
- Outros usuários são integrantes da função sem serem atribuídos como integrantes da função. Em vez disso, eles atendem à regra para serem integrantes da função.

  Os integrantes da função usam a função Contador para gerar pedidos de compra e executar outras tarefas em aplicativos financeiros.

A seção Características da função fornece detalhes sobre regras e outras características de uma função.

Criação de usuários

Os perfis de usuário permitem aos administradores gerenciar as informações do usuário; gerenciar privilégios, aplicativos e acesso a serviços; e conceder aos usuários o autogerenciamento de contas e serviços. A criação de perfis de usuário é uma tarefa comum para um administrador do sistema.

Durante a criação e a configuração de um usuário, considere os seguintes elementos de conta de usuário:

Tarefas de autoatendimento: os perfis de usuário estão configurados por padrão para conceder ao usuário acesso a determinadas tarefas de autoatendimento como, por exemplo, alterar a senha e as informações do perfil. Um administrador do sistema com tarefas apropriadas pode modificar quais as tarefas de autoatendimento são concedidas a um usuário por padrão.

Grupos: os grupos simplificam o gerenciamento de função. Por exemplo, um administrador do sistema com as tarefas adequadas pode configurar várias funções para que o sistema atribua automaticamente a um usuário que for adicionado como integrante de um grupo.

Funções administrativas: as funções administrativas definem as tarefas que podem ser executadas por um usuário no console de usuário. Por exemplo, uma tarefa pode permitir que um usuário modifique as informações da conta de usuário, como endereço ou cargo. Outra tarefa poderá permitir que o usuário administre tarefas como, por exemplo, conceder uma associação de usuário em um grupo. Ao atribuir uma função administrativa a um usuário, ele poderá executar as tarefas associadas à função.

Contas de terminal e funções de provisionamento: as contas existentes em outros sistemas são chamadas de contas de terminal. Você pode atribuir contas em terminais a usuários do CA CloudMinder por meio de funções de provisionamento. Por exemplo, um usuário precisa de uma conta do Exchange para email, uma conta do Oracle para acesso ao banco de dados e uma conta do Active Directory para usar um sistema do Windows. Ao atribuir uma função de provisionamento a um usuário, o usuário recebe as contas de terminal que a função de provisionamento especifica.

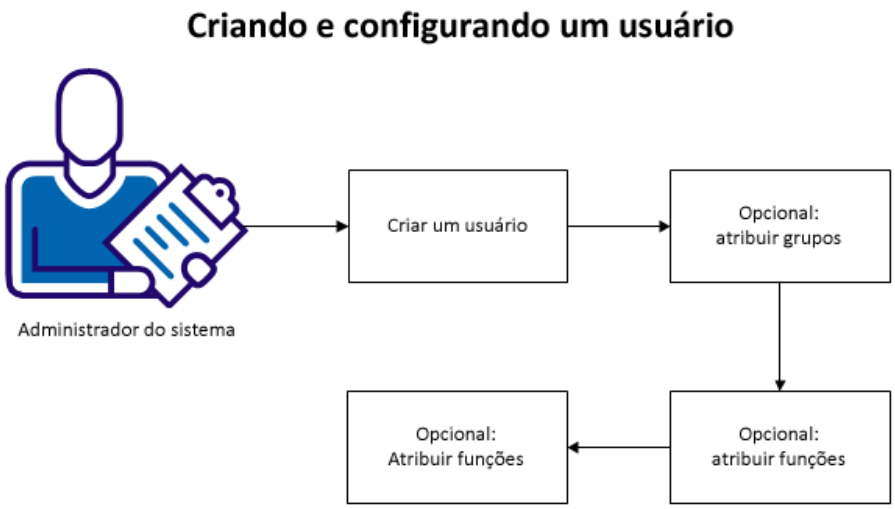
Funções de acesso: as funções de acesso fornecem uma maneira adicional de fornecer direitos no CA Identity Manager ou outro aplicativo. Por exemplo, você pode usar as funções de acesso para realizar as seguintes tarefas:

- Fornecer acesso indireto a um atributo de usuário.
- Criar expressões complexas.
- Definir um atributo em um perfil de usuário, que é usado por outro aplicativo para determinar os direitos.

Serviços: os serviços permitem combinar tarefas de usuário, funções, grupos e atributos de sua escolha em um único pacote. Você pode gerenciar esse pacote de privilégios como um conjunto. Por exemplo, todos os novos funcionários de Vendas precisam acessar um conjunto de tarefas, contas em sistemas específicos do terminal e informações adicionadas aos seus perfis de contas de usuários. Quando você atribui um serviço a um usuário, o usuário recebe o conjunto inteiro de funções, tarefas, grupos e atributos de conta que o serviço especifica.

Políticas de senha: as políticas de senha gerenciam senhas de usuários por meio da aplicação de regras e restrições que controlam a expiração, composição e uso da senha. Se o administrador do sistema tiver criado políticas de senha para o seu ambiente, essas políticas serão aplicadas automaticamente aos novos usuários que corresponderem a uma ou mais regras de políticas de senha. Um administrador do sistema com as tarefas adequadas pode modificar as políticas de senha.

O diagrama a seguir mostra as informações necessárias para compreender, e as etapas a serem executadas para criar e configurar um usuário.



Os tópicos a seguir explicam como criar usuários em detalhes e como configurá-los.

1. Criar um usuário (na página 81)
2. Atribuir grupos (na página 82) (se necessário)
3. Atribuir uma função a um usuário (na página 82) (se necessário)
4. Atribuir serviços (na página 83) (se necessário)

Criar o perfil de usuário

Use este procedimento para criar um perfil de usuário. Dependendo de como a tarefa Criar usuário estiver configurada, também é possível usar essa tarefa para definir outros elementos do perfil. Você pode adicionar um usuário a um grupo, ou tornar o usuário integrante de uma função administrativa ou de provisionamento.

Siga estas etapas:

1. Efetue logon no console de usuário como um usuário com as tarefas de gerenciamento de usuários.

   A função padrão Gerenciador de usuários concede as tarefas adequadas.

2. Selecione Tarefas, Usuários, Gerenciar usuários, Criar usuário.

   A tarefa Criar usuário é exibida.

3. Preencha os campos das informações de perfil de usuário, conforme necessário.
4. Clique em Avançar.
5. Preencha os campos das outras guias da tarefa, se aplicável.

   Por exemplo, adicione o usuário a um grupo ou atribua uma função administrativa, função de provisionamento, ou serviço ao usuário, se essas opções estiverem disponíveis.
6. Clique em Concluir.

   O usuário é criado.

Atribuir um grupo a um usuário

É possível tornar um usuário um integrante de um grupo.

Siga estas etapas:

1. Efetue logon no console de usuário como um usuário com as tarefas de gerenciamento de usuários.
2. Selecione Tarefas, Grupos, Modificar integrantes do grupo.

   Uma lista dos grupos que você pode gerenciar é exibida.
3. Escolha um grupo e clique em Selecionar.

   Uma lista de usuários que estão atribuídos ao grupo é exibida.
4. Clique em Adicionar um usuário.
5. Procure um usuário ao qual deseja atribuir o grupo.

   Para exibir uma lista de todos os usuários sobre os quais você possui privilégios administrativos, clique em Pesquisar sem modificar os critérios de pesquisa.
6. Escolha um usuário e clique em Selecionar.

   Uma lista atualizada de usuários que estão atribuídos ao grupo é exibida.
7. Clique em Enviar.

   O usuário especificado se torna integrante do grupo.

Atribuir uma função a um usuário

Você pode atribuir funções de provisionamento a um usuário individual.

Siga estas etapas:

1. Efetue logon no console de usuário como um usuário com a tarefa Modificar integrantes/administradores da função de provisionamento.
2. Selecione Funções e tarefas.
3. Selecione uma das seguintes tarefas:
   - Funções administrativas, Modificar integrantes/administradores da função administrativa
   - Funções de provisionamento, Modificar integrantes/administradores da função de provisionamento
   - Funções de acesso, Modificar integrantes/administradores da função de acesso

   Uma tela de pesquisa é exibida.
4. Selecione a função que deseja atribuir ao usuário.

   A guia Associação é exibida.
5. Clique em Adicionar usuário.
6. Procure um usuário ao qual deseja atribuir a função.

   Para exibir uma lista de todos os usuários para os quais você possui tarefas administrativas, clique em Pesquisar sem modificar os critérios de pesquisa.
7. Escolha um usuário e clique em Selecionar.
8. Clique em Enviar.

   As funções especificadas são atribuídas ao usuário.

Atribuir um serviço a um usuário

É possível atribuir um serviço diretamente a um usuário específico. Esse usuário se torna um *integrante* do serviço.

Siga estas etapas:

1. Vá até Serviços, Solicitar e Exibir acesso.

   Uma lista de serviços que você pode administrar é exibida.
2. Selecione o serviço que deseja atribuir a um usuário e clique em Selecionar.

   Uma lista de usuários que estão atribuídos ao serviço é exibida.
3. Clique em Solicitar acesso.
4. Procure um usuário ao qual deseja atribuir o serviço.

   Para exibir uma lista de todos os usuários sobre os quais você possui privilégios administrativos, clique em Pesquisar sem modificar os critérios de pesquisa.

5. Escolha um usuário e clique em Selecionar.

   Uma lista atualizada de usuários que estão atribuídos ao serviço é exibida.

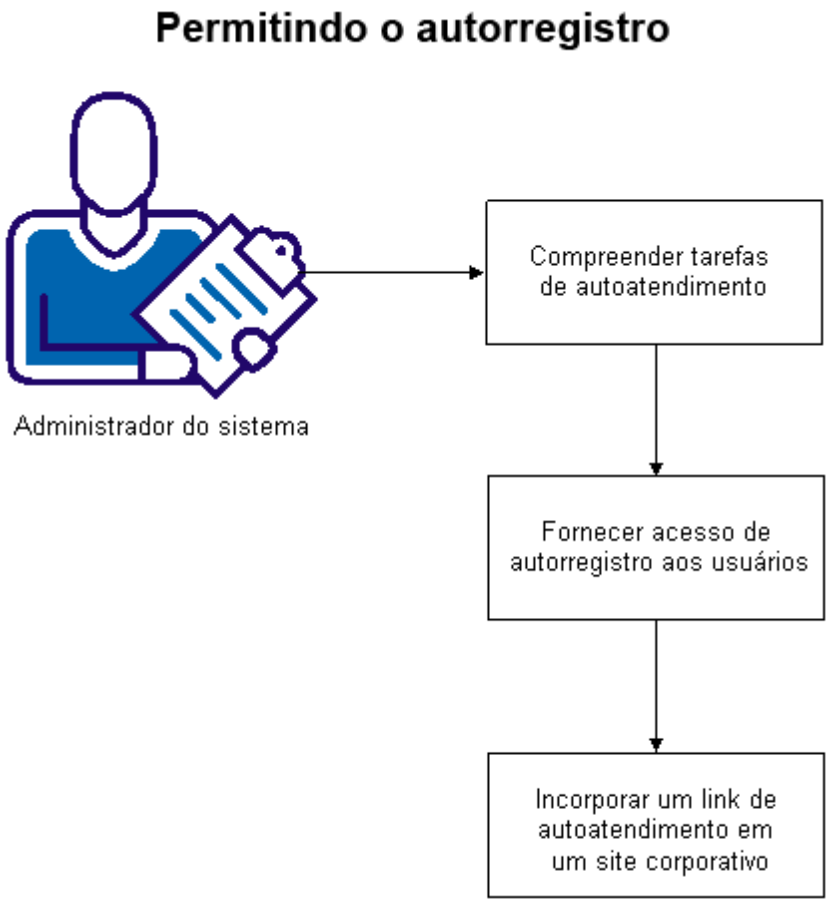
6. Clique em Salvar alterações.

   O usuário recebe o serviço especificado. O usuário recebe todos os aplicativos, funções, grupos e atributos incluídos no serviço.

Permitindo o autorregistro dos usuários

As tarefas de autoatendimento permitem que os usuários gerenciem seu próprio ambiente. A tarefa Autorregistro permite aos usuários criar sua própria conta e perfil de usuário a partir de um console de usuário disponível ao público. Por exemplo, a Bentley Cola permite que novos funcionários e clientes criem suas próprias contas e perfis de usuário por meio de um link incorporado no site corporativo da Bentley Cola.

O diagrama a seguir mostra as informações necessárias para compreender, e as etapas a serem executadas para permitir o autorregistro dos usuários.



Os tópicos a seguir fornecem detalhes sobre como conceder acesso de autorregistro aos usuários.

1. Entender as tarefas de autoatendimento (na página 86).
2. Conceder a usuários acesso de autorregistro (na página 86).
3. Incorporar um link de autoatendimento em um site corporativo (na página 87).

Tarefas de autoatendimento

Tarefas de autoatendimento são ações que os usuários podem realizar, geralmente no console de usuário, para gerenciar seus próprios perfis. As contas de usuário estão configuradas por padrão para conceder ao usuário acesso a determinadas tarefas de autoatendimento como, por exemplo, alterar a senha e as informações do perfil. Um administrador do sistema com privilégios apropriados pode modificar quais as tarefas de autoatendimento são concedidas a um usuário por padrão.

As tarefas de autoatendimento são divididas em dois tipos:

- Tarefas públicas - Tarefas que os usuários podem acessar sem fornecer suas credenciais de logon. Exemplos de tarefas públicas são tarefas de autorregistro, senha esquecida e ID de usuário esquecida.
- Tarefas protegidas - Tarefas para as quais os usuários fornecem credenciais válidas. Os exemplos incluem tarefas para alterar senhas ou informações do perfil.

A tabela a seguir lista as tarefas de autoatendimento padrão.

Tipo de tarefa	Tarefas
Tarefa pública	■ Autorregistro - Permite que os usuários se registrem em um site corporativo ■ Redefinir senha esquecida - Permite que os usuários redefinam uma senha esquecida ■ Senha esquecida - Exibe uma senha temporária que os usuários podem usar para efetuar logon no CA Identity Manager. Quando os usuários efetuam logon, são solicitados a fornecer uma nova senha ■ ID de usuário esquecida - Recupera ou redefine uma ID de usuário esquecida
Tarefa protegida	■ Solicitar e exibir acesso - Permite que os usuários solicitem acesso e removam serviços ■ Alterar minha senha - Permite que os usuários redefinam sua senha ■ Modificar meu perfil - Mantém informações de perfil, como endereço e número de telefone ■ Modificar meus grupos - Permite que os usuários inscrevam-se para grupos ■ Exibir minhas funções - Exibe as funções de um usuário ■ Exibir minhas tarefas enviadas - Exibe as tarefas do CA Identity Manager que o usuário iniciou

Acesse as tarefas de autoatendimento

Após configurar as tarefas de autoatendimento para o seu ambiente, você pode adicionar URLs para essas tarefas a um site corporativo.

Os URLs para as tarefas de autoatendimento têm o seguinte formato:

https://*domain*/iam/im/*public_alias*/ui7/index.jsp?task.tag=*task_tag*

onde:

- *domínio* é o nome de domínio totalmente qualificado do servidor web no ambiente onde o CA CloudMinder está em execução.
- *public_alias* é o alias público do ambiente. O administrador do sistema define o alias público quando o ambiente é criado.
- *task_tag* é o identificador exclusivo da tarefa.

  Para a tarefa padrão de redefinição de senha esquecida, o tag da tarefa é ForgottenPasswordReset.

  https://*domain*/iam/im/*public_alias*/ui7/index.jsp?task.tag=ForgottenPasswordReset

  Para a tarefa padrão de ID de usuário esquecida, o tag da tarefa é ForgottenUserID:

  https://*domain*/iam/im/*public_alias*/ui7/index.jsp?task.tag=ForgottenUserID

Incorporar um link de autoatendimento em um site corporativo

Para permitir o acesso a uma tarefa de autoatendimento pública em um site corporativo, você pode adicionar um link a qualquer página da web. Quando um usuário clica no link, uma tela de tarefa é exibida. Quando o usuário conclui a tarefa, é redirecionado para o console de usuário por padrão.

Para alterar a página para a qual os usuários serão redirecionados, é possível acrescentar o tag RedirectURL ao URL associado ao link, da seguinte maneira:

<A
href="http://*domain*/iam/im/*public_alias*/ui7/index.jsp?task.tag=*tasktag*&task.RedirectURL=http://*domain*/*redirect_URL*">*link text*</A>

domínio

O nome de domínio totalmente qualificado do servidor web no ambiente onde o CA Identity Manager está em execução.

public_alias

Uma sequência de caracteres exclusiva que é adicionada ao URL para o acesso a tarefas públicas.

As tarefas públicas são tarefas de autoatendimento, como autorregistro ou senha esquecida. Os usuários não precisam efetuar logon para acessar tarefas públicas.

Observação: para obter mais informações sobre tarefas públicas e alias, consulte o *Guia de Configuração*.

tasktag

O identificador exclusivo da tarefa. Para determinar o tag de tarefa, use a tarefa Modificar tarefa administrativa para exibir o perfil da tarefa.

redirect_URL

O URL para o qual o usuário é direcionado após o envio da tarefa.

Por exemplo, você pode redirecionar os usuários para uma página de boas-vindas após o autorregistro.

link text

O texto que os usuários clicam para acessar o URL de destino.

Por exemplo, uma empresa pode adicionar um link que permite aos usuários redefinir uma senha esquecida e, em seguida, direcionar esses usuários para uma página de boas-vindas.

O HTML a seguir representa um exemplo de texto do link:

<A href="http://myserver.mycompany.org/iam/im/Employees/ui7/index.jsp?task.tag=ForgottenPasswordReset&task.RedirectURL=http://myserver.mycompany.org/ welcome.html">Reset My Password</A>

Para retornar os usuários para a página onde acessaram a tarefa de autoatendimento, especifique RefererURL como o valor do tag task.RedirectURL, da seguinte maneira:

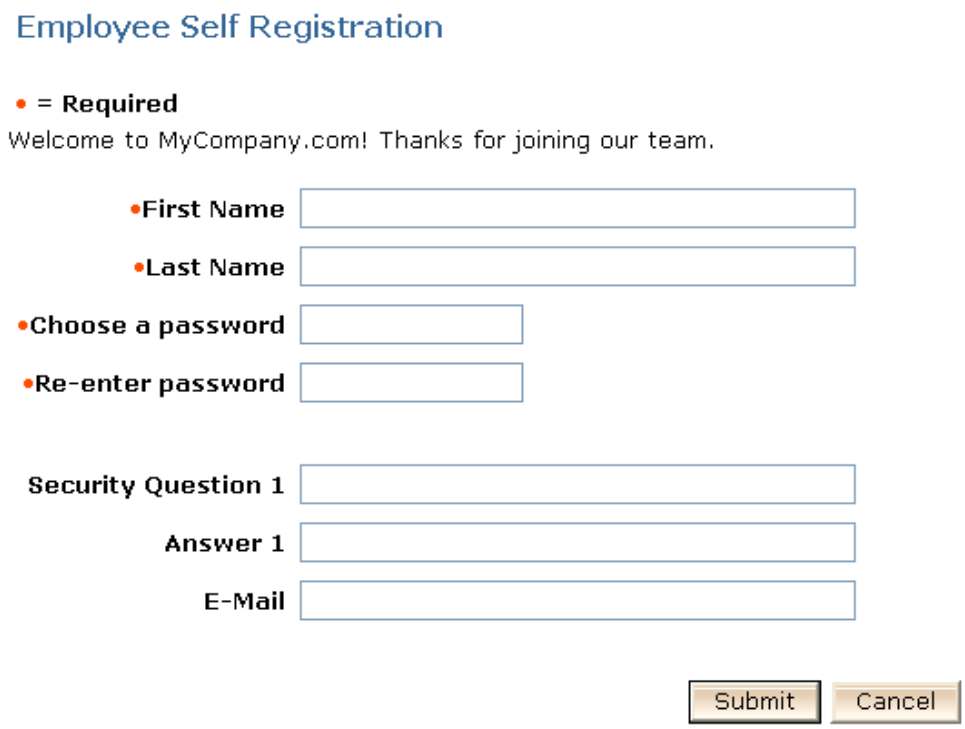
<A href="http://*domain*/iam/im/*public_alias*/ui7/index.jsp?task.tag=*tasktag*&task.RedirectURL=RefererURL</A>

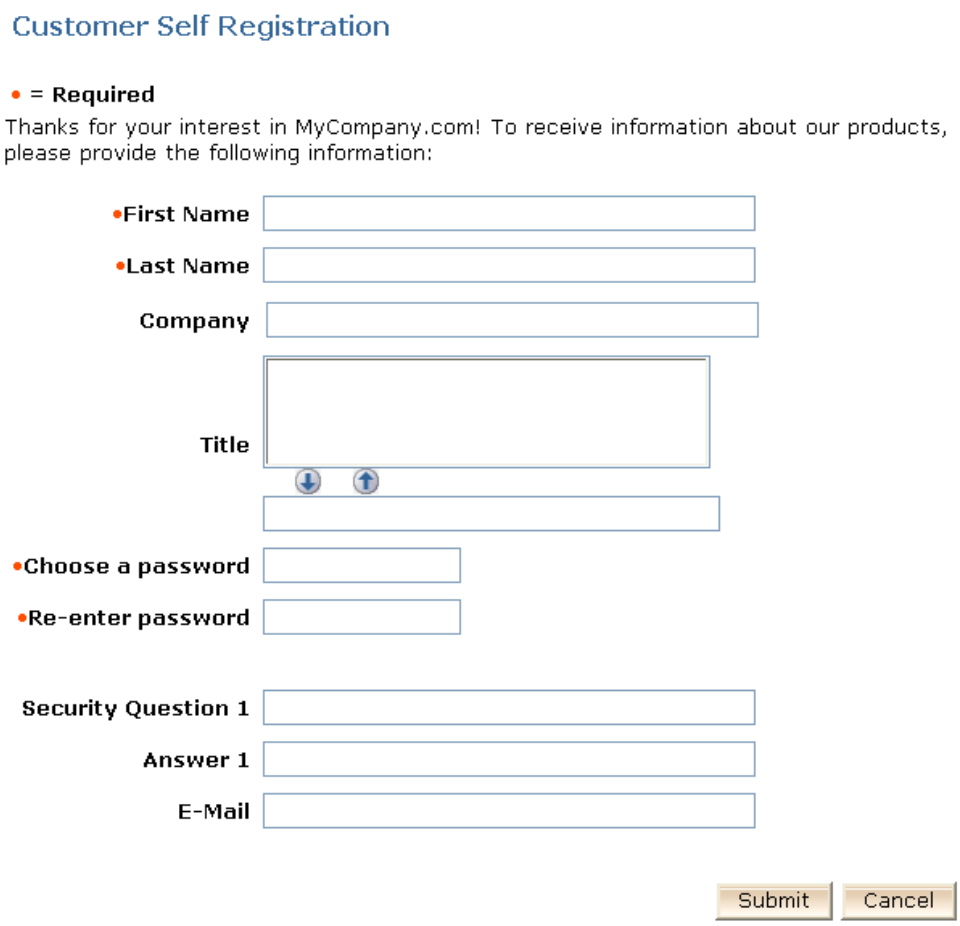
Configurar várias tarefas de autoatendimento

É possível criar várias tarefas de autoatendimento para tipos diferentes de usuário. Por exemplo, você pode criar uma tarefa para registrar novos funcionários e outra tarefa para registrar clientes. Ao usar diferentes tarefas de autorregistro, você pode:

- Coletar informações diferentes
- Registrar os usuários em organizações diferentes
- Redirecionar os usuários para diferentes páginas de logoff após o registro
- Usar uma identidade visual diferente

As figuras a seguir mostram a tarefa de autorregistro para novos funcionários e clientes, respectivamente.





Para configurar várias tarefas de autoatendimento do mesmo tipo, especifique um tag exclusivo ao criar a tarefa. O campo Tag está localizado na tela Configurar perfil da tarefa.

Ao adicionar a um site o link para acessar a tarefa, você acrescenta o tag da tarefa, criando um URL exclusivo.

Por exemplo, você pode criar duas tarefas, da seguinte maneira:

Tarefa	Qualificador	URL
Registrar como um novo funcionário	selfregistration_employee	http://*domain*/iam/im/*alias*/index.jsp?task.tag=SelfRegistration_employee
Registrar como um cliente	selfregistration_customer	http://*domain*/iam/im/*alias*/index.jsp?task.tag=SelfRegistration_customer

Restringir o acesso à função Autogerenciador

Por padrão, a função Autogerenciador, que permite que os usuários gerenciem suas informações de perfil e exibam suas funções e tarefas enviadas, é atribuída a todos os usuários.

Para conceder a função Autogerenciador para um subconjunto de usuários, exclua a política de integrante existente e crie uma política, como descrito em Definir políticas de integrante para uma função administrativa.

Capítulo 5: Gerenciamento de senha

Esta seção contém os seguintes tópicos:

Gerenciamento de senha do CA Identity Manager

O CA Identity Manager inclui vários recursos para gerenciar senhas de usuário:

- Políticas de senha - essas políticas gerenciam as senhas do usuário aplicando regras e restrições que controlam a validade, a composição e a utilização da senha.
- Gerenciadores de senha - administradores que têm a função Gerenciador de senha podem redefinir uma senha quando um usuário liga para o Suporte técnico.
- Gerenciamento de senha por autoatendimento - o CA Identity Manager inclui várias tarefas de autoatendimento que permitem que os usuários gerenciem suas próprias senhas. Essas tarefas incluem:
  - Autorregistro - os usuários especificam uma senha quando se registram em um site corporativo.
  - Alterar minha senha - os usuários podem modificar suas senhas sem a ajuda da equipe de TI ou do suporte técnico.
  - Senha esquecida - os usuários podem redefinir ou recuperar uma senha esquecida depois que o CA Identity Manager verifica sua identidade.
  - Redefinir senha ou desbloquear conta - os usuários podem redefinir ou recuperar uma senha esquecida, ou debloquear uma conta do Windows em um sistema em que acessam o CA Identity Manager.
  - ID de usuário esquecida - os usuários podem recuperar uma ID de usuário esquecida depois que o CA Identity Manager verifica sua identidade.
- Sincronização de senhas em contas de terminal - as alterações na senha são sincronizadas no CA Identity Manager, no Servidor de provisionamento e em seus sistemas de destino. As novas senhas são verificadas em relação às políticas de senha do CA Identity Manager.

Visão geral das políticas de senha

Uma política de senha é um conjunto de regras e restrições. Essas regras especificam a criação e a expiração de senhas. Ao configurar uma política de senha em um ambiente do CA Identity Manager, a política se aplicará ao repositório de usuários associado ao ambiente. Se um diretório de usuários estiver associado a vários ambientes, uma política de senha definida em um ambiente poderá ser aplicada em outros ambientes.

Em uma política de senha, é possível definir as seguintes configurações:

Observação: algumas dessas configurações exigem mapeamentos do diretório de usuários para determinados atributos. Consulte Ativar políticas de senha adicionais (na página 95).

- Aplicar senhas para um conjunto específico de usuários
- Expiração da senha — define eventos, como um número de dias transcorridos ou um número de tentativas de logon sem êxito, que fazem com que as senhas expirem. Quando a senha expira, a conta do usuário é desativada.
- Composição de senha — especifica os requisitos de conteúdo para as novas senhas. Por exemplo, você pode definir as configurações que exigem que os usuários criem senhas que tenham ao menos oito caracteres, além de números e letras.
- Expressões regulares — fornece uma expressão que determina o formato de uma senha válida. Você pode especificar se as senhas correspondem ou não ao formato. Você também pode especificar várias expressões regulares.
- Restrições de senha — define os limites de reutilização de senha. Por exemplo, os usuários devem aguardar 90 dias antes de reutilizar uma senha.
- Opções de senha avançada — especifica as ações que o CA Identity Manager assume, como tornar as senhas minúsculas, antes de processar uma senha. Também é possível especificar a prioridade de uma política de senha quando várias políticas de senha se aplicarem.

Os usuários do SiteMinder também podem configurar políticas de senha na interface de usuário administrativa do SiteMinder. Essas políticas são exibidas no console de usuário do CA Identity Manager.

Observação: quando o CA Identity Manager se integra com o SiteMinder, o SiteMinder aplica *todas* as políticas de senha.

Criar uma política de senha

Você cria as políticas de senha no console de usuário do CA Identity Manager.

Observação: a disponibilidade de algumas opções de políticas de senha exige o mapeamento de determinados atributos conhecidos. Consulte Ativar políticas de senha adicionais (na página 95).

Siga estas etapas:

1. No Console do usuário, selecione uma destas opções:
   - Diretivas, Gerenciar diretivas de senha, Criar diretiva de senha.
   - Tarefas, Diretivas, Gerenciar diretivas de senha, Criar diretiva de senha.
2. Digite um nome exclusivo e uma descrição opcional para a política de senha.
3. Defina as configurações de política de senha que melhor se adaptam à sua implementação:
   - Aplicar uma política de senha a um conjunto de usuários (na página 96)
   - Configurar expiração da senha (na página 98)
   - Configurar composição de senha (na página 101)
   - Especificar expressões regulares (na página 103)
   - Definir restrições de senha (na página 105)
   - Configurar opções de senha avançada (na página 108)

Ativar políticas de senha adicionais

O CA Identity Manager permite criar políticas de senha básicas que gerenciam senhas de usuários por meio da aplicação de expiração, composição e uso de senha. Você também pode definir essas regras e restrições de senha adicionais:

- Expiração da senha:
  - Rastrear logons com falha ou logons bem-sucedidos.
  - Autenticar um logon.
  - Expiração da senha, se não for alterada
  - Inatividade da senha
  - Senha incorreta
  - Várias expressões regulares

- Restrições de senha:
  - Mínimo de dias antes da reutilização
  - Número mínimo de senhas antes da reutilização
  - Percentual de diferença em relação à última senha
  - Ignorar sequência ao verificar se há diferenças.

Siga estas etapas:

1. Vá para Diretórios, <nome do diretório>, Usuário no Management Console.
2. Verifique se %PASSWORD DATA% e %ENABLED STATES% -> 'STATE' são mapeados para atributos físicos.
3. Esses atributos são mapeados por padrão nos arquivos directory.xml de exemplo. Se esses atributos não forem mapeados, consulte o *Guia de Configuração do Identity Manager* para obter informações adicionais.

Aplicar uma política de senha a um conjunto de usuários

É possível especificar regras que determinam o conjunto de usuários ao qual uma política de senha aplica-se. Esse recurso permite ter uma política de senha para funcionários em geral e uma política mais rígida para os gerentes de alto nível.

Siga estas etapas:

1. Crie ou modifique uma política de senha no console de usuário.
2. Selecione o tipo de filtro a ser configurado no campo Filtro de diretório.

   Consulte a tabela a seguir para obter uma descrição de cada tipo de filtro.

   Observação: o tipo de repositório de usuários para o qual a política de senha aplica-se determinará as opções da caixa de listagem Filtro de diretório. Alguns tipos de filtro não estão disponíveis em bancos de dados relacionais e repositórios de usuários do CA Directory quando o CA Identity Manager estiver integrado ao SiteMinder.
3. Especifique uma condição, selecionando um atributo e um operador e digitando um valor.
4. Para adicionar outras condições, clique no sinal de mais.

A tabela a seguir descreve as opções para os tipos de filtros de diretório, além de fornecer exemplos de cada tipo de filtro. Os atributos do lado esquerdo de "=" nos exemplos a seguir mostram como eles são marcados na área de definição do diretório de usuários. Para as tarefas de usuário do tipo Criar, as políticas de senha com filtros de diretório configurados são aplicados apenas quando as duas condições a seguir forem atendidas:

- O CA Identity Manager não está integrado ao SiteMinder.
- O tipo de filtro de diretório não é Usuário, Grupo, Filtro de grupo ou Pesquisa de grupo.

Tipo de filtro	Use esse filtro para...	Exemplo
Em uma organização	Procurar e selecionar uma organização.	
Em um grupo	Procurar e selecionar um grupo.	
Um usuário	Procurar e selecionar um único usuário.	
Filtro de usuário (Não disponível para bancos de dados relacionais quando integrado ao SiteMinder)	Especifique um filtro para os usuários.	Tipo de funcionário = Prestador de serviço Departamento = Segurança
Expressão de pesquisa de usuário	Digite uma consulta de pesquisa para os usuários.	uid=jsmith (para LDAP) TBLUSERS.ID = jsmith (para bancos de dados relacionais)
Filtro de grupo (Não disponível para bancos de dados relacionais quando integrado ao SiteMinder)	Especifique um filtro para os grupos.	Autoinscrição = *
Expressão de pesquisa de grupo	Digite uma consulta de pesquisa para os grupos.	cn=Sales (para LDAP) TBLGROUPS.NAME=GroupA (para bancos de dados relacionais
Filtro de organização (Não disponível para bancos de dados relacionais quando integrado ao SiteMinder)	Especifique um filtro para as organizações.	Nome da organização = *Marketing

Tipo de filtro	Use esse filtro para...	Exemplo
Expressão de pesquisa da organização	Digite uma consulta de pesquisa para as organizações.	ou=Boston (para LDAP) TBLORGANIZATIONS.NAME=Boston (para bancos de dados relacionais)
Pesquisar	Especifique uma consulta que não esteja incluída nas outras opções para o tipo de filtro.	(&(uid=*smith)(ou=Boston))

Configurar expiração da senha

Para ajudar a gerenciar o acesso de usuários, é possível definir eventos, como várias tentativas de logon sem êxito ou inatividade da conta. Quando esses eventos ocorrem, o CA Identity Manager desativa a conta de usuário responsável. Quando o CA Identity Manager estiver integrado ao SiteMinder, é possível especificar um redirecionamento.

Observação: essas definições exigem uma configuração adicional. Consulte Ativar políticas de senha adicionais (na página 95).

É possível definir as seguintes configurações para a expiração da senha:

- Caixa de seleção Rastrear logons com falha/Rastrear logons bem-sucedidos
- Caixa de seleção Falha de rastreamento ao autenticar logon
- Configurações de A senha expira se não for alterada
- Configurações de A senha expira mediante inatividade
- Configurações de Senha incorreta

Caixa de seleção Rastrear logons com falha/Rastrear logons bem-sucedidos

Essa caixa de seleção ativa e desativa o rastreamento de tentativas de logon, incluindo a hora da última tentativa de logon. Se você ativar essa caixa de seleção, o CA Identity Manager gravará as informações de logon em um atributo de dados de senha no repositório de usuários.

Observação: essa definição exige uma configuração adicional. Consulte Ativar políticas de senha adicionais (na página 95).

Quando a caixa de seleção Rastrear logons com falha estiver ativada, a seção Senha incorreta e a caixa de seleção Falha de rastreamento ao autenticar logon ficarão ativas. Quando a caixa de seleção Rastrear logons bem-sucedidos estiver ativada, a seção A senha expira mediante inatividade e a caixa de seleção Falha de rastreamento ao autenticar logon ficarão ativas.

Se você tiver várias políticas de senha, certifique-se de que todas as políticas de senha aplicáveis desativam os detalhes de logon. Caso contrário, uma única política que permite o rastreamento de detalhes de logon pode fazer com que as políticas de senha se comportem incorretamente.

Caixa de seleção Falha de rastreamento ao autenticar logon

Marcar essa caixa de seleção permite efetuar logon quando o rastreamento de usuários falha. Por padrão, essa caixa de seleção fica desativada. Quando o rastreamento de logon estiver desativado, os usuários não poderão efetuar logon.

Ao marcar essa caixa de seleção, selecione também a caixa de seleção Rastrear logons com falha ou Rastrear logons bem-sucedidos.

Observação: essa definição exige uma configuração adicional. Consulte Ativar políticas de senha adicionais (na página 95).

Configurações de A senha expira se não for alterada

No campo A senha expira se não for alterada, você pode configurar o comportamento para senhas que expiraram. Opcionalmente, você pode especificar com quanto tempo de antecedência os usuários são avisados de que a senha está prestes a expirar.

Observação: essa definição exige uma configuração adicional. Consulte Ativar políticas de senha adicionais (na página 95).

Você pode configurar os seguintes campos:

Após *<número>* dias

Determina o número de dias após a expiração da senha que o CA Identity Manager aguardará antes de desativar o usuário ou forçar uma alteração de senha.

Observação: o CA Identity Manager não desativa a conta de usuário até que o usuário tente efetuar logon após a expiração do número de dias especificado.

Desativar usuário

Selecionar esse botão de opção desativa o usuário quando a senha expira. Usuários desativados podem ser ativados usando:

- A tarefa Ativar/desativar usuário no console de usuário. (As funções padrão de Gerente do sistema, Gerenciador da organização e Gerenciador de segurança incluem a tarefa Ativar/desativar usuário.)
- A interface de usuário administrativa do SiteMinder.

  Observação: para obter mais informações, consulte o *Guia de Administração do Servidor de Políticas do CA SiteMinder*.

Forçar alteração de senha

Selecionar esse botão de opção força a alteração de uma senha quando o usuário tenta efetuar logon.

Emitir avisos de expiração para *<número>* dias

Insira com quantos dias de antecedência o usuário será notificado de que a senha está prestes a expirar.

Configurações de A senha expira mediante inatividade

As configurações de A senha expira mediante inatividade permitem especificar o tempo entre as tentativas de logon do usuário. Após esse tempo, uma conta de usuário é considerada inativa. Você também pode usar essa seção para especificar uma ação quando um usuário cuja conta é considerada inativa tem permissão para efetuar logon.

Para definir as configurações na seção A senha expira mediante inatividade, certifique-se de marcar as caixas de seleção de rastreamento de detalhes de logon.

Observação: essa definição exige uma configuração adicional. Consulte Ativar políticas de senha adicionais (na página 95).

A seção A senha expira mediante inatividade contém as seguintes configurações:

- Após *<número>* dias - Determina o número de dias de inatividade após o qual uma senha expira.
- Desativar usuário - Desativa o usuário quando a senha expira devido à inatividade. A conta de usuário é desativada. Os usuários desativados devem ser ativados usando a tarefa Ativar/desativar usuários.
- Forçar alteração de senha - Força uma alteração de senha quando a senha expira devido à inatividade. O usuário altera a senha na próxima tentativa de logon.

Configurações de Senha incorreta

Na seção de configurações de Senha incorreta, é possível especificar quantos logons com falha são permitidos antes de desativar a conta de usuário. Você também pode especificar por quanto tempo a conta fica desativada antes que o usuário possa tentar efetuar logon novamente. Essa seção se aplica apenas quando você tiver marcado a caixa de seleção Rastrear logons com falha.

Observação: essa definição exige uma configuração adicional. Consulte Ativar políticas de senha adicionais (na página 95).

A seção Senha incorreta contém os seguintes campos:

Conta desativada após *<número>* senhas incorretas sucessivas

Essa configuração determina o número de tentativas consecutivas de logon com falha que um usuário pode fazer. Limitar o número de tentativas com falha protege contra programas que são projetados para acessar um recurso por meio de tentativas repetidas até que a senha correta seja encontrada. Se um usuário não conseguir efetuar logon corretamente após o número definido de tentativas, o CA Identity Manager desativará a conta. Um administrador deverá ativar a conta.

Após *<número>* minutos

Essa configuração determina o tempo que o usuário deve esperar antes de fazer outra tentativa de logon ou até que a conta seja reativada. Se o usuário digitar outra senha incorreta, o CA Identity Manager desativará a conta novamente. O usuário aguarda o tempo especificado antes de tentar novamente.

Permitir uma tentativa de logon

Essa configuração especifica o número de minutos até uma tentativa de logon adicional depois que o usuário digitar uma senha incorreta.

Reativar conta

Essa configuração reativa uma conta após o número especificado de minutos.

Configurar composição de senha

É possível especificar regras que determinam a composição de caracteres de senhas criadas recentemente. Certifique-se de levar em conta o tamanho máximo das senhas ao determinar valores para requisitos de caracteres. Se o número total de letras e números exceder o comprimento máximo, todas as senhas serão recusadas. Por exemplo, se Letras e Dígitos forem definidos como seis, todas as senhas deverão conter pelo menos 12 caracteres (seis letras e seis dígitos). Neste exemplo, se o tamanho máximo da senha for de oito caracteres, todas as senhas serão recusadas.

As configurações de composição de senha incluem:

Comprimento mínimo da senha

Especifica um tamanho mínimo para senhas de usuários.

Comprimento máximo da senha

Especifica o tamanho máximo para senhas de usuários.

Máximo de caracteres repetidos

Determina o número máximo de caracteres idênticos que podem ser exibidos consecutivamente em uma senha.

Por exemplo, se esse valor for definido como 3, "aaac" "não poderá aparecer na senha. Entretanto, "aaa" é aceitável em uma senha. Defina esse valor para garantir que os usuários não poderão digitar senhas de um único caractere.

Letras maiúsculas

Especifica se caracteres alfabéticos em maiúsculas são permitidos e, em caso afirmativo, o número mínimo que uma senha deverá conter.

Letras minúsculas

Especifica se caracteres alfabéticos em minúsculas são permitidos e, em caso afirmativo, o número mínimo que uma senha deverá conter.

Letras

Especifica se letras são permitidas e, em caso afirmativo, o número mínimo que uma senha deverá conter.

Observação: a caixa de seleção Letras é marcada automaticamente quando você permite maiúsculas ou minúsculas.

Dígitos

Especifica se números são permitidos e, em caso afirmativo, o número mínimo que uma senha deverá conter.

Letras e dígitos

Especifica se letras e dígitos são permitidos e, em caso afirmativo, o número mínimo que uma senha deverá conter. Se essa configuração estiver definida em conjunto com Dígitos, os caracteres podem satisfazer os dois requisitos. Por exemplo, se essa configuração e Dígitos estiverem definidos como 4, a senha "1234" será uma senha válida.

Observação: a caixa de seleção Letras e dígitos é marcada automaticamente quando você permite maiúsculas ou minúsculas, ou números.

Pontuação

Especifica se pontuações são permitidas e, em caso afirmativo, o número mínimo que uma senha deverá conter. Pontuações podem ser pontos finais, vírgulas, pontos de exclamação, barras, traços e hífens.

Não imprimível

Especifica se caracteres não imprimíveis são permitidos e, em caso afirmativo, o número mínimo que uma senha deverá conter. Esses caracteres não podem ser exibidos em uma tela de computador.

Observação: alguns navegadores não oferecem suporte a caracteres não imprimíveis.

Não alfanumérico

Especifica se caracteres não alfanuméricos, como pontuações e outros símbolos ("@", "$" e "*"), são permitidos e, em caso afirmativo, o número mínimo que uma senha deverá conter. Caracteres não imprimíveis também estão incluídos. Um caractere não alfanumérico também atende aos requisitos de pontuação e caracteres não imprimíveis.

Especificar expressões regulares

Expressões regulares de senha permitem especificar padrões de texto de expressões regulares para a sequência de caracteres que corresponde ou não a cada senha para ser válida. Esse teste pode ser útil, por exemplo, quando você deseja exigir que o primeiro caractere seja um dígito e o último caractere não seja.

É possível configurar várias expressões para uma única política de senha. Se você criar várias expressões, as senhas aceitáveis corresponderão a *todas* as expressões especificadas.

Siga estas etapas:

1. Digite um tag descritivo para a expressão (sem espaços em branco) no campo Nome.
2. Digite uma expressão regular com a sintaxe descrita na Sintaxe de expressões regulares no campo Deve corresponder a.
3. Se a senha não corresponder à expressão regular, marque a caixa de seleção na coluna Não deve corresponder a.

Observação: você pode especificar várias expressões, clicando no sinal de mais (+) para adicionar a expressão.

Exemplo: a definição de expressão regular a seguir pode ser usada para exigir que todas as senhas iniciem com uma letra maiúscula ou minúscula: Nome: MustStartAlpha

Expressão: [a-zA-Z].*

Sintaxe de expressões regulares

Esta seção descreve a sintaxe usada para criar expressões regulares para a correspondência de senha. Essa sintaxe é consistente com a sintaxe da expressão regular com suporte para a correspondência de recursos ao especificar realms.

Caracteres	Resultados
\	Usado para cotação de um metacaractere (como '*')
\\	Corresponde a um único caractere '\'
(A)	Agrupa subexpressões (afeta a ordem da avaliação de padrões)
[abc]	Classe de caracteres simples (qualquer caractere dentro de colchetes corresponde ao caractere de destino)
[a-zA-Z]	Classe de caracteres com intervalos (qualquer intervalo de caracteres dentro de colchetes corresponde ao caractere de destino)
[^abc]	Classe de caracteres negada
.	Corresponde a qualquer caractere, exceto nova linha
^	Corresponde somente no início de uma linha
$	Corresponde somente no final de uma linha
A*	Corresponde a A 0 ou mais vezes (greedy)
A+	Corresponde a A 1 ou mais vezes (greedy)
A?	Corresponde a A 1 ou 0 vez (greedy)
A*?	Corresponde a A 0 ou mais vezes (reluctant)
A+?	Corresponde a A 1 ou mais vezes (reluctant)
A??	Corresponde a A 0 ou 1 vez (reluctant)
AB	Corresponde a A seguido por B
A|B	Corresponde a A ou B
\1	Referência inversa à primeira subexpressão entre parênteses
n	Referência inversa à *n* subexpressão entre parênteses

Todos os operadores de fechamento (+, *, ?) são greedy por padrão, o que significa que eles correspondem ao maior número de elementos da sequência de caracteres que for possível sem fazer com que a correspondência geral falhe. Se desejar que um fechamento seja reluctant (não greedy), poderá simplesmente adicionar um '?'. Um fechamento reluctant corresponderá ao menor número de elementos da sequência de caracteres que for possível quando encontrar correspondências.

Definir restrições de senha

É possível colocar restrições no uso da senha. As restrições incluem por quanto tempo um usuário deve aguardar antes de reutilizar uma senha e quão diferente a senha deve ser daquelas selecionadas anteriormente. Também é possível impedir que os usuários especifiquem palavras que você determina que são um risco de segurança ou contêm informações pessoais.

Observação: essa definição exige uma configuração adicional. Consulte Ativar políticas de senha adicionais (na página 95).

A seção Restrição inclui os seguintes campos:

Mínimo de dias até poder reutilizar

Determina quantos dias um usuário deve aguardar antes de reutilizar uma senha.

Número mínimo de senhas antes da reutilização

Determina quantas senhas devem ser usadas antes que uma senha possa ser reutilizada.

Observação: se você especificar um período de tempo e um número de senhas, os dois critérios devem ser atendidos antes que uma senha possa ser reutilizada. Por exemplo, você pode configurar uma política de senha que exige que os usuários aguardem 365 dias e especifiquem 12 senhas antes de reutilizar uma senha. Após um ano, se apenas seis senhas tiverem sido usadas, outras seis deverão ser usadas para que o usuário possa reutilizar a primeira senha.

Percentual de diferença em relação à última senha

Especifica a porcentagem de caracteres que uma nova senha deve conter. É possível definir o valor para 100. Nesse caso, a nova senha não pode conter caracteres que estavam na senha anterior.

Ignorar sequência ao verificar se há diferenças

Ignora a posição dos caracteres na senha ao determinar a porcentagem.

Por exemplo, se uma senha inicial for BASEBALL12 e a caixa de seleção Ignorar sequência ao verificar se há diferenças estiver marcada, 12BASEBALL não será aceitável. Com a caixa de seleção desmarcada, 12BASEBALL é uma senha aceitável porque cada letra ocorre em uma posição diferente.

Para obter mais segurança, a caixa de seleção Ignorar sequência ao verificar se há diferenças está marcada.

Senhas	Diferença de porcentagem	Ignorar sequência	Aceito
BASEBALL12 (antiga)	0	Selecionado	Y

Senhas	Diferença de porcentagem	Ignorar sequência	Aceito
12BASEBALL		Não selecionado	Y
BASEBALL12 (antiga) 12BASEBALL	100	Selecionado Não selecionado	N Y
BASEBALL12 (antiga) 12SOFTBALL	0	Selecionado Não selecionado	Y Y
BASEBALL12 (antiga) 12SOFTBALL	90	Selecionado Não selecionado	N Y
BASEBALL12 (antiga) 12SOFTBALL	100	Selecionado Não selecionado	N N

Atributos de perfil

A configuração do campo Coincidir tamanho impede que os usuários usem informações pessoais em suas senhas. O campo Coincidir tamanho determina o tamanho mínimo da sequência da política de senha em comparação aos atributos na entrada de diretório. Por exemplo, se esse valor for definido como quatro, o CA Identity Manager verifica se a senha não inclui os últimos quatro caracteres dos atributos de perfil do usuário, por exemplo, sobrenome ou telefone.

Dicionário

Especifica uma lista de sequências de caracteres que não podem ser usadas nas senhas.

Observação: um retorno de carro segue a última linha da entrada do dicionário.

As configurações de Dicionário incluem os seguintes campos:

- Caminho - Contém o caminho completo e o nome do arquivo de dicionário.
- Coincidir tamanho - Controla o tamanho das sequências de caracteres que são comparadas com os valores no arquivo de dicionário. A comparação ignora as maiúsculas e minúsculas das sequências de caracteres. Você pode deixar o campo Coincidir tamanho em branco ou defini-lo como zero. Nesses casos, o CA Identity Manager recusa apenas as senhas correspondentes a uma sequência de caracteres exatamente igual no dicionário. Quando Coincidir tamanho é maior que zero, o CA Identity Manager recusa entradas durante as seguintes condições:
  - A senha contém uma subsequência de caracteres que começa com a mesma série de caracteres que uma entrada do dicionário.
  - O número de caracteres correspondentes consecutivos é maior ou igual ao número especificado no campo Coincidir tamanho.

  Por exemplo, considere um arquivo de dicionário que contenha as seguintes entradas:
  - lion
  - tiger
  - bear

  Quando o campo Coincidir tamanho estiver definido como quatro resultados nas seguintes ações:

  "TeddyBear", recusado porque Bear corresponde à entrada bear no arquivo de dicionário.

  "prestige", recusado porque "tige" corresponde aos quatro primeiros caracteres da entrada tiger no arquivo de dicionário.

  "Geiger Counter", aceito porque "iger" não inclui a primeira letra da entrada tiger no arquivo de dicionário.

Configurar opções de senha avançada

As opções de políticas de senha avançada permitem configurar o pré-processamento das senhas enviadas antes da validação e do repositório. Você também pode atribuir à política uma prioridade para permitir a avaliação previsível de várias políticas de senha que se aplicam ao mesmo diretório do usuário ou espaço para nome.

Não forçar o uso de letras maiúsculas/minúsculas | Forçar uso de letra maiúscula | Forçar o uso de letra minúscula

Determine se o uso de maiúsculas ou minúsculas é forçado para as senhas antes do processamento e repositório. Escolha uma opção de uso de letras maiúsculas/minúsculas clicando no botão de opção Forçar uso de letra maiúscula ou Forçar o uso de letra minúscula. Caso contrário, verifique se o botão de opção Não forçar o uso de letras maiúsculas/minúsculas (o padrão) está selecionado.

Importante: certifique-se de que a opção de uso de letras maiúsculas/minúsculas que você especificar é consistente com os requisitos de composição relacionados a letras maiúsculas/minúsculas especificados.

Remover espaços em branco à esquerda

Selecione para remover espaços em branco à esquerda das senhas antes do processamento.

Remover espaços em branco à direita

Selecione para remover espaços em branco à direita das senhas antes do processamento.

Remover espaços em branco incorporados

Selecione para remover todos os espaços em branco incorporados antes do processamento.

Observação: algumas implementações de diretório do usuário automaticamente eliminam espaços em branco à esquerda ou à direita de valores de atributo (no qual as senhas do usuário estão armazenadas) antes de armazená-los. As configurações especificadas em sua política de senha não têm efeito.

Prioridade da avaliação

Especifica a prioridade da avaliação para a política de senha. O valor está no intervalo de 0 (o padrão) a 999. As políticas aplicáveis são avaliadas em ordem decrescente (999 primeiro; 0 por último).

Aplicar políticas de senha de baixa prioridade

Determina se as políticas de senha de prioridade mais baixa serão aplicadas após esta.

Gerenciar políticas de senha

Os administradores com os privilégios apropriados podem gerenciar as políticas de senha usando as tarefas Exibir, Modificar, Criar e Excluir política de senha. Por padrão, essas tarefas são exibidas na categoria Políticas.

Quando você acessa uma dessas tarefas, o CA Identity Manager exibe uma lista de políticas de senha que se aplicam ao repositório de usuários associado ao ambiente atual do CA Identity Manager. Se o CA Identity Manager se integrar ao SiteMinder, a lista pode incluir políticas de senha que são criadas na interface de usuário administrativa do SiteMinder usando serviços de senha. Você pode gerenciar as políticas de senha que são criadas no CA Identity Manager ou no SiteMinder.

Políticas de senha e bancos de dados relacionais

Se você configurar uma política de senha que se aplica a um banco de dados relacional, deverá usar o seguinte formato para configurar o atributo de dados de senha no diretório de usuários do SiteMinder:

nome_da_tabela.nome_da_coluna

Para evitar problemas de sintaxe durante a execução, é recomendável que esse campo resida na tabela principal.

Critérios de senha para integração do CA Identity Manager e do SiteMinder

Quando o CA Identity Manager está integrado ao SiteMinder e usa o recurso de manipulação de senhas do SiteMinder, as políticas de senha são obtidas do repositório de políticas do SiteMinder. Nesse caso, crie senhas que atendam aos critérios de senha do SiteMinder. Os seguintes caracteres de pontuação são os únicos que estão de acordo com os critérios de senha do <stmdr>:

'*', '(', '\',',','@','"',':','#','_','-','!','&','?',')','(','{','}','*','.','/'

Importante: o CA Identity Manager não impõe restrições quanto ao uso de caracteres de pontuação em senhas. No entanto, se você pretende usar o recurso de senhas do SiteMinder, é recomendada a criação de senhas que atendam às restrições do SiteMinder.

Redefinir senha ou desbloquear conta

Caso os usuários esqueçam as respectivas senhas nos sistemas Windows, você pode configurar o Autoatendimento para solicitar o usuário na tela de logon do Windows. Você pode usar este recurso instalando o Provedor de credenciais para os sistemas Windows VISTA e Windows 7

Com esse recurso, o usuário é conectado ao Autoatendimento por meio do navegador web do Cubo, em que é exibida uma página de solicitação de alteração de senha. Depois de preencher a página, o usuário clica em Retornar para voltar à tela de Logon do Windows.

Instalar o Provedor de credenciais

Siga estas etapas:

1. Localize o download dos Componentes de provisionamento do CA Identity Manager ou outra mídia de instalação.
2. Execute o instalador em Agente.

   Observação: para o Provedor de Credenciais em um sistema operacional de 64 bits, escolha a versão de 64 bits deste software.
3. Siga as solicitações do assistente para responder às perguntas.
4. Se você instalou o Provedor de Credenciais em um sistema operacional de 64 bits, faça download do Microsoft Visual C++ 2008 SP1 (64 bits).
5. Assim que a instalação estiver concluída, configure o Provedor de Credenciais.

Configurar o Provedor de Credenciais

Você pode usar uma ferramenta de configuração para configurar um sistema em que você instalou o Provedor de Credenciais.

Para configurar o Provedor de Credenciais

1. No Windows Explorer, vá até o diretório em que você instalou o Provedor de Credenciais. Por exemplo:

   C:\Arquivos de Programa\CA\Identity Manager\Provedor de Credenciais
2. Clique duas vezes no executável a seguir:

   CAIMCredProvConfig.exe

3. Selecione o primeiro provedor de credenciais como o padrão.

   A tela de logon não poderá usar essa configuração se um segundo provedor de credenciais estiver em uso, como o provedor de credenciais de senha da Microsoft. Se ambos os fornecedores tentarem ser o provedor padrão, a tela de logon escolherá um provedor padrão.

4. Desative o provedor de credenciais padrão.

5. Preencha os campos em Configurações do Provedor de Credenciais, como se segue:

   Link1 URL

   O URL usado quando um usuário clica no link Esqueceu a senha. Esse link deve ser um URL em uma interface da web para redefinição de senha.

   Veja a seguir um link de exemplo:

   `http://eastern.local:8080/iam/im/`*`environment`*`/ca12/index.jsp?task.tag=forgottenpassword&facesViewId=/app/page/screen/fp_identify_user.jsp&action.forgottenpassword.identify=1&USER_ID=%username%`

   Para obter esse URL, o autorregistro deve estar funcionando no ambiente. Além disso, verifique se o URL de Autoatendimento para o ambiente do CA Identity Manager funciona no sistema em que você está instalando o Provedor de Credenciais. As ocorrências de %username% serão substituídas pelo valor no campo de nome do usuário na caixa de diálogo Logon.

   URL do Link2

   O URL usado quando um usuário clica no link Desbloquear conta. Esse link deve ser um URL para uma interface da web que permita a um usuário desbloquear uma conta. As ocorrências de %username% serão substituídas pelo valor no campo de nome do usuário na caixa de diálogo Logon.

   Link3 URL

   O URL usado quando um usuário clica no link Nova conta. Esse link deve ser um URL para uma interface da web que permita a um usuário criar uma conta. O qualificador %username% não é esperado como parte do URL

Usar título personalizado

Uma sequência de caracteres personalizada substitui a sequência "Fornecido por..." que aparece na barra de título ou na caixa de dialogo Retornar do Provedor de Credenciais. O local da sequência de caracteres está de acordo com a configuração de conformidade com a Seção 508.

Domínio

O nome do domínio de provisionamento.

Conformidade com Seção 508 (use Retornar no menu)

Ativa a função Retornar em um menu. Se desmarcada, a caixa de diálogo Retornar será usada.

Desativar todas as caixas de diálogo

Impede que o Secure Browser gere novas janelas de caixa de diálogo, como pop-ups, erros e caixas de diálogo de impressão e salvamento. O recurso *Desativar todas as caixas diálogo* é ativado para melhorar a segurança do sistema, mas pode ser desativado para a solução de problemas.

6. Preencha os campos em Configurações do Secure Browser, como se segue:

   Lista de permissão

   Um padrão de expressão regular que corresponde a URLs aos quais o acesso sempre deve ser permitido.

   Lista de negação

   Um padrão de expressão regular que corresponde a URLs aos quais o acesso sempre deve ser negado.

7. (Opcional) Clique em Exportar para exportar as configurações para outro sistema.
8. Clique em OK para salvar as configurações.
9. Reinicie o sistema.

Configurações de Registro do Provedor de Credenciais

Se você optar por não usar a ferramenta de configuração do Provedor de Credenciais, edite as configurações de Registro do Windows na seguinte chave:

`[HKEY_LOCAL_MACHINE\SOFTWARE\CA\CAIMCredentialProvider]`

link1_cmd

Esse link deve ser o URL para o qual navegar quando um usuário clicar no link 1.

link2_cmd

Esse link deve ser o URL para o qual navegar quando um usuário clicar no link 2. Por exemplo, você pode adicionar um link que leve a um site para desbloqueio de contas.

Se link2_cmd estiver em branco, somente link1_cmd será exibido na janela da caixa de diálogo Logon.

link3_cmd

Esse link deve carregar um URL para uma interface da web que permita a um usuário criar uma conta.

comp508

Ativa a função Retornar em um menu. Se desmarcada, a caixa de diálogo Retornar será usada

domain

O nome do domínio de provisionamento.

langdir

O local das DLLs de idioma localizadas.

disablepwdcp

A opção Desativar Provedor de Credenciais de senha da Microsoft. 1 está desativada. 0 está ativada.

CredentialProviderInstallPath

O caminho completo do diretório onde o Provedor de Credenciais está instalado.

configdir

O caminho completo do diretório onde o Provedor de Credenciais está instalado.

selectdefaultcredential

Selecione o primeiro provedor de credenciais como a opção padrão. Sim está ativada. Não está desativada.

Configurações de Registro do navegador do Cubo

O componente Secure Browser do Cubo possui vários valores de Registro que controlam seu comportamento. Essas configurações estão na seguinte chave do Registro:

`[HKEY_LOCAL_MACHINE\SOFTWARE\CA\Cube]`

Tipo

`REG_SZ(String)`

404

O caminho para um documento HTML padrão a ser exibido se a máquina não puder contatar o CA Identity Manager na inicialização.

default

A página padrão para a qual navegar quando nenhum URL for incluído no Comando Link1 ou Comando Link2.

allow

Permissão explícita da ACL. Uma expressão regular para URLs de correspondência padrão que é sempre permitida. Para obter mais informações, consulte Listas de controle de acesso do Cubo (na página 115).

close

Fecha o navegador seguro e retorna o usuário à caixa de diálogo de senha esquecida do Provedor de credenciais.

deny

Negação explícita da ACL. Uma expressão regular para URLs de correspondência padrão que sempre deve ser acesso negado. Para obter mais informações, consulte Listas de controle de acesso do Cubo (na página 115).

langdir

O local das DLLs de idioma localizadas.

rejectinvalidcerts

Controla se o Provedor de Credenciais aceita apenas certificados SSL válidos. Quando configurado como Não, essa opção permite certificados SSL inválidos ou vencidos.

Os valores válidos para essa chave são *sim* e *não*.

unreachable

Redireciona para um URL quando o Cubo encontra problemas de conectividade.

Valor de exemplo: arquivo:///C:\unreachable.html

usecustomtitle

Permite o título personalizado para o Provedor de Credenciais.

customtitle

Este é o título que você deseja que apareça no Provedor de Credenciais.

Listas de controle de acesso do Cubo

As ACLs do Cubo são padrões de expressão regular que permitem ou negam permissão explicitamente para navegar até um URL selecionado. As ACLs avaliam na seguinte ordem:

1. Permitir (a permissão é automaticamente concedida em primeiro lugar)
2. Negar (os URLs negados são verificados em segundo lugar)

Exemplos de listas do Access Control

"allow"="(.pdf)"

Permita que todos os documentos PDF sejam exibidos.

"deny"="(.doc|.xls)"

Negue acesso a documentos do Microsoft Word e Excel.

Personalizar a mensagem Fornecido por

Você poderá perceber a mensagem "Fornecido por..." na caixa de diálogo ou opção de menu Retornar, do provedor de credenciais. É possível editar ou remover essa mensagem.

Para personalizar a mensagem Fornecido por

1. Faça download de ResEdit, um editor de recursos gratuito em http://www.resedit.net.
2. Inicie o ResEdit.
3. Edite o arquivo 1033.dll na pasta de idiomas.
4. Clique duas vezes em String Table.
5. Remova ou modifique a ID 135 do recurso, a versão em inglês do recurso dessa mensagem.

Redefinir uma senha para um Logon do Windows

Depois que o Provedor de credenciais estiver instalado em um sistema Windows, o link "Esqueceu a sua senha?" será exibido na caixa de diálogo de logon padrão do Microsoft Windows. Use esse link para redefinir sua senha ou veja as dicas que ajudarão a se lembrar dela.

Para redefinir uma senha para um Logon do Windows

1. Clique em Efetuar logon na caixa de diálogo Segurança do Windows. A caixa de diálogo Logon do Windows é exibida.
2. Insira um nome de usuário válido.
3. Clique em Esqueceu a senha.

   A página Password Clue do CA Identity Manager é exibida.

   Se você se lembrar da sua senha, retorne para a caixa de diálogo de logon para continuar. Caso contrário, execute a etapa 4 para se autenticar no Autoatendimento do CA Identity Manager.
4. Digite as respostas às perguntas de autenticação.

   Observação: caso não saiba as respostas de todas as perguntas, clique em Solicitar para que a senha possa ser redefinida por um administrador.

   Em seguida, será solicitado que você altere sua senha na próxima tela.

Instalação silenciosa do Provedor de Credenciais

O Provedor de Credenciais oferece suporte a um modo de instalação silencioso. Seis propriedades são suportadas

LINK1

Refere-se a SOFTWARE\CA\CAIMCredentialProvider\link1_cmd no Registro.

LINK2

Refere-se a SOFTWARE\CA\CAIMCredentialProvider\link2_cmd no Registro.

LINK3

Refere-se a SOFTWARE\CA\CAIMCredentialProvider\link3_cmd no Registro.

DOMAIN

Refere-se a SOFTWARE\CA\CAIMCredentialProvider\domain no Registro.

COMP508

Refere-se a SOFTWARE\CA\CAIMCredentialProvider\comp508 no Registro.

USECUSTOMTITLE

Refere-se a SOFTWARE\CA\Cube\usecustomtitle no Registro.

CUSTOMTITLE

Refere-se a SOFTWARE\CA\Cube\customtitle no Registro.

REJECTINVALIDCERTS

Refere-se a SOFTWARE\ComputerAssociates\Cube\rejectinvalidcerts no Registro.

UNREACHABLE

Refere-se ao local da página inacessível.

Veja a seguir a sintaxe para definir o valor dessas propriedades:

```
setup /s /v"/qn LICENSE=Yes INSTALLDIR=\"C:\Program Files\CA\Identity
Manager\Credential Provider\" LINK1=\"<url>\" LINK2=\"<url>\"LINK3=\"<url>\"
COMP508=\"yes\" REJECTINVALIDCERTS=\"yes\" USECUSTOMTITLE=\"yes\"
CUSTOMTITLE=\"custom cp title\""
```

ou

```
setup /s /v"/qn LICENSE=Yes INSTALLDIR=\"C:\Program Files\CA\Identity
Manager\Credential Provider\" LINK1=\"<url>\" LINK2=\"<url>\" LINK3=\"<url>\"
COMP508=\"yes\" USECUSTOMTITLE=\"yes\" CUSTOMTITLE=\"custom cp title\"
SELECTDEFAULTCREDENTIAL=\"yes\" UNREACHABLE=\"<url>\""
```

ou

```
setup /s /v"/qn LICENSE=Yes INSTALLDIR=\"C:\Program Files\CA\Identity
Manager\Credential Provider\"
LINK1=\"<url>\" LINK2=\" <url>\" LINK3=\"<url>\" COMP508=\"yes\"
USECUSTOMTITLE=\"yes\" CUSTOMTITLE=\"custom cp title\"
SELECTDEFAULTCREDENTIAL=\"yes\" UNREACHABLE=\"file:///[INSTALLDIR]<file
name>\"CUBE_ALLOW=\"\"CUBE_DENY=\"\""
```

[INSTALLDIR]

Refere-se ao valor da propriedade INSTALLDIR.

<url>

Especifica o URL para desbloqueio de conta ou uma senha esquecida.

<file name>

Define o nome do arquivo inacessível.

CUBE_ALLOW

Refere-se a permitir a invocação do URL do cubo.

CUBE_DENY

Refere-se a restringir a invocação do URL do cubo.

Sincronizando senhas nos terminais

Você pode instalar um agente de sincronização de senhas em determinados terminais suportados pelo CA Identity Manager. O agente intercepta as solicitações de alteração de senha no terminal e envia as alterações ao Servidor de provisionamento.

Sincronização de senhas no Windows

O CA Identity Manager pode interceptar a alteração de senha de uma conta nativa do Windows e propagar a nova senha para um usuário e todas as contas que pertencem a ele.

Quando o Agente de sincronização de senhas detecta uma tentativa de alteração de senha, ele intercepta a solicitação e a envia ao Servidor de provisionamento. O Servidor de provisionamento então propaga a nova senha para o usuário e outras contas associadas a ele.

A sincronização de senhas apresenta os seguintes requisitos:

- O Agente de sincronização de senhas deve ser instalado no sistema em que alterações de senhas são interceptadas.
- O sistema deve ser gerenciado como um terminal adquirido.
- A caixa de seleção Agente de sincronização de senhas instalado deve ser marcada na guia Configurações do Terminal adquirido.
- As contas em sistemas gerenciados devem ser exploradas e correlacionadas com os usuários do CA Identity Manager.
- O ambiente deve permitir que as alterações de senha venham de contas de terminal. Um administrador com acesso ao Management Console ativa esse recurso.

Importante: tenha cuidado na formulação das regras de senha, de modo que uma senha se aplique a todos os sistemas. Por exemplo, se as senhas do Windows devem ter 12 caracteres, qualquer sistema que aceite senhas de até somente 10 caracteres rejeitará a alteração durante a sincronização.

O Servidor do CA Identity Manager não reconhece as restrições de senha no terminal. Ao trabalhar com contas de terminal, a política de senha deve ser mais rígida que a política de senha dos terminais.

Instalar o Agente de sincronização de senhas do Windows

É possível instalar o Agente de sincronização de senhas em qualquer computador Windows gerenciado em que os usuários globais efetuam logon. O Agente é executado em segundo plano nessas máquinas.

Executar o programa de instalação

Observe os seguintes requisitos:

- O Servidor de provisionamento deve gerenciar o sistema no qual você está instalando o Agente.
- Crie um usuário para atuar como administrador de alterações de senha: o nome sugerido é etapwsad. Esse usuário deve ter o perfil PasswordAdministrator.
- Há dois Agentes de sincronização de senhas do Windows na mídia de instalação: um para Windows de 32 bits e o outro de 64 bits. O Agente de sincronização de senhas de 32 bits não é suportado em Windows de 64 bits. O FIPS é suportado apenas pelo Agente de sincronização de senhas de 32 bits.

Siga estas etapas:

1. Localize a mídia de instalação do CA Identity Manager.
2. Navegue até \Agent\PasswordSync ou \Agent\PasswordSync-x64.
3. Execute setup.exe.
4. Responda ao Assistente de configuração da seguinte maneira:
   a. No campo Nome do host, digite o nome do sistema do Servidor de provisionamento.
   b. Altere a porta, conforme a necessidade, se a instalação do Servidor de provisionamento usar uma porta não padrão.

      A porta LDAP sugerida que é usada para se conectar ao Servidor de provisionamento é a 20390.
   c. Clique no botão Localizar domínio para recuperar o domínio do Servidor de provisionamento.
   d. Se a instalação do Servidor de provisionamento for configurada para tolerância a falhas, siga as instruções na tela para adicionar uma lista de servidores separados por vírgula.
   e. Clique em Avançar.
   f. No campo Administrator, digite etapwsad como o nome padrão do usuário global para o Agente de sincronização de senhas. Esse usuário deve ter o perfil PasswordAdministrator. Ele não existe por padrão.
   g. No campo Administrator de senha, insira a senha do administrador.
   h. Clique em Avançar.
   i. Na lista suspensa Tipo de terminal, selecione o Tipo de terminal do host no qual você está instalando o Agente.
   j. Na lista suspensa Nome do terminal, selecione o Nome do terminal que foi usado na criação do terminal no Console de usuário.

k. Clique em Configurar.

5. Clique em Concluir quando for solicitada a conclusão da instalação e reinicialize.

Atualizar o terminal na Console de usuário

No Console de usuário, atualize o terminal para indicar que o agente está instalado.

Siga estas etapas:

1. Efetue logon no console de usuário.
2. Procure o terminal com o agente instalado.
3. Clique na guia Configurações do terminal.
4. Marque a caixa de seleção Agente de sincronização de senhas instalado.

Ativar um ambiente para sincronização de senhas

Após instalar o Agente de sincronização de senhas, você poderá ativar o ambiente para receber alterações de senha que tenham sido feitas nos terminais. Para essa tarefa, um administrador precisa acessar o Management Console e o CA Directory de modo a ativar o ambiente para aceitar as alterações.

Siga estas etapas:

1. Para novos usuários, você deve usar o Management Console, como se segue:
   a. Selecione o ambiente.
   b. Clique em Advanced Settings, Provisioning.
   c. Marque a caixa de seleção Enable Password Changes from Endpoint Account.
2. Para usuários existentes, defina o atributo eTPropagatePassword como 1 no CA Directory.

Configurar o agente para servidores alternativos

Para configurar o Agente de sincronização de senhas para usar um servidor alternativo, use o assistente Configuração do agente de sincronização de senhas.

Para configurar um servidor alternativo para o agente

1. Execute PwdSyncConfig.exe, localizado em *password_sync_folder*\bin.
2. Insira as informações de configuração a seguir:

   Host

   Especifique o nome do sistema do Servidor de provisionamento.

   Isso preenche o campo URL do servidor com o nome do host especificado.

   Porta LDAP

   Especifique a porta LDAP usada para estabelecer conexão com o Servidor de provisionamento é a 20390. Altere essa porta, conforme a necessidade, se a instalação do Servidor de provisionamento usar uma porta não padrão.
3. Clique no botão Localizar domínio para recuperar o domínio do Servidor de provisionamento.
4. Adicione o nome do host e a porta dos servidores alternativos no campo URLs do servidor usando o seguinte formato:

   ldaps://*host_principal*:20390,ldaps://*host_alternativo_1*:20390
5. Clique em Avançar.
6. Preencha os campos restantes no assistente de configuração.

Como o Agente de sincronização de senhas funciona

O processo de propagação começa quando a senha de um usuário é alterada em um sistema Windows usando qualquer método. Depois que a senha é inserida, ocorre o seguinte:

1. O sistema operacional Windows verifica se a senha cumpre a respectiva política de senha. Se o Windows não aceitar a senha, a solicitação de mudança será rejeitada, uma mensagem de erro será exibida, e nenhuma ação adicional, incluindo a sincronização, será executada.
2. O sistema Windows envia a solicitação de alteração de senha ao Agente de sincronização de senhas, que, se configurado para verificação de qualidade de senha, envia a senha ao Servidor de provisionamento para execução da verificação. Se a senha não estiver de acordo com as regras de qualidade do CA Identity Manager, a solicitação de mudança será rejeitada e uma mensagem de erro será exibida. A senha do Windows permanece inalterada e a sincronização não ocorre.

3. Uma senha que cumpra as regras de qualidade do Windows e do CA Identity Manager é enviada pelo Agente de sincronização de senhas ao Servidor de provisionamento para propagação.
4. O CA Identity Manager atualiza a senha de usuário global e propaga a nova senha para as contas associadas ao usuário global.

Observação: as regras de senha do Windows e do CA Identity Manager devem ser idênticas ou consistentes, pois as mensagens de erro exibidas têm como base a política de senha do Windows, mesmo que o CA Identity Manager rejeite a solicitação.

O parâmetro de configuração password_update_timeout (eta_pwdsync.conf) especifica quanto tempo (em segundos) o PSA aguarda a confirmação de senha/alteração/propagação do CA Identity Manager. Se o PSA não receber uma confirmação durante esse período, ele continuará como se a propagação tivesse sido bem-sucedida e registrará um aviso (eta_pwdsync.log) que a propagação de alteração de senha não pôde ser verificada. O valor mínimo para o parâmetro é zero (0), o que significa que o PSA não esperará pela confirmação.

Verificação de qualidade de senha em nível de conta

A verificação de qualidade de senha é executada quando as contas em terminais gerenciados são criadas ou modificadas ou quando as senhas de usuário do CA Identity Manager são definidas. A verificação de qualidade de senha em contas é limitada a verificações de acordo com os caracteres na senha. As verificações de senhas do usuário global que têm como base o histórico de alterações recentes (frequência de atualização de senha e frequência de reutilização da senha) não são executadas em contas, pois o CA Identity Manager não pode interceptar todas as alterações para senhas de conta. Portanto, ele não pode ter uma visão precisa do histórico de alterações de senhas com o qual executar essas verificações.

A verificação de senhas da conta é controlada pelos seguintes parâmetros de configuração do domínio:

- Terminal/verificar senhas da conta
- Terminal/verificar senhas da conta em branco

O valor de cada parâmetro especifica para cada terminal gerenciado o nível de verificação que deve ser realizada. O terminal pode ser especificado das seguintes maneiras:

```
ALL
-ALL
<NamespaceName>
-<NamespaceName>
<NamespaceName>:<DirectoryName>
-<NamespaceName>:<DirectoryName>
```

Os formulários que incluem um sinal de menos (-), desativam o parâmetro. Os formulários sem ele, ativam o parâmetro. Os formulários [-]<NamespaceName> controlam todos os terminais do tipo indicado, enquanto os formulários [-]<NamespaceName>:<DirectoryName> controlam terminais individuais. Os formulários [-]ALL controlam todos os terminais de todos os tipos. O valor padrão para ambos os parâmetros é -ALL.

Cada um desses parâmetros pode ser especificado várias vezes. Se vários valores especificarem o mesmo terminal, será usado o último valor. É possível definir regras gerais e regras específicas posteriormente para substituir a regra geral.

O parâmetro Verificação de senhas da conta fornece verificação equivalente à verificação de qualidade de senha do usuário global. Com esse parâmetro ativado para um terminal, o CA Identity Manager verifica qualquer senha em uma alteração solicitada para uma conta existente, incluindo tentativas de definir uma senha em branco. Durante a criação da conta, se nenhuma senha for fornecida, a verificação de qualidade de senha não será executada.

O parâmetro Verificar senhas de conta em branco fornece a verificação adicionada de senhas em branco na criação de contas. Se o perfil de senha estiver ativado e exigir pelo menos uma senha de um único caractere, uma senha em branco causará uma falha na criação da conta. Esse parâmetro é diferente do parâmetro Verificar senhas da conta porque em alguns tipos de terminal é aceitável criar uma conta sem nenhuma senha.

Observação: a verificação de qualidade de senha da conta será ignorada para senhas de conta sincronizadas se a senha fornecida corresponder à senha atual do usuário global.

Aplicação de qualidade de senha

A opção Sincronização de senhas intercepta as solicitações de alteração de senha em sistemas nativos (por exemplo, Windows NT/ADS) e as envia ao CA Identity Manager. O CA Identity Manager sincroniza a senha do usuário global e as senhas da conta associadas ao usuário global. As regras de qualidade de senha do CA Identity Manager para um perfil de senha e as regras de qualidade de senha do sistema nativo (Windows NT/ADS) podem ser usadas para aplicar o controle de qualidade de senha.

Configurar sincronização de senhas

O Agente de sincronização de senhas, inicialmente, é configurado durante a instalação e pode ser reconfigurado a qualquer momento usando o assistente de configuração para Sincronização de senhas. É possível definir outras configurações. Por exemplo, você pode alterar as configurações de verificação de qualidade de senha ou modificar os tempos limite usando o arquivo eta_pwdsync.conf.

Esse arquivo está localizado na pasta password_sync_folder\data\. Todas as chaves nesse arquivo de configuração são definidas durante a instalação do Agente de sincronização de senhas. Portanto, altere essas chaves apenas se for realmente necessário. Consulte o texto nesse arquivo para obter mais informações.

Importante: como precaução, crie um backup do arquivo de configuração antes de editá-lo.

Seção [servidor]

Chave	Descrição	Padrão
host	Especifica o servidor de domínio que gerencia a propagação da senha.	Nenhum
port	Especifica a porta de escuta LDAP do Servidor de provisionamento.	20411
use_tls	Especifica se o protocolo TLS/SSL é usado para proteger a comunicação entre o Agente de sincronização de senhas e o Servidor de provisionamento.	Sim
admin_suffix	Especifica o sufixo de domínio do usuário administrativo que o Agente de sincronização de senhas usa para efetuar logon no CA Identity Manager.	Nenhum
admin	Especifica o nome da conta do usuário administrativo que o Agente de sincronização de senhas usa para efetuar logon no CA Identity Manager.	Nenhum
password	Especifica a senha para o nome da conta especificado na chave administrativa.	Nenhum

Seção [eTaDomain]

Chave	Descrição	Padrão
Domínio	Especifica o domínio de provisionamento em que você instalou o Agente de sincronização de senhas.	Nenhum
etrust_suffix	Especifica o sufixo para o produto CA Identity Manager inteiro.	Nenhum
domain_suffix	Especifica o sufixo de domínio para o domínio de provisionamento.	Nenhum
endpoint type	Especifica o tipo de terminal onde você instalou o Agente de sincronização de senhas.	Nenhum
terminal	Especifica o terminal para o qual o Agente de sincronização de senhas intercepta senhas.	Nenhum
endpoint_dn	Especifica o Nome distinto do terminal.	Nenhum
container_dn	Especifica o Nome distinto do recipiente que contém as contas cujas senhas estão sendo alteradas.	Nenhum
acct_attribute_name	Especifica o nome do atributo da conta, por exemplo, eTN16AccountName para Windows NT.	Depende do tipo de terminal
acct_object_class	Especifica o objectClass das contas.	Depende do tipo de terminal

Seção [PasswordProfile]

Chave	Descrição	Padrão
profile_enabled	Especifica se o recurso de verificação do perfil de senha está ativado.	Não
profile_dn	Especifica se o Assistente de configuração de senha gerará um DN para o perfil de senha.	eTPasswordProfileName=Password Profile,eTPasswordProfileContainerName=Password Profile,eTNamespaceName=CommonObjects,dc=cai,dc=eta

Seção [Timeout]

Chave	Descrição	Padrão
search_acct_dn	Especifica o valor do tempo limite ao pesquisar o DN da conta.	120 segundos

Chave	Descrição	Padrão
pwd_update	Especifica o valor do tempo limite na propagação de senhas.	400 segundos
pwd_quality_check	Especifica o valor do tempo limite (em segundos) ao executar a verificação de qualidade de senha.	1

Seção [Logs]

Chave	Descrição	Padrão
log_file	Especifica o arquivo de log que contém mensagens registradas do Agente de sincronização de senhas.	..\Arquivos de programas\CA\Identity Manager Password Sync Agent
log_level	Especifica o nível de log. Os valores válidos são: 1 - Arquivo inicial 2 - Atualização de senha bem-sucedida ou com falha 3 - Depuração de conexão 4 - Rastreamento	0 para sem log

Tolerância a falhas

Se o Servidor de provisionamento estiver desligado ou sobrecarregado, o Agente de sincronização de senhas pode executar a tolerância a falhar em outro servidor. A tolerância a falhas exige que vários Servidores de provisionamento atendam ao mesmo domínio e ao Agente que usa esses servidores.

A seção sobre como configurar o agente para usar servidores alternativos (na página 121) fornece as instruções de configuração.

Ativar mensagens de log

Para descobrir por que uma modificação de senha foi rejeitada, exiba os logs do Agente de sincronização de senhas. Todas as mensagens registradas são armazenados no arquivoeta_pwdsync.log. Por padrão, esse arquivo está localizado na pasta password_sync_folder\Logs.

O log do Agente de sincronização de senhas pode conter o seguinte:

- Mensagens de erro, que sempre serão registradas.
- Mensagens de diagnóstico (fluxo de processo, rastreamento), que podem ser ativadas ou desativadas com base no valor do parâmetro logging_enabled=yes|no no arquivo eta_pwdsync.conf.

Para obter mais informações, examine o arquivo eta_pwdsync.log e os logs do Servidor de provisionamento do mesmo período de tempo.

O parâmetro de configuração log_level anterior foi substituído, mas mantido para compatibilidade com a versão anterior: log_level=0 é traduzido em logging_enabled=no e log_level=anything, que também é traduzido em logging_enabled=yes. Se os parâmetros antigos e novos estiverem presentes no arquivo de configuração, a configuração explícita do parâmetro logging_enabled=yes|no substituirá a configuração indireta executada por meio do parâmetro log_level=number antigo.

Verificar a instalação

Após a conclusão da instalação do Agente de sincronização de senhas, altere uma senha no sistema Windows para verificar se a senha do usuário global associada à conta também é alterada.

Sincronização de senhas no UNIX e Linux

O CA Identity Manager pode interceptar a alteração de senha de uma conta em um sistema UNIX ou Linux e a propaga para todas as outras contas associadas a seu Usuário global. O componente usado para autenticar as senhas em sistemas de segurança externos é chamado de módulo PAM (Pluggable Authentication Module). Com o módulo PAM, o CA Identity Manager autentica senhas em sistemas de segurança externos para que os usuários globais possam usar as respectivas senhas de sistema existentes para entrar no CA Identity Manager.

Sincronização de senhas do UNIX

É fornecido um módulo de sincronização de senha que detecta eventos de alteração de senha por meio da estrutura UNIX PAM. O módulo Sincronização de senhas do UNIX notifica o Servidor de provisionamento quando há alterações de senha. O Servidor de provisionamento localiza o Usuário global associado e propaga automaticamente as alterações para outras contas relacionadas.

Os sistemas operacionais UNIX que oferecem suporte à estrutura PAM são:

- AIX v5.3 na plataforma Power com o módulo PAM ativado
- HP-UX v11.00 em uma plataforma PA-RISC e em plataformas Itanium® 2
- Solaris v2.6 e superior em plataformas Sparc e Intel
- Linux de 32 bits com glibc v2.2 e superior em plataformas s390 ou Intel i386

  Observação: para plataformas Linux, o binário test_sync deve estar no CAMINHO de todos os usuários, mas somente o usuário raiz, o proprietário, deve ter permissão de execução.

  Para adicionar essa biblioteca ao caminho de todos os usuários, inclua este comando no arquivo global /etc/bashrc:

  ```
  export PATH=$PATH:/etc/pam_CA_eta
  ```

Como o UNIX PAM funciona

O processo a seguir descreve as funções do recurso UNIX PAM:

1. A senha do usuário do UNIX deverá ser alterada por um dos seguintes motivos:
   - Decisão do usuário.
   - O usuário é forçado a alterar a senha pelas configurações do sistema ou por intervenção manual.
   - A senha do usuário é alterada por um administrador.
2. A nova senha é enviada para o serviço de senha da estrutura PAM.
3. O serviço de senha da estrutura PAM chama a biblioteca PAM para atualizar os arquivos de segurança local do UNIX.
4. O serviço de senha da estrutura PAM chama o módulo de sincronização de senhas do UNIX (pam_CA_eta) para notificar o Servidor de provisionamento sobre a alteração da senha.
5. O Servidor de provisionamento atualiza a senha do Usuário global associado e de todas as contas associadas ao Usuário global.

Requisitos para uso da sincronização de senhas do UNIX

Veja a seguir os requisitos para usar o recurso Sincronização de senhas do UNIX:

- O agente de Sincronização de senhas do UNIX deve estar instalado no sistema UNIX em que você deseja detectar alterações de senha.
- O agente remoto do UNIX e o CAM devem estar instalados no sistema UNIX em que o agente de Sincronização de senhas do UNIX reside.
- O sistema deve ser gerenciado como um terminal adquirido. A caixa de seleção O agente de sincronização de senhas está instalado deve estar marcada nas propriedades do terminal adquirido.
- As contas em sistemas gerenciados devem ser exploradas e correlacionadas com usuários globais.
- O ambiente deve permitir que as alterações de senha venham de contas de terminal. Um administrador com acesso ao Management Console ativa esse recurso.

Instalar o recurso UNIX PAM

Siga o procedimento a seguir para instalar o UNIX PAM.

Para instalar o recurso UNIX PAM

1. Selecione o arquivo de pacote que corresponde à sua plataforma UNIX:

Sistema operacional UNIX	Nome do arquivo de pacote
HP-UX v11 PA-RISC	pam_CA_eta-1.1.HPUX.tar.Z
HP-UX Itanium2	pam_CA_eta1.1HPUX-IA64.tar.Z
AIX v5.3 Power	pam_CA_eta-1.1.AIX.tar.Z
Solaris Sparc	pam_CA_eta-1.1.Solaris.tar.Z
Solaris Intel	pam_CA_eta-1.1.SolarisIntel.tar.Z
Linux x86	pam_CA_eta-1.1.Linux.tar.gz
Linux s390	pam_CA_eta-1.1.LinuxS390.tar.gz

2. Transfira o arquivo de pacote escolhido para uma pasta temporária (/tmp) no servidor UNIX usando o FTP no modo binário ou qualquer outra ferramenta de transferência de arquivo que ofereça suporte a arquivos binários. Uma sessão de transferência de exemplo pode parecer da seguinte maneira:

```
W:\Pam>ftp user01
Connected to user01.company.com.
220 user01 FTP server (Version 1.2.3.4) ready.
User (user01,company.com:(none)): root
331 Password required for root.
Password:
230 User root logged in.
ftp> cd /tmp
250 CWD command successful.
ftp> bin
200 Type set to I.
ftp> put pam_CA_eta-1.1.HPUX.tar.Z
200 PORT command successful.
150 Opening BINARY mode data connection for pam_CA_eta-1.1.HPUX.tar.Z.
226 Transfer complete.
ftp: 117562 bytes sent in 0,09Seconds 1306,24Kbytes/sec.
ftp> quit
```

3. Efetue logon como usuário raiz no servidor Unix e extraia o arquivo de pacote:

```
# cd /tmp
# zcat pam_CA_eta-1.1.<platform>.tar.Z | tar -xf -
```

No Linux, use o comando:

```
# tar -xzf pam_CA_eta-1.1.<platform-hardware>.tar.gz
```

4. Copie os arquivos TLS e de configuração na pasta de configuração padrão:

```
# cd pam_CA_eta-1,1
# mv pam_CA_eta /etc
```

5. Copie o módulo pam_CA_eta na pasta Bibliotecas de segurança:

   No AIX, use o comando:

   ```
   # cp -p pam_CA_eta.o /usr/lib/security/
   ```

   No HP-UX, use o comando:

   ```
   # cp -p libpam_CA_eta.1 /usr/lib/security/
   ```

   No HP-UX Itanium2, use o comando:

   ```
   # cp -p libpam_CA_eta.1 /usr/lib/security/hpux32
   ```

   No Linux i386 ou s390, use o comando:

   ```
   # cp -p pam_CA_eta.so /lib/security/
   ```

   No Solaris Sparc ou Intel, use o comando:

   ```
   # cp -p pam_CA_eta.so /usr/lib/security/
   ```

6. (Opcional) Copie os programas de teste:

   ```
   # cp -p test_* /etc/pam_CA_eta
   # cp -p pam_test* (/usr)/lib/security/
   ```

Mais informações

Solução de problemas de sincronização de senhas do UNIX (na página 138)

Atualizar o terminal na Console de usuário

No Console de usuário, atualize o terminal para indicar que o agente está instalado.

Siga estas etapas:

1. Efetue logon no console de usuário.
2. Procure o terminal com o agente instalado.
3. Clique na guia Configurações do terminal.
4. Marque a caixa de seleção Agente de sincronização de senhas instalado.

Ativar um ambiente para sincronização de senhas

Após instalar o Agente de sincronização de senhas, você poderá ativar o ambiente para receber alterações de senha que tenham sido feitas nos terminais. Para essa tarefa, um administrador precisa acessar o Management Console e o CA Directory de modo a ativar o ambiente para aceitar as alterações.

Siga estas etapas:

1. Para novos usuários, você deve usar o Management Console, como se segue:
   a. Selecione o ambiente.
   b. Clique em Advanced Settings, Provisioning.
   c. Marque a caixa de seleção Enable Password Changes from Endpoint Account.
2. Para usuários existentes, defina o atributo eTPropagatePassword como 1 no CA Directory.

Configurando o recurso Sincronização de senhas do UNIX

O recurso Sincronização de senhas do UNIX envolve configuração de parâmetros nos seguintes arquivos:

- /etc/pam_CA_eta/pam_CA_eta.conf
- /etc/pam.conf

Importante: uma vez que a senha de um usuário altamente privilegiado é armazenada no arquivo de configuração pam_CA_eta.conf, esse arquivo deve poder ser lido somente pela conta raiz. Observe que as configurações do arquivo de pacote incluem owner=root e mode=500 e que a opção -p do comando cp os preserva durante a instalação.

Configurar o arquivo pam_CA_eta.conf

Execute o procedimento a seguir para configurar o arquivo pam_CA_eta.conf.

Para configurar o arquivo pam_CA_eta.conf

1. Navegue até a pasta /etc/pam_CA_eta.
2. Edite o arquivo pam_CA_eta.conf. Esse arquivo de configuração contém sua própria documentação.

```
#
#   CA - CA Identity Manager
#
#   pam_CA_eta.conf
#
#   Configuration file for the Unix PAM password module "pam_CA_eta"
#

# keyword: server
# description: the CA Identity Manager LDAP server primary and optional
alternate server hostname
# value: a valid hostname and an optional server
# default: no default
server ETA_SERVER ALT_SERVER

#

# keyword: port
# description: the numeric TCP/IP port number of the CA Identity Manager LDAP
server
# value: a valid TCP/IP port number
# default: 20390
# port 20390


# keyword: use-tls
# description: does it use the secured LDAP over TLS protocol ?
# value: yes or no
# default: yes
# use-tls yes
```

```
# keyword: time-limit
# description: the maximum time in seconds to wait for the end of an LDAP
operation.
# value: a numeric value of seconds
# default: 300
# time-limit 300

# keyword: remote-server
# description: identifies whether on premise or cloud Identity Manager
#              server is used.
#              Cloud based server is accessed by proxying the requests
#              through the on-premise CS, requiring use of remote-server
#              set to 'yes'.
# value: yes or no
# default: no
# remote-server no

# keyword: size-limit
# description: the maximum number of entries returned by the CA Identity
Manager server
# value: a numeric value
# default: 100
# size-limit 100


# keyword: root
# description: the root DN of the CA Identity Manager server
# value: a valid DN string
# default: dc=eta
# root dc=eta


# keyword: domain
# description: the name of the CA Identity Manager domain
# value: a string
# default: im
# domain    im


# keyword: user
# description: the CA Identity Manager Global User name used to bind to the
CA Identity Manager server
# value: a valid Global User name string
# default: etaadmin
# user etaadmin


# keyword: password
# description: the clear-text password of the "binding" CA Identity Manager
Global User
# value: the password of the above Global User
# default: no default
```

```
password SECRET


# keyword: directory-type
# description: the CA Identity Manager Unix Endpoint type of this Unix server
# value: ETC or NIS
# default: ETC
# endpoint-type ETC


# keyword: endpoint-name
# description: the CA Identity Manager Unix Endpoint name of this Unix server
# value: a valid Unix Endpoint name string
# default:
# ETC: the result of the "hostname" command (ie: gethostname() system call)
# NIS: "domain [hostname]" where "domain" is the result of the "domainname"
command
#  (ie: getdomainname() system call) and "hostname" the result of the
"hostname"
#    command (ie: gethostname() system call)
# endpoint-name dirname


# keyword: tls-cacert-file
# description: the name of the CA Identity Manager CA certificate file
# value: a valid full path file name
# default: /etc/pam_CA_eta/et2_cacert.pem
# tls-cacert-file /etc/pam_CA_eta/et2_cacert.pem


# keyword: tls-cert-file
# description: the name of the CA Identity Manager client certificate file
# value: a valid full path file name
# default: /etc/pam_CA_eta/eta2_clientcert.pem
# tls-cert-file /etc/pam_CA_eta/eta2_clientcert.pem


# keyword: tls-key-file
# description: the name of the CA Identity Manager client private key file
# value: a valid full path file name
# default: /etc/pam_CA_eta/eta2_clientkey.pem
# tls-key-file /etc/pam_CA_eta/eta2_clientkey.pem


# keyword: tls-random-file
# description: the name of the "pseudo random number generator" seed file
# value: a valid full path file name
# default: /etc/pam_CA_eta/prng_seed
# tls-random-file /etc/pam_CA_eta/prng_seed


# keyword: use-status
```

```
# description: this module will exit with a non-zero status code in case of
failure.
# value: yes or no
# default: no
# use-status no


# keyword: verbose
# description: this module will display informational or error messages to
the user.
# value: yes or no
# default: yes
# verbose yes
```

Observação: os parâmetros de servidor, domínio e senha não têm um valor padrão e precisam ser atualizados.

Configurar o arquivo pam.conf

O arquivo /etc/pam.conf é o principal arquivo de configuração do módulo PAM. Você deve editar o arquivo para inserir uma linha na pilha de serviços de senha. Em alguns sistemas Linux, o arquivo pam.conf é substituído pelo /etc/pam.d, de modo que você precisará editar o arquivo /etc/pam.d /system-auth.

Para configurar o arquivo pam.conf

1. Navegue até o diretório /etc ou /etc/pam.d se você estiver configurando o módulo PAM em um sistema Linux apropriado.
2. Edite o arquivo pam.conf para inserir uma linha de sincronização de senhas na pilha de serviços de senha. Para configurações específicas de plataforma, consulte os exemplos a seguir:

   passwd password required /usr/lib/security/pam_unix.so

   passwd password optional /usr/lib/security/pam_CA_eta.so

3. (Opcional) É possível adicionar os seguintes parâmetros opcionais na linha do módulo pam_CA_eta:

   config=/path/file

   Indica o local de um arquivo de configuração alternativo.

   syslog

   Envia mensagens de erro e informativas ao serviço do syslog local.

   trace

   Gera um arquivo de rastreamento para cada operação de atualização de senha. Os arquivos de rastreamento são denominados /tmp/pam_CA_eta-trace.<nnnn>, onde <nnnn> é o número PID do processo de senha.

4. Implemente as alterações de configuração específicas de plataforma a seguir:

   Em sistemas AIX, adicione as seguintes linhas ao fim do arquivo /etc/pam.conf:

```
#
# CA Identity Manager Unix Password Synchronization
#
login   password  optional    /usr/lib/security/pam_CA_eta.so syslog
passwd  password  optional    /usr/lib/security/pam_CA_eta.so syslog
rlogin  password  optional    /usr/lib/security/pam_CA_eta.so syslog
su      password  optional    /usr/lib/security/pam_CA_eta.so syslog
telnet  password  optional    /usr/lib/security/pam_CA_eta.so syslog
sshd    password  optional    /usr/lib/security/pam_CA_eta.so syslog
OTHER   password  optional    /usr/lib/security/pam_CA_eta.so syslog
```

   Em sistemas HP-UX, adicione as seguintes linhas ao fim do arquivo /etc/pam.conf:

```
#
# CA Identity Manager Unix Password Synchronization
#
login    password optional    /usr/lib/security/libpam_CA_eta.1 syslog
passwd   password optional    /usr/lib/security/libpam_CA_eta.1 syslog
dtlogin  password optional    /usr/lib/security/libpam_CA_eta.1 syslog
dtaction password optional    /usr/lib/security/libpam_CA_eta.1 syslog
OTHER    password optional    /usr/lib/security/libpam_CA_eta.1 syslog
```

   Em sistemas HP-UX Itanium 2, adicione as seguintes linhas ao fim do arquivo /etc/pam.conf:

```
#
# CA Identity Manager Unix Password Synchronization
#
login    password optional    /usr/lib/security/$ISA/libpam_CA_eta.1 syslog
passwd   password optional    /usr/lib/security/$ISA/libpam_CA_eta.1 syslog
```

```
dtlogin  password optional    /usr/lib/security/$ISA/libpam_CA_eta.1 syslog
dtaction password optional    /usr/lib/security/$ISA/libpam_CA_eta.1 syslog
OTHER    password optional    /usr/lib/security/$ISA/libpam_CA_eta.1 syslog
```

Em sistemas Sun Solaris, adicione a linha pam_CA_eta depois da linha pam_unix existente:

```
#
# Password management
#
other   password required       /usr/lib/security/pam_unix.so.1
other   password optional       /usr/lib/security/pam_CA_eta.so syslog
```

Em sistemas Linux, adicione a linha pam_CA_eta entre as linhas pam_cracklib e pam_unix existentes:

```
password    required     /lib/security/pam_cracklib.so retry=3 type=
password    optional     /lib/security/pam_CA_eta.so syslog
password    sufficient   /lib/security/pam_unix.so nullok use_authtok md5
shadow
password    required     /lib/security/pam_deny.so
```

5. Em sistemas AIX, edite o arquivo /etc/security/login.cfg para definir auth_type = PAM_AUTH. Isso ativa a estrutura PAM, que não é ativada por padrão. Essa é uma configuração de tempo de execução, de modo que não é preciso reinicializar o sistema para que ela entre em vigor.

Solução de problemas de sincronização de senhas do UNIX

Você pode solucionar problemas do recurso UNIX PAM usando as mensagens de rastreamento e do syslog, bem como testando a configuração, a conexão LDAP/TLS, a sincronização de senhas e a estrutura PAM.

Mais informações

Ativando mensagens do syslog (na página 138)
Ativando mensagens de rastreamento (na página 139)

Ativando mensagens do syslog

Adicione o parâmetro de syslog à linha pam_CA_eta no arquivo /etc/pam.conf para permitir que o módulo pam_CA_eta gere mensagens informativas e de erro. Quando a opção de geração de log estiver em uso, o administrador do UNIX verá mensagens informativas nos arquivos de syslog sempre que uma conta do UNIX tiver sua senha alterada. Essas mensagens devem fornecer informações suficientes para o diagnóstico de problemas básicos.

Você pode definir essa opção permanentemente em sistemas de produção, pois ela não exige muito mais recursos do que a execução no serviço silencioso.

Ativando mensagens de rastreamento

Se as mensagens do syslog não fornecerem informações suficientes, o modo de rastreamento poderá fornecer mais detalhes. Para cada operação de atualização de senha, o módulo de rastreamento gera um arquivo denominado /tmp/pam_CA_eta-trace.<nnnn> (onde <nnnn> é o PID do processo de senha) com uma entrada para a maioria das chamadas de função usadas pelo módulo e pelos dados usados ou retornados por essas funções.

Embora os arquivos de rastreamento possam ser lidos apenas pela conta raiz, eles conterão as novas senhas com texto não criptografado. Por esse motivo, esse parâmetro não deve ser usado de forma permanente em um sistema de produção.

Testando o arquivo de configuração

Você pode usar a ferramenta test_config, que está localizada no diretório /etc/pam_CA_eta, para verificar o arquivo de configuração. Primeiramente, você configura a estrutura de pastas da seguinte maneira:

1. Mova a pasta pam_CA_eta em /etc.
2. Copie tudo que está sob pam_CA_eta-1.1 to /etc/pam_CA_eta.

Veja a seguir um exemplo de entrada de linha de comando:

```
/etc/pam_CA_eta/test_config [config=/path/to/config_file]
```

Veja a seguir um exemplo de sessão:

```
./test_config [config=/path/to/config_file]
# ./test_config
./test_config: succeeded
Trace file is /tmp/test_config-trace.1274
```

Conforme mostra a saída do comando, um arquivo de rastreamento foi gerado, contendo todos os detalhes da análise do arquivo de configuração.

Exibir o serviço do CAM

Você pode executar o procedimento a seguir para descobrir quem iniciou o serviço.

Para exibir o serviço do CAM

1. Efetue logon na máquina UNIX como usuário raiz usando o cliente Telnet ou SSH.
2. Emita o comando UNIX a seguir:

   ```
   ps -ef | grep cam
   ```

   Uma exibição semelhante a esta é exibida:

   ```
   root 13822        1 11 11:30:12 ?   0:00 cam
   root 13843 13753  3 11:56:31 pts/5  0:00 grep cam
   ```

Observação: se o usuário raiz do sistema não iniciar os serviços, eles aparecerão iniciados, mas você não poderá usá-los. O CA Identity Manager emite a seguinte mensagem: "Permissão negada: o usuário deve ser raiz".

Testando o conexão LDAP/TLS

Você pode usar a ferramenta test_ldap, localizada no diretório /etc/pam_CA_eta, para verificar a conexão com o Servidor de provisionamento (usando os parâmetros do arquivo de configuração). Veja a seguir um exemplo de entrada de linha de comando:

```
/etc/pam_CA_eta/test_ldap [config=/path/to/config_file]
```

Veja a seguir um exemplo de sessão:

```
./test_ldap [config=/path/to/config_file]
# ./test_ldap: succeeded
Trace file is /tmp/test_ldap-trace.1277
```

Conforme mostra a saída do comando, um arquivo de rastreamento foi gerado, contendo todos os detalhes da análise do arquivo de configuração e a conexão com o Servidor de provisionamento.

Testando a sincronização de senhas

Você pode usar a ferramenta test_sync, localizada na pasta /etc/pam_CA_eta, para verificar se a atualização da senha de uma conta local foi eficazmente propagada pelo Servidor de provisionamento. Veja a seguir um exemplo de entrada de linha de comando:

```
/etc/pam_CA_eta/test_sync <user> <password> [config=/path/to/config_file]
```

Veja a seguir um exemplo de sessão:

```
# /etc/pam_CA_eta/test_sync pam002 newpass1234
CA Identity Manager password synchronization started.
:ETA_S_0245<MGU>, Global User 'pam002' and associated account passwords updated
successfully: (accounts updated: 2, unchanged: 0, failures: 0)
CA Identity Manager password synchronization succeeded.
/etc/pam_CA_eta/test_sync: succeeded
Trace file is /tmp/test_sync-trace.2244
```

Conforme mostra a saída do comando, um arquivo de rastreamento foi gerado, contendo todos os detalhes da análise do arquivo de configuração, a conexão com o Servidor de provisionamento e a atualização da conta.

Ao usar o modo detalhado (usando o parâmetro yes do modo detalhado padrão no arquivo de configuração), o comando fornece mensagens informativas e de possíveis erros sobre a propagação da senha.

Testar a estrutura PAM

Uma biblioteca de testes do módulo PAM está disponível para verificar se as alterações de senha foram corretamente detectadas pela estrutura PAM.

Para testar a estrutura PAM

1. Copie o arquivo pam_test na pasta /usr/lib/security(/hpux32).
2. Adicione uma linha de classe de senha para a biblioteca pam_test sem nenhum parâmetro.

   Veja um exemplo para o Solaris:

   ```
   other password optional /usr/lib/security/pam_test
   ```
3. Emita um comando de senha em um usuário de teste e procure pela linha marcada pam_test[<pid>] no arquivo do syslog.

   A saída do comando mostra o nome do arquivo de rastreamento gerados, por exemplo:

   ```
   pam_test[1417]: Succeeded, trace file is /tmp/pam_test-trace.1417
   ```

Sincronização de senhas no OS400

O Agente de sincronização de senhas permite que as alterações de senha, feitas no sistema do terminal OS/400, sejam propagadas para suas outras contas gerenciadas pelo CA Identity Manager. O Agente de sincronização de senhas funciona da seguinte maneira:

1. Instale e execute o agente no sistema do terminal OS/400

   Como parte da instalação, o programa é registrado com o sistema OS/400 de modo que, quando os usuários mudam suas senhas, o agente envie as alterações de senha ao Servidor de provisionamento.

2. O Servidor de provisionamento propaga a alteração de senha para as contas associadas.

   As alterações de senha iniciadas a partir do comando Alterar senha (CHGPWD) ou da API de alteração de senha (QSYCHGPW) são recebidas pelo agente.

3. O agente registra o sucesso ou a falha da operação em um arquivo de log localizado em PWDSYNCH/LOG.

Para instalar o Agente de sincronização de senhas

1. Localize a mídia de instalação do Componente de provisionamento.
2. Execute o instalador do Agente de sincronização de senhas ou o OS/400, em \Agent
3. Siga as instruções exibidas na tela para concluir a instalação.

   Observação: as instruções de instalação do link Software do agente de terminal estão incluídas nas seções a seguir.

Instalar o Agente de sincronização de senhas do OS400

Você deve ter os privilégios *ADDOBJ e os seguintes itens são necessários para que o agente receba notificações de alteração de senha:

- O valor do sistema QPWDVLDPGM deve ser definido como *REGFAC
- O programa deve ser registrado com o comando WRKREGINF EXITPNT (QIBM_QSY_VLD_PASSWRD)
- O ambiente deve permitir que as alterações de senha venham de contas de terminal. Um administrador com acesso ao Management Console ativa esse recurso.

O agente é iniciado somente quando uma alteração de senha é feita. Para alterar a senha, emita o comando CHGPWD.

Observação: o Usuário global deve ser sinalizado para sincronização de senha.

No iSeries

1. Efetue logon como um usuário com os privilégios *ALLOBJ e *SECADM (por exemplo, QSECOFR).
2. Crie um usuário chamado PWDSYNCH:

   ```
   CRTUSRPRF USRPRF(PWDSYNCH) PWDEXP(*YES)
   ```

   Observação: como medida de segurança, o usuário é criado com a senha expirada.
3. Crie um savefile para armazenar o pacote de instalação em uma biblioteca de sua escolha (por exemplo, MYLIB):

   ```
   CRTSAVF MYLIB/PWDSYNCH
   ```
4. No computador Windows com o savefile, use o FTP para transferir o savefile para o iSeries:

   ```
   ftp <hostname>
   binary
   cd MYLIB
   put PWDSYNCH.FILE
   ```
5. No iSeries, extraia o programa do savefile:

   ```
   RSTLIB SAVLIB(PWDSYNCH) DEV(*SAVF) SAVF(MYLIB/PWDSYNCH)
   ```

   Esse comando extrai e instala o agente de sincronização na biblioteca PWDSYNCH.
6. Verifique a instalação:

   ```
   DSPLIB PWDSYNCH
   ```

   Os objetos a seguir devem ser exibidos:

Objeto	Tipo	Atributo
PWDSYNCH	*PGM	CLE
CONFIG	*ARQUIVO	PF
LOG	*ARQUIVO	PF

7. Configure o iSeries para usar PWDSYNCH como o programa de saída de validação da senha:

   ```
   CHGSYSVAL SYSVAL(QPWDVLDPGM) VALUE(*REGFAC)
   ADDEXITPGM EXITPNT(QIBM_QSY_VLD_PASSWRD) FORMAT(VLDP0100) PGMNBR(1)
   PGM(PWDSYNCH/PWDSYNCH) TEXT('eTrust Admin Password Synch Agent')
   ```
8. No iSeries, especifique os parâmetros de conexão para o Servidor de conectores do CA IAM:

   ```
   EDTF FILE(PWDSYNCH/CONFIG)
   ```

Instalar o Agente de sincronização de senhas do OS400

Você deve ter os privilégios *ADDOBJ e os seguintes itens são necessários para que o agente receba notificações de alteração de senha:

- O valor do sistema QPWDVLDPGM deve ser definido como *REGFAC
- O programa deve ser registrado com o comando WRKREGINF EXITPNT (QIBM_QSY_VLD_PASSWRD)
- O ambiente deve permitir que as alterações de senha venham de contas de terminal. Um administrador com acesso ao Management Console ativa esse recurso.

O agente é iniciado somente quando uma alteração de senha é feita. Para alterar a senha, emita o comando CHGPWD.

Observação: o Usuário global deve ser sinalizado para sincronização de senha.

No iSeries

1. Efetue logon como um usuário com os privilégios *ALLOBJ e *SECADM (por exemplo, QSECOFR).
2. Crie um usuário chamado PWDSYNCH:

   ```
   CRTUSRPRF USRPRF(PWDSYNCH) PWDEXP(*YES)
   ```

   Observação: como medida de segurança, o usuário é criado com a senha expirada.
3. Crie um savefile para armazenar o pacote de instalação em uma biblioteca de sua escolha (por exemplo, MYLIB):

   ```
   CRTSAVF MYLIB/PWDSYNCH
   ```
4. No computador Windows com o savefile, use o FTP para transferir o savefile para o iSeries:

   ```
   ftp <hostname>
   binary
   cd MYLIB
   put PWDSYNCH.FILE
   ```
5. No iSeries, extraia o programa do savefile:

   ```
   RSTLIB SAVLIB(PWDSYNCH) DEV(*SAVF) SAVF(MYLIB/PWDSYNCH)
   ```

   Esse comando extrai e instala o agente de sincronização na biblioteca PWDSYNCH.
6. Verifique a instalação:

   ```
   DSPLIB PWDSYNCH
   ```

   Os objetos a seguir devem ser exibidos:

Objeto	Tipo	Atributo
PWDSYNCH	*PGM	CLE
CONFIG	*ARQUIVO	PF
LOG	*ARQUIVO	PF

7. Configure o iSeries para usar PWDSYNCH como o programa de saída de validação da senha:

```
CHGSYSVAL SYSVAL(QPWDVLDPGM) VALUE(*REGFAC)
ADDEXITPGM EXITPNT(QIBM_QSY_VLD_PASSWRD) FORMAT(VLDP0100) PGMNBR(1)
PGM(PWDSYNCH/PWDSYNCH) TEXT('eTrust Admin Password Synch Agent')
```

8. No iSeries, especifique os parâmetros de conexão para o Servidor de conectores do CA IAM (CA IAM CS):

```
EDTF FILE(PWDSYNCH/CONFIG)
```

Atualizar o terminal na Console de usuário

No Console de usuário, atualize o terminal para indicar que o agente está instalado.

Siga estas etapas:

1. Efetue logon no console de usuário.
2. Procure o terminal com o agente instalado.
3. Clique na guia Configurações do terminal.
4. Marque a caixa de seleção Agente de sincronização de senhas instalado.

Ativar um ambiente para sincronização de senhas

Após instalar o Agente de sincronização de senhas, você poderá ativar o ambiente para receber alterações de senha que tenham sido feitas nos terminais. Para essa tarefa, um administrador precisa acessar o Management Console e o CA Directory de modo a ativar o ambiente para aceitar as alterações.

Siga estas etapas:

1. Para novos usuários, você deve usar o Management Console, como se segue:
   a. Selecione o ambiente.
   b. Clique em Advanced Settings, Provisioning.
   c. Marque a caixa de seleção Enable Password Changes from Endpoint Account.
2. Para usuários existentes, defina o atributo eTPropagatePassword como 1 no CA Directory.

Configuração do SSL

O SSL é usado para criptografar a comunicação entre o agente de sincronização e o Servidor de provisionamento. Isso é importante para o agente de sincronização porque o SSL envia senha pela rede. É recomendável sempre usar o SSL.

O agente de sincronização deve confiar no certificado do Servidor de provisionamento para se conectar ao SSL. Desse modo, o certificado deve ser instalado na máquina iSeries e configurado para que o agente de sincronização possa confiar nele. Essas tarefas são executadas pelo Gerenciador de certificados digitais, um componente opcional do OS/400. Siga a documentação do OS/400 para instalar e configurar o Gerenciador de certificados digitais.

Instalar o certificado do Servidor de provisionamento

Os seguintes componentes de sistema operacional devem estar instalados na sua máquina iSeries para usar o SSL:

- Programa licenciado de provedor de acesso criptográfico (5722-AC3)
- Gerenciador de certificados digitais (Opção 34 do OS/400)
- IBM HTTP Server para iSeries (5722-DG1)

No iSeries

1. Faça upload do certificado do Servidor de provisionamento da máquina com o Servidor de provisionamento para o iSeries. O certificado pode ser encontrado em:

   ```
   C:\Arquivos de programa\CA\Identity Manager\Provisioning
   Server\Data\Tls\server\et2_cacert.pem
   ```

2. Efetue logon no DCM.

   Usando um navegador web, acesse http://<nome_do_host>: 2001. Quando solicitado, efetue logon como QSECOFR e clique em Gerenciador de certificados digitais.

3. Clique em Selecionar um repositório de certificados e selecione o repositório de certificados *SYSTEM. Se esse repositório não existir, crie um chamado *SYSTEM e, em seguida, insira a senha do repositório de certificados.

4. Importe o certificado como um certificado da CA usando o DCM.

   Clique em Gerenciar certificados, Importar certificado. Selecione a opção CA (Autoridade de Certificação) e insira o nome do arquivo do certificado do servidor de provisionamento. (Esse é o local para onde você transferiu o certificado na etapa 1). Insira o rótulo Servidor de provisionamento para o certificado.

5. Depois de importar o certificado CA para o repositório de chaves *SYSTEM do terminal, verifique se o cliente do IBM Directory QIBM_GLD_DIRSRV_CLIENT pode acessar o repositório de chaves *SYSTEM. Caso contrário, haverá falha na chamada de inicialização do SSL do PSA.

6. Configure o aplicativo cliente de serviços do diretório para confiar no certificado do servidor de provisionamento abrindo Gerenciar aplicativos, Definir lista de CAs confiáveis e escolhendo Cliente de serviços do diretório.

   O certificado do Servidor de provisionamento deverá estar listado aqui se foi importado corretamente da etapa 4.

   Clique em Confiável para o certificado do servidor de provisionamento e, em seguida, clique em OK.

7. Forneça a permissão de leitura PUBLIC aos arquivos SSL e conceda acesso de leitura ao repositório de certificados *SYSTEM:

   `(/QIBM/userdata/ICSS/Cert/Server/default.kdb)`

   Conceda permissão de leitura e execução à pasta pai

   `(/QIBM/userdata/ICCS/Cert/Server)`

   Observação: a adoção da autoridade de usuário PWDSYNCH não funciona no sistema de arquivos /, de modo que o acesso deve ser concedido a todos os usuários.

Desinstalar o Agente de sincronização de senhas

Se for necessário desinstalar o Agente de sincronização de senhas, siga este procedimento.

Do ponto de saída de validação da senha

1. Remova PWDSYNCH:

   ```
   RMVEXITPGM EXITPNT(QIBM_QSY_VLD_PASSWRD) FORMAT(VLDP0100) PGMNBR(1)
   ```

2. Exclua a biblioteca de agentes de sincronização:

   ```
   DLTLIB PWDSYNCH
   ```

3. Exclua o usuário PWDSYNCH

   ```
   DLTUSRPRF PWDSYNCH
   ```

4. Remova o certificado do Servidor de provisionamento seguindo as instruções do SSL para entrar no DCM e trabalhar com o repositório de certificados *SYSTEM:

   Clique em Gerenciar certificados, Excluir certificado e selecione CA (Autoridade de Certificação)

   Selecione o certificado Servidor de provisionamento e clique em Excluir.

O parâmetro do agente de senha do OS/400 deve ser definido corretamente

O parâmetro pwd_case_action deve ter o valor definido corretamente para que funcione. Os valores corretos incluem:

- pwd_case_action = pwd_case_unchanged
- pwd_case_action = pwd_to_uppercase
- pwd_case_action = pwd_to_lowercase

Se pwd_case_action = [invalid value], a senha deverá ser em letras maiúsculas.

Observação: ao definir o sinalizador pwd_case_action para pwd_to_uppercase ou pwd_to_lowercase no arquivo de configuração PSA do OS400, a senha poderá não ser propagada de volta ao usuário global se as senhas fornecidas não forem compatíveis com as configurações de política de senha no Servidor de provisionamento. Por exemplo, algumas políticas de senha podem exigir que os valores contenham, pelo menos, 1 valor de letra maiúscula ou minúscula.

Observação: observe o valor do sistema QPWDLVL (Nível de senha) ao configurar o Agente de sincronização de senhas.

- Quando QPWDLVL for definido como 0 (valor padrão) no sistema AS400, as senhas com um comprimento de 1 a 10 caracteres maiúsculos serão suportadas.
- Quando QPWDLVL for definido como 2 ou 3, serão permitidas as senhas de 1 a 128 caracteres com uma combinação de letras maiúsculas e minúsculas.

Por padrão, o PSA propaga a senha não alterada para o Servidor de provisionamento. No entanto, independentemente do valor de QPWDLVL, você pode forçar o PSA a propagar as senhas com maiúsculas ou minúsculas definindo pwd_case_action para pwd_to_uppercase ou pwd_to_lowercase, respectivamente.

Capítulo 6: Grupos

É possível criar vários tipos de grupos ou uma combinação deles:

- Grupo estático - Uma lista de usuários adicionados de forma interativa
- Grupo dinâmico - Os usuários pertencem ao grupo quando correspondem a uma consulta LDAP (Requer um diretório LDAP como repositório de usuários.)

  Observação: o campo Consulta de grupo dinâmico não é incluído na tarefa Criar grupo ou em outras tarefas de grupo, mesmo que esse campo exista no directory.xml para um grupo. Você inclui o campo Consulta de grupo dinâmico na tarefa editando a tela do perfil associado.
- Grupo aninhado - um grupo que contém outros grupos (Requer um diretório LDAP como repositório de usuários.)

Observação: para exibir os grupos estáticos, dinâmicos e aninhados aos quais um usuário pertence, use a guia Grupos do objeto do usuário. A guia aparece nas tarefas Exibir usuário e Modificar usuário por padrão.

Esta seção contém os seguintes tópicos:

Criar um grupo estático

É possível associar um conjunto de usuários a um *grupo estático*. Para gerenciar o grupo estático, adicione ou remova usuários da lista de associações do grupo. Para ver a lista de integrantes de um grupo, use a guia Associação, que é incluída nas tarefas Exibir grupo e Modificar grupo por padrão.

Observação: a guia Associação exibe somente os integrantes explicitamente adicionados ao grupo. Não exibe os integrantes adicionados dinamicamente.

Para criar um grupo estático:

1. No console de usuário, selecione Grupos, Criar grupo.
2. Escolha se deseja criar um grupo ou uma cópia de um grupo e clique em **OK**.
3. Na guia Perfil, digite um nome de grupo, organização do grupo, descrição e nome do administrador do grupo.

4. Clique na guia Associação.
5. Clique em Adicionar um usuário.
6. Pesquise os usuários para incluir.
7. Coloque uma marca de seleção ao lado dos usuários e clique em Selecionar.
8. Clique em Enviar.

Criar um grupo dinâmico

É possível criar um *grupo dinâmico* definindo uma consulta por filtro LDAP usando o console de usuário para determinar dinamicamente a associação de grupo em tempo de execução, sem precisar procurar e adicionar usuários individualmente.

Por exemplo, se desejar gerar um grupo que lista todos os funcionários de NeteAuto dos EUA, você pode definir um filtro de pesquisa LDAP semelhante ao seguinte no campo Consulta de grupo dinâmico do console de usuário:

ldap:///cn=Employees,o=NeteAuto,c=US??sub

Você também pode modificar essa consulta para localizar os funcionários fora dos Estados Unidos.

A Amostra de grupos estáticos, dinâmicos e aninhados (na página 155) mostra um exemplo de um grupo criado por grupos estáticos, dinâmicos e aninhados.

Você inclui o campo Consulta de grupo dinâmico na tarefa editando a tela do perfil associado. Ele não é incluído por padrão na tarefa Criar grupo.

Observação: para ativar grupos dinâmicos, os administradores do sistema configuram o suporte no arquivo de configuração de diretório (directory.xml):

- Adicione o elemento GroupTypes à seção Comportamento de grupos de diretórios da seguinte maneira:

  <GroupTypes type=*type*>

  tipo pode ser ANINHADO (na página 153), DINÂMICO ou TUDO.

  O GroupTypes diferenciam maiúsculas de minúsculas.
- Mapear o conhecido atributo %DYNAMIC_GROUP_MEMBERSHIP% para um atributo físico que existe no armazenamento de usuários.

Para criar um grupo dinâmico:

1. No console de usuário, selecione Grupos, Criar grupo.
2. Escolha se deseja criar um grupo ou uma cópia de um grupo e clique em **OK**.

3. Na guia Perfil, digite um nome de grupo, organização do grupo, descrição e nome do administrador do grupo.
4. Digite um filtro de pesquisa LDAP semelhante ao seguinte exemplo no campo Consulta de grupo dinâmico:

   ldap:///cn=Employees,o=NeteAuto,c=US??sub?
5. Clique em Enviar.

Observação: apenas um administrador com a tarefa Modificar grupo pode alterar a associação dinâmica a um grupo.

Parâmetros de consulta de grupo dinâmico

Você pode usar os seguintes parâmetros de consulta dinâmica na pesquisa:

ldap:///*<search_base_DN>*??*<search_scope>*?*<searchfilter>*

- *<search_base_DN>* é o ponto a partir do qual iniciar a pesquisa no diretório LDAP. Se não especificar o DN base na consulta, a organização do grupo será o DN base padrão.
- *<search_scope>* especifica a extensão da pesquisa e inclui:
  - sub - retorna entradas em nível equivalente ou inferior ao do DN base.
  - one - retorna entradas um nível abaixo do DN base especificado no URL. (padrão)
  - base - usa one, ignorando base como opção de pesquisa.

  Usar one ou base obtém apenas os usuários na organização do DN base.

  Usar sub obtém todos os usuários abaixo da organização do DN base e todas as suborganizações na árvore.

- *<searchfilter>* é o filtro que deseja aplicar às entradas dentro do escopo da pesquisa. Ao inserir um filtro de pesquisa, use a sintaxe de consulta LDAP padrão, como segue:

  (<logical operator ><comparison><comparison...>)

  - <logical operator> é um dos seguintes:

    Logical OR: |

    Logical AND: &

    Logical NOT: !

  - <comparison> indica <attribute><operator><value>

  Por exemplo:

  (&(city=boston)(state=Massachusetts))

  O filtro de pesquisa padrão é (objectclass=*).

Observe o seguinte ao criar uma consulta dinâmica:

- O prefixo "ldap" deve estar em letra minúscula, por exemplo:

  ldap:///o=MyCorporation??sub?(title=Manager)

- Não é possível especificar o nome do host nem o número da porta do servidor LDAP. Todas as pesquisas ocorrem dentro do diretório LDAP associado ao ambiente.

A tabela a seguir contém exemplos de consultas LDAP:

Descrição	**Consulta**
Todos os usuários que são gerentes.	ldap:///o=MyCorporation??sub?(title=Manager)
Todos os gerentes na filial do oeste de Nova Iorque	ldap:///o=MyCorporation??one?(&(title=Manager) (roomNumber=NYWest))
Todos os técnicos com celular	ldap:///o=MyCorporation??one? (&(employeetype=technician) (mobile=*))
Todos os funcionários cujo número de funcionário está entre 1000 e 2000	ldap:///o=MyCorporation, (& (ou=employee) (employeenumber >=1000) (employeenumber <=2000))
Todos os administradores da central de atendimento empregados há mais de 6 meses	ldap:///o=MyCorporation,(& (cn=helpdeskadmin) (DOH => 2004/04/22) **Observação:** esta consulta requer que você crie um atributo DOH para a data de contratação do usuário.

Observação: as comparações > e < (maior que e menor que) são lexicográficas, não aritméticas. Para obter detalhes sobre seu uso, consulte a documentação do servidor de diretórios LDAP.

Criar um grupo aninhado

Se o repositório de usuários for um diretório LDAP, você pode adicionar um grupo como integrante de outro grupo. O grupo é chamado de *grupo aninhado*.

O grupo que contém o grupo aninhado é chamado de *grupo pai*. Os integrantes do grupo aninhado se tornam integrantes do grupo pai. No entanto, os integrantes do grupo pai não se tornam integrantes de um grupo aninhado.

Grupos aninhados são semelhantes às listas de distribuição de email, em que uma lista pode ser integrante de outra. Com grupos aninhados, você pode adicionar grupos e usuários como integrantes do grupo. Ao aninhar um grupo em outra lista de associações do grupo, você pode incluir todos os integrantes dos grupos aninhados.

Por exemplo, se você criou grupos separados para as divisões de manufatura, design, remessa e contabilidade de uma empresa, você pode construir um grupo pai para a empresa inteira aninhando todos os grupos de divisões separadas como integrantes do grupo pai da empresa. Como resultado, todas as alterações feitas nos grupos aninhados de manufatura, design, remessa e contabilidade serão automaticamente refletidas no grupo aninhado para a empresa inteira. Um grupo que está aninhado em outro grupo pode ser dinâmico e/ou conter outros grupos aninhados.

A figura na Amostra de grupos estáticos, dinâmicos e aninhados (na página 155) mostra um grupo pai criado por grupos estáticos, dinâmicos e aninhados.

Esteja ciente do seguinte antes de criar um grupo aninhado:

- Apenas um administrador com a tarefa Modificar integrantes do grupo pode adicionar ou modificar grupos aninhados na lista de integrantes estáticos do grupo no console de usuário.
- Apenas usuários com os privilégios de administrador apropriados podem modificar, adicionar ou remover integrantes de um grupo.

  Por exemplo, se um grupo pai A tiver sido criado pelos grupos aninhados B e C, o administrador do grupo A pode modificar apenas os integrantes do Grupo A, e não do B e C. Os Grupos B e C podem ser modificados apenas por seus administradores apropriados.
- Para ativar os grupos aninhados, os administradores do sistema configuram o suporte de grupo aninhado no arquivo de configuração de diretório (diretório.xml):
  - Adicione o elemento GroupTypes à seção Comportamento de grupos de diretórios da seguinte maneira:

    <GroupTypes type=*type*>

    tipo pode ser ANINHADO, DINÂMICO (na página 150) ou TUDO.

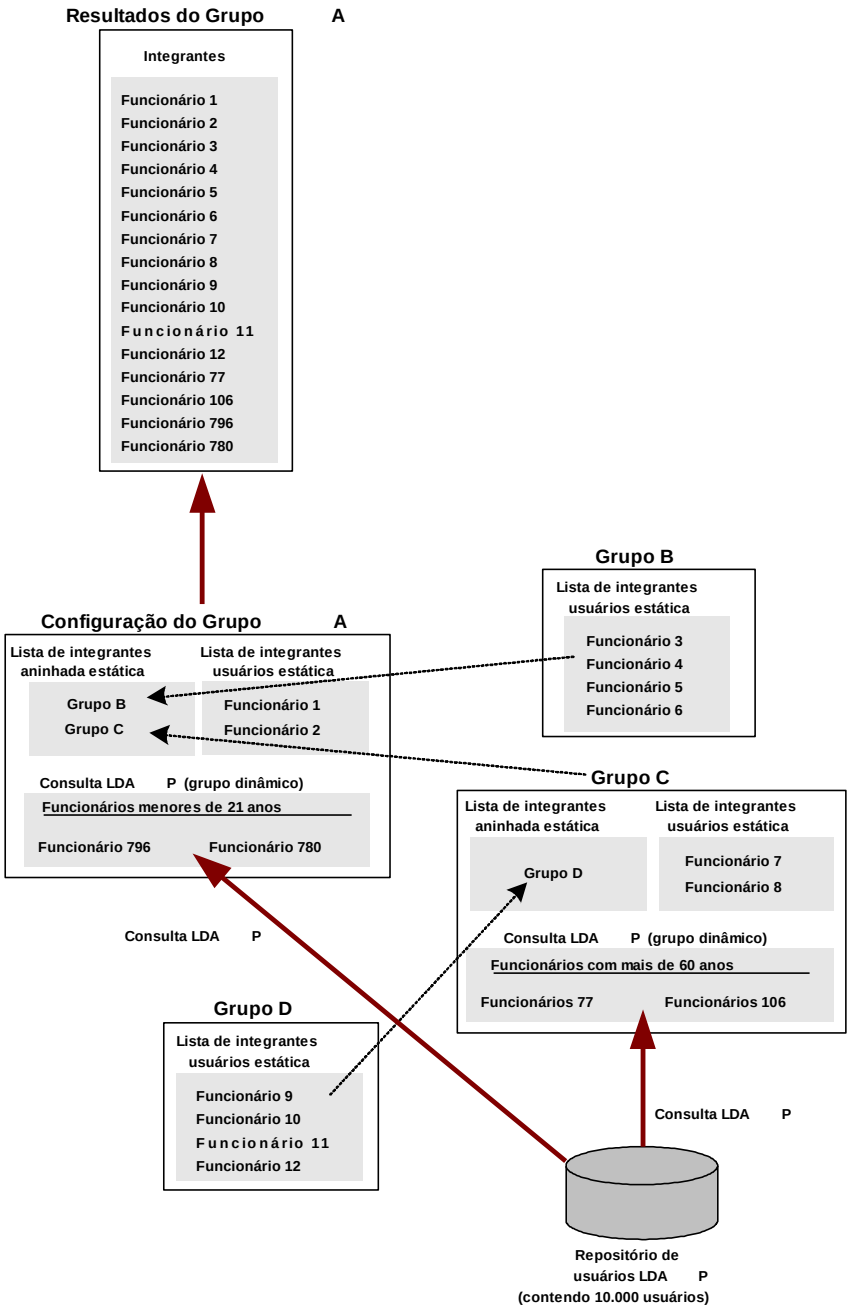
    O GroupTypes diferenciam maiúsculas de minúsculas.
  - Mapeie o conhecido atributo %NESTED_GROUP_MEMBERSHIP% para um atributo físico que existe no armazenamento de usuários.

Para criar um grupo aninhado:

1. No console de usuário, selecione Grupos, Criar grupo.
2. Escolha se deseja criar um grupo ou uma cópia de um grupo e clique em **OK**.
3. Na guia Perfil, digite um nome de grupo, organização do grupo, descrição e nome do administrador do grupo.
4. Na guia Associação:
   a. Clique em Adicionar um grupo para adicionar um grupo aninhado a esse grupo.
   b. Pesquise um grupo existente.
   c. Coloque uma marca de seleção ao lado do grupo e clique em Selecionar.
   d. Clique em Enviar.

Amostra de grupos estáticos, dinâmicos e aninhados

Os grupos podem ser complexos, consistindo em uma combinação de grupos dinâmicos, estáticos ou aninhados. A figura a seguir mostra um exemplo de um grupo pai criado por grupos estáticos, dinâmicos e aninhados.



Na figura anterior:

- O Grupo pai A contém os grupos aninhados B e C, dois usuários estáticos e uma consulta LDAP dinâmica que lista todos os funcionários com menos de 21 anos.
- O Grupo B é composto de quatro usuários estáticos.
- O Grupo pai C contém o Grupo aninhado D, dois usuários estáticos e uma consulta LDAP dinâmica que lista todos os funcionários com mais de 60 anos.
- O Grupo D contém quatro usuários estáticos.
- A parte superior da figura lista os integrantes do Grupo A que resultaram das listas de integrantes de grupos aninhados, consultas dinâmicas e usuários estáticos dos Grupos B, C e D.

Administradores de grupo

Na guia Administradores das tarefas Criar grupo ou Modificar grupo, você pode especificar usuários e grupos como administradores de um grupo. Ao atribuir um usuário como administrador de grupo, verifique se o administrador tem uma função com escopo apropriado para gerenciar o grupo. Por exemplo:

1. Use Modificar grupo para atribuir um usuário como administrador de um grupo.
2. Atribua a esse usuário uma função administrativa com tarefas de gerenciamento de grupos, como Modificar integrantes do grupo, ou tarefas de gerenciamento de usuários com uma guia Grupos.
3. Verifique se a função tem o escopo apropriado sobre o grupo.
   a. Use a opção Exibir função administrativa na função que você atribuiu com tarefas de gerenciamento de grupos.
   b. Na guia Integrantes, certifique-se de que existe uma política com o seguinte:

      Uma regra de integrante que o administrador do grupo atende

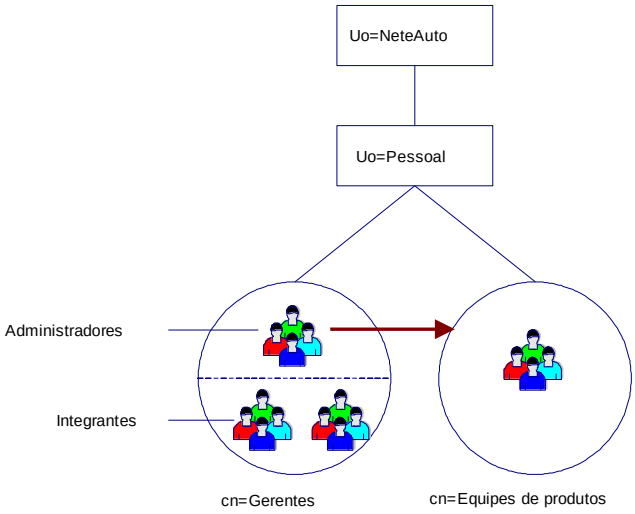
      Uma regra de escopo que inclui o grupo

      Uma regra de escopo que inclui alguns usuários que podem ser adicionados ao grupo

Observação: para ativar os grupos que serão os administradores de outros grupos, os administradores do sistema configuram o suporte a administradores de grupos no arquivo de configuração de diretório (diretório.xml):

- Defina o AdminGroupTypes type=ALL na seção de Comportamento de Grupos de administração de diretório. O AdminGroupTypes diferencia maiúsculas de minúsculas.
- Mapeie o conhecido atributo %GROUP_ADMIN_GROUP% para um atributo físico que existe no armazenamento de usuários.

Ao atribuir um grupo como um administrador, apenas os administradores desse grupo serão os administradores do grupo que você estiver criando ou modificando. Integrantes do grupo do administrador que você especificar não terão privilégios para gerenciar o grupo. A ilustração a seguir mostra um grupo como administrador de outro grupo.



Neste exemplo:

- O grupo de gerentes é um administrador do grupo de equipes do produto.
- Os administradores do grupo de gerentes podem gerenciar o grupo de equipes do produto. Os integrantes do grupo de gerentes não podem.

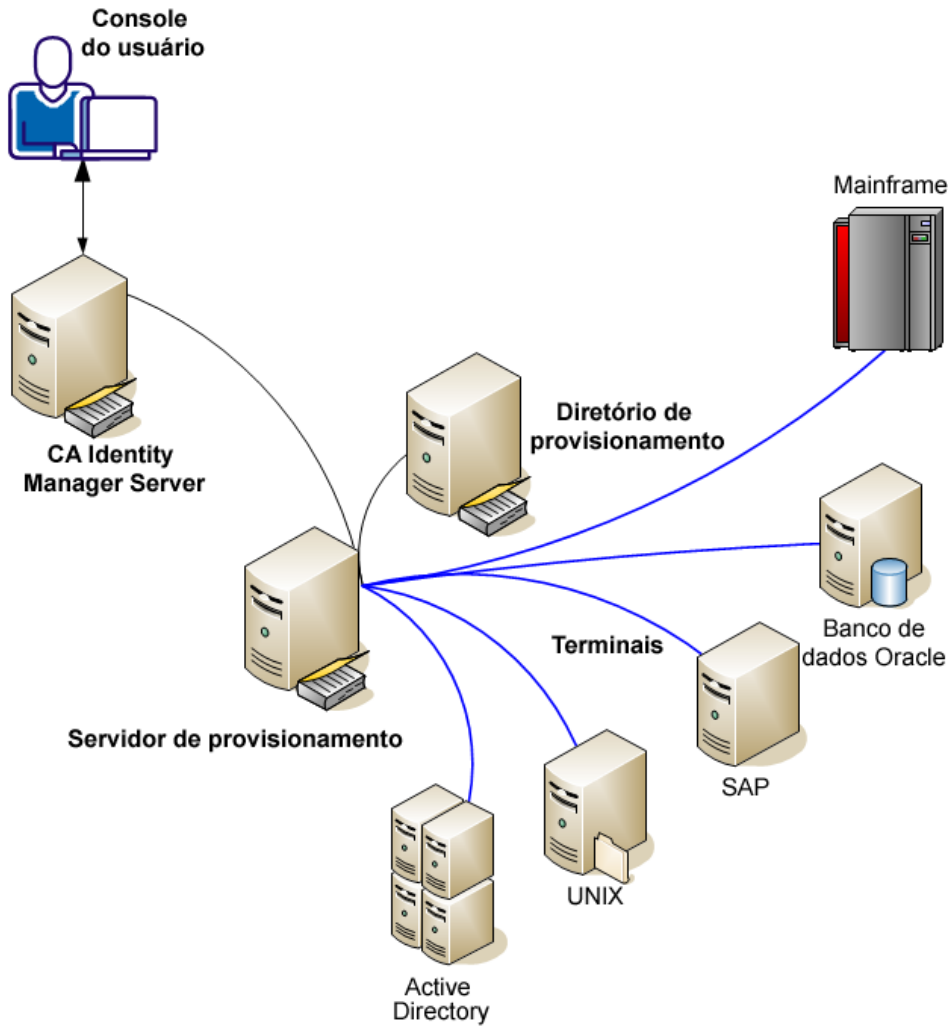
Capítulo 7: Contas de terminal gerenciadas

No CA Identity Manager, você pode gerenciar contas nos sistemas do terminal se a sua instalação do CA Identity Manager tiver um servidor de provisionamento. Você pode gerenciar contas, como uma conta do Exchange, Windows NT ou Oracle, e gerenciar contas órfãs e do sistema, que são contas que não estão associadas ao CA Identity Manager.

Esta seção contém os seguintes tópicos:

Integrando terminais gerenciados

Com o CA Identity Manager, você pode gerenciar contas de vários sistemas em uma única interface de usuário: o console de usuário. As contas estão em sistemas que são chamados de terminais gerenciados ou apenas de terminais. No exemplo a seguir, você gerencia os usuários em cinco terminais.



Você pode atribuir contas em qualquer combinação de terminais para um usuário. Ao integrar o terminal, o CA Identity Manager associa cada conta do terminal a um usuário no diretório de provisionamento.

Os procedimentos a seguir descrevem como integrar os terminais, de forma que as contas de terminal possam ser gerenciadas no console de usuário.

1. Importar o arquivo de definição de função (na página 161)
2. Criar regras de correlação
3. Adicionar o terminal ao ambiente
4. Criar uma definição para a opção Explorar e correlacionar
5. Explorar e correlacionar o terminal

Importar o arquivo de definição de função

Importe as definições de função a partir de um arquivo que se aplica ao novo terminal. Esse procedimento requer acesso ao Management Console.

Siga estas etapas:

1. No Management Console, clique em Ambiente.
2. Selecione o ambiente onde estiver adicionando o terminal.
3. Clique em Role and Task Settings.
4. Clique em Importar.
5. Selecione um terminal em Tipo de terminal.
6. Clique em Finalizar.

   O status da importação é exibido na janela atual.
7. Clique em Continuar para sair.
8. Reinicie o ambiente para que as alterações entrem em vigor.

Criar regras de correlação

Um administrador de hospedagem ou um administrador com a tarefa Configurar atributos de correlação pode criar regras que são usadas quando você explora um terminal. A tarefa Executar a opção Explorar e correlacionar usa essas regras para a parte de correlação da tarefa.

As regras de correlação determinam como um atributo da conta do terminal é mapeado para um atributo de usuário no console de usuário. Por exemplo, no Access Control, um atributo chamado AccountName existe. É possível criar uma regra para mapeá-lo para FullName no console de usuário. Se as regras fizerem com que dois mapeamentos sejam aplicados a um atributo de usuário, o primeiro valor do parâmetro será usado.

Siga estas etapas:

1. Efetue logon no console de usuário.
2. Clique em Sistema, Configuração de provisionamento, Configurar atributos de correlação.
3. Clique em Adicionar.
4. Defina uma regra de correlação, da seguinte maneira:
   a. Selecione uma lista de atributos de usuário global.

      Esse valor se refere ao atributo de usuário listado no diretório de provisionamento.

   b. Marque a caixa de seleção Definir um atributo de conta específico.
   c. Selecione um tipo de terminal.
   d. Selecione um atributo de conta aplicável ao atributo de usuário global.
   e. Opcionalmente, preencha os campos de subsequência de caracteres.

      Se o campo Subsequência de caracteres de estiver em branco, o processamento será iniciado no início da sequência de caracteres. Se o campo Subsequência de caracteres para estiver em branco, o processamento será iniciado no final da sequência de caracteres.
5. Clique em OK.
6. Clique em Enviar.

Observação: sempre que alterar uma regra de correlação, não deixe de explorar o terminal, mesmo que ele tenha sido explorado previamente.

Exemplo de regras de correlação

O exemplo a seguir fornece amostras de configurações para um terminal do Active Directory.

```
GlobalUserName
FullName=LDAP Namespace:globalFullName
FullName=ActiveDirectory:DisplayName
 CustomField01=ActiveDirectory:Telephone
```

As ações a seguir ocorrerem para cada conta previamente sem correlação que for encontrada durante a correlação de contas em um recipiente do Active Directory:

1. O servidor de provisionamento compara o primeiro valor do parâmetro (GlobalUserName) com o atributo da conta do terminal do Active Directory (NT_AccountID). O servidor tentará localizar o usuário global exclusivo cujo nome corresponde ao valor do atributo NT_AccountID para essa conta. Se uma correspondência exclusiva for encontrada, o servidor de provisionamento associará a conta ao usuário global. Se mais de uma correspondência for encontrada, o servidor de provisionamento executará a Etapa 5. Se nenhuma correspondência for encontrada, o servidor de provisionamento executará a próxima etapa.
2. O servidor de provisionamento considera o segundo valor do parâmetro (FullName=LDAP Namespace:globalFullName). Como esse valor é específico para outro tipo de terminal, será ignorado, e o servidor de provisionamento executará a próxima etapa.
3. O servidor de provisionamento considera o terceiro valor do parâmetro (FullName=ActiveDirectory:DisplayName). Como esse valor é específico para o Active Directory, será usado. O servidor tentará localizar o usuário global exclusivo cujo FullName corresponde ao valor do atributo DisplayName para essa conta. Se uma correspondência exclusiva for encontrada, o servidor de provisionamento associará a conta ao usuário global. Se mais de uma correspondência for encontrada, o servidor de provisionamento executará a Etapa 5. Se nenhuma correspondência for encontrada, o servidor de provisionamento executará a Etapa 4.
4. O servidor de provisionamento considera o valor final do parâmetro (CustomField01=ActiveDirectory:Telephone). Como esse valor é específico para o Active Directory, será usado. O servidor tentará localizar o usuário global exclusivo cujo atributo Custom Field #01 é igual ao valor do atributo Telephone para essa conta. O nome que você der ao atributo do usuário global personalizado usando as propriedades globais de Tarefa do sistema não é exibido aqui. Se uma correspondência exclusiva for encontrada, o servidor de provisionamento associará a conta ao usuário global. Se mais de uma correspondência for encontrada, o servidor de provisionamento executará a Etapa 5. Se nenhuma correspondência for encontrada, o servidor de provisionamento executará a próxima etapa.
5. O servidor de provisionamento associa a conta ao objeto [de usuário padrão]. Se o objeto [de usuário padrão] não existir, o servidor irá criá-lo.

Adicionar o terminal ao ambiente

Adicione o terminal ao ambiente onde você pretende gerenciá-lo. Qualquer administrador com a tarefa Criar terminal pode executar esse procedimento.

Siga estas etapas:

1. Selecione Terminais, Manage Endpoints, Criar terminal.
2. Selecione um tipo de terminal.
3. Preencha as guias para preencher os campos.

   Os campos necessários começam com um círculo vermelho.

   Observação: evite usar um símbolo # no nome do terminal, pois esse caractere não pode ser pesquisado.
4. Clique em Enviar.

Você está pronto para criar uma definição para a opção Explorar e correlacionar (na página 164), para que suas contas possam ser gerenciadas.

Criar uma definição para a opção Explorar e correlacionar

Para adicionar usuários existentes em um terminal, você cria uma definição para a opção Explorar e correlacionar para esse terminal. Qualquer administrador com a tarefa Criar definição para a opção Explorar e correlacionar pode criar a definição.

Siga estas etapas:

1. Em um ambiente, clique em Terminais, Definição para a opção Explorar e correlacionar, Criar definição para a opção Explorar e correlacionar.
2. Clique em OK para iniciar uma nova definição.
3. Preencha Explorar e correlacionar com um nome significativo.
4. Clique em Selecione o recipiente/terminal/método de exploração para escolher um terminal e recipientes, se eles existirem. Para um terminal grande, uma pesquisa de recipientes pode demorar um pouco; é possível usar o filtro de pesquisa para limitá-la.
5. Clique em um método de exploração de um recipiente. O processo de explorar e correlacionar inclui recipientes selecionados e seus sub-recipientes. Para um recipiente de diretórios, inclui todos os recipientes da subárvore.

6. Clique em Ação de exploração/correlação para executar:
   - **Explorar diretório para objetos gerenciados** — Localiza objetos que estão armazenados no terminal, e não no diretório de provisionamento.
   - **Correlacionar contas a usuários** — Correlaciona os objetos que foram encontrados na função de exploração a usuários no diretório de provisionamento. Existem duas opções de correlação.
     - **Usar usuários existentes**

       Use essa opção para uma regra de correlação (na página 161) que corresponde cada conta a um usuário criado anteriormente.

       Se o usuário for encontrado, a conta será correlacionada a esse usuário. Se vários usuários forem encontrados, a conta será correlacionada com o usuário padrão. Se nenhum usuário for encontrado, essa opção cria o usuário (se todos os atributos obrigatórios forem conhecidos) e correlaciona a conta com esse usuário; caso contrário, correlaciona a conta com o usuário padrão.
     - **Criar usuários, conforme necessário**

       Use essa opção quando correlacionar contas no terminal principal. Essa opção pressupõe que as contas no terminal são nomeadas exatamente da mesma forma que os usuários. O algoritmo de correlação e correspondência não é usado com esta opção. Em vez disso, cada conta é associada ao usuário com o mesmo nome. Se o usuário ainda não existir, será criado. Nenhuma conta é associada ao usuário padrão.
   - **Atualizar campos de usuário** — Se um mapeamento existir entre os campos de objetos e os campos de usuários, os campos de usuários serão atualizados com os dados dos campos de objetos.

     Os usuários são criados sem atributos opcionais, como nome completo, endereço e telefones. Durante a aquisição inicial de um terminal, use essa opção para definir esses atributos de usuário usando os valores de atributo da conta. Durante as ações subsequentes de explorar e correlacionar, use essa opção para atualizar os atributos do usuário e aplicar as alterações feitas nos atributos da conta, talvez realizadas por outras ferramentas, diferentes do CA Identity Manager.
7. Clique em Enviar.

Agora, um administrador com a tarefa Executar a opção Explorar e correlacionar (na página 166) conclui a integração do terminal.

Explorar e correlacionar o terminal

Um administrador de hospedagem ou outro administrador com a tarefa Executar a opção Explorar e correlacionar executa esse procedimento. A fase de exploração da tarefa identifica as contas no terminal. A fase de correlação corresponde as contas aos usuários no CA Identity Manager ou cria as contas.

Siga estas etapas:

1. Em um ambiente, clique em Terminais, Executar a opção Explorar e correlacionar.
2. Selecione Executar agora para executar a opção Explorar e correlacionar imediatamente, ou selecione Programar nova tarefa (na página 411) para executar a opção Explorar e correlacionar mais tarde ou em uma programação recorrente.

   Observação: essa operação exige que o navegador cliente esteja no mesmo fuso horário que o servidor. Por exemplo, se a hora do cliente for 22h00 às terças e a hora do servidor for 7h00, a definição para a opção Explorar e correlacionar não funcionará.
3. Clique em uma definição para a opção Explorar e correlacionar a ser executada.
4. Clique em Enviar.

   As contas de usuário existentes no terminal são criadas ou atualizadas no CA Identity Manager de acordo com a definição para a opção Explorar e correlacionar que você criou.
5. Verifique se a tarefa obteve êxito, da seguinte maneira:
   a. Clique em Sistema, Exibir tarefas enviadas.
   b. Preencha o campo de nome da tarefa da seguinte maneira: Executar a opção Explorar e correlacionar
   c. Clique em Pesquisar.

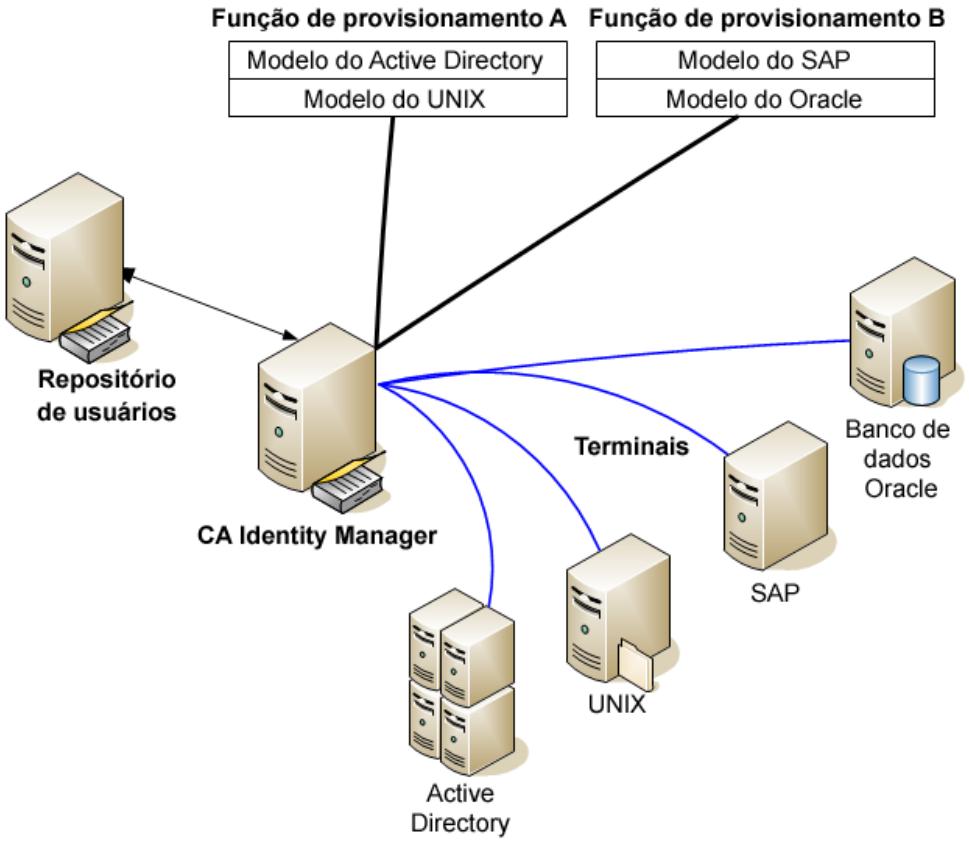
   Os resultados mostram se a tarefa obteve êxito.

Observação: você pode cancelar uma tarefa Explorar e correlacionar ao exibir o status da tarefa em Exibir tarefas enviadas (VST). O cancelamento interrompe o processamento da tarefa, deixando a tarefa no estado que estiver quando for cancelada. Qualquer notificação gerada é enviada, de forma que todos os sistemas sejam mantidos sincronizados.

Sincronizar usuários, contas e funções

A integração de vários terminais e contas em um único sistema de gerenciamento de usuários pode resultar na perda de sincronização. As funções de provisionamento ou os modelos de conta que são atribuídos a um usuário podem ser diferentes das contas reais que existem para esse usuário.

Por exemplo, considere uma situação com duas funções de provisionamento, uma com modelos de conta do Active Directory e UNIX e outra função com modelos do SAP e Oracle. O usuário joão_silva tem a Função de provisionamento A, que contém modelos de conta do Active Directory e UNIX, mas esse usuário tem apenas uma conta do Active Directory. Possivelmente, o modelo de conta do UNIX foi adicionado à função depois que ela havia sido atribuída ao usuário. Portanto, o administrador deve sincronizar o usuário com a definição da função atual.



As situações a seguir são outros motivos pelos quais os usuários perdem a sincronização com funções de provisionamento ou modelos de conta:

- As tentativas anteriores de criar as contas necessárias falharam devido a problemas de software ou hardware na rede, resultando em contas ausentes.
- As funções de provisionamento e modelos de conta mudam e isso cria contas extras ou ausentes.
- Contas foram atribuídas a modelos de conta após a criação, portanto, as contas existentes, mas não estão sincronizadas com seus modelos de conta.
- A criação de uma conta foi atrasada porque a conta foi especificada para ser criada posteriormente.
- Um novo terminal foi adquirido. Durante a exploração e a correlação, o servidor de provisionamento não atribuiu funções de provisionamento para os usuários automaticamente. Você atualiza a função para indicar os usuários que precisam de contas no terminal. Qualquer conta que estava correlacionada a um usuário é listada como uma conta extra quando o usuário é sincronizado.
- Uma conta existente foi atribuída a um usuário, copiando a conta para o usuário.
- Uma conta foi criada para um usuário sem atribuir o usuário a uma função. Por exemplo, você copiou um usuário para um modelo de conta que não está em uma função de provisionamento para esse usuário. A conta é listada como uma conta extra ou como uma conta com um modelo de conta extra. Se você copiar o usuário para um terminal para criar uma conta usando o modelo de conta padrão, essa pode ser uma conta extra.

As seções a seguir explicam como realizar os três tipos de sincronização:

1. Sincronizar usuários com funções (na página 169).
2. Sincronizar usuários com modelos de conta (na página 169).
3. Sincronizar conta do terminal com modelos de conta (na página 171).

Sincronizar usuários com funções

Essa tarefa cria, atualiza ou exclui contas, de forma que elas estejam de acordo com as funções de provisionamento atribuídas a um usuário. Por exemplo, os administradores usam ferramentas nativas em um terminal para adicionar ou excluir contas, mas você não explorou novamente esse terminal para atualizar o diretório de provisionamento. Portanto, os usuários têm contas extras ou ausentes. Essa tarefa também garante que cada conta pertence aos modelos de conta corretos.

Siga estas etapas:

1. Efetue logon no console de usuário.
2. Selecione Tarefas, Usuários, Sincronização, Verificar sincronização de funções.
3. Selecione um usuário.

   Uma tela é exibida, mostrando as contas esperadas, extras e ausentes.
4. Clique em Sincronizar para fazer com que as contas correspondam ao modelo nessa função.

   a. É possível marcar uma caixa de seleção para criar a conta no terminal. Se mais de um modelo de conta para o usuário indicar a mesma conta, a conta será criada, mesclando todos os modelos de conta relevantes.

      Essa conta é atribuída aos modelos de conta que, no momento, não estão sincronizados com a conta.

   b. É possível marcar uma caixa de seleção para excluir as contas extras. No entanto, os usuários podem ter motivos válidos para ter essas contas. Se for esse o caso, deixe essa opção desmarcada.

      Em determinados terminais, a função de exclusão da conta está desativada; portanto, a conta não será excluída.

Sincronizar usuário com modelos de conta

Essa tarefa sincroniza os atributos para as contas do terminal com os modelos de conta associados a um usuário. No entanto, a sincronização completa depende destes fatores:

- A sincronização completa da conta ocorre em duas situações. Um modelo de conta usa a sincronização forte (na página 172), ou dois ou mais modelos de conta foram adicionados a uma conta.
- Se um modelo de conta usa a sincronização fraca (na página 172), essa tarefa inicia uma sincronização de conta que envolve apenas esse modelo. Se a conta estava fora da sincronização de conta com outros modelos de conta antes dessa atualização, também poderá estar fora da sincronização de conta posteriormente.

Siga estas etapas:

1. Efetue logon no console de usuário.
2. Selecione Tarefas, Usuários, Sincronização, Verificar sincronização de modelo de conta.
3. Selecione um usuário.

   Uma tela é exibida, mostrando as contas esperadas, extras e ausentes.
4. Clique em Sincronizar para fazer com que as contas correspondam ao modelo.
   a. É possível marcar uma caixa de seleção para criar a conta no terminal. Se mais de um modelo de conta para o usuário indicar a mesma conta, a conta será criada, mesclando os modelos de conta relevantes.

      Essa conta é atribuída aos modelos de conta que não estão sincronizados com a conta. A sincronização de conta não é necessária em contas recém-criadas.
   b. É possível marcar uma caixa de seleção para excluir as contas extras. No entanto, os usuários podem ter motivos válidos para ter essas contas. Se for esse o caso, deixe essa opção desmarcada.

      Em determinados terminais, a função de exclusão da conta está desativada; portanto, a conta não será excluída.

Atributos somente para novas contas

Em um modelo de conta, determinados atributos são aplicados somente ao criar a conta. Por exemplo, o atributo Senha é uma expressão de regra, que define a senha para novas contas. Essa expressão de regra nunca atualiza a senha de uma conta. As alterações feitas na expressão de regra de senha só afetam as contas criadas após a definição da expressão de regra.

Da mesma forma, uma expressão de regra de modelo para um atributo da conta somente leitura afeta somente as contas criadas após a definição da expressão de regra. A alteração não terá efeito em contas existentes.

Sincronizar contas do terminal com modelos de conta

Essa tarefa sincroniza uma conta do terminal após a modificação de um modelo de conta associado. Por exemplo, uma conta do Active Directory não tem grupos, mas o modelo de conta associado está definido para incluir grupos.

Siga estas etapas:

1. Efetue logon no console de usuário.
2. Selecione Tarefas, Terminais, Gerenciar terminais, Verificar sincronização de contas de terminais.
3. Selecione um terminal.

   Uma tela é exibida mostrando as contas no terminal em questão, os modelos de conta associados e quais atributos não estão sincronizados.
4. Clique em Sincronizar para fazer com que os atributos para essas contas correspondam ao que está definido no modelo de conta.

   As alterações que você fizer nos modelos de conta afetam as contas existentes da seguinte maneira:

   - Se você alterar o valor de um atributo de recurso, o atributo da conta correspondente será atualizado para ser sincronizado com o valor do atributo do modelo de conta. Consulte a descrição de sincronização fraca e forte.
   - Alguns atributos de conta são designados pelo conector como não sendo atualizados após alterações no modelo de conta. Os exemplos incluem determinados atributos que o tipo de terminal permite que sejam definidos apenas durante a criação da conta, e o atributo Senha.

Quais atributos são atualizados

Quando você altera os atributos de capacidade em um modelo de conta, o atributo correspondente nas contas é alterado. Essa alteração tem um impacto nos atributos da conta. O impacto tem como base os seguintes fatores:

- Se o modelo de conta está definido para usar sincronização fraca ou forte.
- Se a conta pertence a vários modelos de conta.

Sincronização fraca

A *sincronização fraca* garante que os usuários tenham o mínimo de atributos de capacidade para suas contas. A sincronização fraca é o padrão na maioria dos tipos de terminal. Se você atualizar um modelo que usa sincronização fraca, o CA Identity Manager atualizará os atributos de capacidade da seguinte maneira:

- Se um campo de número for atualizado em um modelo de conta e o número novo for maior do que o número na conta, o CA Identity Manager alterará o valor na conta para corresponder ao novo número.
- Se uma caixa de seleção não tiver sido marcada em um modelo de conta e você marcá-la depois, o CA Identity Manager atualizará a caixa de seleção em qualquer conta em que a caixa de seleção não estiver marcada.
- Se uma lista for alterada em um modelo de conta, o CA Identity Manager atualizará todas as contas para incluir qualquer valor da nova lista que não foi incluído na lista de valores da conta.

Se uma conta pertencer a outros modelos de conta (se esses modelos usarem sincronização fraca ou forte), o CA Identity Manager consultará apenas o modelo que está sendo alterado. Essa ação é mais eficiente do que a verificação de todos os modelos de conta. Como a sincronização fraca apenas adiciona capacidades às contas, geralmente não é necessário consultar os outros modelos de conta.

Observação: quando se propaga a partir de um modelo de conta de sincronização fraca, as alterações que poderiam remover ou reduzir as capacidades podem deixar algumas contas não sincronizadas. Lembre-se de que, com a sincronização fraca, as capacidades nunca são removidas ou reduzidas. Sem consultar outros modelos para uma conta, a propagação não considera se a sincronização fraca é suficiente.

Nessa situação, use Sincronizar usuários com modelos de conta para sincronizar a conta com seus modelos de conta.

Sincronização forte

A sincronização forte garante que as contas possuam exatamente os atributos de conta que são especificados no modelo de conta.

Por exemplo, suponhamos que você adicione um grupo a um modelo de conta do UNIX existente. Originalmente, o modelo de conta tornou as contas integrantes do grupo Equipe. Agora, você deseja tornar as contas integrantes dos grupos Equipe e Sistema. Todas as contas associadas ao modelo de conta são consideradas sincronizadas quando cada conta é integrante dos grupos Equipe e Sistema (e de nenhum outro grupo). Qualquer conta que não fizer parte do grupo Equipe é adicionada aos dois grupos.

Alguns outros fatores a serem considerados incluem as seguintes situações:

- Se o modelo de conta usar a sincronização forte, qualquer conta que pertencer a grupos que não sejam Equipe e Sistema será removida dos grupos adicionais.
- Se o modelo de conta usar a sincronização fraca, as contas serão adicionadas aos grupos Equipe e Sistema. Qualquer conta que tiver grupos adicionais que estiverem definidos para ela permanecerá um integrante desses grupos.

Observação: sincronize as contas com seus modelos regularmente para garantir que as contas permaneçam sincronizadas com seus modelos de conta.

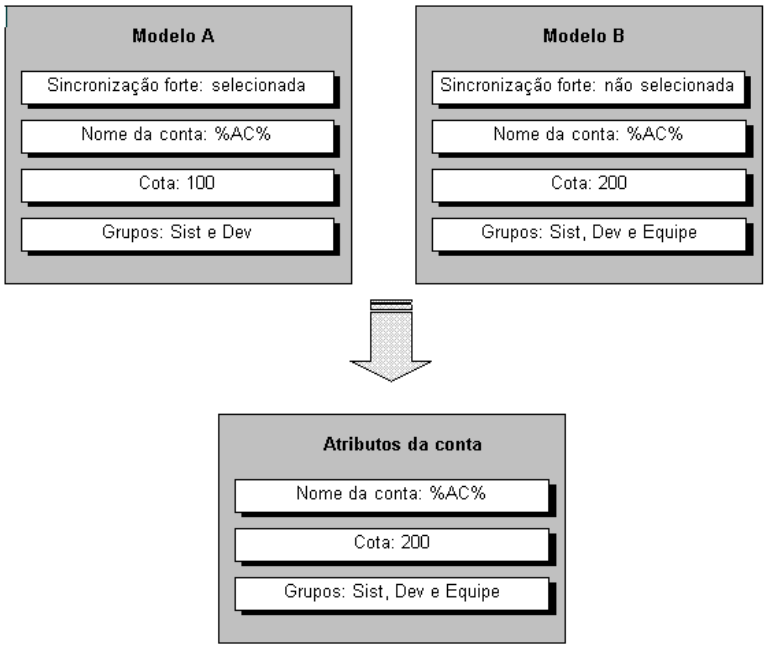
Contas com vários modelos

A sincronização depende também se a conta pertence a mais de um modelo de conta. Se a conta tiver apenas um modelo de conta e esse modelo usar a sincronização forte, cada atributo é atualizado para corresponder exatamente ao valor de atributo de modelo de conta. O resultado é o mesmo de quando o atributo for um atributo inicial.

Uma conta pode pertencer a vários modelos de conta, como seria o caso se um usuário pertencer a várias funções de provisionamento, cada uma delas com algum nível de acesso no mesmo terminal gerenciado. Quando isso acontecer, o CA Identity Manager combina esses modelos de conta em um modelo de conta em vigor que indica o superconjunto de recursos a partir dos modelos de conta. Esse modelo de conta é considerado para usar a sincronização fraca se todos os modelos de contas forem fracos, ou a sincronização forte se qualquer um dos modelos de conta for forte.

Observação: muitas vezes, você usa apenas a sincronização fraca ou apenas a sincronização forte para os modelos de conta que controlam uma conta, dependendo se as funções da empresa definem completamente os acessos que seus usuários precisam. Se os usuários não se encaixarem em funções claras e você precisar da flexibilidade para conceder recursos adicionais para as contas de usuário, use a sincronização fraca. Se for possível definir as funções para especificar exatamente os acessos que seus usuários precisam, use a sincronização forte.

O exemplo a seguir demonstra como vários modelos de conta são combinados em um único modelo de conta em vigor. Neste exemplo, um modelo de conta será marcado para sincronização fraca e o outro para sincronização forte. Portanto, o modelo de conta em vigor criado pela combinação dos dois modelos de conta será tratado como um modelo de conta de sincronização forte. O atributo inteiro Cota assume o maior valor dos dois modelos de conta, e o atributo Grupo com vários valores assume a união de valores das duas políticas.



Sincronização reversa com contas de terminal

Embora seja responsabilidade do CA Identity Manager criar, excluir e modificar contas, não é possível impedir que um usuário de sistema do terminal execute essas operações por conta própria. Essa situação pode ocorrer devido a alguma emergência, ou por motivos mal-intencionados, como um hacker. A sincronização reversa garante o controle das contas por um usuário em cada terminal ao identificar discrepâncias entre contas do CA Identity Manager e contas nos terminais.

Por exemplo, se uma conta tiver sido criada no domínio do Active Directory usando uma ferramenta externa, o CA Identity Manager deve estar ciente desse problema de segurança em potencial. Além disso, ignorar o CA Identity Manager causa a falta de processos de aprovação e de relatórios de auditoria.

Os dois tipos de discrepância entre o CA Identity Manager e os terminais gerenciados são os seguintes:

- Uma nova conta detectada
- Uma alteração em uma conta existente

É possível resolver ambos os casos por meio da definição de políticas para lidar com a alteração. Em seguida, usando a opção Explorar e correlacionar para atualizar o CA Identity Manager, você aciona a execução de políticas.

Como funciona a sincronização reversa

A sincronização reversa com contas de terminal ocorre da seguinte maneira:

1. Um administrador ou um usuário mal-intencionado cria ou modifica uma conta em um terminal.
2. Quando a opção Explorar e correlacionar é executada nesse terminal, a conta nova ou modificada é detectada.
3. O servidor de provisionamento envia uma notificação ao servidor do CA Identity Manager.
4. O servidor do CA Identity Manager procura uma política de sincronização reversa que corresponda à alteração no terminal.
5. Se uma política correspondente for encontrada, será executada. Se mais de uma política se aplicar a essa conta e essas políticas tiverem o mesmo escopo, a política de prioridade mais alta será executada.
6. Dependendo da política, uma das seguintes ações ocorre:
   - Para uma nova conta, a política aceita, exclui ou suspende a conta, ou a envia para aprovação de fluxo de trabalho.
   - Para uma conta modificada, a política aceita o valor, reverte-o para o último valor conhecido ou o envia para aprovação de fluxo de trabalho.
7. Se o fluxo de trabalho estiver selecionado, um novo evento para o fluxo de trabalho será gerado e os aprovadores serão definidos. Em seguida, uma das seguintes ações ocorre:
   - Para uma nova conta, o aprovador pode aceitar, excluir ou suspender a conta ou atribuí-la a um usuário.
   - Para uma conta modificada, o processo de fluxo de trabalho é o mesmo de quando o valor é alterado no console de usuário, exceto que os valores recusados são revertidos ao terminal.

Mapear atributos do terminal

Para usar a sincronização reversa em um atributo de uma conta do terminal, primeiro é preciso mapeá-lo para um atributo visível no console de usuário. Alguns atributos, como nome da conta e senha, são mapeados por padrão. Outros atributos não são mapeados. Por exemplo, o atributo do Active Directory de associação de grupo não é mapeado. Para alguns tipos de terminal, nenhum atributo é mapeado.

Para verificar se o atributo pode ser mapeado:

1. No Console do usuário, clique em Terminais ou em Tarefas, Terminais.
2. Clique em Conta modificada pela sincronização reversa, Criar diretiva de conta modificada pela sincronização reversa.
3. Escolha a opção de criar uma política ou a cópia de uma política.
4. Clique em Tipo de terminal e escolha um terminal, como o Active Directory.
5. Clique em Nome do atributo para exibir uma lista de atributos que podem ser mapeados.
6. Clique em Cancelar.

   Cancele a política, pois você está usando-a somente para verificar que atributos podem ser mapeados.

Importante: você pode gerenciar determinados atributos apenas por meio de ferramentas nativas no terminal. Portanto, se um usuário do terminal modificar esse tipo de atributo, o evento reverso falhará quando a política de sincronização reversa for acionada. No entanto, as mudanças em outros atributos nesse evento reverso não são revertidas. Portanto, evite o mapeamento de atributos que podem ser gerenciados apenas no terminal.

Para mapear atributos do terminal para sincronização reversa:

1. Clique em Terminais, Modificar terminal.
2. Procure e selecione um terminal que exija a sincronização reversa.
3. Clique na guia Mapeamento de atributos.
4. Selecione Usar configurações personalizadas.
5. Clique em Adicionar para adicionar um novo atributo personalizado.
6. Selecione um atributo personalizado disponível. Por exemplo, use 10 CustomField se não estiver em uso em seu ambiente.

7. Mapeie o atributo personalizado para o nome do atributo da conta que deseja gerenciar.
8. Repita as etapas de 5 a 7 para adicionar mapeamentos entre todos os atributos da conta exigidos e o atributo personalizado selecionado.

   Você pode usar o mesmo atributo personalizado (CustomField 10 em nosso exemplo) para todos os atributos que deseja gerenciar.
9. Clique em Enviar.

Para criar valores de linha de base para esse terminal:

Uma vez que todos os valores para um terminal estiverem mapeados, você pode explorar o terminal. Para essa operação, você desativa a notificação de entrada e a ativa depois de terminar de explorar. Desativar a notificação elimina as notificações que são desnecessárias. Caso contrário, todas as contas que tiverem valores nos novos atributos gerariam uma notificação durante o processo de exploração.

1. No gerenciador de provisionamento, desative a notificação de entrada da seguinte maneira:
   a. Clique em Sistema, Configuração de domínio, Servidor do CA Identity Manager, Enable Notification.
   b. Selecione Não.
   c. Reinicie o servidor de provisionamento para garantir que a alteração seja aplicada.
2. No console de usuário, clique em Terminais, Executar a opção Explorar e correlacionar.

   Escolha uma definição para a opção explorar e correlacionar que tenha correlacionar desmarcado.

   Essa ação preenche novamente os atributos de repositório do usuário com os novos dados do atributo do terminal. Essa tarefa pode levar algum tempo se o terminal for grande.
3. Reative a notificação de entrada no gerenciador de provisionamento.
4. Reinicie o servidor de provisionamento.

Na próxima operação de explorar e correlacionar para esse terminal, as notificações de modificação de contas são geradas. As notificações são geradas quando uma alteração tiver ocorrido para um atributo que é mapeado para um atributo de usuário global e uma política se aplicar ao atributo.

Mais informações:

Atributos iniciais e de capacidade (na página 207)

Políticas para sincronização reversa

Quando uma conta é criada ou modificada em um terminal, as políticas de sincronização reversa podem executar as ações apropriadas em resposta. Por exemplo, um usuário cria algumas contas do Active Directory em diversas OUs no domínio corporativo. Além disso, o usuário modifica algumas contas do Microsoft Exchange. É possível detectar as contas novas e alteradas e fornecer as ações apropriadas em resposta usando políticas de conta de sincronização reversa.

É possível executar as seguintes ações por meio da sincronização reversa:

- Configurar uma política para aceitar a nova conta, recusá-la ou enviá-la para aprovação de fluxo de trabalho.
- Configurar uma política para aceitar uma alteração em um atributo, revertê-lo para o atributo original ou enviá-lo para aprovação de fluxo de trabalho.
- Quando uma conta é enviada para aprovação de fluxo de trabalho, o aprovador pode executar uma das seguintes ações:
  - Recusar (excluir/suspender a conta do terminal ou alterar o valor para corresponder ao valor do repositório de usuários do CA Identity Manager).
  - Aceitar e atualizar o repositório de usuários do CA Identity Manager para fazer correspondência com a conta.
  - Atribuir a conta a um usuário no console de usuário (no caso de criação da conta).

Criar uma política para novas contas

Se desejar definir um processo para quando uma nova conta for detectada em um terminal, você cria uma política de conta que se aplica a novas contas. Políticas de novas contas são executadas quando as contas são detectadas quando a opção Correlacionar está incluída na definição para a opção Explorar e correlacionar. Se uma conta for encontrada ao executar apenas a opção Explorar, a política será executada na próxima vez que a opção Correlacionar for incluída ao explorar esse terminal.

Para criar uma política para novas contas:

1. No Console do usuário, clique em Terminais ou clique em Tarefas, Terminais.
2. Nova conta para sincronização reversa, Criar diretiva de nova conta para sincronização reversa.
3. Insira um nome e uma descrição para a política.
4. Digite os seguintes parâmetros:
   - Prioridade — A prioridade da política. A política de prioridade mais alta é aquela com o número mais baixo. Se duas políticas tiverem a mesma prioridade e o mesmo escopo, qualquer uma delas poderá ser executada. Portanto, certifique-se de definir diferentes níveis de prioridade.
   - Tipo de terminal — Todos os terminais ou um determinado tipo de terminal.
   - Terminal — O nome do terminal específico. Se Tipo de terminal for Tudo, a única opção é Todos os terminais.
   - Recipiente — O recipiente em que a conta está localizada. Esse campo só se aplica a terminais hierárquicos. Insira o recipiente como uma lista de nós, terminando com o terminal. Por exemplo, para uma OU do Active Directory com o caminho "ou=child,ou=parent,ou=root,dc=domain,dc=name", o formato "child,parent,root" está correto.
   - Usuário correlacionado — Controla quando executar a política se um usuário correlacionado for encontrado no diretório de provisionamento.

5. Selecione uma das seguintes ações:
   - Aceitar — não executa nenhuma ação na conta. Essa opção pode ser útil se existirem duas políticas: uma que recusa todas as contas novas, e uma política de prioridade mais alta que aceita as contas criadas em uma determinada OU. Portanto, se a conta tiver sido criada nessa OU, será aceita. A prioridade de recusa não será executada, pois tem uma prioridade mais baixa.
   - Excluir — remove a conta do terminal.
   - Suspender — mantém a conta no terminal, mas a suspende.
   - Enviar para aprovação — envia a mudança para aprovação de fluxo de trabalho.
6. Execute as seguintes etapas se você definir a ação Enviar para aprovação:
   a. Clique no ícone ao lado de Processo de fluxo de trabalho.
   b. Selecione um processo de fluxo de trabalho.
   c. Clique em OK.
7. Clique em Enviar.

Se você tiver atribuído um processo de fluxo de trabalho para a política, será necessário criar uma tarefa de aprovação (na página 182).

Criar uma política para contas modificadas

Qualquer atributo da conta em uma conta do terminal pode ser gerenciado por sincronização reversa, desde que esteja definido no mapeamento de atributos (na página 176).

Para definir um processo para quando uma discrepância for encontrada entre contas do terminal existentes e seus valores conhecidos no CA Identity Manager, você pode criar uma política de conta que se aplica a contas existentes. Se um atributo tiver vários valores, mais de um valor pode ter sido adicionado ou removido. Nesse caso, a política é aplicada a cada valor separadamente, ou você pode criar políticas diferentes para valores distintos.

Para criar uma política para contas modificadas:

1. No Console do usuário, clique em Terminais ou clique em Tarefas, Terminais.
2. Clique em Conta modificada pela sincronização reversa, Criar diretiva de conta modificada pela sincronização reversa.
3. Insira um nome e uma descrição para a política.
4. Digite os seguintes parâmetros:
   - Prioridade — A prioridade da política. A política de prioridade mais alta é aquela com o número mais baixo. Se duas políticas tiverem a mesma prioridade e o mesmo escopo, qualquer uma delas poderá ser executada. Portanto, certifique-se de definir diferentes níveis de prioridade.
   - Tipo de terminal — Todos os terminais ou um determinado tipo de terminal.
   - Terminal — O nome do terminal específico. Se Tipo de terminal for Tudo, a única opção é Todos os terminais.
   - Recipiente — O recipiente em que a conta está localizada. Esse campo só se aplica a terminais hierárquicos. Insira o recipiente como uma lista de nós, terminando com o terminal. Por exemplo, para uma OU do Active Directory com o caminho "ou=child,ou=parent,ou=root,dc=domain,dc=name", o formato "child,parent,root" está correto.
   - Atributo — O nome físico.
   - Valor — Uma representação de sequência de caracteres do valor, que pode conter * (asterisco) como um curinga. O curinga se refere a qualquer valor na alteração.

5. Selecione uma das seguintes ações:
   - Aceitar — atualiza o valor da conta no repositório de usuários do CA Identity Manager para corresponder ao valor na conta do terminal.
   - Recusar — reverte o atributo para reintegrar o valor original sem afetar outras alterações em atributos para a conta.
   - Enviar para aprovação — envia a mudança para aprovação de fluxo de trabalho.
6. Execute as seguintes etapas se você definir a ação Enviar para aprovação:
   a. Clique no ícone ao lado de Processo de fluxo de trabalho.
   b. Selecione um processo de fluxo de trabalho.
   c. Clique em OK.
7. Clique em Enviar.

Se você tiver atribuído um processo de fluxo de trabalho para a política, será necessário criar uma tarefa de aprovação (na página 182).

Criar uma tarefa de aprovação para sincronização reversa

Você cria tarefas de aprovação de sincronização reversa para políticas que tiverem uma ação de enviar para o fluxo de trabalho. Considere as seguintes diretrizes para criar as tarefas:

- Para as tarefas que aprovam novas contas, há duas opções.
  - Você pode criar uma tela de aprovação genérica para as contas. A tela do perfil para a tarefa mostra apenas as informações gerais sobre a conta. A tarefa de aprovação de nova conta para sincronização reversa funciona dessa maneira.
  - Se o aprovador precisar ver os detalhes da nova conta, essa tela deverá ser específica para o tipo de terminal. Portanto, a tarefa de aprovação com a tela deve ser usada somente para políticas que forem específicas desse tipo de terminal. A tarefa deve incluir a guia Tarefa de aprovação de sincronização reversa.
- Para as tarefas que aprovam modificações de conta, a tela de aprovação deve ser específica para um tipo de terminal, de modo que o aprovador possa ver os valores alterados.

As tarefas de aprovação de sincronização reversa são idênticas às tarefas de aprovação usadas para alterações em contas. Se uma tarefa de aprovação para um determinado tipo de terminal já existir, essa tarefa pode ser usada. Para uma nova conta, uma guia adicional de aprovação de sincronização reversa é necessária. Se não houver uma tarefa de aprovação para o tipo de terminal, use o procedimento a seguir.

Para criar uma tarefa de aprovação para sincronização reversa:

1. No console do usuário, clique em Tarefas, Funções e tarefas, ou clique em Funções e tarefas.
2. Clique em Tarefas administrativas, Criar tarefa administrativa.
3. Selecione a tarefa de modificação para o terminal.

   O nome deve começar com modificar e indicar o nome do tipo de terminal. Modificar a conta do Active Directory é um exemplo.
4. Faça as seguintes alterações na guia Perfil:
   - Altere o nome da nova tarefa.
   - Altere o tag da tarefa.
   - Altere a ação para Aprovar evento.
5. Faça as seguintes alterações na guia Guias:
   a. Remova todas as guias de relacionamento.
   b. Adicione a guia Tarefa de aprovação de sincronização reversa se a tarefa for aprovar novas contas. Mova essa guia para que se torne a primeira guia.
   c. Copie e edite as telas de aprovação nas guias, conforme necessário.

      Observação: você pode encontrar problemas ao usar algumas telas de conta em uma tarefa de aprovação. Se isso acontecer, modifique a tela de conta padrão para a guia para fazê-la funcionar na tarefa.
6. Clique em Enviar.
7. Se a tarefa for para aprovações de novas contas, adicione a tarefa a uma função à qual o aprovador pertence. A função define o escopo do usuário, que é usado para pesquisar usuários para os quais a nova conta pode ser atribuída.

Executar a sincronização reversa

A sincronização reversa ocorre quando você usa a tarefa Executar a opção Explorar e correlacionar. Usando essa tarefa, você atualiza o repositório de provisionamento do CA Identity Manager com as contas novas ou alteradas em um terminal.

Para executar a sincronização reversa:

1. Crie uma definição para a opção explorar e correlacionar que inclui uma opção Correlacionar. A correlação é necessária para detectar novas contas.
2. Clique em Tarefas, Terminais, Executar a opção Explorar e correlacionar.
3. Escolha uma definição que se aplica ao terminal com as contas novas ou modificadas.

   Observação: na correlação com o usuário existente, o usuário deve existir no diretório de provisionamento, caso contrário, o usuário é correlacionado ao usuário padrão desse diretório. O repositório de usuários do CA Identity Manager não está no escopo da tarefa Explorar e correlacionar.
4. Clique em Enviar.

Se uma política não tiver nenhum processo de fluxo de trabalho, as contas serão processadas conforme definido na política.

Observação: se vários atributos tiverem sido recusados em uma conta que foi detectada pela política de sincronização reversa, todas as ações serão colocadas em um único evento. No entanto, se esse evento falhar devido a um problema com um dos atributos, nenhum atributo será atualizado.

Se o fluxo de trabalho fizer parte da política, qualquer aprovação gerada pela sincronização reversa será exibida em Fluxo de trabalho, Exibir minha lista de tarefas para o aprovador.

Para novas contas, o aprovador tem as seguintes opções:

- O aprovador pode suspender ou excluir a conta no terminal ao selecionar Excluir ou Suspender e, em seguida, clicar em Recusar.
- Caso contrário, o aprovador pode aceitar a nova conta clicando em Aprovar.

  Se um aprovador não selecionar um usuário no campo Usuário correlacionado, a conta será atribuída ao usuário padrão. Se o campo Usuário correlacionado estiver preenchido na tarefa de aprovação, a conta será correlacionada com esse usuário. O campo Usuário correlacionado contém o nome de usuário sugerido encontrado pelo mecanismo de correlação se um usuário puder ser encontrado.

Para contas modificadas, o aprovador tem as seguintes opções:

- Para cada conta, o aprovador vê quais valores foram alterados e pode aprová-los ou recusá-los exatamente como se as alterações tivessem sido iniciadas nas telas de gerenciamento de contas.

- O aprovador vê alterações em atributos de capacidade (como grupos do Active Directory) como eventos de aprovação separados.

Para verificar se a sincronização reversa foi bem-sucedida:

1. Vá para Sistema, Exibir tarefas enviadas.
2. Preencha o campo de nome da tarefa da seguinte maneira: Atividade de provisionamento
3. Clique em Pesquisar.

Os resultados mostram se os eventos de sincronização reversa foram concluídos com êxito.

Estender atributos personalizados em terminais

O servidor de provisionamento pode gerenciar atributos de terminal personalizados. Para permitir que o CA Identity Manager leia atributos de terminal personalizados que são associados a funções de provisionamento, são necessárias etapas adicionais.

Para estender atributos personalizados em terminais:

1. Gere metadados na tabela do analisador se esse conector tiver sido criado antes do CA Identity Manager r12.5.

   Consulte o *Guia de Programação do Conector*.
2. Use o Connector Xpress da seguinte maneira:
   a. Instale metadados no nó de espaço para nome.
   b. Gere um arquivo JAR, um arquivo de propriedades e um arquivo de definição da função usando o Gerador de definição de funções.

      Para obter detalhes, consulte o *Guia do Connector Xpress*.

3. Copie o arquivo JAR para este local:
   - (Windows) *app server home*/iam_im.ear/user_console.war/WEB-INF/lib
   - (UNIX) *app server home*\iam_im.ear\user_console.war\WEB-INF\lib

     Observação: para o WebSphere, copie o arquivo JAR para: WebSphere_home/AppServer/profiles/*Profile_Name*/config/cells/*Cell_name*/applications/iam_im.ear/user_console.war/WEB-INF
4. Copie o arquivo de propriedades para este local:
   - (Windows) *app server home*/iam_im.ear/custom/provisioning/resourceBundles
   - (UNIX) *app server home**i*am_im.ear\custom\provisioning\resourceBundles

     Observação: para o WebSphere, copie o arquivo de propriedades para:

     WebSphere_home/AppServer/profiles/*Profile_Name*/config/cells/*cell_name*/applications/iam_im.ear\custom\provisioning\resourceBundles
5. Repita as duas etapas anteriores para cada nó se você tiver um agrupamento.
6. Reinicie o servidor de aplicativos.
7. Importe o arquivo de definição da função da seguinte maneira:
   a. No Management Console, selecione o ambiente.
   b. Selecione Role and Task Settings.
   c. Clique em Importar.
   d. Selecione o tipo de terminal e clique em Finalizar.

Tarefas da conta

No console de usuário, é possível criar, modificar e excluir as contas de terminal que estão associadas a um usuário do CA Identity Manager. Você também pode atribuir outras contas de terminal que não estão associadas a um usuário do CA Identity Manager.

Existem quatro tipos de conta do terminal:

Provisionada

Contas criadas quando o usuário recebe uma função de provisionamento

Exceção

Contas criadas quando o usuário recebe um modelo de conta

Órfã

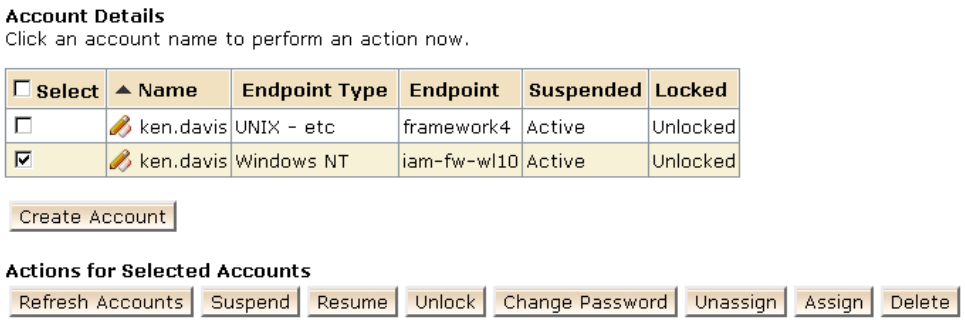
Contas criadas no sistema do terminal e que não estão associadas a nenhum usuário do CA Identity Manager

Sistema

Contas criadas no sistema do terminal, não associadas a nenhum usuário do CA Identity Manager e usadas para gerenciar o sistema do terminal

Exibir ou modificar contas de terminal

Tarefas que permitem a exibição do perfil de um usuário, por exemplo, Exibir Usuário ou Modificar meu perfil, incluem uma guia Contas que lista as contas desse usuário nos terminais.



Para cada conta, o CA Identity Manager exibe informações, como o nome da conta, o terminal onde a conta existe e o status da conta. Para uma tarefa de modificação, opções adicionais estão disponíveis para alterar a senha de um usuário e bloquear ou suspender uma conta.

Neste exemplo, a guia Contas inclui um botão Pesquisar, o que significa que a guia é configurada com uma tela de pesquisa. É possível configurar essa guia para usar uma tela de lista, uma tela de pesquisa, ou ambas.

- Quando ambas as tela forem configuradas, a tela de pesquisa determinará os campos nos resultados da pesquisa.
- Se apenas uma tela de lista for configurada, determinará os campos nos resultados da pesquisa.
- Se nenhuma tela for configurada, a guia Contas usará uma exibição de lista estática, o que significa que a guia Contas não pode ser personalizada para exibir colunas.

Para obter detalhes sobre as outras opções que você pode fornecer na guia Contas, consulte a ajuda do console de usuário para a configuração da guia Contas.

Criar uma conta provisionada

A maneira recomendável de criar uma conta do terminal para um usuário do <idmgr> é atribuir uma função de provisionamento para o usuário. O usuário receberá a conta com os atributos definidos nos modelos de conta para a função. Quando necessário, as alterações nesse modelo de conta, como o tamanho da caixa de correio para as contas do Exchange, atualizam a conta do terminal.

Para criar uma conta provisionada:

1. No console de usuário, selecione Gerenciar usuários, Modificar usuário.
2. Selecione um usuário a ser modificado.
3. Clique na guia Funções de provisionamento.
4. Clique em Adicionar uma função de provisionamento.
5. Selecione uma função.
6. Clique em Enviar.

Criar uma exceção

É possível criar uma conta diretamente na guia Contas ao usar Modificar usuário em um usuário. Essa conta é chamada de exceção. No entanto, uma vez que nenhuma função de provisionamento está envolvida com essa conta, a sincronização de funções com os usuários não atualiza essa conta.

Para criar uma exceção:

1. No console de usuário, selecione Usuários, Modificar as contas de terminal do usuário.
2. Selecione um usuário a ser modificado.
3. Clique em Criar.
4. Selecione um terminal.
5. Selecione um recipiente, caso seja exigido, para esse tipo de terminal.
6. Preencha os campos em cada guia.
7. Clique em Enviar.

Atribuir contas órfãs

No console de usuário, você pode gerenciar contas órfãs, que são contas que não estão associadas a usuários do CA Identity Manager.

Para criar um usuário padrão para contas órfãs:

Se o diretório de provisionamento for separado do repositório de usuários do CA Identity Manager, crie o usuário padrão do servidor de provisionamento no repositório de usuários do CA Identity Manager. O usuário padrão é usado para contas órfãs.

1. No Console de usuário, clique em Usuários.
2. Clique em Gerenciar usuários, Criar usuário.
3. Nomeie o usuário da seguinte maneira, incluindo os colchetes:
   `[usuário padrão]`

   Agora, é possível atribuir contas órfãs para os usuários.

Para atribuir uma conta órfã:

1. No console de usuário, clique em Terminais.
2. Clique em Gerenciar contas órfãs.
3. Pesquise e selecione um usuário.
4. Clique em um usuário para atribuir aos usuários órfãos.

Atribuir contas do sistema

No console de usuário, você pode gerenciar contas do sistema, que são contas de terminal usadas para administrar o sistema do terminal.

Para atribuir uma conta do sistema a um usuário, é preciso criar uma tarefa administrativa com base na tarefa de gerenciar contas do sistema. A nova tarefa tem um determinado usuário do CA Identity Manager que se aplica para um terminal específico. É possível criar uma tarefa para cada tipo de terminal.

Para configurar uma tarefa para atribuir contas do sistema:

1. No console de usuário, clique em Funções e tarefas, Tarefa administrativa, Criar tarefa administrativa.
2. Baseie a nova tarefa na tarefa de gerenciar contas do sistema.

   Por exemplo, você pode criar uma tarefa chamada *Gerenciar contas do sistema Oracle* para atribuir contas do sistema em um tipo de terminal Oracle.
3. Na guia Pesquisar, clique no botão Procurar para editar a tela de pesquisa. Nessa tela, inclua um filtro de pesquisa para que um usuário atribua a essa conta do sistema.
4. Envie a tarefa.
5. Inclua essa tarefa em uma função.
6. Atribua a função a um usuário que deve atribuir contas do sistema de um terminal para um usuário.

   O usuário com essa função pode executar a nova tarefa para atribuir usuários do sistema para um usuário do CA Identity Manager.

Mover tela de tarefa da conta

Use essa tela de tarefa para mover contas de um recipiente em um terminal para outro. Os campos dessa tela são listados abaixo:

Mover detalhes da conta

Especifica a conta, o recipiente pai, o recipiente de destino, o terminal e o tipo de terminal que deseja mover.

Selecione o botão Recipiente.

Clique para pesquisar os recipientes de contas disponíveis e pertencentes ao terminal.

Excluir uma conta do terminal

É possível excluir uma conta de terminal de duas maneiras:

1. Usando a tarefa Modificar usuário, na guia Funções de provisionamento, remova a função que criou a conta.
2. Usando a tarefa Modificar as contas de terminal do usuário, exclua a conta.

Para excluir uma conta com Modificar as contas de terminal do usuário:

1. No console de usuário, selecione Usuários, Modificar as contas de terminal do usuário.
2. Selecione um usuário a ser modificado.
3. Pesquise contas com base em um tipo de terminal.
4. Selecione uma conta.
5. Clique no botão Excluir.

As contas excluídas são criadas quando você usa o gerenciador de provisionamento da seguinte maneira:

- Sincronizar usuário com funções recria contas provisionadas, contas criadas quando um usuário possui uma função de provisionamento.
- Sincronizar contas com modelo de conta recria a exceção (se a conta tiver um modelo de conta) e contas provisionadas.

Alterar a senha de uma conta do terminal

Você pode alterar a senha de uma conta do terminal sem saber a senha atual.

Para alterar a senha de uma conta do terminal:

1. No console de usuário, selecione Usuários, Modificar as contas de terminal do usuário.
2. Selecione um usuário a ser modificado.
3. Pesquise contas com base em um tipo de terminal.
4. Selecione uma ou mais contas.
5. Clique no botão Alterar a senha.
6. Digite a nova senha.

   As políticas de senha do CA Identity Manager validam a nova senha.
7. Clique em Enviar.

Executando ações em várias contas

Você pode realizar várias outras ações em uma ou mais contas. Por exemplo, é possível retomar uma conta suspensa, desbloquear uma conta quando o usuário tiver inserido a senha errada, ou atribuir ou remover a atribuição de uma conta para um usuário. As ações se aplicam a todas as contas selecionadas e o procedimento é o mesmo.

Para executar as tarefas em várias contas:

1. No console de usuário, selecione Usuários, Modificar as contas de terminal do usuário.
2. Selecione um usuário a ser modificado.
3. Pesquise contas com base em um tipo de terminal.
4. Selecione uma ou mais contas.
5. Clique em um dos botões abaixo de Ações para as contas selecionadas.
6. Responda a caixa de diálogo que é exibida e clique em Enviar.

Operações avançadas da conta

No Gerenciador de provisionamento, você pode executar várias operações adicionais em contas:

- Associar uma conta a usuários globais diferentes
- Explorar contas automaticamente
- Excluir contas
- Usar Excluir itens pendentes
- Recriar contas excluídas

Alterar o usuário global de uma conta

Veja a seguir as instâncias de quando você desejar associar uma conta a um usuário global diferente:

- Você tem dois usuários globais com o mesmo nome e o CA Identity Manager correlaciona a conta à pessoa errada
- O CA Identity Manager correlacionou uma conta ao objeto do [usuário padrão] e você deseja associá-la a outro objeto de usuário global
- Você criou uma conta usando a opção Novo e agora deseja associá-la a um usuário global

Para associar uma conta a outro usuário global no Gerenciador de provisionamento, arraste e solte a conta no usuário global correto.

Como funciona a Exploração automática

A adição ou exclusão de contas, ou outros objetos, usando ferramentas nativas no terminal não são notadas pelo CA Identity Manager até que você explore o terminal. O processo de exploração nota as adições e exclusões (e, em alguns casos, modificações) ocorridas e aplica essas alterações na representação do objeto do CA Identity Manager no diretório de provisionamento.

No entanto, se você usar o Gerenciador de provisionamento para tentar criar um objeto com o mesmo nome antes que essa exploração ocorra, o CA Identity Manager notará que um objeto com esse nome já existe e relatará esse erro. Desse modo, o CA Identity Manager explora esse objeto, criando uma representação dele no diretório de provisionamento. Você pode iniciar imediatamente o trabalho com esse objeto. A exploração automática de um objeto ocorre sempre que uma operação Adicionar, Mover ou Renomear gerar um erro que já existe no terminal quando o objeto não existir no diretório de provisionamento.

É possível combinar a exploração automática com o parâmetro de configuração de domínio Sincronização/correlação automática descrito no *Guia de Referência de Provisionamento*. Quando esses recursos trabalham juntos, primeiramente eles processam uma tentativa de criar uma conta usando um modelo de conta como uma tentativa de criar uma nova conta. Em seguida, o processamento usa as seguintes etapas:

- Observa uma conta inexplorada
- Explora essa conta automaticamente
- Correlaciona a conta automaticamente com o usuário global
- Adiciona um modelo de conta à conta como se fosse uma conta existente correlacionada a esse usuário global.

Excluir contas

Caso seja necessário excluir uma conta, é possível usar os métodos a seguir no Gerenciador de provisionamento:

- Clique com o botão direito do mouse na conta e selecione Excluir
- Clique com o botão direito do mouse em um usuário global e selecione Excluir usuário e contas
- Execute o assistente Excluir contas
- Sincronize usuários globais com funções de provisionamento e especifique que deseja excluir as contas extras

Quando você remove um usuário global de uma função de provisionamento, o Gerenciador de provisionamento fornece as seguintes opções para exclusão da conta:

- Se você decidir excluir as contas, o CA Identity Manager removerá as contas do diretório de provisionamento.
- Se você decidir não excluir as contas, será possível usar a opção Sincronizar usuário com funções e selecionar a opção Excluir conta.

Ao remover um usuário global de uma função de provisionamento antes de excluir as contas, você poderá listar as contas do usuário global. Clique com o botão direito do mouse no usuário global e selecione Listar contas.

- A lista de contas exibe as funções de provisionamento às quais a conta pertence. Se uma conta pertencer a uma função de provisionamento, ela será excluída quando você remover esse usuário dessa função e aceitar a ação de sincronização do usuário para excluir as contas.
- Se uma conta não pertencer a nenhuma função de provisionamento, significa que é uma conta extra e é apontada pela opção Check User Synchronization. A conta será excluída se você selecionar o item de menu Sincronizar o usuário com funções no usuário global.

Usar Excluir itens pendentes

O CA Identity Manager pode ser configurado de terminal em terminal, de modo que as contas em um terminal não são excluídas quando os administradores iniciam as ações de exclusão ou sincronização que geralmente excluem as contas. Em vez disso, as contas são colocadas em um estado Excluir itens pendentes no Console de usuário e em um estado Suspenso no terminal gerenciado. O CA Identity Manager também remove todos os modelos de conta das contas suspensas e limpa todos os atributos de recurso de valor múltiplo nas contas suspensas.

As contas no estado Excluir itens pendentes podem ser identificadas no Gerenciador de provisionamento, na guia Estatísticas das propriedades da conta. Uma conta suspensa tem um motivo de suspensão Excluir itens pendentes e um carimbo de data/hora de quando entrou nesse estado. O armazenamento do status Excluir itens pendentes e do carimbo de data/hora Suspenso permite a gravação de um utilitário que identifique essas contas Excluir itens pendentes e as exclui do Servidor de provisionamento e do terminal gerenciado posteriormente.

Recriar contas excluídas

Se você excluir uma conta em um terminal gerenciado usando uma ferramenta que não seja o CA Identity Manager, o recurso Check Account Synchronization apontará a conta como ausente, pois ela já existe no Diretório de provisionamento, mas não no terminal gerenciado. Quando isso acontecer, recrie a conta no terminal executando a função Synchronize Account with Account Templates, que cria uma conta usando os modelos associados à conta.

O CA Identity Manager registrará as contas conforme elas forem recriadas. Essas contas podem ser identificadas separadamente das contas que foram atualizadas, pois os administradores precisam estar cientes de que atributos diferentes dos atributos de recurso (por exemplo, senhas) foram definidos para os valores do modelo da conta original.

Capítulo 8: Funções de provisionamento

Esta seção contém os seguintes tópicos:

Funções de provisionamento e modelos de conta

Para simplificar o gerenciamento de contas, é possível criar e manter contas usando modelos de conta, que são usados em funções de provisionamento. Uma função de provisionamento contém um ou mais modelos de conta. Quando você aplica essa função a um usuário, ele receberá as contas de acordo com o que for definido pelos modelos.

Esses modelos fornecem a base para contas em um tipo de terminal específico. Oferecem o mesmo tipo de recurso que as políticas de provisionamento forneciam no eTrust Admin.

Usando os modelos de conta, é possível:

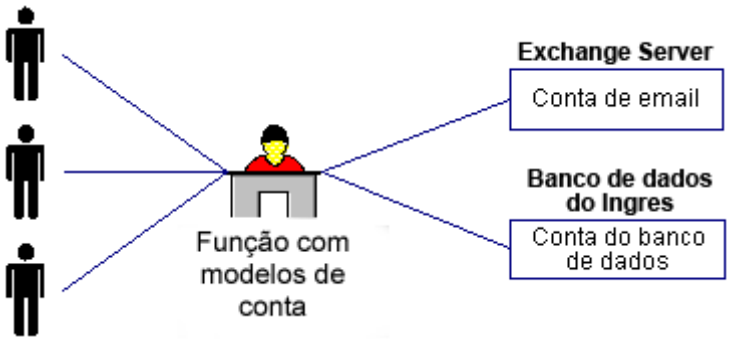
- Controlar os atributos de conta que os usuários do CA Identity Manager têm em um terminal quando suas contas são criadas.
- Definir os atributos usando sequências de caracteres da regra ou valores.
- Combinar atributos de conta de diferentes funções de provisionamento, para que os usuários tenham apenas uma conta em um terminal específico, com todos os atributos de conta necessários.
- Criar ou atualizar os atributos de conta quando os usuários globais alterarem as funções de provisionamento.

Criando funções para atribuir contas

Na maioria das organizações, os administradores gastam muito tempo para fornecer aos usuários contas de logon para diferentes sistemas e aplicativos. Para simplificar essa atividade repetitiva, você pode criar funções de provisionamento, que são funções que contêm modelos de conta. Os modelos definem os atributos que existem em um tipo de conta. Por exemplo, um modelo de conta para uma conta do Exchange define atributos, como o tamanho da caixa de correio. Os modelos de conta também definem como os atributos do usuário são mapeados para as contas.

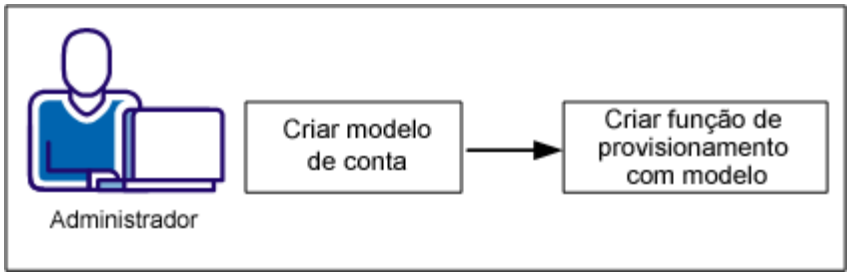
Considere um exemplo em que cada funcionário da Forward, Inc. precisa ter acesso a um banco de dados e a um email. Um administrador deseja evitar a criação de uma conta de banco de dados e de uma conta de email para cada funcionário, uma de cada vez. Portanto, o administrador cria uma função de provisionamento para essa empresa. A função contém um modelo de conta para um servidor Microsoft Exchange, para fornecer contas de email, e um modelo para um banco de dados Oracle. Neste exemplo, o servidor Exchange e o banco de dados Oracle são chamados de terminais, que são o sistema ou o aplicativo onde as contas existem.

Observação: a Forward, Inc. é um nome de empresa fictício que é usado estritamente para fins informativos e não faz referência a nenhuma empresa existente.



Após a criação das funções, os administradores de negócios, como gerentes ou a equipe de suporte, podem atribuir essas funções a usuários para fornecer contas em terminais. Depois que os usuários recebem a função, podem efetuar logon no terminal.

A criação de uma função de provisionamento que inclui um modelo de conta é um processo de duas etapas, conforme indicado a seguir:



As seções a seguir explicam como criar uma função que pode ser usada para atribuir contas:

1. Criar um modelo de conta (na página 200)
2. Criar uma função de provisionamento (na página 201)

Criar um modelo de conta

Para simplificar o gerenciamento de contas, é possível criar e manter contas usando modelos de conta, que são usados em funções de provisionamento. Uma função de provisionamento contém um ou mais modelos de conta. Quando você aplica essa função a um usuário, ele receberá as contas de acordo com o que for definido pelos modelos.

Esses modelos fornecem a base para contas em um tipo de terminal específico.

Usando os modelos de conta, é possível:

- Controlar os atributos de conta que os usuários têm em um terminal quando suas contas são criadas
- Definir os atributos usando sequências de caracteres da regra ou valores.
- Combinar atributos de conta de diferentes funções de provisionamento, para que os usuários tenham apenas uma conta em um terminal específico, com todos os atributos de conta necessários.
- Criar ou atualizar os atributos de conta quando os usuários globais alterarem as funções de provisionamento.

Um modelo de conta padrão para cada tipo de terminal é instalado com o servidor do CA Identity Manager. Em uma função de provisionamento, você pode usar o modelo de conta padrão ou criar seus próprios modelos de conta para qualquer terminal que tiver configurado.

Para criar um modelo de conta

1. Vá para Terminais, os quais podem estar listados sob Tarefas, e clique em Modelos de conta, Criar modelo de conta.
2. Selecione um tipo de terminal para o modelo.
3. Defina o Nome do terminal como o nome do sistema do terminal ou localhost, se aplicável.
4. Selecione um terminal para usar na guia Terminais.
5. Preencha os campos nas guias ou use os valores padrão.

   Cada tipo de terminal possui um conjunto diferente de guias. Clique em Ajuda para obter definições dos campos.
6. Clique em Enviar.

Observação: se mais de um terminal for especificado durante a pesquisa de objetos de terminal no modelo de conta, o subconjunto comum (interseção) dos objetos relacionados será retornado. Um exemplo é um grupo do Active Directory que existe em cada um dos terminais selecionados que estão associados ao modelo de conta. Quando os resultados da pesquisa mostram atributos diferentes do nome do objeto, são mostrados os valores de atributo dos objetos que estão associados ao primeiro terminal. Um exemplo é o atributo de descrição para o objeto de idioma em um conector do PeopleSoft.

Criar uma função de provisionamento

Você cria uma função de provisionamento depois de decidir sobre os requisitos da função:

- Quais usuários precisam de outras contas
- Quais contas estão associadas à função
- Quem são os integrantes, os administradores e os proprietários da função

Para criar uma função de provisionamento:

1. No console de usuário, vá para Funções e tarefas, Funções de provisionamento, Criar função de provisionamento.

   Para obter detalhes sobre cada guia, clique no link Ajuda na tela.

2. Preencha a guia Perfil. Somente o campo Nome é obrigatório.

   Observação: é possível especificar atributos personalizados na guia Perfil que especificam informações adicionais sobre as funções de provisionamento. Você pode usar essas informações adicionais para facilitar as pesquisas de funções em ambientes que incluem um número significativo de funções.

3. Preencha a guia Modelos de conta.

   a. Clique em um tipo de terminal, como um ActiveDirectory.

   b. Clique em um modelo de conta.

      O tipo de terminal determina os modelos que podem ser clicados.

   c. Adicione mais modelos de conta, conforme necessário, para diferentes tipos de terminal.

4. Preencha a guia Funções de provisionamento se desejar aninhar funções de provisionamento nessa guia.

   Essa etapa exige que você tenha ativado funções aninhadas (na página 206) para esse ambiente.

5. Preencha a guia Administradores adicionando regras administrativas que controlam quem gerencia os integrantes e os administradores dessa função.

6. Preencha a guia Proprietários, adicionando regras de proprietário que controlam quem pode modificar essa função.
7. Clique em Enviar.
8. Para verificar se a função foi criada, clique em Funções de provisionamento, Exibir função de provisionamento.

Tarefas de função e modelo

No console de usuário, você pode criar e gerenciar funções de provisionamento, escolhendo Funções e tarefas e selecionando uma tarefa em Funções de provisionamento. Tarefas existem para as operações padrão, como tornar um usuário integrante de uma função e modificar ou excluir uma função.

Antes de criar uma função de provisionamento, é necessário um modelo de conta para incluir nessa função ou uma função de provisionamento que deseja importar. Você pode importar as funções que foram criadas no Gerenciador de provisionamento ou no eTrust Admin. No entanto, o CA Identity Manager não oferece suporte a funções aninhadas que foram criadas no eTrust Admin.

Importar uma função de provisionamento

Embora as funções de provisionamento sejam gerenciadas no console de usuário, algumas delas podem ter sido criadas no Gerenciador de provisionamento ou em um aplicativo externo. Para essas funções de provisionamento, é possível redefinir o proprietário da função para ser um administrador do CA Identity Manager, portanto, para que seja possível gerenciá-lo no console de usuário.

Para importar uma função de provisionamento:

1. Efetue logon no console de usuário como um usuário com a função de gerente do sistema. Clique em Tarefas, Funções e tarefas.
2. Clique em Funções de provisionamento, Redefinir os proprietários da função de provisionamento e selecione uma função de provisionamento criada no Gerenciador de provisionamento.
3. Preencha a guia Proprietários, adicionando regras de proprietário que controlam quem pode modificar essa função.
4. Clique em Enviar.

Agora, a função pode ser modificada, atribuída ou exibida usando tarefas na categoria Funções de provisionamento.

Atribuir novos proprietários a funções de provisionamento

Você pode selecionar uma ou mais funções de provisionamento e atribuir políticas de proprietário para controlar quem pode modificar as funções.

Para atribuir novos proprietários a funções de provisionamento:

1. Efetue logon no console de usuário como um usuário com a função de gerente do sistema.
2. Clique em Tarefas, Funções ou clique em Funções e Tarefas.
3. Clique em Funções de provisionamento, Criar políticas de proprietário para funções de provisionamento.
4. Selecione uma ou mais funções de provisionamento.
5. Preencha a guia Proprietários, adicionando regras de proprietário que controlam quem pode modificar essa função.
6. Clique em Enviar.

Os usuários que atenderem às novas políticas de proprietário poderão modificar as funções de provisionamento selecionadas.

Senhas de contas criadas por funções de provisionamento

Quando uma função de provisionamento é atribuída a um usuário, a criação de uma conta para esse usuário falhará se a senha do usuário do CA Identity Manager não atender aos requisitos de senha do terminal. Essa situação inclui a criação de um usuário com uma senha temporária.

Portanto, defina a política de senha para corresponder ou ser mais rígida do que os requisitos de senha do terminal. Você pode definir a política de senha usando a Política de senha do CA Identity Manager ou o perfil de senha de provisionamento. Se os dois métodos forem usados, as políticas devem coincidir.

Ordem de processamento do evento de função de provisionamento

Algumas tarefas padrão do CA Identity Manager incluem os *eventos*, que são ações que o CA Identity Manager executa para concluir uma tarefa e que determinam a associação da função de provisionamento. Por exemplo, a tarefa padrão Modificar usuário inclui os eventos AssignProvisioningRoleEvent e RevokeProvisioningRoleEvent. A atribuição ou revogação de uma função de provisionamento pode adicionar ou remover uma conta em um terminal. Em alguns casos, o terminal pode exigir que todas as ações de adição ocorram antes das ações de remoção.

Para fazer com que o CA Identity Manager processe as ações de adição primeiro, você deve ativar a configuração Accumulation of Provisioning Role Membership Events no Management Console. Quando essa configuração está ativada, o CA Identity Manager reúne todas as ações de adição e remoção em um único evento, chamado de AccumulatedProvisioningRolesEvent. Por exemplo, se a tarefa Modificar usuário atribuir um usuário a três funções de provisionamento e remover esse usuário de duas outras funções de provisionamento, será gerado um evento AccumulatedProvisioningRolesEvent que contém cinco ações: 3 ações de adição e 2 ações de remoção.

Quando esse evento é executado, todas as ações de adição são reunidas em uma única operação e enviadas ao servidor de provisionamento para processamento. Após a conclusão do processamento das ações de adição, o CA Identity Manager reúne as ações de remoção em uma única operação e envia essa operação ao servidor de provisionamento.

A ativação dessa configuração afeta as seguintes funcionalidades do CA Identity Manager:

- **Guia Funções de provisionamento em tarefas do usuário**

  Quando um administrador adiciona ou remove um usuário de uma função de provisionamento usando a guia Funções de provisionamento, o CA Identity Manager reúne essas ações em um único evento.

- **Políticas de identidade**

  Todos os eventos de associação da função de provisionamento (AssignProvisioningRoleEvent ou RevokeProvisioningRoleEvent) que são gerados como resultado de uma avaliação de Política de identidade são reunidos em um único evento AccumulatedProvisioningRolesEvent. O CA Identity Manager executa esse evento como qualquer outro evento secundário. Por exemplo, considere um conjunto de políticas de identidade que inclui duas políticas de identidade: a Política A revoga a associação na Função de provisionamento A, e a Política B torna os usuários integrantes da Função de provisionamento B. Se o CA Identity Manager determinar que um usuário não satisfaz mais a Política A, mas agora satisfaz a Política B, um evento AccumulatedProvisioningRolesEvent que contém duas ações (uma para a ação de remoção e outra para a ação de adição) é gerado. A ação de adição é executada primeiro e, em seguida, a ação de remoção é executada.

- **Exibir tarefas enviadas**

  Para exibir o status do evento AccumulatedProvisioningRolesEvent e o status de cada uma das ações individuais, use a tarefa Exibir tarefas enviadas, para exibir os detalhes do evento.

  Se uma das ações individuais falhar, o status do evento se tornará Com falha, o que moverá a tarefa para um estado com falha.

- **Fluxo de trabalho**

  Você pode associar um processo de fluxo de trabalho com o evento AccumulatedProvisioningRolesEvent. Nesse caso, um aprovador pode aprovar ou recusar o evento inteiro, o que aprova ou recusa cada um dos eventos individuais.

  É necessário definir configurações adicionais para ativar o fluxo de trabalho para os eventos individuais do evento AccumulatedProvisioningRolesEvent.

- **Auditoria**

  O CA Identity Manager auditora informações sobre o evento AccumulatedProvisioningRolesEvent e cada evento individual.

Ativar a acumulação de evento de associação da função de provisionamento

O CA Identity Manager fornece uma opção de configuração no Management Console que possibilita a combinação de todas as ações de adição e remoção para um evento de associação da função de provisionamento em uma única operação. Quando combinadas, o CA Identity Manager processa as ações de adição como uma única operação antes de processar as ações de remoção.

Essa configuração permite o sequenciamento de eventos exigidos por alguns tipos de terminal.

Observação: esse recurso vem desativado por padrão.

Para ativar a acumulação de evento de associação da função de provisionamento:

1. Acesse o Management Console do CA Identity Manager.
2. Clique em Ambientes.
3. Selecione o ambiente que deseja configurar.
4. Abra Configurações avançadas, Provisionamento.
5. Marque a caixa de seleção Enable Accumulation of Provisioning Role Membership Events.
6. Reinicie o servidor de aplicativos.

Ativar funções aninhadas em um ambiente

Você pode incluir uma função de provisionamento dentro de outra função de provisionamento. A função incluída é chamada de função aninhada.

Por exemplo, você pode criar uma função de provisionamento Employee. A função Employee forneceria as contas necessárias para todos os funcionários, como contas de email. Você inclui a função Employee em funções de provisionamento de departamentos específicos, como uma função de Finanças e uma função de Vendas. As funções de provisionamento de departamentos forneceriam contas relacionadas apenas a esse departamento. Essa combinação de funções fornece as contas certas para cada usuário.

Para ativar funções aninhadas em um ambiente:

1. No Management Console, selecione o ambiente.
2. Clique em Role and Task Settings, Importar.
3. Selecione Suporte a funções de provisionamento aninhadas.
4. Clique em Finalizar.
5. Reinicie o ambiente.

Incluir uma função em uma função de provisionamento

Para incluir uma função em uma função de provisionamento:

1. Vá para Funções e tarefas, Funções de provisionamento, Modificar funções de provisionamento.
2. Preencha a guia Funções de provisionamento, clicando em Adicionar uma função, e selecione uma função de provisionamento.

   Por motivos de desempenho, é recomendável limitar o aninhamento de funções a três níveis. Por exemplo, caso esteja incluindo outra função (função de segundo nível), que pode conter uma função de terceiro nível, na função de provisionamento atual (função de primeiro nível). Recomendamos que a função de terceiro nível não contenha outras funções.
3. Preencha a política de proprietário, modificando a regra de proprietário.

   O escopo deve ser igual ou maior do que o escopo para a função adicionada.
4. Clique em Enviar.

Atributos em modelos de conta

Os atributos em modelos de conta determinam como os atributos são definidos na conta.

Atributos iniciais e de capacidade

Os modelos de conta incluem dois tipos de atributo:

- Os *atributos de capacidade* representam informações de conta, como tamanho do repositório, quantidade, limites de frequência ou associações do grupo. O Gerenciador de provisionamento deixa os atributos de capacidade em negrito em todas as telas do modelo de conta para facilitar a identificação dos atributos de capacidade.
- Os *atributos iniciais* representam todas as informações definidas inicialmente para uma conta, como nome, senha e status da conta, além de informações pessoais, tais como nome, endereço e números de telefone.

As contas são consideradas sincronizadas com seus modelos de conta quando todos os atributos de capacidade estiverem sincronizados. Esses são os atributos que diferem de um tipo de terminal para o outro, como associações do grupo, privilégios, cotas e restrições de logon. Eles controlam o que o usuário pode fazer quando efetuar logon na conta.

A sincronização não atualiza outros atributos da conta. Eles são iniciados nos modelos de conta durante a criação da conta e também podem ser atualizados durante as funções de propagação. O servidor de provisionamento fornece duas funções de propagação (uma atualização imediata de contas no momento em que o modelo de conta é alterado e uma atualização de contas no momento em que os atributos do usuário global são alterados).

Localizando atributos iniciais e de capacidade

Para saber diferenciar os atributos iniciais e de capacidade, é necessário gerar o arquivo eTACapability.txt. Digite o comando a seguir em um prompt de comando do Windows:

```
PS_HOME\dumpptt.exe -c > eTACapability.txt
```

PS_Home

Especifica C:\Arquivos de programa\CA\Identity Manager\Provisioning Server\bin

Uma versão do arquivo é gerada para todos os conectores instalados.

Sequências de caracteres de regra em modelos de conta

Quando você cria um modelo de conta, usa as sequências de caracteres de regra para definir o formato de vários atributos da conta. As sequências de caracteres de regra são variáveis para o valor real. As sequências de caracteres de regra são úteis quando você deseja gerar atributos que mudam de uma conta para outra. Quando as regras são avaliadas, o CA Identity Manager substitui as sequências de caracteres de regra inseridas nos modelos de conta por dados especificados no objeto de usuário.

Observação: a avaliação de regra não é executada em contas criadas durante uma exploração ou em contas criadas sem funções de provisionamento.

A tabela a seguir lista as sequências de caracteres de regra do CA Identity Manager:

Sequência de caracteres de regra	Descrição
%AC%	Nome da conta
%D%	A data atual no formato *dd/mm/aaaa* (a data é um valor calculado que não envolve as informações do usuário global*).* Essa sequência de caracteres de regra é equivalente a uma das seguintes opções: %$$DATE()% %$$DATE%
%EXCHAB%	Ocultar caixa de correio do catálogo de endereços do Exchange
%EXCHS%	Nome do servidor principal da caixa de correio
%EXCMS%	Nome do repositório da caixa de correio
%GENUID%	Identificador numérico de usuário do UNIX/POSIX Essa variável de regra é igual a %UID%, desde que o valor da UID do usuário global esteja definido. No entanto, se o usuário global não tiver nenhum valor de UID atribuído, e a geração de UID estiver ativada (Propriedades Globais em Tarefa do Sistema), várias ações ocorrem. O próximo valor do UID disponível é alocado, atribuído ao usuário global e usado como o valor dessa variável de regra.
%P%	Senha
%U%	Nome do usuário global.
%UA%	Endereço completo (gerado com rua, cidade, estado e CEP).
%UB%	Edifício
%UC%	Cidade
%UCOMP%	Nome da empresa
%UCOUNTRY%	País

Sequência de caracteres de regra	Descrição
%UCU*xx*% ou %UCU*xxx*%	Campo personalizado (*xx* ou *xxx* representa a ID de campo de dois ou três dígitos, conforme especificado na guia Custom User Fields no quadro de Tarefa do Sistema)
%UD%	Descrição
%UDEPT%	Departamento
%UE%	Endereço de email
%UEP%	Endereço de email principal
%UES%	Endereços de email secundários
%UF%	Nome
%UFAX%	Número de Fac-símile
%UHP%	Página inicial
%UI%	Iniciais
%UID%	Identificador numérico de usuário do UNIX/POSIX
%UL%	Sobrenome
%ULOC%	Local
%UMI%	Inicial do segundo nome
%UMN%	Segundo nome
%UMP%	Número de celular
%UN%	Nome completo
%UO%	Nome do escritório
%UP%	Telefone
%UPAGE%	Pager
%UPC%	CEP
%UPE%	Ramal do telefone
%US%	Estado
%USA%	Rua
%UT%	Cargo

Sequência de caracteres de regra	Descrição
%XD%	Gera o carimbo de data/hora atual no formato XML dateTimeValue, um formato de sequência de caracteres de comprimento fixo. Em um atributo dateValue ou timeValue, é possível gravar uma expressão de subsequência de caracteres (:offset,length) para extrair as partes da data ou hora do dateTimeValue. Por exemplo, %XD:1,10 % gera AAAA-MM-DD; e %XD:12,8% gera HH:MM:SS.

Valores de atributos

Para usar um valor constante e específico para um atributo de conta, digite o valor no campo do modelo de conta, em vez de em uma sequência de caracteres de regra. Por exemplo, é possível inserir os valores para especificar limites de frequência, tamanho ou quantidade.

Se o valor do atributo constante precisar conter mais de um sinal de porcentagem, digite dois sinais de porcentagem (%%) de cada vez. O CA Identity Manager irá convertê-los em um sinal de porcentagem (%) durante a criação do valor de atributo da conta. Se o valor do modelo de conta contiver somente um sinal de porcentagem, o CA Identity Manager não gerará um erro. A regra declara que, se você desejar um valor literal de 25%, deve especificar 25%%. No entanto, em um caso especial, 25% será aceito.

Expressões de regras avançadas

Para fornecer mais flexibilidade do que a simples substituição de atributo de usuário global, é possível digitar expressões de regras avançadas, incluindo o seguinte:

- Subsequências de caracteres de expressões de regra usando Deslocamento e Comprimento.
- Combinações de sequências de caracteres de regra e valores.
- Expressões de regra para definir vários valores para atributos de conta com vários valores.
- Variáveis de regra de outros atributos de usuário global.
- Invocação de funções integradas.
- Invocação de funções de encerramento de programa escritas pelo cliente.

Combinação de sequências de caracteres de regra e valores

É possível combinar sequências de caracteres de regra e valores constantes em um valor de atributo de modelo de conta. Por exemplo, se não houver nenhuma sequência de caracteres de regra %UI%, você pode obter o mesmo efeito pela concatenação de várias expressões de regra, da seguinte maneira:

```
%UF:,1%%UMI:,1%%UL:,1%
```

A sequência de caracteres de regra %UA% é equivalente ao seguinte:

```
%USA%, %UC%, %US%, %UPC%
```

Você também pode combinar uma sequência de caracteres de regra com um valor constante para criar um atributo do terminal inicial do UNIX, da seguinte maneira:

```
/u/home/%AC%
```

Subsequências de caracteres de regra

A seguir, há a sintaxe para criar um valor de subsequência de caracteres de uma variável de regra:

```
%var[:offset,length]%
```

var

Representa o nome da variável de regra predefinida, conforme definido na tabela mostrada anteriormente.

offset

(Opcional) Define o deslocamento inicial do sufixo da subsequência de caracteres. O número 1 representa o primeiro caractere.

length

(Opcional) Define o deslocamento final do sufixo da subsequência de caracteres. Um valor de comprimento de asterisco (*) indica o fim do valor.

Por exemplo, para definir um atributo de conta para os quatro primeiros caracteres de um atributo Edifício de um usuário global, use o seguinte para definir a variável:

```
%UB:1,4%
```

Se o atributo Edifício estiver vazio ou tiver menos de quatro caracteres, o valor de atributo da conta resultante terá menos do que quatro caracteres.

Expressões de regra com vários valores

A maioria das expressões de regra tem um valor único. Elas iniciam a partir de um valor de atributo do usuário (possivelmente vazio) e resultam em um valor de atributo da conta (também possivelmente vazio). No entanto, talvez às vezes você deseje considerar um atributo do usuário vazio como 0 valor. Às vezes, talvez você deseje gerar vários valores para preencher um valor de atributo da conta com vários valores.

A sintaxe da regra a seguir permite que você trabalhe com zero ou mais valores que um atributo do usuário pode conter:

%*_var_%

O asterisco opcional (*) sinalizador com vários valores imediatamente após o primeiro símbolo de porcentagem % de uma expressão de regra indica que o resultado dessa expressão de regra deve ser 0, 1 ou mais de 1 valor, dependendo do número de valores que o atributo de usuário referenciado contém.

A maioria dos valores de atributos de usuário tem valor único, portanto, pode conter apenas 0 ou 1 valor. No entanto, os atributos personalizados (CustomField01 a CustomField99) são atributos com vários valores; portanto, uma variável de regra que faz referência a esses atributos pode conter 0, 1 ou mais de 1 valor.

Se um atributo de usuário possuir mais de 1 valor, mas você não incluir o asterisco (*) em sua expressão de regra, o resultado da avaliação de regra será o do primeiro valor. No entanto, na maioria dos casos, os valores de atributo são oficialmente desordenados e, como resultado, o valor que o CA Identity Manager considera primeiro não pode ser controlado.

Se um atributo de usuário tiver mais de um valor, e você incluir o * na expressão de regra, vários valores serão gerados para o atributo da conta. Não defina esse tipo de expressão de regra com vários valores em um modelo de conta se o atributo da conta que estiver sendo definido no atributo de modelo de conta não tiver vários valores.

É possível definir um atributo de conta estendido como com vários valores no tipo de terminal ADS e usar essa sintaxe da expressão de regra com vários valores para definir esse atributo. Por exemplo, considere um ambiente que define um atributo de conta estendido ADS denominado patentes e um atributo de usuário personalizado número três também denominado patentes.

Um modelo de conta ADS pode definir, para o atributo patentes, a sequência de caracteres de regra %*UCU03%. Em seguida, você pode alterar o atributo patentes de um usuário adicionando um ou mais valores. Ao aplicar as alterações ao usuário, selecione a opção de atualização das contas do usuário. Essa opção consulta o modelo de conta da conta, encontre a variável de regra %*UCU03% e sabe copiar todas as patentes do usuário para o atributo patentes da conta.

Da mesma forma, durante a criação de uma conta, sequências de caracteres de regra são avaliadas. Além disso, durante a alteração do modelo de conta, se a sequência de caracteres de regra tiver sido alterada, é possível recalcular a regra para todas as contas associadas ao modelo de conta.

A sintaxe %**var*% também é significativa para as variáveis *var* que fazem referência a atributos de usuário de valor único. Isso se aplica apenas quando a concatenação estiver envolvida e se os atributos referenciados forem redefinidos para os usuários.

O asterisco opcional (*) sinalizador com vários valores indica que a regra que contém uma variável de regra %**var*% é avaliada como nenhum valor se o atributo de usuário não tiver valores. É diferente da expressão de regra de valor único %*var*%, que é sempre avaliada como um valor único, mesmo que seja uma sequência de caracteres vazia.

Para compreender essa diferença, considere as seguintes sequências de caracteres de regra:

```
(310)%UP%
 (310)%*UP%
```

As duas sequências de caracteres de regra são exibidas para acrescentar o código de área 310 ao telefone. No entanto, são diferentes porque se os usuários não tiverem nenhum valor para seu número de telefone, a primeira regra será avaliada como o valor da conta (310). A segunda sequência de caracteres de regra não gera nenhum valor e mantém o atributo da conta não definido.

Por outro lado, considere as seguintes sequências de caracteres de regra que são exibidas para acrescentar o ramal ao número de telefone:

```
%UP% %UPE%
%UP% %*UPE%
```

Se todos tiverem um número de telefone, mas alguns não tiverem ramais, a primeira sequência de caracteres de regra gerará um valor que inclui o número de telefone para cada usuário sem nenhum ramal. A segunda sequência de caracteres de regra não gerará nenhum valor. Nesse caso, use a primeira regra com %UPE%.

Regras de atributo explícitas de usuário global

Cada usuário tem muito mais atributos do que estão listados na tabela de regras anterior. Você provavelmente não precisará criar expressões de regra que fazem referência a algum desses outros atributos. No entanto, se surgir a necessidade, você poderá usar a sintaxe a seguir para fazer referência a um determinado atributo de usuário:

```
%#ldap-attribute%
```

Por exemplo, se fosse necessário determinar o valor do campo Suspenso do usuário, você determinaria o nome do atributo LDAP correspondente para este campo (que é eTSuspended) e criaria a expressão de regra que é avaliada como 0 ou 1, como eTSuspended:

```
%#eTSuspended%
```

Como outro exemplo, você pode obter as funções de provisionamento atribuídas do usuário com a seguinte expressão de regra:

```
%*#eTRoleDN%
```

Essas funções de provisionamento são valores de nome distintos de LDAP completo. Talvez em conjunto com a função integrada RDNVALUE (consulte a tabela a seguir), os valores seriam um pouco mais úteis. Observe o asterisco indicador com vários valores (*), de modo a obter todas as funções de provisionamento atribuídas do usuário como vários valores.

A sintaxe de subsequência de caracteres também é aplicável a essas expressões de regra, portanto, você pode usar %#eTTelephone:6,*% para significar a mesma coisa que %UP:6,*. Cada uma solicita que o CA Identity Manager remova os primeiros cinco caracteres do campo de telefone do usuário.

Funções de regras integradas

Você pode usar funções de regras integradas em suas expressões de regra para executar várias transformações nos valores. O formato geral de invocação de funções de regras integradas é:

```
%[*]$$function(arg[,…])[:offset,length]%
```

em que o asterisco indicador com vários valores (*) e as especificações de subsequência de caracteres de deslocamento e comprimento são mais uma vez opcionais.

As funções integradas reconhecidas são as seguintes:

Função de regra integrada	Descrição
ALLOF	Mescla todos os parâmetros em um atributo com vários valores. A ordem é preservada e as duplicatas são removidas. Por exemplo, se os atributos de usuário estiverem definidos para o seguinte: eTCustomField01: { A, B } eTCustomField02: { A, C } Então, a regra: %*ALLOF(%*UCU01%,%*UCU02%)% retorna três valores {A, B, C}.
DATE	Retorna a data atual em formato *dd/mm/aaaa*. A expressão de regra %D% é equivalente a uma das seguintes: %$$DATE()% %$$DATE%
FIRSTOF	Retorna o primeiro valor de qualquer um dos parâmetros. Usado para inserir um valor padrão se um atributo não for definido: %$$FIRSTOF(%UCU01%,'unknown')% %$$FIRSTOF(%LN%,%UCU01%,%U%)% Se nenhum dos valores estiver definido, o resultado será nenhum valor. Para incluir uma sequência de caracteres constante em um argumento, coloque-a entre aspas simples.
INDEX	Retorna um valor de um atributo com vários valores. Índice 1 é o primeiro valor. Se o índice for maior do que o número de valores, o resultado será o valor não definido (vazio). As regras a seguir são equivalentes ao seguinte: %$$INDEX(%*UCU01%,1)% %$$FIRSTOF(%*UCU01%)%

Função de regra integrada	Descrição
NOTEMPTY	Retorna o único valor de seu argumento, mas informa uma falha se o valor deste atributo não estiver definido. Exemplo 1: Falha na criação ou atualização da conta se o usuário não tiver um atributo UID atribuído: %$$NOTEMPTY(%UID%)% Exemplo 2: Use o nome. Caso não esteja definido, use o sobrenome. Se nenhum dos dois estiver definido, haverá falha na criação ou atualização da conta. %$$NOTEMPTY(%$$FIRSTOF(%UF%, %UL%)%)%
PRIMARYEMAIL	Retorna o endereço de email principal extraído dos vários endereços de email. A expressão %UE% é equivalente ao seguinte: %$$PRIMARYEMAIL(%UEP%)%
RDNVALUE	Trata o valor do atributo como um nome distinto LDAP e extrai o nome comum do objeto do DN: %*$$RDNVALUE(%#eTRoleDN%)% Essa função retorna os nomes comuns de todas as funções de provisionamento atribuídas. Se o usuário pertencer a duas funções de provisionamento com o mesmo nome comum, esse nome da função será listado uma vez.
TOLOWER	Converte texto com letra maiúscula em texto com letra minúscula: %$$TOLOWER(%AC%)%
TOUPPER	Converte texto com letra minúscula em texto com letra maiúscula: %$$TOUPPER(%U%)%

Função de regra integrada	Descrição
TRIM	Remove espaços em branco à direita e à esquerda de um valor de atributo. Por exemplo, “%UF %UL%” geralmente cria um valor com um nome e um sobrenome separados por um espaço em branco. No entanto, se o usuário possui um atributo de nome em branco, esta regra gera um valor que termina com um espaço em branco à direita. No entanto, usar “%$$TRIM(%UF% %UL%)% garante que nenhum espaço em branco à direita ou à esquerda existe no valor de atributo da conta, mesmo se um ou outro de Nome e Sobrenome não estiver definido.

Desempenho da função de provisionamento

Ao usar o CA Identity Manager com um servidor de provisionamento, há alguns aprimoramentos de desempenho de provisionamento que podem ser considerados.

Cache do objeto JIAM

O CA Identity Manager se comunica com o servidor de provisionamento por meio da API do Java IAM (JIAM). Para melhorar o desempenho de comunicação, você configura um cache para objetos recuperados a partir do servidor de provisionamento.

Ativar o cache do JIAM

Para ativar o cache do JIAM:

1. Acesse as configurações de ambiente por meio do Management Console. Clique em Configurações avançadas, Diversos.
2. Configure a propriedade definida pelo usuário para o cache do JIAM.
   - **Propriedade**—JIAMCache
   - **Valor**—verdadeiro
3. Clique em Adicionar.
4. Clique em Salvar.

   A propriedade definida pelo usuário é salva.

Definir a vida útil do cache do JIAM

O cache do JIAM armazena informações para um determinado período de tempo antes da expiração dos dados. Esse período de tempo é conhecido como vida útil (TTL). Você define o valor de TTL do cache do JIAM (em segundos) para definir por quanto tempo os dados permanecem no cache.

Visando a obter o máximo benefício dos dados armazenados em cache localmente, é possível equilibrar os ganhos de desempenho em relação aos dados em tempo hábil. É recomendável um valor de TTL mínimo de 1 dia, com um valor máximo de 7 dias. Consulte a tabela a seguir para encontrar os valores de vida útil a serem usados:

Tempo de vida desejado	Configurações de vida útil (s)
24 horas (1 dia)	86,400
72 horas (3 dias)	259,200
120 horas (5 dias)	432,000
168 horas (7 dias)	604,800

Para definir a vida útil do cache do JIAM

1. Acesse Ambiente por meio do Management Console. Clique em Configurações avançadas, Diversos.
2. Configure a propriedade definida pelo usuário para o TTL do cache do JIAM.
   - **Propriedade**—JIAMCacheTTL
   - **Valor**—tempo em segundos que os dados permanecem no cache do JIAM

     Padrão: 300
3. Clique em Adicionar.
4. Clique em Salvar.

   A propriedade definida pelo usuário é salva.

Pools de sessão

Para melhorar o desempenho, o CA Identity Manager pode pré-alocar um número de sessões a serem agrupadas para uso quando se comunicarem com o servidor de provisionamento.

Para obter mais informações sobre o pool de sessão, consulte a *Ajuda online do Management Console*.

Tarefas de provisionamento para ambientes existentes

Se você importar definições de funções personalizadas e desejar ativar o provisionamento para um ambiente, você *também* deve importar as definições de função apenas de provisionamento no Management Console. Essas definições de função podem ser encontradas nesta pasta:

`iam_im.ear\management_console.war\WEB-INF\Template\environment`

Observação: para obter mais informações sobre a importação de definições de função, consulte o *Guia de Configuração*.

Capítulo 9: Serviços gerenciados (Solicitações de acesso básico)

Esta seção contém os seguintes tópicos:

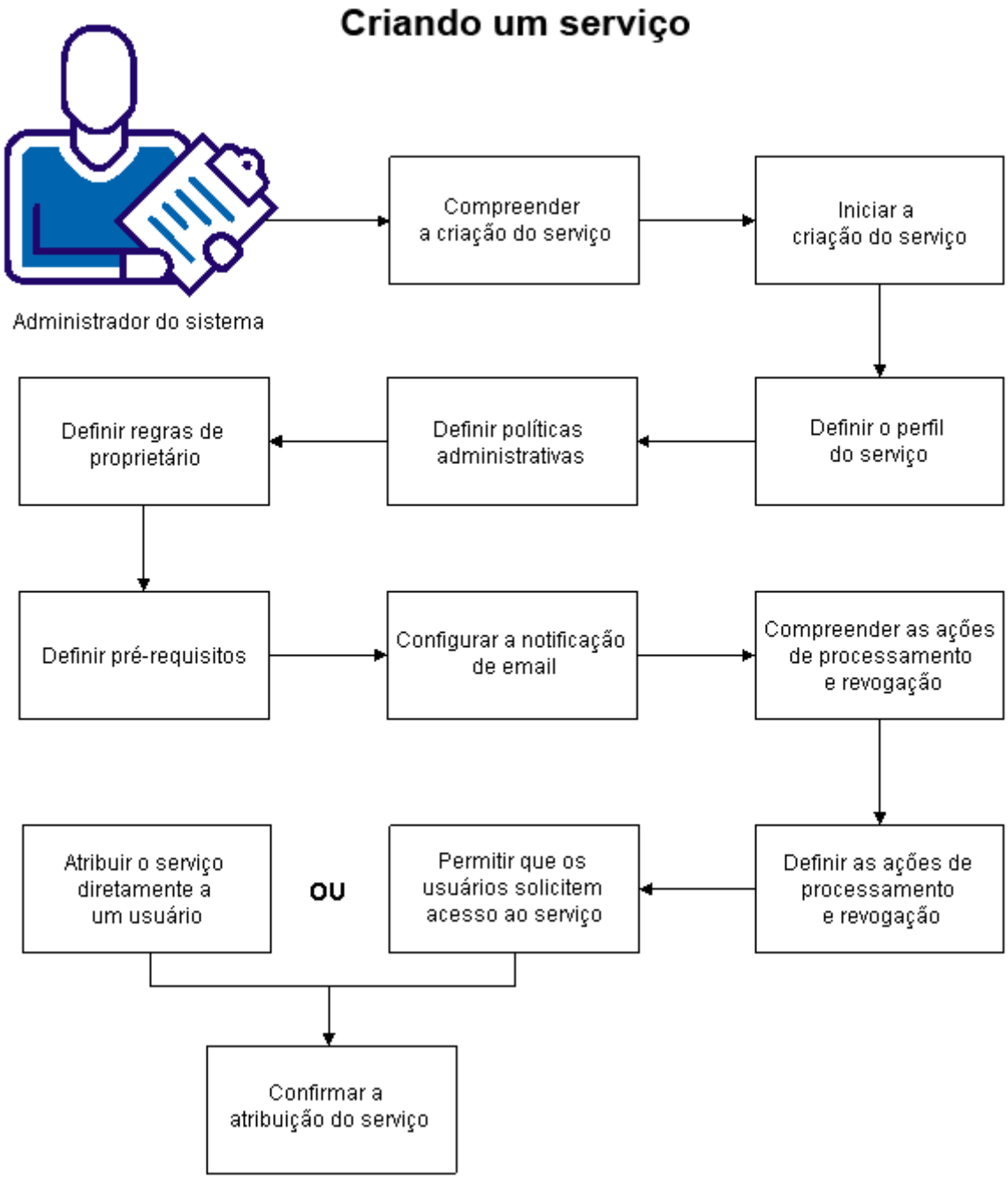
Criando um serviço

Os serviços simplificam o gerenciamento de direitos. Um serviço reúne todos os direitos - tarefas, funções, grupos e atributos - que um usuário precisa para uma determinada função de negócios. Os serviços estão disponíveis ao usuário por meio de tarefas de solicitação de acesso no console de usuário do CA CloudMinder. As tarefas de solicitação de acesso permitem que um usuário ou administrador solicite, atribua, revogue e renove um serviço.

Os serviços permitem que um administrador combine os direitos de usuário em um único pacote, que são gerenciados como um conjunto. Por exemplo, todos os novos funcionários de Vendas precisam acessar um conjunto de tarefas e contas definidas em sistemas de terminal específicos. Eles também precisam de informações específicas adicionadas aos respectivos perfis de contas de usuário. Um administrador cria um serviço denominado Administração de vendas, que contém todas as informações necessárias de tarefas, funções, grupos e atributos de perfil para um novo funcionário de Vendas. Quando um administrador atribui o serviço Administração de vendas a um usuário, ele recebe o conjunto completo de funções, tarefas, grupos e atributos de conta que são definidos pelo serviço.

Os usuários também podem acessar serviços solicitando acesso por conta própria. No console de usuário, cada usuário tem uma lista de serviços disponíveis para sua solicitação. Essa lista é preenchida com os serviços marcados como Autoinscrição por um administrador com os privilégios apropriados, geralmente durante a criação do serviço. Na lista de serviços disponíveis, os usuários podem solicitar acesso aos serviços de que precisam. Quando o usuário solicita acesso a um serviço, a solicitação é processada automaticamente, e os direitos associados são atribuídos ao usuário imediatamente. Um administrador com os privilégios apropriados também pode configurar o processamento de serviço para exigir aprovação de fluxo de trabalho ou para gerar notificações por email.

O diagrama a seguir mostra as informações necessárias para compreender, e as etapas a serem executadas para criar um serviço.


Criando um serviço
Administrador do sistema
Compreender a criação do serviço
Iniciar a criação do serviço
Definir o perfil do serviço
Definir políticas administrativas
Definir regras de proprietário
Definir pré-requisitos
Configurar a notificação de email
Compreender as ações de processamento e revogação
Definir as ações de processamento e revogação
Permitir que os usuários solicitem acesso ao serviço
OU
Atribuir o serviço diretamente a um usuário
Confirmar a atribuição do serviço

Os tópicos a seguir explicam como criar um serviço e torná-lo disponível aos usuários:

1. Entender a criação do serviço (na página 224).
2. Iniciar a criação do serviço (na página 225).
3. Definir o perfil de serviço (na página 225).
4. Definir políticas administrativas para o serviço (na página 227).
5. Definir regras de proprietário para o serviço (na página 228).
6. Definir pré-requisitos para o serviço (na página 228).
7. Configurar a notificação por email para renovação de serviço. (na página 229)
8. Entender as ações de processamento e revogação (na página 230).
9. Definir ações de processamento e revogação para o serviço. (na página 230)
10. Permitir que os usuários solicitem acesso a serviços.

    No console de usuário, quando o usuário clica em Meu acesso, Solicitar e exibir acesso, vê uma lista de serviços disponíveis para sua solicitação. Os serviços que aparecem nessa lista são aqueles marcados como Autoinscrição por um administrador com os privilégios apropriados, geralmente durante a criação do serviço.
11. Atribuir um serviço diretamente a um usuário (na página 83).
12. Confirmar a atribuição de serviço.

Entender a criação do serviço

Antes de criar um serviço, considere as informações e direitos de pré-requisito que são necessários para criar e processar o serviço.

Considere as seguintes perguntas:

1. Esse serviço é voltado para qual necessidade de negócios? Por exemplo, você pode criar um serviço que torne uma conta no Salesforce.com disponível para todos os novos funcionários.
2. Os integrantes do serviço precisam de determinadas funções administrativas? Em caso afirmativo, crie ou identifique essas funções administrativas.
3. Os integrantes do serviço devem receber acesso a um ou mais terminais? Em caso afirmativo, crie ou identifique esses terminais.
4. Se os integrantes do serviço precisarem de acesso a terminais, crie ou identifique as funções de provisionamento e os modelos de conta associados.

5. Os integrantes do serviço devem ser integrantes de determinados grupos? Em caso afirmativo, crie ou identifique esses grupos.
6. Determinados atributos de usuário devem ser referenciados ou modificados quando um usuário se torna integrante do serviço? Por exemplo, quando um usuário recebe o serviço do Salesforce.com, é necessário confirmar se o atributo de departamento para esse usuário está definido como Vendas? Em caso afirmativo, crie ou identifique esses atributos de usuário.

Depois de criar ou identificar esses pré-requisitos, é possível iniciar a criação do serviço (na página 225).

Iniciar a criação do serviço

Você cria um serviço no console de usuário.

Siga estas etapas:

1. Faça logon em uma conta que possua privilégios de gerenciamento de serviços.

   Por exemplo, o primeiro usuário de um ambiente tem a função de Gerente do sistema, que tem a tarefa Criar serviço.
2. No menu de navegação, selecione Serviços, que podem estar incluídos na lista de tarefas.
3. Clique em Gerenciar serviços e, em seguida, em Criar serviço.
4. Definir o perfil de serviço.

Definir o perfil de serviço

Na guia Perfil, você define as características básicas do serviço.

Siga estas etapas:

1. Digite um nome e um qualificador. Um qualificador é um identificador exclusivo do serviço.

   Observação: os qualificadores podem conter apenas caracteres alfanuméricos e sublinhados, e não podem começar com um número. Uma vez criado, um nome de qualificador não pode ser alterado, ou reutilizado, mesmo se um serviço for excluído posteriormente.
2. Selecione Ativado se desejar disponibilizar o serviço aos usuários assim que criá-lo.
3. Selecione Autoinscrição se desejar que esse serviço seja exibido na lista de serviços disponíveis para que os usuários o solicitem. Quando Autoinscrição é ativado, os usuários podem solicitar acesso a esse serviço por meio do Console de usuário.

4. (Opcional) Adicione uma ou mais categorias. Digite um nome de categoria e clique na seta para cima para adicioná-la ao serviço.

   As categorias adicionam mais informações a um serviço. Você pode usar essas informações adicionais para facilitar a pesquisa de serviços em ambientes que incluem um número significativo de serviços.

5. Especifique uma Tela de dados do usuário em tempo de execução do serviço se desejar coletar dados adicionais do usuário no momento em que um usuário solicitar o serviço.

   Use uma Tela de dados do usuário do serviço em tempo de execução para ajudar a garantir que todos os dados de usuários necessários para atender ao serviço existem no sistema. Por exemplo, um endereço de email válido é necessário para atender a um serviço que cria uma conta do Google Apps. Se o endereço de email de um usuário não existir no repositório de usuários do CA CloudMinder, o usuário será solicitado a fornecê-lo ao solicitar o serviço.

   a. Clique em Procurar.

      Uma lista de telas de perfil disponíveis é exibida. Geralmente, essas telas são usadas para coletar dados do usuário.

   b. Selecione uma tela de perfil que contenha os dados do usuário que você deseja coletar. Escolha uma das seguintes opções:

      - Clique em Selecionar para coletar todos os dados do usuário contidos nessa tela.

      OU

      - Clique em Copiar para personalizar os dados do usuário que você deseja coletar. Especifique um nome e um qualificador exclusivo para a nova tela. Adicione, edite ou remova elementos de dados do usuário e clique em OK.

      OU

      - Clique em Editar para alterar os dados do usuário contidos nessa tela. Adicione, edite ou remova elementos de dados do usuário e clique em OK.

      Importante: se você editar uma tela de dados do usuário, suas alterações serão aplicadas em todos os lugares onde a tela é usada no console de usuário. Em vez disso, pense em copiar e personalizar a tela de perfil.

   c. Clique em Selecionar.

      Os elementos de dados do usuário que você selecionou são coletados no momento em que o usuário solicita o serviço.

      Observação: se os dados necessários existirem no sistema quando um usuário solicitar um serviço, os dados serão pré-preenchidos na tela de perfil.

6. Definir políticas administrativas para o serviço (na página 227).

Definir políticas administrativas para o serviço

Na guia Administradores, você define quem pode adicionar ou remover usuários como integrantes e administradores desse serviço. As políticas administrativas contêm regras administrativas e de escopo, e pelo menos um privilégio de administrador (Gerenciar integrantes ou Gerenciar administradores).

As regras administrativas definem quem pode administrar esse serviço. As regras de escopo limitam quais usuários podem se tornar administradores. Por exemplo, uma regra administrativa pode permitir que todos os integrantes do grupo Vendas administrem um serviço. Em seguida, uma regra de escopo pode limitar esses usuários a apenas integrantes do grupo Vendas em Boston, MA.

Siga estas etapas:

1. Na guia Administradores, clique em Adicionar.

   A tela Política administrativa é exibida.

2. Defina uma regra administrativa por meio da qual os usuários podem administrar esse serviço. Por exemplo, você pode especificar os usuários que são integrantes do grupo Vendas, ou que têm o atributo de perfil de cargo específico de Gerente de vendas.

   Clique na seta para a esquerda para editar uma parte previamente especificada de uma regra.

3. Defina uma regra de escopo para limitar os usuários que podem administrar esse serviço. Por exemplo, se você especificou usuários que são integrantes do grupo Vendas na regra administrativa, em seguida, você pode limitar o escopo dessa regra apenas a usuários cuja cidade é Boston, MA.

   Observação: é possível adicionar várias políticas administrativas com regras e privilégios diferentes para cada serviço.

4. Se desejar permitir que os administradores adicionem ou removam integrantes desse serviço, clique em Pode gerenciar os integrantes de serviço.

5. Clique em OK.

6. Para editar outras informações de uma política, clique no ícone Editar. Para remover uma política, clique no ícone do sinal de menos.

7. Definir regras de proprietário para o serviço. (na página 228)

Definir regras de proprietário para o serviço

Na guia Proprietários, defina regras sobre quem pode ser um proprietário do serviço. Um proprietário é um usuário que pode modificar o serviço.

Siga estas etapas:

1. Na guia Proprietários, clique em Adicionar.

   A tela Regra de proprietário é exibida.

2. Defina uma regra de proprietário por meio da qual os usuários podem ser proprietários desse serviço. Por exemplo, você pode especificar os usuários que são integrantes do grupo Vendas, ou que têm o atributo de perfil de cargo específico de Gerente de vendas.

   Clique na seta para a esquerda para editar uma parte previamente especificada de uma regra.

3. Clique em OK.

4. Definir pré-requisitos para o serviço. (na página 228)

Definir pré-requisitos para o serviço

Na guia Pré-requisitos, você pode definir os serviços que os usuários devem ter antes de solicitar esse serviço. Um serviço só é exibido na lista de serviços disponíveis para um determinado usuário se o usuário for integrante de todos os serviços de pré-requisito.

Se uma duração for definida para um serviço de pré-requisito, essa duração se aplicará ao serviço que você estiver definindo. Por exemplo, Serviço A é um pré-requisito para o Serviço B. O Serviço A tem uma duração de uma semana. Nesse caso, o Serviço B também expira em uma semana.

Siga estas etapas:

1. Na guia Pré-requisitos, clique em Adicionar o serviço.

   Uma tela de pesquisa é exibida.

2. Pesquise um serviço que deseja designar como um pré-requisito para esse serviço.

   Para exibir uma lista de todos os serviços sobre os quais você possui privilégios administrativos, clique em Pesquisar sem modificar os critérios de pesquisa.

3. Escolha um serviço e clique em Selecionar.

   Uma lista atualizada dos pré-requisitos para esse serviço é exibida.

Configurar a notificação por email para renovação de serviço

Alguns serviços expiram após um período determinado.

Na guia Email, você pode configurar uma notificação por email que serve como lembrete para que os integrantes do serviço renovem sua associação antes da data de expiração. Os integrantes podem, em seguida, usar a função Renovar o serviço para renovar seu acesso.

O CA CloudMinder fornece um modelo de email padrão que inclui conteúdo dinâmico. Esse conteúdo é preenchido automaticamente quando o email é enviado. O conteúdo dinâmico, que é exibido entre chaves ({ }) no editor de notificação por email, adiciona um determinado nome de usuário, o nome do serviço e a data de expiração ao email.

Você pode modificar o conteúdo da notificação por email no editor. Por exemplo, você pode modificar o corpo ou o texto de assunto, alterar a fonte ou remover o conteúdo dinâmico.

Observe os seguinte itens ao configurar notificações por email:

- Se estiver incluindo conteúdo dinâmico na notificação por email, não modifique o texto entre as chaves ({ }).
- Se o serviço tiver um serviço de pré-requisito que expira, as notificações por email são enviadas somente para o serviço de pré-requisito, mesmo quando as notificações por email estiverem configuradas para ambos os serviços.

Siga estas etapas:

1. Na guia Email, marque a caixa de seleção Notificação por email aos usuários antes da expiração de um serviço para ativar as notificações.
2. (Opcional) Personalize a notificação por email usando os controles no editor.

   O editor de notificação por email oferece suporte a HTML. Você pode adicionar conteúdo HTML ao corpo da notificação por email, clicando no botão Toggle HTML Source (<>) na barra de ferramentas.
3. Entender as ações de processamento e revogação. (na página 230)

Entender as ações de processamento e revogação

Na guia Ações, é possível definir os direitos e informações - tarefas, funções, grupos e atributos - a serem adicionados, modificados ou removidos quando um serviço é atribuído ou revogado. Basicamente, as ações do serviço definem as ações que um serviço executa.

O CA CloudMinder usa uma política do Policy Xpress para definir as circunstâncias nas quais as ações de processamento e revogação ocorrem. O CA CloudMinder predefine essa política, de forma que quando um usuário solicitar um serviço, as condições e os dados adequados existam. O serviço é automaticamente processado ou revogado.

Um administrador deve definir as ações que o sistema executa para o processamento ou a revogação de um serviço. Por exemplo, ao criar um serviço, um administrador pode especificar que os integrantes do serviço recebem a função administrativa de Gerente de vendas, a função de provisionamento Salesforce.com e o grupo Vendas. Da mesma forma, o administrador pode especificar que esses direitos sejam removidos quando o serviço for revogado.

Definir ações de processamento e revogação para o serviço

Na guia Ações, é possível definir os direitos e as informações que o sistema adiciona, modifica ou remove quando um serviço é atribuído a um usuário ou removido dele.

Siga estas etapas:

1. Clique na guia Ações.

   A tela de ações de processamento e revogação é exibida.

2. Clique no botão Gerenciar ações de processamento de pedidos ou Gerenciar ações de revogação.

   A tela Criar política do Policy Xpress é exibida.

   Os campos a seguir são predefinidos para criar uma regra de ação:

   Nome

   Fornece um nome amigável para a regra de ação. Esse nome deve ser exclusivo.

   Descrição

   Define o significado da regra de ação.

   Prioridade

   Define qual regra de ação é executada, caso existam várias regras de ação correspondentes. Esse campo é útil para definir ações padrão. Por exemplo, se você possui várias regras, cada uma delas para um nome de departamento, é possível definir uma padrão adicionando uma regra sem condições, mas com uma prioridade mais baixa (como 10, se todas as outras forem 5). Se nenhuma das regras de departamento for correspondente, a padrão será usada.

3. Especifique os critérios de correspondência em Condições da regra de ação.
4. Em Adicionar ações, clique no botão Ação de adição mediante correspondência.

   A tela Ação de adição mediante correspondência é exibida. Nessa tela, você define as ações que o sistema executa quando a regra é correspondida.

5. Insira um nome amigável que defina a finalidade da ação.

   Por exemplo, digite "Adicionar a função administrativa de Gerente de vendas".

6. Selecione a categoria da ação que você deseja que o sistema execute.

   Por exemplo, para adicionar uma função, selecione a categoria Funções.

7. Selecione o tipo de ação que você deseja que o sistema execute.

   Por exemplo, para adicionar ou remover uma função administrativa, selecione o tipo Função administrativa definida.

8. Selecione a função que você deseja que o sistema execute.

   Por exemplo, para adicionar uma função administrativa, selecione a função Adicionar.

   Observação: quando você seleciona uma função, uma descrição dessa função é exibida. Essa descrição pode ajudar a determinar se a função selecionada resulta no comportamento do sistema que você deseja.

9. Defina a ação específica que você deseja que o sistema execute.

   Por exemplo, para adicionar uma função administrativa denominada "Gerente de vendas", digite o nome da função, ou clique no botão Procurar e selecione Gerente de vendas na lista de funções administrativas disponíveis.

10. Clique em OK.

    Repita esse procedimento até que você tenha adicionado todas as ações desejadas para esse serviço.

11. Clique em OK.

    O sistema associa ao serviço o processamento de pedidos e as ações de revogação designados. Quando um usuário recebe o serviço, as informações e os direitos associados são adicionados, modificados ou removidos.

12. Agora, é possível atribuir um serviço a um usuário (na página 83).

Atribuir um serviço a um usuário

É possível atribuir um serviço diretamente a um usuário específico. Esse usuário se torna um *integrante* do serviço.

Siga estas etapas:

1. Vá até Serviços, Solicitar e Exibir acesso.

   Uma lista de serviços que você pode administrar é exibida.

2. Selecione o serviço que deseja atribuir a um usuário e clique em Selecionar.

   Uma lista de usuários que estão atribuídos ao serviço é exibida.

3. Clique em Solicitar acesso.

4. Procure um usuário ao qual deseja atribuir o serviço.

   Para exibir uma lista de todos os usuários sobre os quais você possui privilégios administrativos, clique em Pesquisar sem modificar os critérios de pesquisa.

5. Escolha um usuário e clique em Selecionar.

   Uma lista atualizada de usuários que estão atribuídos ao serviço é exibida.

6. Clique em Salvar alterações.

   O usuário recebe o serviço especificado. O usuário recebe todos os aplicativos, funções, grupos e atributos incluídos no serviço.

Confirmar atribuição de serviço

Após atribuir um serviço a um usuário, verifique se todas as tarefas associadas ao serviço foram concluídas com êxito.

Siga estas etapas:

1. Vá até Serviços, Exibir o histórico da solicitação de acesso ao serviço.

   Uma tela de pesquisa é exibida.

2. Pesquise o serviço atribuído a um usuário.

   Para exibir uma lista de todos os serviços sobre os quais você possui privilégios administrativos, clique em Pesquisar sem modificar os critérios de pesquisa.

   Uma lista de serviços que você pode administrar é exibida.

3. Selecione o serviço que você atribuiu e clique em Selecionar.

   Um histórico das ações associadas ao serviço é exibido.

4. Clique em Última alteração para ver as ações mais recentes primeiro.

5. Confirme se o usuário em questão recebeu o serviço com êxito.

6. Clique em Fechar.

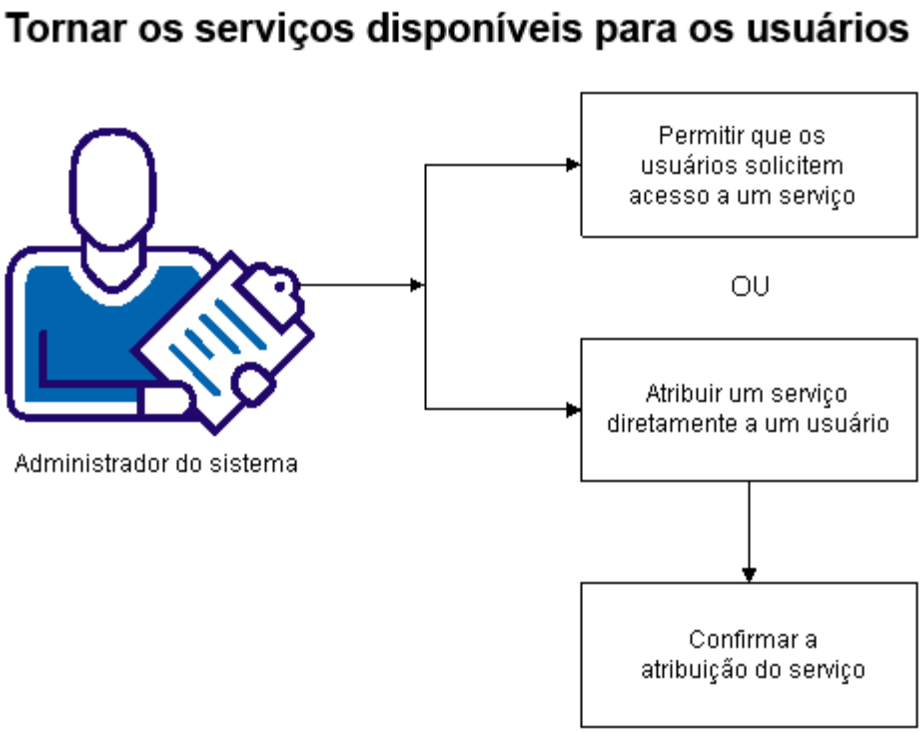
Disponibilizando serviços para os usuários

Os serviços simplificam o gerenciamento de direitos. Um serviço reúne todos os direitos que um usuário precisa para uma determinada função de negócios. Os serviços estão disponíveis ao usuário por meio de tarefas de solicitação de acesso no console de usuário. As tarefas de solicitação de acesso permitem que um usuário ou administrador solicite, atribua, revogue e renove um serviço na interface de usuário.

Os serviços permitem que um administrador do sistema combine as atividades e informações dos usuários - tarefas, funções, grupos e atributos - em um único pacote, para serem gerenciadas como um conjunto. Por exemplo, todos os novos funcionários de Vendas precisam acessar um conjunto de tarefas, contas em sistemas específicos do terminal e informações específicas adicionadas aos seus perfis de contas de usuários. Um administrador do sistema cria um serviço denominado Administração de vendas, que contém todas as informações necessárias de tarefas, funções, grupos e atributos de perfil para um novo funcionário de Vendas. Quando um administrador atribui o serviço Administração de vendas a um usuário, ele recebe o conjunto completo de funções, tarefas, grupos e atributos de conta que são definidos pelo serviço.

Os usuários também podem acessar serviços solicitando acesso por conta própria. No console de usuário, cada usuário tem uma lista de serviços disponíveis para sua solicitação. Essa lista é preenchida com os serviços marcados como Autoinscrição por um administrador do sistema com os privilégios apropriados, geralmente durante a criação do serviço. Na lista de serviços disponíveis, os usuários podem solicitar acesso aos serviços de que precisam. Quando o usuário solicita acesso a um serviço, a solicitação é processada automaticamente. As tarefas, funções, grupos e atributos associados são atribuídos ao usuário imediatamente. Um administrador do CA CloudMinder com os privilégios apropriados também pode configurar o processamento de serviço para exigir aprovação de fluxo de trabalho ou para gerar notificações por email.

O diagrama a seguir mostra as informações necessárias para compreender, e as etapas a serem executadas para disponibilizar os serviços para os usuários.



É possível disponibilizar os serviços para os usuários usando os seguintes métodos:

1. Permitir que os usuários solicitem acesso.

   No console de usuário do CA CloudMinder, quando o usuário clica em Meu acesso, Solicitar e exibir acesso, vê uma lista de serviços disponíveis para sua solicitação. Os serviços que aparecem nessa lista são aqueles marcados como Autoinscrição por um administrador do CA CloudMinder com os privilégios apropriados, geralmente durante a criação do serviço.

   Quando o usuário solicita acesso, o sistema atribui o serviço ao usuário. O usuário recebe todos os aplicativos, funções, grupos e atributos associados ao serviço. Se o serviço incluir uma Função inicial para um aplicativo, um ícone e um link para o aplicativo são exibidos na página inicial do console de usuário.

2. Atribuir um serviço diretamente a um usuário (na página 83).

3. Se você atribuir um serviço diretamente a um usuário, confirme a atribuição de serviço (na página 236).

Atribuir um serviço a um usuário

É possível atribuir um serviço diretamente a um usuário específico. Esse usuário se torna um *integrante* do serviço.

Siga estas etapas:

1. Vá até Serviços, Solicitar e Exibir acesso.

   Uma lista de serviços que você pode administrar é exibida.

2. Selecione o serviço que deseja atribuir a um usuário e clique em Selecionar.

   Uma lista de usuários que estão atribuídos ao serviço é exibida.

3. Clique em Solicitar acesso.

4. Procure um usuário ao qual deseja atribuir o serviço.

   Para exibir uma lista de todos os usuários sobre os quais você possui privilégios administrativos, clique em Pesquisar sem modificar os critérios de pesquisa.

5. Escolha um usuário e clique em Selecionar.

   Uma lista atualizada de usuários que estão atribuídos ao serviço é exibida.

6. Clique em Salvar alterações.

   O usuário recebe o serviço especificado. O usuário recebe todos os aplicativos, funções, grupos e atributos incluídos no serviço.

Confirmar atribuição de serviço

Após atribuir um serviço a um usuário, verifique se todas as tarefas associadas ao serviço foram concluídas com êxito.

Siga estas etapas:

1. Vá até Serviços, Exibir o histórico da solicitação de acesso ao serviço.

   Uma tela de pesquisa é exibida.

2. Pesquise o serviço atribuído a um usuário.

   Para exibir uma lista de todos os serviços sobre os quais você possui privilégios administrativos, clique em Pesquisar sem modificar os critérios de pesquisa.

   Uma lista de serviços que você pode administrar é exibida.

3. Selecione o serviço que você atribuiu e clique em Selecionar.

   Um histórico das ações associadas ao serviço é exibido.

4. Clique em Última alteração para ver as ações mais recentes primeiro.

5. Confirme se o usuário em questão recebeu o serviço com êxito.

6. Clique em Fechar.

Modificando um serviço

Como administrador do sistema, você pode modificar um serviço que você criou anteriormente. Por exemplo, você pode alterar os direitos que o serviço concede aos integrantes do serviço adicionando uma função ao serviço. Também é possível ajustar regras administrativas e de proprietário para o serviço, pré-requisitos de serviço e outros detalhes administrativos.

Se o CA CloudMinder tiver processado um serviço para um determinado usuário, todas as alterações feitas no serviço não serão propagadas para esse usuário. Se decidir modificar um serviço, os usuários que receberem o serviço antes da alteração terão os direitos originais. Os usuários que receberem o serviço após a alteração terão os direitos que o serviço modificado concede. Por exemplo, considere o seguinte cenário:

Como administrador do sistema, você cria um serviço Gerente de vendas que concede a função de Gerente de vendas e o grupo Vendas a integrantes do serviço. Os usuários solicitam o serviço Gerente de vendas, e o CA CloudMinder processa o serviço, concedendo a função e o grupo apropriados aos usuários. Você decide modificar o serviço Gerente de vendas para incluir a função de Gerente de funcionários. Nesse caso, os integrantes existentes do serviço não recebem a função de Gerente de funcionários. Apenas novos integrantes do serviço Gerente de vendas recebem a função de Gerente de funcionários, além da função de Gerente de vendas e o grupo Vendas.

Portanto, considere a modificação de um serviço apenas se o serviço não possuir integrantes. Ou seja, modifique um serviço apenas se nenhum usuário tiver solicitado e recebido o serviço, e se nenhum administrador tiver atribuído o serviço para um usuário.

É possível modificar informações administrativas, regras administrativas e de proprietário, pré-requisitos de serviço e direitos - tarefas, funções, grupos e atributos - do serviço.

Siga estas etapas:

1. Faça logon em uma conta do CA CloudMinder que possua privilégios de gerenciamento de serviços.

   Por exemplo, o primeiro usuário de um ambiente tem a função de Gerente do sistema, que tem a tarefa Alterar serviço.

2. No menu de navegação, selecione Tarefas, Serviços.
3. Clique em Gerenciar serviços e, em seguida, Alterar serviço.

   Uma tela de pesquisa é exibida.

4. Pesquise um serviço que deseja modificar.

   Para exibir uma lista de todos os serviços sobre os quais você possui privilégios administrativos, clique em Pesquisar sem modificar os critérios de pesquisa.

5. Escolha um serviço e clique em Selecionar.

   Uma mensagem de confirmação é exibida.

6. Clique em Sim.
7. Clique em Enviar.

   O CA CloudMinder aplica as alterações ao serviço.

Adicionar uma pesquisa para Solicitar e exibir acesso

A tarefa Solicitar e exibir acesso exibe uma lista de serviços; no entanto, não há campos para procurar mais serviços. Para adicionar um campo de pesquisa:

1. Selecione Funções e tarefas, Tarefa administrativa, Modificar tarefa administrativa.
2. Pesquisar por Solicitar e exibir acesso.
3. Selecione a tarefa na categoria Serviço.
4. Clique em Guias.
5. Na guia, clique no ícone de edição à esquerda de Gerenciar o acesso.
6. Clique em Procurar na linha da tela de lista.
7. Configurar a opção aplicável ao adicionar a pesquisa correta.
8. Selecione a tela necessária e clique no botão Editar para editar a tela.
9. Em Configurar, Tela da lista padrão, vá para a seção Selecione os campos em que um usuário pode pesquisar.
10. Selecione os campos de pesquisa e configure os nomes de campo de pesquisa.
11. Clique em OK para salvar as alterações.

Informações sobre a solicitação de serviço, como a Duração da solicitação de serviço e Dados de usuários, são exibidas no item do fluxo de trabalho de aprovação da Solicitação de serviço. Além disso, essas informações são enviadas por email se atribuir o fluxo de trabalho com base em diretiva AddServiceToUserEvent à tarefa Solicitar e exibir acesso.

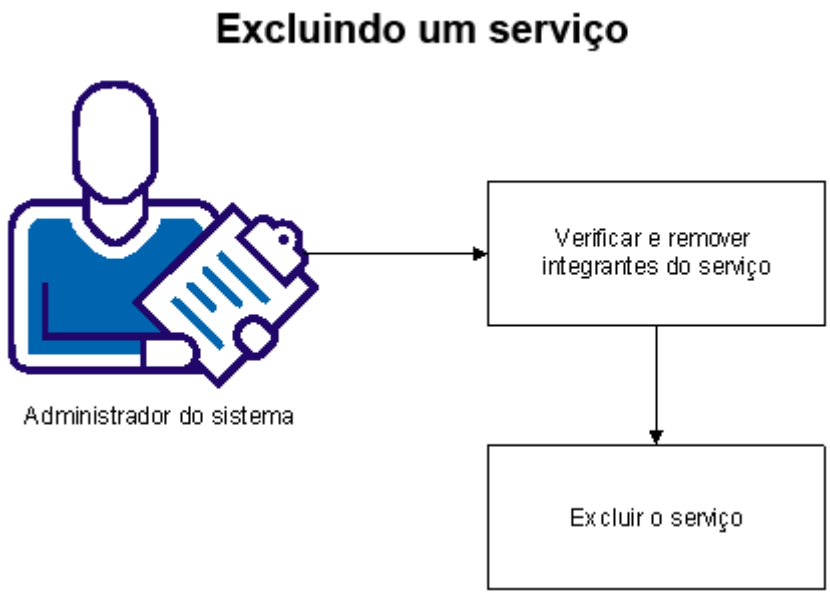
Excluindo um serviço

Como administrador do sistema, você pode excluir um serviço. Um serviço excluído é totalmente removido do sistema.

Se usuários forem atribuídos a um serviço, não será possível excluí-lo. Antes de excluir um serviço, primeiro verifique e remova todos os usuários atribuídos ou *integrantes*.

Observação: da mesma forma, se um usuário for integrante de um serviço, não será possível excluir o usuário. Primeiro, remova o usuário como integrante do serviço e, em seguida, exclua o usuário.

O diagrama a seguir mostra as informações necessárias para compreender, e as etapas a serem executadas para excluir um serviço.



Os tópicos a seguir explicam como excluir um serviço:

1. Verificar e remover integrantes do serviço (na página 240)
2. Excluir o serviço (na página 240)

Verificando e removendo integrantes do serviço

Antes de excluir um serviço, primeiro verifique e remova os integrantes existentes.

Siga estas etapas:

1. Faça logon em uma conta do CA CloudMinder que possua privilégios de gerenciamento de serviços.

   Por exemplo, o primeiro usuário de um ambiente tem a função de Gerente do sistema, que tem a tarefa Alterar serviço.

2. Selecione Tarefas, Serviços, Solicitar e exibir acesso.

   Uma lista de serviços que você pode administrar é exibida.

3. Selecione o serviço que deseja excluir e clique em Selecionar.

   Uma lista de usuários que estão atribuídos ao serviço é exibida.

4. Se o serviço possuir integrantes, desmarque as caixas de seleção ao lado de todos os usuários.

5. Clique em Salvar alterações.

   Uma mensagem de confirmação é exibida.

6. Clique em Sim.

   O CA CloudMinder remove os integrantes do serviço.

Excluindo um serviço

Você pode excluir um serviço que não possui integrantes do serviço.

Para excluir um serviço:

1. Faça logon no CA CloudMinder com uma conta que possua privilégios de gerenciamento de serviços.

   Por exemplo, o primeiro usuário de um ambiente tem a função de Gerente do sistema, que tem a tarefa Excluir serviço.

2. Vá até Serviços no painel esquerdo ou selecionando Tarefas.

3. Clique em Gerenciar serviços e, em seguida, em Excluir serviço.

   Uma tela de pesquisa é exibida.

4. Pesquise o serviço que deseja excluir.

   Para exibir uma lista de todos os serviços sobre os quais você possui privilégios administrativos, clique em Pesquisar sem modificar os critérios de pesquisa.

5. Escolha o serviço e clique em Selecionar.

   Uma mensagem de confirmação é exibida.

6. Clique em Sim.

   O serviço é excluído.

Renovando o acesso a um serviço

Alguns serviços expiram após um período determinado. Os administradores podem renovar um serviço para os usuários para evitar uma interrupção em seus acessos.

Você pode renovar um serviço usando um dos seguintes métodos:

- Selecione o serviço e, em seguida, selecione o acesso de usuário a renovar.
- Selecione o usuário e, em seguida, selecione o serviço que deseja renovar.

Observação: dependendo de como um ambiente foi configurado, os usuários finais também podem renovar seu acesso usando a tarefa Renovar o acesso.

O procedimento a seguir descreve como renovar o acesso selecionando o serviço primeiro. Se desejar selecionar o usuário primeiro, use as tarefas Solicitações de acesso do usuário e Gerenciar solicitações de renovação de usuário na categoria Usuários.

Siga estas etapas:

1. Clique em Serviços, Renovar o acesso, no console de usuário.
2. Procure e selecione o serviço que deseja renovar.

   O console de usuário exibe uma lista de usuários que têm acesso ao serviço selecionado, e a data em que o acesso expira.
3. Selecione a duração da renovação na coluna Solicitação de acesso e, em seguida, clique em OK.

   As opções do campo Duração são determinadas quando o serviço é criado.
4. Clique em Salvar alterações.

É possível exibir o status da renovação do serviço usando Exibir pesquisa de histórico de solicitações de acesso no console de usuário.

Capítulo 10: Sincronização

Esta seção contém os seguintes tópicos:

Sincronização de usuário entre servidores

Configure a sincronização no CA Identity Manager para ter certeza de que os usuários do diretório de provisionamento e repositório de usuários do CA Identity Manager possuem dados correspondentes. Para lidar com alterações no diretório ou no repositório de usuários, configure a sincronização de entrada e saída.

Sincronização de entrada

A *sincronização de entrada* mantém os usuários do CA Identity Manager atualizados com as alterações que ocorrem no diretório de provisionamento. As alterações no diretório de provisionamento incluem as que foram realizadas usando sistemas com conectores para o Servidor de provisionamento. A sincronização usa os mapeamentos definidos na tela Provisioning do Management Console.

Tolerância a falhas para sincronização de entrada

A tolerância a falhas em um URL do servidor alternativo do CA Identity Manager ocorrerá somente se o servidor de aplicativos apontado por um URL não estiver em execução. Se o servidor de aplicativos estiver em execução e aceitar a notificação, mas, em seguida, encontrar erros de configuração, como ambiente desconhecido ou de ambiente não iniciado, esses erros bloquearão a entrega das notificações. Esses problemas devem ser resolvidos para que as notificações de entrada funcionem corretamente.

Sincronização de saída

A *sincronização de saída* envolve o uso do CA Identity Manager na criação e atualização de usuários no diretório de provisionamento.

Criando usuários do diretório de provisionamento

A criação de usuários no diretório de provisionamento ocorre apenas para eventos relacionados ao provisionamento, como atribuição de uma função de provisionamento a um usuário. Um usuário é criado no diretório de provisionamento *apenas* quando você usa uma tarefa administrativa que atribui uma função para criar o usuário.

Observação: um usuário do Diretório de provisionamento também é chamado de usuário global. O usuário global é o único usuário que se conecta a contas de terminal.

Quando a criação de usuários no CA Identity Manager dispara a criação de usuários no diretório de provisionamento, o CA Identity Manager envia um email com uma senha temporária ao endereço de email do novo usuário, conforme definido no diretório de provisionamento. O usuário pode efetuar logon no Console de usuário com essa senha, no entanto, depois ele deverá alterá-la. Consequentemente, a senha é sincronizada entre o repositório de usuários e o diretório de provisionamento.

Se o usuário não tiver um endereço de email, ele não poderá acessar o Console de usuário enquanto não alterar a senha no repositório de usuários.

Observação: para enviar uma senha temporária por email, as notificações por email devem ser ativadas para o Ambiente e CreateProvisioningUserNotificationEvent deve ser configurado para notificação por email. (Consulte o *Guia de Configuração*.)

Atualizar usuários globais usando o CA Identity Manager

As atualizações para usuários no diretório de provisionamento ocorrem quando você usa uma tarefa administrativa que modifica os usuários. Se não existir nenhum usuário global, não ocorrerá nenhuma sincronização.

Os mapeamentos de saída correspondem aos eventos de usuário do CA Identity Manager para um evento de saída que afeta o diretório de provisionamento.

Identity Manager User Event	Outbound Event
☐ DeleteUserEvent	POST_DELETE_GLOBAL_USER
☐ DisableUserEvent	POST_DISABLE_GLOBAL_USER
☐ EnableUserEvent	POST_ENABLE_GLOBAL_USER
☐ ModifyUserEvent	POST_MODIFY_GLOBAL_USER
☐ ResetPasswordEvent	POST_CHANGE_GLOBAL_USER_PWD

Se um usuário existir no diretório de provisionamento, mas não no CA Identity Manager, você poderá criar esse usuário no Console de usuário. Se você mapeou atributos para a tarefa de criação e os usuários tiverem a mesma ID de usuário, os atributos para o usuário do provisionamento serão atualizados no diretório de provisionamento. Agora, você pode gerenciar esse usuário no Console de usuário.

Observação: se um evento atualizar os atributos do usuário e você desejar que os valores sejam sincronizados com o CA Identity Manager, será preciso mapear os eventos para o Event de saída: POST_MODIFY_GLOBAL_USER.

Excluir usuários globais usando o CA Identity Manager

Por padrão, a sincronização de saída é configurada para o evento Excluir usuário. Quando um usuário é excluído do CA Identity Manager, ele também é excluído do diretório de provisionamento e de todas as contas de terminal.

Se o CA Identity Manager não puder excluir uma conta de usuário em um terminal gerenciado, ele excluirá o usuário das contas restantes, mas não excluirá o usuário do diretório de provisionamento.

Por exemplo, suponha que o usuário A tenha uma conta do UNIX e uma conta do Exchange, que são gerenciadas no Servidor de provisionamento. Quando o usuário A é excluído do CA Identity Manager, o Servidor de provisionamento tentará excluir as contas de usuário. Se o Servidor de provisionamento não puder excluir a conta do Exchange devido a um erro de comunicação, ele excluirá a conta do UNIX do usuário A, mas não excluirá o usuário do diretório de provisionamento. No entanto, o usuário A não é restaurado no repositório de usuários.

Ativar sincronização de senhas

O Servidor de provisionamento permite a sincronização de senhas entre usuários do CA Identity Manager e as contas de usuário do terminal associadas. São necessárias duas configurações para ativar as alterações iniciadas pelo terminal:

- Os terminais devem ser configurados para capturar alterações iniciadas pelo terminal e encaminhá-las ao Servidor de provisionamento.
- O atributo Ativar agente sincronização de senhas deve ser ativado para o Usuário global.

Siga estas etapas:

1. No Management Console, escolha Advanced Settings, Provisioning.
2. Marque Enable Password Changes from Endpoint Accounts.
3. Clique em Salvar.
4. Reinicie o servidor de aplicativos.

Sincronizar usuários nas tarefas de criação ou modificação de usuário

Na guia do perfil de uma tarefa que cria ou modifica usuários, os controles de sincronização garantem que as alterações feitas no CA Identity Manager também sejam feitas no usuário global. Se você criar tarefas administrativas que criam ou modificam usuários e tiver Políticas de identidade, defina os controles de sincronização como se segue:

- Defina a Sincronização de usuário para Ao concluir a tarefa.
- Defina a Sincronização de conta para Ao concluir a tarefa.

Observação: para obter um melhor desempenho, selecione a opção Ao concluir a tarefa. No entanto, se você selecionar a opção Ao concluir a tarefa para uma tarefa que inclui vários eventos, o CA Identity Manager não será sincronizado até que todos os eventos da tarefa sejam concluídos. Se um ou mais desses eventos exigirem uma aprovação de fluxo de trabalho, esse procedimento pode levar vários dias. Para evitar que o CA Identity Manager aguarde para aplicar as políticas de identidade ou para sincronizar as contas até que todos os eventos estejam concluídos, selecione a opção Em cada evento.

Se você adicionar atributos às tarefas administrativas que gerenciam usuários, será preciso atualizar os Mapeamentos de atributos na tela Provisioning do Management Console. Para cada atributo de usuário no CA Identity Manager, existe um atributo de provisionamento padrão.

User Attribute	Provisioning Attribute
%ADMIN_ROLE_CONSTRAINT%	%ADMIN_ROLE_CONSTRAINT%
%EMAIL%	%EMAIL%
%ENABLED_STATE%	%ENABLED_STATE%
%FIRST_NAME%	%FIRST_NAME%
%FULL_NAME%	%FULL_NAME%
%IDENTITY_POLICY%	%IDENTITY_POLICY%
%LAST_NAME%	%LAST_NAME%
%PASSWORD%	%PASSWORD%
%PASSWORD_DATA%	%PASSWORD_DATA%
%USER_ID%	%USER_ID%

Tarefas de sincronização

É possível executar os seguintes tipos de sincronização:

Sincronização de usuário

Garante que cada usuário tenha as contas necessárias nos terminais gerenciados apropriados e que cada conta seja atribuída aos modelos de conta apropriados, conforme descrito pelas funções de provisionamento do usuário.

Sincronização de conta

Garante que os valores de atributo de recurso nas contas sejam os valores apropriados, conforme indicado pelos modelos de conta atribuídos pela conta. A sincronização de conta pode ser forte ou fraca. A sincronização fraca garante que os atributos de recurso das contas tenham pelo menos a capacidade mínima exigida pelos seus modelos de conta. A sincronização forte garante que os atributos de recurso da conta tenham a capacidade exata exigida pelos seus modelos de conta. A sincronização de conta será forte se a conta pertencer a pelo menos um modelo de conta cuja caixa de seleção Sincronização forte esteja marcada.

A caixa de seleção Nenhuma sincronização forte correspondente controla a Sincronização de usuário, mas existe um conceito semelhante. Quando você seleciona o item de menu Sincronizar usuário com funções em um usuário, são apresentadas duas opções de sincronização:

- Adicionar atribuições de modelo de conta e contas ausentes.
- Excluir atribuições de modelo de conta e contas extras.
- Ao marcar apenas a caixa de seleção Adicionar, que é semelhante à opção Weak Account Synchronization, você quer que os usuários globais tenham, no mínimo, todas as contas exigidas pelas funções de provisionamento atribuídas, mas permite que os usuários tenham contas adicionais não prescritas pelas funções de provisionamento atuais.

Marque as caixas de seleção Adicionar e Excluir, que é semelhante à opção Sincronização de conta forte, para que as funções de provisionamento definam exatamente quais contas o usuário deve ter. Todas as contas adicionais são excluídas.

Escolha Weak/Strong Account Synchronization ou Weak/Strong User Synchronization com base no grau de precisão em que as funções de provisionamento estão definidas. Se os usuários se enquadrarem nas funções de provisionamento definidas claramente, em que o acesso à conta está associado a essas funções, você deverá usar Sincronização forte.

Observação: alguns tipos de terminal definem a sincronização forte como o padrão. Para obter mais informações, consulte o *Guia de Conectores*.

A sincronização de usuário e a sincronização de conta são tarefas distintas que devem ser executadas individualmente. Normalmente, você executa a sincronização de usuário primeiro para garantir que todas as contas necessárias sejam criadas e executa a sincronização de conta posteriormente para que o Servidor de provisionamento atribua ou altere os valores dos atributos de conta.

O Servidor de provisionamento fornece dois conjuntos de opções de menu de sincronização para objetos:

- As opções de menu Verificar sincronização verificam a sincronização e retornam uma lista das contas que não estão em conformidade com as funções de provisionamento ou com os modelos de conta.
- As opções de menu Sincronizar sincronizam usuários globais com as respectivas funções de provisionamento ou contas com os respectivos modelos de conta.

Se você executar as funções de verificação de sincronização primeiro, o Servidor de provisionamento informará quais correções as funções de sincronização executarão. Se as funções de verificação de sincronização não encontrarem nenhum problema, as funções de sincronização não serão executadas.

Por que usuários ficam fora de sincronia

Veja a seguir alguns dos motivos pelos quais os usuários ficam fora de sincronia com suas funções de provisionamento ou modelos de conta:

- As tentativas anteriores de criar as contas necessárias falharam devido a problemas de software ou hardware na rede, resultando, assim, em contas ausentes.
- As funções de provisionamento e os modelos de conta podem ter sido alterados, criando, assim, contas extras ou ausentes.
- As contas foram atribuídas a modelos de conta depois que foram criadas. Desse modo, há contas que não foram sincronizadas com os respectivos modelos de conta.
- A criação de uma conta foi atrasada porque a conta foi especificada para ser criada posteriormente.
- Um novo terminal foi adquirido. Durante a exploração e correlação, o Servidor de provisionamento não atribui funções de provisionamento aos usuários automaticamente, de modo que você deve atualizar a função para indicar quais usuários devem ter contas no novo terminal. Qualquer conta que estava correlacionada a um usuário é listada como uma conta extra quando o usuário é sincronizado.
- Uma conta existente foi atribuída a um usuário pela cópia da conta para o usuário, executando, assim, uma correlação manual e estabelecendo uma conta extra.
- Uma conta foi criada para um usuário sem atribuir o usuário a uma função. Por exemplo, se você copiar um usuário em um modelo de conta que não esteja em nenhuma das funções de provisionamento do usuário, a conta será listada como uma conta extra ou como uma conta com um modelo de conta extra. Se você copiar o usuário em um terminal para criar uma conta usando o modelo de conta padrão do terminal, essa conta poderá ser uma conta extra.

Sincronização de usuário

A sincronização de usuário cria, atualiza ou exclui contas para que estejam em conformidade com a função de provisionamento atribuída a um usuário. Portanto, se os administradores adicionarem ou excluírem contas no terminal gerenciado usando ferramentas nativas, e você não tiver executado uma nova exploração recente do seu terminal para atualizar o diretório de provisionamento, a Sincronização de usuário poderá indicar que não há nenhum problema quando, na verdade, um usuário pode ter contas extras ou ausentes.

Sincronização de usuário com funções

É possível verificar a sincronização em usuários para listar contas extras ou modelos de conta, bem como contas que não estão presentes. Quando você solicita a sincronização do usuário com funções, o Servidor de provisionamento assegura que o usuário tenha todas as contas exigidas pelas funções de provisionamento da pessoa e que cada conta pertença aos modelos de conta corretos.

- Com essa tarefa, você pode marcar uma caixa de seleção para criar a conta no terminal. Se mais de um modelo de conta nas funções de provisionamento do usuário prescrever a mesma conta, esta será criada pela combinação de todos os modelos de conta relevantes.
- Durante a sincronização do usuário com funções, você tem a opção de excluir contas extras. Você pode determinar que os usuários tenham motivos legítimos para ter contas além daquelas exigidas pelas respectivas funções de provisionamento. Nesse caso, você não deve selecionar essa opção de exclusão.

  Se uma conta que estiver sendo excluída residir em um terminal gerenciado para o qual as exclusões de conta foram desativadas, a conta não será excluída de fato.

Criar contas

Uma vez que as funções de provisionamento contêm modelos de conta, e os modelos de conta são associados aos terminais, um usuário deve ter contas listadas em cada terminal com os atributos de conta corretos.

Com essa tarefa, você pode marcar uma caixa de seleção para criar a conta no terminal. Se mais de um modelo de conta nas funções de provisionamento do usuário prescrever a mesma conta, esta será criada pela combinação de todos os modelos de conta relevantes.

Essa conta é atribuída aos modelos de conta que, no momento, não estão sincronizados com a conta. A sincronização de conta não é necessária em contas recém-criadas.

Excluir contas

Durante a sincronização do usuário com funções, você tem a opção de excluir contas extras. Você pode determinar que os usuários tenham motivos legítimos para ter contas além daquelas exigidas pelas respectivas funções de provisionamento. Nesse caso, você não deve selecionar essa opção de exclusão.

Se uma conta que estiver sendo excluída residir em um terminal gerenciado para o qual as exclusões de conta foram desativadas, a conta não será excluída de fato.

Adicionar modelos de conta a contas

Se uma conta não possuir uma ou mais atribuições de modelo de conta, a sincronização de usuário com modelos de conta atribuirá uma conta existente a esses Modelos de conta. Quando uma conta é atribuída a um ou mais Modelos de conta novos, a sincronização de conta será executada automaticamente para atualizar os atributos de recurso da conta para recursos especificados pelo Modelos de conta.

Após atualização da conta a partir da sincronização de usuário com modelos de conta, a conta poderá ou não estar sincronizada com seus Modelos de conta. Se um dos Modelos de conta adicionado era um modelo de conta de sincronização forte ou se dois ou mais Modelos de conta foram adicionados a uma conta, a sincronização de usuário com funções iniciará uma sincronização de conta completa na conta. No entanto, se apenas um modelo de conta de sincronização fraca foi adicionado, a sincronização de usuário com sincronização de modelos de conta iniciará uma sincronização de conta envolvendo somente esse modelo de conta único. Se a conta anteriormente estava fora da sincronização de conta com seus outros Modelos de conta antes dessa atualização, posteriormente, ela poderá continuar fora da sincronização de conta.

Removendo modelos de conta de contas

A sincronização de usuário com funções também pode ser usada para remover modelos de conta extra de uma conta. Isso será feito apenas se você selecionar a opção de exclusão. Quando a sincronização de usuário determina que uma conta precisa ser atualizada para a remoção de um ou mais modelos de conta extra, a sincronização de conta é executada automaticamente na conta para sincronizar seus atributos de recurso com os modelos de conta restantes na conta.

Essa sincronização de conta que ocorre na remoção de modelos de conta de uma conta usará a sincronização forte se qualquer um dos modelos de conta restantes for marcado para sincronização forte e a sincronização fraca se todos os demais modelos de conta forem marcados para sincronização fraca.

Se as sincronizações fraca ou forte forem usadas, isso decidirá se os recursos da conta concedidos anteriormente quando um modelo de conta foi atribuído a uma conta serão retirados quando esse modelo de conta for removido posteriormente. Com a sincronização forte, um recurso concedido por um modelo de conta, como associação de grupo ou cota mais alta, será retirado (associação de grupo removida ou cota reduzida) se nenhum dos demais modelos de conta na conta prescrever esse recurso. Entretanto, com a sincronização fraca, normalmente, a conta não é alterada, pois o Servidor de provisionamento não faz diferença entre os recursos extras sob demanda e os recursos concedidos por meio de modelos de conta.

A exceção a essa regra é para determinados atributos de recurso de valor múltiplo designados como atributos SyncRemoveValues. Um atributo simples de valor múltiplo que representa um conjunto de valores atribuídos à conta (uma lista de associações de grupo, por exemplo), geralmente será listado como um atributo SyncRemoveValues. Para esses atributos, a ação de sincronização fraca que ocorre na remoção de um modelo de conta de uma conta removerá valores prescritos pelo modelo que está sendo removido, desde que esses valores não sejam prescritos por um dos modelos de conta restantes.

Por exemplo, se você criar modelos de conta em que cada um atribui uma associação de grupo exclusiva à sua conta, o recurso SyncRemoveValues significará que, quando você alterar uma função de provisionamento de um usuário global, de modo a não precisar mais de um determinado modelo de conta, a conta será atualizada para não pertencer mais ao grupo de prescrito por esse modelo de conta. Você observará que isso não é exatamente igual à sincronização forte, pois as associações de grupo fornecidas às contas além das prescritas aos modelos de conta são retidas.

Para todos os atributos de valor único e determinados atributos de valor múltiplo, que não sejam designados como atributos SyncRemoveValues, a ação de sincronização fraca na remoção de um modelo de conta de uma conta é igual a uma ação de sincronização fraca normal; isto é, os recursos nunca são removidos.

Se desejar que os recursos nunca sejam removidos pela sincronização fraca, desative o recurso SyncRemoveValues definindo o parâmetro de configuração de domínio Sincronizar/Remover valores do modelo de conta das contas como Não.

Sincronização de modelo de conta

As alterações que você fizer nos modelos de conta afetam as contas existentes da seguinte maneira:

- Se você alterar o valor de um atributo de recurso, o atributo de conta correspondente será atualizado, se necessário, para estar em sincronia com o valor de atributo do modelo de conta. Consulte a descrição de sincronização fraca e forte.
- Alguns atributos de conta são designados pelo conector como não sendo atualizados após alterações no modelo de conta. Exemplos disso são determinados atributos que o tipo de terminal só permite que sejam definidos durante a criação da conta e o atributo Senha.

Quais atributos são atualizados

Quando você altera os atributos de capacidade em um modelo de conta, o atributo correspondente nas contas é alterado. Essa alteração tem um impacto nos atributos da conta. O impacto tem como base os seguintes fatores:

- Se o modelo de conta está definido para usar sincronização fraca ou forte.
- Se a conta pertence a vários modelos de conta.

Sincronização fraca

A *sincronização fraca* garante que os usuários tenham o mínimo de atributos de capacidade para suas contas. A sincronização fraca é o padrão na maioria dos tipos de terminal. Se você atualizar um modelo que usa sincronização fraca, o CA Identity Manager atualizará os atributos de capacidade da seguinte maneira:

- Se um campo de número for atualizado em um modelo de conta e o número novo for maior do que o número na conta, o CA Identity Manager alterará o valor na conta para corresponder ao novo número.
- Se uma caixa de seleção não tiver sido marcada em um modelo de conta e você marcá-la depois, o CA Identity Manager atualizará a caixa de seleção em qualquer conta em que a caixa de seleção não estiver marcada.
- Se uma lista for alterada em um modelo de conta, o CA Identity Manager atualizará todas as contas para incluir qualquer valor da nova lista que não foi incluído na lista de valores da conta.

Se uma conta pertencer a outros modelos de conta (se esses modelos usarem sincronização fraca ou forte), o CA Identity Manager consultará apenas o modelo que está sendo alterado. Essa ação é mais eficiente do que a verificação de todos os modelos de conta. Como a sincronização fraca apenas adiciona capacidades às contas, geralmente não é necessário consultar os outros modelos de conta.

Observação: quando se propaga a partir de um modelo de conta de sincronização fraca, as alterações que poderiam remover ou reduzir as capacidades podem deixar algumas contas não sincronizadas. Lembre-se de que, com a sincronização fraca, as capacidades nunca são removidas ou reduzidas. Sem consultar outros modelos para uma conta, a propagação não considera se a sincronização fraca é suficiente.

Nessa situação, use Sincronizar usuários com modelos de conta para sincronizar a conta com seus modelos de conta.

Sincronização forte

A sincronização forte garante que as contas possuam exatamente os atributos de conta que são especificados no modelo de conta.

Por exemplo, suponhamos que você adicione um grupo a um modelo de conta do UNIX existente. Originalmente, o modelo de conta tornou as contas integrantes do grupo Equipe. Agora, você deseja tornar as contas integrantes dos grupos Equipe e Sistema. Todas as contas associadas ao modelo de conta são consideradas sincronizadas quando cada conta é integrante dos grupos Equipe e Sistema (e de nenhum outro grupo). Qualquer conta que não fizer parte do grupo Equipe é adicionada aos dois grupos.

Alguns outros fatores a serem considerados incluem as seguintes situações:

- Se o modelo de conta usar a sincronização forte, qualquer conta que pertencer a grupos que não sejam Equipe e Sistema será removida dos grupos adicionais.
- Se o modelo de conta usar a sincronização fraca, as contas serão adicionadas aos grupos Equipe e Sistema. Qualquer conta que tiver grupos adicionais que estiverem definidos para ela permanecerá um integrante desses grupos.

Observação: sincronize as contas com seus modelos regularmente para garantir que as contas permaneçam sincronizadas com seus modelos de conta.

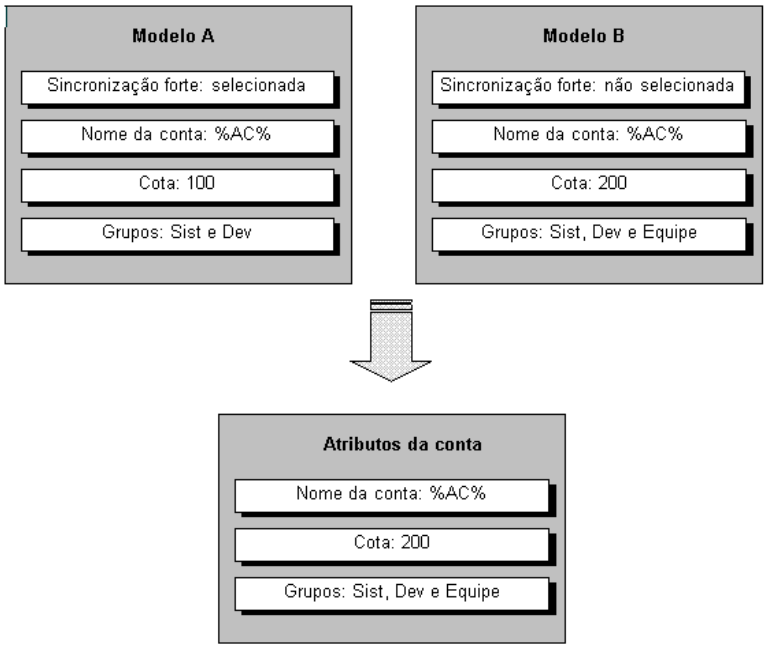
Contas com vários modelos

A sincronização depende também se a conta pertence a mais de um modelo de conta. Se a conta tiver apenas um modelo de conta e esse modelo usar a sincronização forte, cada atributo é atualizado para corresponder exatamente ao valor de atributo de modelo de conta. O resultado é o mesmo de quando o atributo for um atributo inicial.

Uma conta pode pertencer a vários modelos de conta, como seria o caso se um usuário pertencer a várias funções de provisionamento, cada uma delas com algum nível de acesso no mesmo terminal gerenciado. Quando isso acontecer, o CA Identity Manager combina esses modelos de conta em um modelo de conta em vigor que indica o superconjunto de recursos a partir dos modelos de conta. Esse modelo de conta é considerado para usar a sincronização fraca se todos os modelos de contas forem fracos, ou a sincronização forte se qualquer um dos modelos de conta for forte.

Observação: muitas vezes, você usa apenas a sincronização fraca ou apenas a sincronização forte para os modelos de conta que controlam uma conta, dependendo se as funções da empresa definem completamente os acessos que seus usuários precisam. Se os usuários não se encaixarem em funções claras e você precisar da flexibilidade para conceder recursos adicionais para as contas de usuário, use a sincronização fraca. Se for possível definir as funções para especificar exatamente os acessos que seus usuários precisam, use a sincronização forte.

O exemplo a seguir demonstra como vários modelos de conta são combinados em um único modelo de conta em vigor. Neste exemplo, um modelo de conta será marcado para sincronização fraca e o outro para sincronização forte. Portanto, o modelo de conta em vigor criado pela combinação dos dois modelos de conta será tratado como um modelo de conta de sincronização forte. O atributo inteiro Cota assume o maior valor dos dois modelos de conta, e o atributo Grupo com vários valores assume a união de valores das duas políticas.



Atributos somente para novas contas

Em um modelo de conta, determinados atributos são aplicados somente ao criar a conta. Por exemplo, o atributo Senha é uma expressão de regra, que define a senha para novas contas. Essa expressão de regra nunca atualiza a senha de uma conta. As alterações feitas na expressão de regra de senha só afetam as contas criadas após a definição da expressão de regra.

Da mesma forma, uma expressão de regra de modelo para um atributo da conta somente leitura afeta somente as contas criadas após a definição da expressão de regra. A alteração não terá efeito em contas existentes.

Sincronização de conta

A sincronização de conta atualiza os atributos de recurso para garantir que a conta tenha os recursos especificados pelos modelos de conta. Essa sincronização não afeta os atributos iniciais da conta.

Para sincronizar as alterações do atributo de recurso em um modelo de conta com suas contas, use uma das opções de menu de sincronização discutidas nesta seção.

Verificar sincronização de conta

É possível verificar a sincronização de conta para terminais e usuários. Essa ação retorna uma lista de contas que não estão de acordo com os modelos de conta. A tabela a seguir descreve o que acontece quando você verifica a sincronização de contas em cada objeto:

Objeto	Sincroniza
Terminal	Atributos de conta para cada conta em um terminal, além de garantir que estejam em conformidade com os modelos de conta associados.
Usuário global	Atributos de conta para cada uma das contas do usuário, além de garantir que estejam em conformidade com modelos de conta associados.

Sincronizar contas

Você pode executar a sincronização de conta em terminais, usuários e modelos de contas. A tabela a seguir lista os efeitos da sincronização de conta em cada objeto:

Objeto	Sincroniza
Terminal	Cada conta em um terminal com seus modelos de conta associados.
Usuário global	Cada conta de um usuário global com cada modelo de conta associado a ela.

Capítulo 11: Fluxo de trabalho

Esta seção contém os seguintes tópicos:

Visão geral do fluxo de trabalho

O recurso de fluxo de trabalho do CA Identity Manager permite que uma tarefa do CA Identity Manager seja controlada por um processo de fluxo de trabalho. Um *processo de fluxo de trabalho* é uma ou mais etapas que devem ser executadas antes que o CA Identity Manager possa concluir uma tarefa que está sob controle do fluxo de trabalho. Uma *tarefa* é uma instância de tempo de execução de um processo de fluxo de trabalho.

Interface de desenho do WorkPoint é um software da WorkPoint LLC, uma subsidiária da Planet Group, Inc., que é integrado ao CA Identity Manager. A Interface de desenho do WorkPoint permite gerenciar processos e tarefas de fluxo de trabalho.

Um processo de fluxo de trabalho é composto de uma ou mais etapas, chamadas de *atividades*, que devem ser executadas para realizar alguma tarefa comercial, como a criação ou modificação da conta de usuário de um funcionário. Em geral, um processo de fluxo de trabalho inclui uma ou mais atividades manuais que exigem um usuário autorizado, ou participante, para aprovar ou recusar a tarefa.

Um *participante* é uma pessoa que está autorizada a executar uma atividade de fluxo de trabalho. No CA Identity Manager, os participantes também são chamados de *aprovadores*, pois precisam aprovar ou recusar a tarefa no controle de fluxo de trabalho. Um *resolvedor participante* é uma regra ou conjunto de critérios para determinar quem são os participantes.

As atividades manuais individuais em um fluxo de trabalho são chamadas de *itens de trabalho* no CA Identity Manager.

Uma *lista de tarefas* é uma lista de tarefas de aprovação ou *itens de trabalho* gerada pelo fluxo de trabalho, que é exibida no console de usuário do participante autorizado a aprovar a tarefa.

Diagrama de processos do WorkPoint

Em geral, as tarefas do CA Identity Manager acionam eventos do CA Identity Manager. Por exemplo, para criar um usuário, um administrador seleciona uma tarefa Criar usuário. Quando essa tarefa é iniciada, o evento CreateUserEvent é acionado.

O diagrama a seguir é um exemplo de um processo de fluxo de trabalho simples (o processo predefinido CreateUserApproveProcess), conforme exibido na Interface de desenho do WorkPoint. Esse processo é chamado por um CreateUserEvent se a tarefa Criar usuário estiver sob controle do fluxo de trabalho.

O processo inclui uma atividade manual, Aprovar criação de usuário, que corresponde a uma tarefa de aprovação de fluxo de trabalho do CA Identity Manager com o mesmo nome. O participante deve aprovar ou recusar a tarefa de aprovação, geralmente clicando em um botão no console de usuário, antes que a tarefa sob controle do fluxo de trabalho possa ser executada até o fim.

Fluxo de trabalho e notificação por email

Ao iniciar uma tarefa, o CA Identity Manager a envia para processamento. Quando a tarefa é concluída, exibe uma mensagem de confirmação, da seguinte maneira:

```
Confirmação: Tarefa concluída.
```

No entanto, se a tarefa estiver sob controle do fluxo de trabalho e exigir aprovação, a mensagem será a seguinte:

```
Alerta: Tarefa pendente.
```

Além das mensagens na tela, o CA Identity Manager pode gerar notificações por email automaticamente quando:

- Um evento ou tarefa que exige aprovação ou recusa por um aprovador de fluxo de trabalho estiver pendente.
- Um aprovador aprovar um evento ou tarefa.
- Um aprovador recusar um evento ou tarefa.
- Um evento ou uma tarefa for concluída.

Mais informações:

Notificações por email (na página 353)

Documentação do WorkPoint

Para obter informações gerais sobre conceitos de fluxo de trabalho e encontrar instruções sobre processos de fluxo de trabalho, atividades e tarefas na Interface de desenho do WorkPoint, consulte a documentação do WorkPoint. Para isso, abra a seguinte página HTML:

ferramentas_administrativas\WorkPoint\docs\designer\default.htm

ferramentas_administrativas

Define o diretório de instalação das ferramentas administrativas do CA Identity Manager. O diretório de instalação padrão é:

- **Windows:** <caminho_de_instalação>\tools
- **UNIX:** <caminho_de_instalação2>/tools

Observação: o WorkPoint é um produto de terceiros instalado com o CA Identity Manager. O CA Identity Manager oferece suporte a um subconjunto de funcionalidades do WorkPoint. Por exemplo, o CA Identity Manager não oferece suporte ao WpConsole. No entanto, a documentação do WorkPoint descreve todas as funcionalidades do produto. Partes da documentação do WorkPoint não se aplicam a usuários do CA Identity Manager.

Métodos de controle do fluxo de trabalho

O CA Identity Manager fornece dois métodos para colocar tarefas sob controle do fluxo de trabalho.

Método de modelos

O CA Identity Manager inclui modelos de processo de fluxo de trabalho que podem ser usados para colocar tarefas sob controle do fluxo de trabalho. O *método de modelos* permite usar esses modelos para configurar e gerenciar o fluxo de trabalho totalmente a partir do console de usuário. Apresentados no CA Identity Manager r12, esses modelos de processo genéricos podem ser configurados para controlar a maioria das tarefas e eventos do CA Identity Manager.

O método de modelos possui os seguintes novos recursos:

- Controle de fluxo de trabalho em nível de tarefa e em nível de evento
- Configuração simplificada de resolvedor participante para aprovadores do fluxo de trabalho
- Delegação de item de trabalho, que abrange cenários de ausência temporária, permitindo que um usuário delegue outro usuário para aprovar itens de trabalho
- Reatribuição de item de trabalho, que permite que uma tarefa em execução seja reatribuída a outro usuário para aprovação

Método do WorkPoint

O CA Identity Manager também inclui um conjunto de processos de fluxo de trabalho predefinidos com mapeamentos de eventos padrão que correspondem a determinadas tarefas do CA Identity Manager. O *método do WorkPoint* exige que você configure e personalize esses processos na Interface de desenho do WorkPoint. Esses processos predefinidos são compatíveis com as releases anteriores ao CA Identity Manager r12.

O método do WorkPoint também possui os seguintes novos recursos:

- Controle de fluxo de trabalho em nível de tarefa e em nível de evento
- Delegação de item de trabalho, que abrange cenários de ausência temporária, permitindo que um usuário delegue outro usuário para aprovar itens de trabalho
- Reatribuição de item de trabalho, que permite que uma tarefa em execução seja reatribuída a outro usuário para aprovação

Observação: para obter mais flexibilidade e facilidade de uso, a CA recomenda usar o método de modelos sempre que possível.

Mais informações:

Usar o controle de fluxo de trabalho – método de modelos (na página 260)

Usar o controle de fluxo de trabalho – método de modelos

Apresentado no CA Identity Manager r12, o método de modelos permite configurar os modelos de processo de fluxo de trabalho no console de usuário sem precisar abrir a Interface de desenho do WorkPoint.

As vantagens do método de modelos são:

- Os modelos de processo com vários estágios podem lidar com a maioria das necessidades do fluxo de trabalho sem que seja preciso personalizar a Interface de desenho do WorkPoint.
- Os modelos oferecem suporte ao controle de fluxo de trabalho em nível de tarefa e em nível de evento.
- O mesmo modelo de processo de fluxo de trabalho pode ser configurado para uso com muitas tarefas diferentes ao mesmo tempo em que a criação do processo permanece inalterada.
- É possível especificar resolvedores participantes com facilidade no console de usuário.
- A delegação de item de trabalho pode ser executada no console de usuário.

Pré-requisito: ativar fluxo de trabalho

Você deve ativar o fluxo de trabalho antes de poder usá-lo para controlar as tarefas do CA Identity Manager. Por padrão, o fluxo de trabalho fica desativado.

Siga estas etapas:

1. No Management Console, selecione Ambiente.
2. Vá para Configurações avançadas, Fluxo de trabalho.
3. Marque a caixa de seleção Ativado e clique em Salvar.

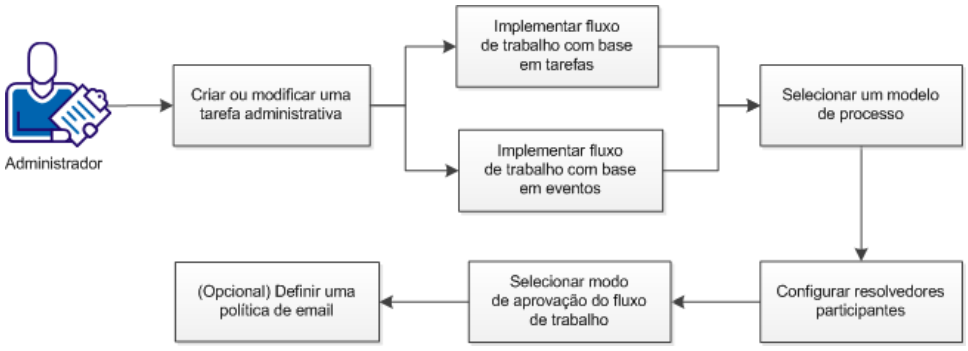
   Observação: os mapeamentos de eventos nessa tela serão aplicados somente se você usar o método do WorkPoint para configurar o fluxo de trabalho. Se você usar o método de modelos (recomendado), não mapeie os eventos para processos usando esse Management Console.
4. Reinicialize o servidor de aplicativos.
5. (Opcional) Configure as ferramentas administrativas do WorkPoint (na página 282).

Mais informações:

Mapear um processo para um evento globalmente (na página 289)
Métodos de controle do fluxo de trabalho (na página 259)

Colocar tarefas administrativas em controle de fluxo de trabalho – método de modelos

Como administrador, pode colocar tarefas administrativas em controle de fluxo de trabalho usando o método de modelos.



Siga estas etapas:

1. No console de usuário, selecione Funções e tarefas, Tarefa administrativa, Modificar (ou Criar) tarefa administrativa.
2. Pesquise a tarefa que desejada sob controle do fluxo de trabalho e clique em Selecionar.
3. Execute *uma* destas ações:
   - Implemente o fluxo de trabalho em nível de tarefa (na página 263) clicando no botão de edição Processo de fluxo de trabalho na guia Perfil.
   - Implemente o fluxo de trabalho em nível de evento (na página 266) selecionando um ou mais eventos na guia Eventos.
4. Selecione um modelo de processo (na página 269).
5. Configure os resolvedores participantes (na página 272).
6. Selecione o modo de aprovação de fluxo de trabalho.
7. (Opcional) Defina uma política de email para o processo de fluxo de trabalho (na página 278).

   Observação: se selecionar o processo EscalationApproval, um campo chamado Tempo limite da aprovação (min) será exibido. Esse campo é especificado em minutos e não pode ser deixado em branco. Por padrão, o tempo é definido como 60 minutos.

Após configurar o controle do fluxo de trabalho, um usuário com a função apropriada poderá executar a tarefa administrativa e o participante de fluxo de trabalho designado poderá aprovar ou rejeitar a tarefa ou o evento.

Fluxo de trabalho com base em tarefas ou eventos

O CA Identity Manager permite associar processos de fluxo de trabalho com tarefas ou eventos. Isso significa que os participantes podem aprovar ou recusar uma tarefa inteira do CA Identity Manager ou um evento específico dentro de uma tarefa.

Por exemplo, algumas tarefas do CA Identity Manager geram diversos eventos, e um aprovador pode precisar revisar todos os eventos antes de decidir aprovar ou recusar uma solicitação. Isso é possível no fluxo de trabalho em nível de tarefa. Quando um processo de fluxo de trabalho for associado a um evento específico dentro de uma tarefa, um aprovador não poderá ver o contexto geral da tarefa na qual uma solicitação é feita.

Fluxo de trabalho em nível de tarefa

O fluxo de trabalho em nível de tarefa permite que os aprovadores revisem todos os eventos antes de decidir aprovar ou recusar uma solicitação. O fluxo de trabalho em nível de tarefa ocorre antes que qualquer atividade da tarefa seja processada. Nenhum evento ou tarefa aninhada é executada antes do início da tarefa do processo de fluxo de trabalho.

Se o fluxo de trabalho em nível de tarefa for recusado, nenhuma parte da tarefa será executada.

Observação: uma tarefa configurada para controle de fluxo de trabalho em nível de tarefa também pode ser configurada para controle de fluxo de trabalho em nível de evento ao mesmo tempo. O controle de fluxo de trabalho em nível de evento simultâneo pode ser aplicado globalmente ou para uma tarefa específica.

Mais informações

Fluxo de trabalho em nível de evento (na página 266)
Processo global para mapeamento de eventos (na página 287)

Atributo do processo em nível de tarefa

Os processos de fluxo de trabalho que são compatíveis com o fluxo de trabalho em nível de tarefa possuem um atributo especial definido na Interface de desenho do WorkPoint. Esse atributo de dados do usuário em nível de processo, chamado TASK_LEVEL, está definido como verdadeiro por padrão nos seguintes modelos de processo:

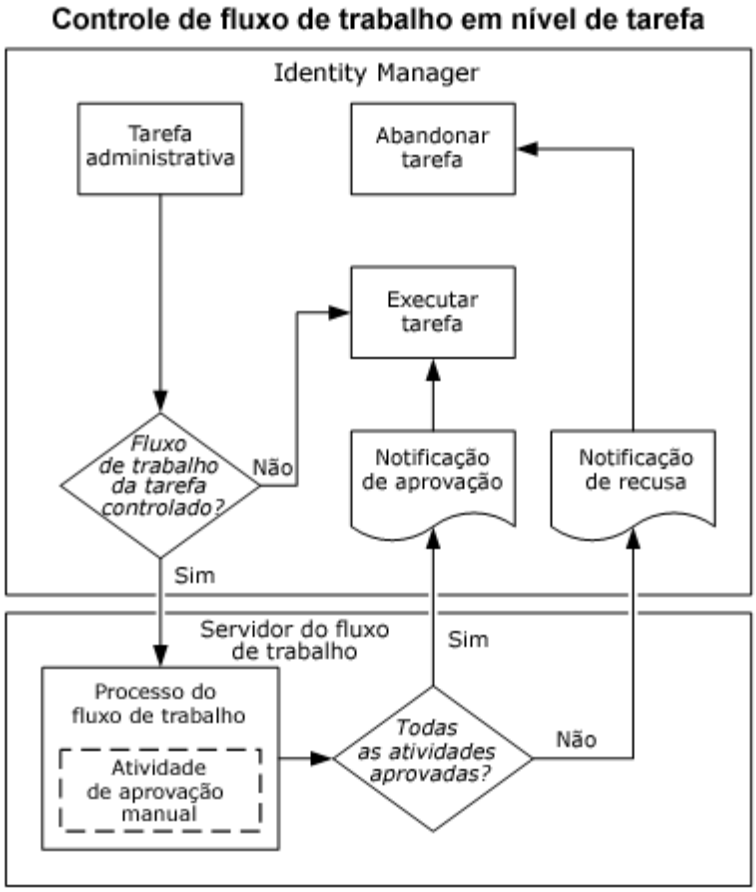
- SingleStepApproval
- TwoStageApprovalProcess
- EscalationApproval

Ao selecionar uma tarefa administrativa para o fluxo de trabalho em nível de tarefa, somente esses modelos de processo estão disponíveis.

Observação: embora TASK_LEVEL esteja definido como verdadeiro, os modelos de processo ainda podem ser usados para o fluxo de trabalho em nível de evento. Não altere esse valor do atributo TASK_LEVEL.

Diagrama de controle em nível de tarefa

O diagrama a seguir ilustra a interação entre o CA Identity Manager e o servidor de fluxo de trabalho quando um típico processo de fluxo de trabalho em nível de tarefa é iniciado:



Mais informações:

Diagrama de controle em nível de evento (na página 267)

Como configurar o fluxo de trabalho em nível de tarefa

O fluxo de trabalho em nível de tarefa ocorre antes que qualquer atividade da tarefa seja processada. Nenhum evento ou tarefa aninhada é executada antes do início da tarefa do processo de fluxo de trabalho.

Para configurar o fluxo de trabalho em nível de tarefa sem base em políticas:

1. No console de usuário, selecione Funções e tarefas, Tarefa administrativa, Modificar (ou Criar) tarefa administrativa.

   Uma tela Selecionar tarefa administrativa é exibida.

2. Pesquise a tarefa que desejada sob controle do fluxo de trabalho e clique em Selecionar.

   A tela Modificar (ou Criar) tarefa administrativa é exibida.

3. Na guia Perfil, verifique se Ativar fluxo de trabalho está marcada.

4. Na guia Perfil, clique no botão Processo de fluxo de trabalho.

   A guia Configuração do fluxo de trabalho em nível de tarefa é exibida.

5. Selecione um dos seguintes modelos de processo na lista Processo do fluxo de trabalho:

   - SingleStepApprovalProcess
   - TwoStageApprovalProcess
   - EscalationApprovalProcess

   A guia Configuração do fluxo de trabalho em nível de tarefa é expandida.

6. Configure resolvedores participantes, conforme necessário, pelo modelo de processo.

   As solicitações do participante são adicionadas ao processo.

7. Clique em OK.

   O CA Identity Manager salva a configuração do fluxo de trabalho em nível de tarefa.

8. Clique em Enviar.

   O CA Identity Manager processa a modificação da tarefa.

Observação: para configurar o fluxo de trabalho em nível de tarefa com base em políticas, consulte a seção Fluxo de trabalho com base em políticas (na página 314).

Fluxo de trabalho em nível de evento

É possível mapear um evento para um processo de fluxo de trabalho. Quando um evento mapeado para um processo de fluxo de trabalho é acionado, o processo de fluxo de trabalho é iniciado. A tarefa que acionou o evento é colocado em um estado pendente e considerado sob controle do fluxo de trabalho.

Um processo de fluxo de trabalho pode exigir que um participante aprove ou recuse um evento ou uma tarefa antes que o processo possa ser concluído. Uma tarefa que exige aprovação de fluxo de trabalho manual por um participante demora mais tempo para ser concluída do que uma tarefa que não está sob controle do fluxo de trabalho.

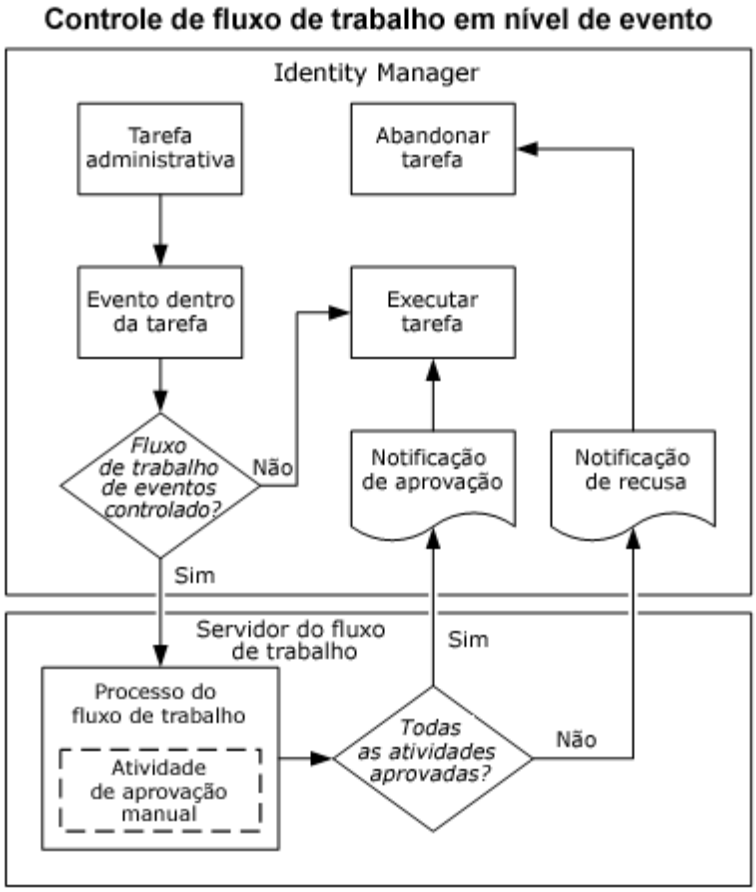
Depois que todas as atividades em um processo de fluxo de trabalho tiverem sido realizadas, o evento mapeado para o processo de fluxo de trabalho será liberado do controle do fluxo de trabalho. Quando todos os eventos acionados por uma determinada tarefa forem liberados do controle do fluxo de trabalho, a tarefa controlada pelo fluxo de trabalho estará concluída.

Enquanto a tarefa estiver sob controle do fluxo de trabalho, o conteúdo das telas de tarefas será salvo no banco de dados de persistência de tarefas. O estado da tarefa de fluxo de trabalho (dados relevantes para o fluxo de trabalho) é armazenado no banco de dados do WorkPoint.

Observação: a guia Eventos exibe os eventos gerados por cada guia em uma tarefa. Depois de adicionar uma nova guia a uma tarefa, você deve enviar e, em seguida, abrir novamente a tarefa usando Modificar tarefa administrativa para que os novos eventos sejam exibidos na guia Eventos.

Diagrama de controle em nível de evento

O diagrama a seguir ilustra a interação entre o CA Identity Manager e o servidor de fluxo de trabalho quando um típico processo de fluxo de trabalho em nível de evento é iniciado:



Mais informações:

Diagrama de controle em nível de tarefa (na página 264)

Como configurar o fluxo de trabalho em nível de evento

O fluxo de trabalho em nível de evento é iniciado quando um evento mapeado para um processo de fluxo de trabalho é acionado. A tarefa que acionou o evento é colocada em um estado pendente até que o participante aprove ou recuse a tarefa.

Para configurar o fluxo de trabalho em nível de evento sem base em políticas:

1. No console de usuário, selecione Funções e tarefas, Tarefa administrativa, Modificar (ou Criar) tarefa administrativa.

   Uma tela Selecionar tarefa administrativa é exibida.

2. Pesquise a tarefa que desejada sob controle do fluxo de trabalho e clique em Selecionar.

   A tela Modificar (ou Criar) tarefa administrativa é exibida.

3. Na guia Perfil, verifique se Ativar fluxo de trabalho está marcada.

4. Na guia Eventos, selecione um evento para mapear para um modelo de processo.

   A tela de mapeamento do fluxo de trabalho é exibida.

5. Selecione um dos seguintes modelos de processo na lista Processo do fluxo de trabalho:

   - SingleStepApproval
   - TwoStageApprovalProcess
   - EscalationApprovalProcess

   A tela de mapeamento do fluxo de trabalho é expandida.

6. Configure resolvedores participantes, conforme necessário, pelo modelo de processo.

   As solicitações do participante são adicionadas ao processo.

7. Clique em OK.

   O CA Identity Manager salva a configuração do fluxo de trabalho em nível de evento.

8. Repita as etapas de 3 a 6 para cada evento que deseja sob controle do fluxo de trabalho.

9. Clique em Enviar.

   O CA Identity Manager processa a modificação da tarefa.

Para configurar o fluxo de trabalho em nível de evento com base em políticas, consulte a seção Fluxo de trabalho com base em políticas (na página 314).

Observação: a lista Processo do fluxo de trabalho inclui os processos para uso com o método do modelo e o método do WorkPoint:

- Quando um processo do método do modelo é selecionado (SingleStepApproval, TwoStageApprovalProcess ou EscalationApproval), a página expande para ativar a configuração de resolvedor participante.
- Quando um processo do método do WorkPoint é selecionado, a página não é expandida. Resolvedores participantes são configurados na Interface de desenho do WorkPoint.

Tipos de modelos de processo

Um modelo de processo de fluxo de trabalho apresenta as seguintes características:

- Definido na Interface de desenho do WorkPoint.
- Possui atividades manuais, que correspondem às tarefas de aprovação do CA Identity Manager.
- Inclui atributos especiais que contêm informações para identificar os participantes (também chamados de aprovadores).

Os modelos de processo de fluxo de trabalho não incluem informações para selecionar participantes específicos. Essa função é fornecida pelo CA Identity Manager depois que um usuário configura um fluxo de trabalho e seus resolvedores participantes. Essas informações são mapeadas para um evento para controle de fluxo de trabalho em nível de evento e para uma tarefa para controle de fluxo de trabalho em nível de tarefa.

Ao usar o modelo de fluxo de trabalho, todas as configurações de fluxo de trabalho e participantes são feitas no console de usuário.

Há três modelos de processo para uso com o método de modelos:

- SingleStepApprovalProcess
- TwoStageApprovalProcess
- EscalationApprovalProcess

Como funciona um modelo de processo

Um modelo de processo de fluxo de trabalho contém um número de locais nos quais solicita listas de participantes. Quando o modelo for mapeado para uma tarefa ou um evento do CA Identity Manager, configure resolvedores participantes dessas listas.

Em tempo de execução, conforme mostrado na figura a seguir, o CA Identity Manager fornece as listas de participantes para o processo de fluxo de trabalho com base em suas informações configuradas:

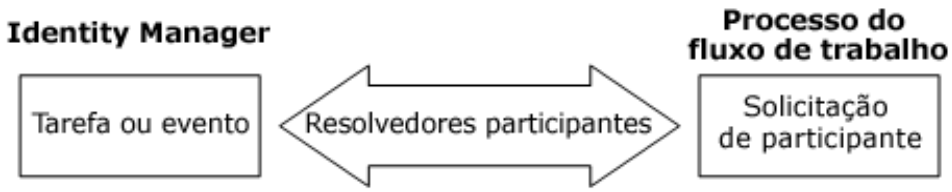


Diagrama de modelo de estágio único

O diagrama a seguir ilustra o modelo de processo SingleStageApproval, conforme exibido na Interface de desenho do WorkPoint. O modelo de processo inclui duas atividades manuais:

- Um nó de aprovação para o participante principal. Se esse usuário aprovar ou recusar a solicitação, o processo será executado até o fim.
- Um nó de aprovação para um participante padrão. Esse usuário pode aprovar ou recusar a solicitação se o participante principal não for encontrado.

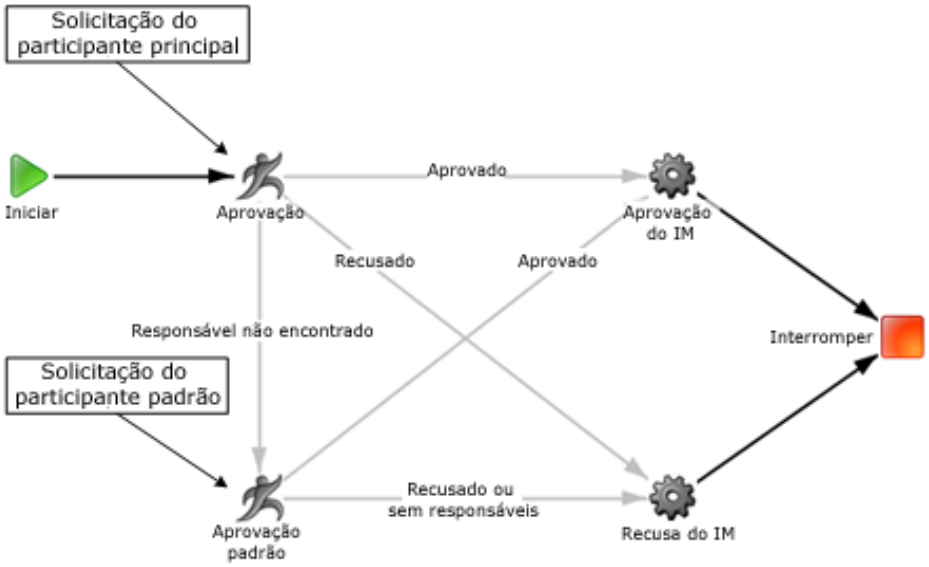


Diagrama de modelo de dois estágios

O diagrama a seguir ilustra o modelo de processo TwoStageApproval, conforme exibido na Interface de desenho do WorkPoint. O modelo de processo TwoStageApproval inclui três atividades manuais:

- Um nó de aprovação para o participante corporativo. Se esse usuário aprovar a solicitação, o processo seguirá para o aprovador técnico; se esse usuário recusar a solicitação, o processo será executado até o fim.
- Um nó de aprovação para o participante técnico. Se esse usuário aprovar ou recusar a solicitação, o processo será executado até o fim.
- Um nó de aprovação para um participante padrão. Esse usuário pode aprovar ou recusar a solicitação se o participante corporativo ou técnico não for encontrado.

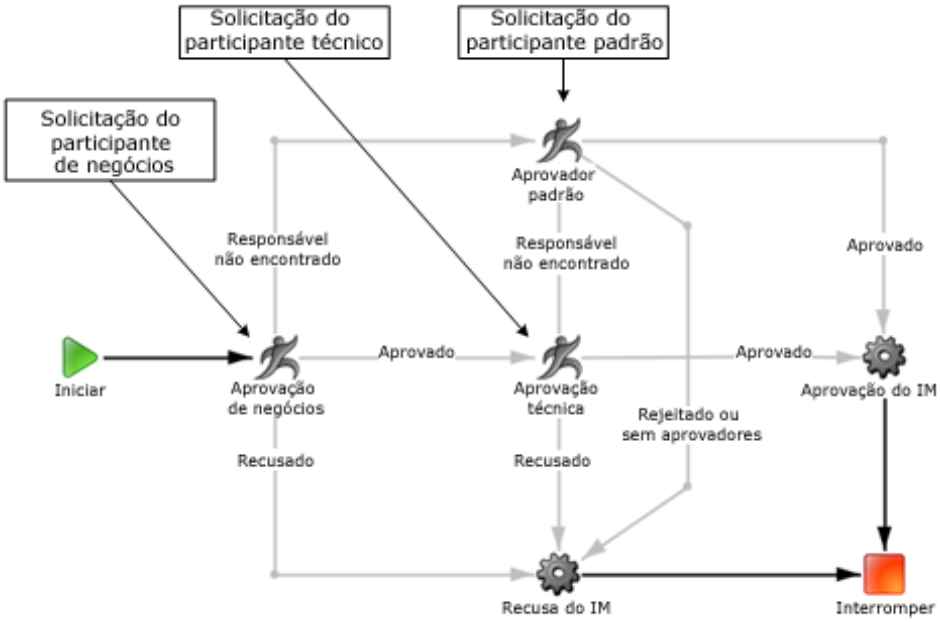
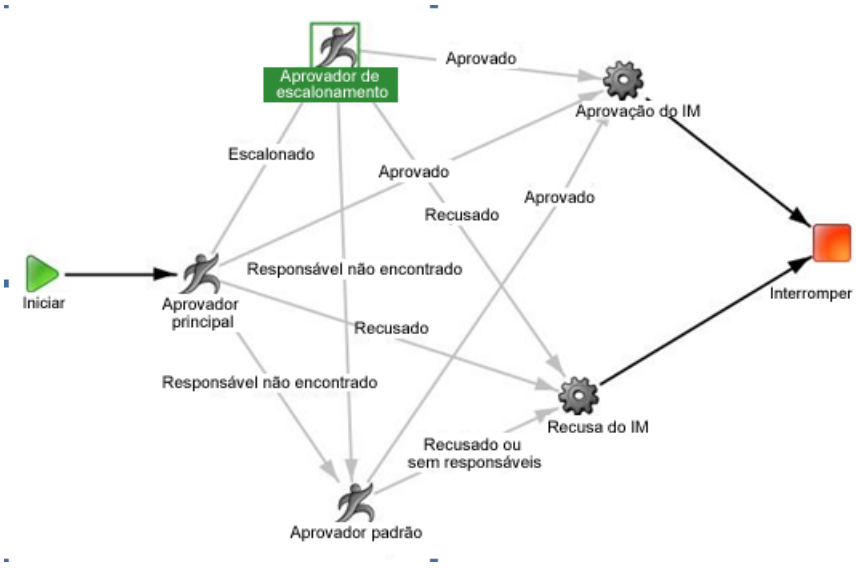


Diagrama de modelo de aprovação de escalonamento

O diagrama a seguir ilustra o modelo de processo EscalationApproval, conforme exibido na Interface de desenho do WorkPoint. O modelo de processo inclui as seguintes atividades manuais:

- Um nó de aprovação para o participante principal. Se esse usuário aprovar ou recusar a solicitação, o processo será executado até o fim.
- Um nó de aprovação para um participante padrão. Esse usuário pode aprovar ou recusar a solicitação se o participante principal não for encontrado.

- Um nó de aprovação com transição determinada do aprovador principal para o aprovador do escalonamento. Esse usuário pode aprovar ou recusar a solicitação se o participante principal não for encontrado, mas não responde no período de tempo limite configurado.



Observação: para adicionar a opção de tempo limite a um processo existente, adicione o campo de dados do usuário PARTICIPANT_TIMEOUT ao nó de atividade e adicione Transição escalonada ao nó no qual precisa que o item de trabalho seja escalonado.

Usando o modelo de aprovação de escalonamento

Para usar o modelo de aprovação de escalonamento, importe o arquivo ZIP a seguir na atualização de r12.5 para 12.6.5:
`12.5to12,5SPUpgradeWFScripts.zip`

O arquivo ZIP está localizado nos seguintes diretórios padrão:

- Windows: <caminho_de_instalação>\tools\WorkflowScripts
- UNIX: <caminho_de_instalação2>/tools/WorkflowScripts

Tipos de resolvedor participante

Para o método de modelos, há sete tipos de resolvedor participante:

Integrantes da função da tarefa de aprovação

Especifica que os participantes são integrantes das funções que concedem acesso para a tarefa de aprovação.

Lista de usuários

Especifica que os participantes são uma lista especificada de usuários.

Integrantes do grupo

Especifica que os participantes são integrantes de uma lista de grupos especificada.

Integrantes com a função administrativa

Especifica que os participantes são integrantes de uma lista de funções administrativas especificada.

Integrantes da tarefa administrativa

Especifica que os participantes são integrantes de funções administrativas associadas a uma lista especificada de tarefas administrativas.

Resolvedor dinâmico

Especifica que os participantes são selecionados dinamicamente dependendo da tarefa ou do evento que está sendo aprovado.

Resolvedor nulo

Determina uma lista nula sem usuários.

Personalizado

Especifica que os participantes são determinados por um resolvedor participante personalizado.

Resolvedor do proprietário do negócio

Especifica a lista de participantes configurada na Regra de catálogo, como Proprietários de negócios de uma entidade.

Resolvedor do proprietário administrador

Especifica a lista de participantes configurada na Regra de catálogo, como Proprietários administradores de uma entidade.

Resolvedor gerente

Especifica o participante que será definido como gerente do objeto de usuário.

Integrantes da função da tarefa de aprovação

Esse resolvedor atribui a atividade para todos os integrantes de todas as funções do CA Identity Manager que concedem acesso à tarefa de aprovação. Esse resolvedor não exige configurações adicionais.

Lista de usuários

Esse resolvedor atribui o item de trabalho para uma lista de usuários especificada.

A definição de escopo não é aplicada. Qualquer usuário pode ser adicionado ou removido da lista por qualquer pessoa que tenha acesso à tela de configuração do fluxo de trabalho.

Esse resolvedor tem as seguintes regras de validação:

- Pelo menos um nome de usuário deve ser fornecido.
- Os nomes devem ser de usuários existentes no momento.

Integrantes do grupo

Esse resolvedor atribui o item de trabalho a todos os integrantes de todos os grupos especificados na lista de grupos.

A avaliação de quem são os integrantes do grupo é realizada no momento em que o item de trabalho é criado, e não na hora em que o resolvedor participante é especificado.

A definição de escopo não é aplicada. Qualquer grupo pode ser adicionado ou removido da lista por qualquer pessoa que tenha acesso à tela de configuração do fluxo de trabalho.

Esse resolvedor tem as seguintes regras de validação:

- Pelo menos um grupo deve ser especificado
- Os nomes devem ser de grupos existentes no momento

Integrantes com a função administrativa

Esse resolvedor atribui o item de trabalho a todos os integrantes das funções administrativas especificadas na lista de funções administrativas.

A avaliação de quem são os integrantes da função é realizada no momento em que o item de trabalho é criado, e não na hora em que o resolvedor participante é especificado.

A definição de escopo não é aplicada. Qualquer função pode ser adicionada ou removida da lista por qualquer pessoa que tenha acesso à tela de configuração do fluxo de trabalho.

Esse resolvedor tem as seguintes regras de validação:

- Pelo menos uma função administrativa deve ser especificada.
- Os nomes devem ser de funções administrativas existentes no momento.

Integrantes da tarefa administrativa

Esse resolvedor atribui o item de trabalho a todos os integrantes de todas funções administrativas associadas às tarefas administrativas especificadas na lista de tarefas administrativas.

A definição de escopo não é aplicada. Qualquer tarefa pode ser adicionada ou removida da lista por qualquer pessoa que tenha acesso à tela de configuração do fluxo de trabalho.

A avaliação de quem são os integrantes da função e que funções estão presentes nas tarefas é realizada no momento em que o item de trabalho é criado, e não na hora em que o resolvedor participante é especificado.

Esse resolvedor tem as seguintes regras de validação:

- Pelo menos uma tarefa administrativa deve ser especificada.
- Os nomes devem ser de tarefas administrativas existentes no momento.

Resolvedor dinâmico

Esse resolvedor retorna uma lista de usuários de acordo com uma regra dinâmica determinada em tempo de execução. Use a caixa de seleção a seguir para definir as restrições de regras dinâmicas:

Aprovadores

Especifica o tipo de usuário para aprovar essa tarefa.

Observação: mostra apenas os objetos que podem conter usuários (ou aprovadores).

Usuário ou objeto

Especifica o usuário ou objeto onde os aprovadores podem ser encontrados.

- Objeto associado ao evento — O evento sob controle do fluxo de trabalho.
- Iniciador desta tarefa — O usuário que iniciou a tarefa administrativa.
- Objeto principal desta tarefa — O objeto que está sendo criado ou modificado pela tarefa.
- Aprovador anterior desta tarefa — Os aprovadores anteriores desta tarefa.

Usuário associado a esta conta

Atualiza o campo de atributos Usuário ou objeto para listar os atributos do usuário do CA Identity Manager, em vez de atributos da conta do terminal. O resolvedor trabalha com os atributos em nível de usuário do CA Identity Manager. Essa caixa de seleção é aplicável quando você seleciona um objeto de conta do terminal, como uma conta do Active Directory.

Atributo

Especifica o atributo que contém os aprovadores.

Observação: a lista de atributos é classificada em ordem alfabética e contém uma lista de nomes de exibição exclusivos. Os atributos estendidos são excluídos da lista.

Tipo de objeto de evento

Especifica o tipo de objeto do evento.

Observação: exibido apenas se "Objeto associado ao evento" estiver selecionado.

Observação: a opção Resolvedor dinâmico com Criar grupo exige a existência do objeto. As informações de associação ao grupo/administradores podem ser usadas com resolvedores de atributo de correspondência/dinâmico somente para grupos existentes.

O Resolvedor dinâmico foi aprimorado para adicionar o aprovador anterior à lista de objetos suportados. Se as informações do gerenciador de hospedagem de atributos físicos forem selecionadas, a configuração enviará a aprovação a um gerenciador.

Para configurar o resolvedor para Aprovação do gerente:

- Definir aprovadores para usuários
- Selecione Aprovador anterior desta tarefa na lista suspensa Usuário ou objeto
- Defina o atributo para o atributo físico que contém as informações do gerenciador

Resolvedor de atributo de correspondência

Esse resolvedor trabalha apenas em objetos do tipo Usuário. Um valor de qualquer objeto disponível é comparado a um campo no objeto de usuário. Use a caixa de seleção a seguir para definir as restrições de regra de atributo de correspondência:

Aprovadores

Especifica o tipo de usuário para aprovar essa tarefa.

Usuário ou objeto

Especifica o valor que os aprovadores terão no atributo selecionado abaixo.

Observação: o valor recuperado do usuário ou objeto deve ser um valor aceitável para uma pesquisa de usuário no atributo selecionado.

- Objeto associado ao evento — O evento sob controle do fluxo de trabalho.
- Iniciador desta tarefa — O usuário que iniciou a tarefa administrativa.
- Objeto principal desta tarefa — O objeto que está sendo criado ou modificado pela tarefa. (Esta opção só estará disponível para mapeamento do evento em nível de tarefa.)
- Aprovador anterior desta tarefa — Os aprovadores anteriores desta tarefa.

Usuário associado a esta conta

Atualiza o campo de atributos Usuário ou objeto para listar os atributos do usuário do CA Identity Manager, em vez de atributos da conta do terminal. O resolvedor trabalha com os atributos em nível de usuário do CA Identity Manager. Essa caixa de seleção é aplicável quando você seleciona um objeto de conta do terminal, como uma conta do Active Directory.

Atributo de usuário ou objeto

Especifica o atributo que contém o valor a ser usado na pesquisa de aprovadores.

Atributo de pesquisa de aprovador

Especifica o atributo a ser usado na pesquisa para correspondência com o valor identificado acima.

Observação: ao definir a tarefa Aprovar criação de usuário como um Resolvedor de atributo de correspondência que funciona em Usuários, Resolvedor participante, será necessário alterar a assinatura do método para o script imApprovers na interface de desenho do WorkPoint para apontar para o nome exclusivo de TwoStageProcessDefinition.

Resolvedor nulo

O resolvedor nulo não retorna usuários. Dependendo de como o processo de fluxo de trabalho foi criado, talvez o processo ignore completamente a aprovação. O resolvedor nulo não exige nenhuma configuração adicional.

Resolvedor participante personalizado

O resolvedor participante personalizado é um objeto Java que determina os participantes da atividade de fluxo de trabalho e retorna uma lista no CA Identity Manager, que, em seguida, passa a lista para o mecanismo de fluxo de trabalho. Normalmente, você deve criar um resolvedor participante personalizado somente se as políticas de participante padrão não puderem fornecer a lista de participantes que uma atividade exige.

Observação: você cria um resolvedor participante personalizado usando a API de resolvedor participante. Para obter mais informações, consulte o *Guia de Programação do Java*.

Definir uma política de email para um processo do fluxo de trabalho

É possível especificar uma política de email para cada etapa do processo de fluxo de trabalho. De acordo com a política de email definida, um email é enviado quando um processo atinge uma etapa ou atividade correspondente. Para notificações por email relacionadas ao processo de fluxo de trabalho, é possível selecionar apenas *Quando enviar* do tipo *Email pendente do fluxo de trabalho*.

Observação: para obter mais informações sobre as políticas de email, consulte Como criar políticas de notificação por email.

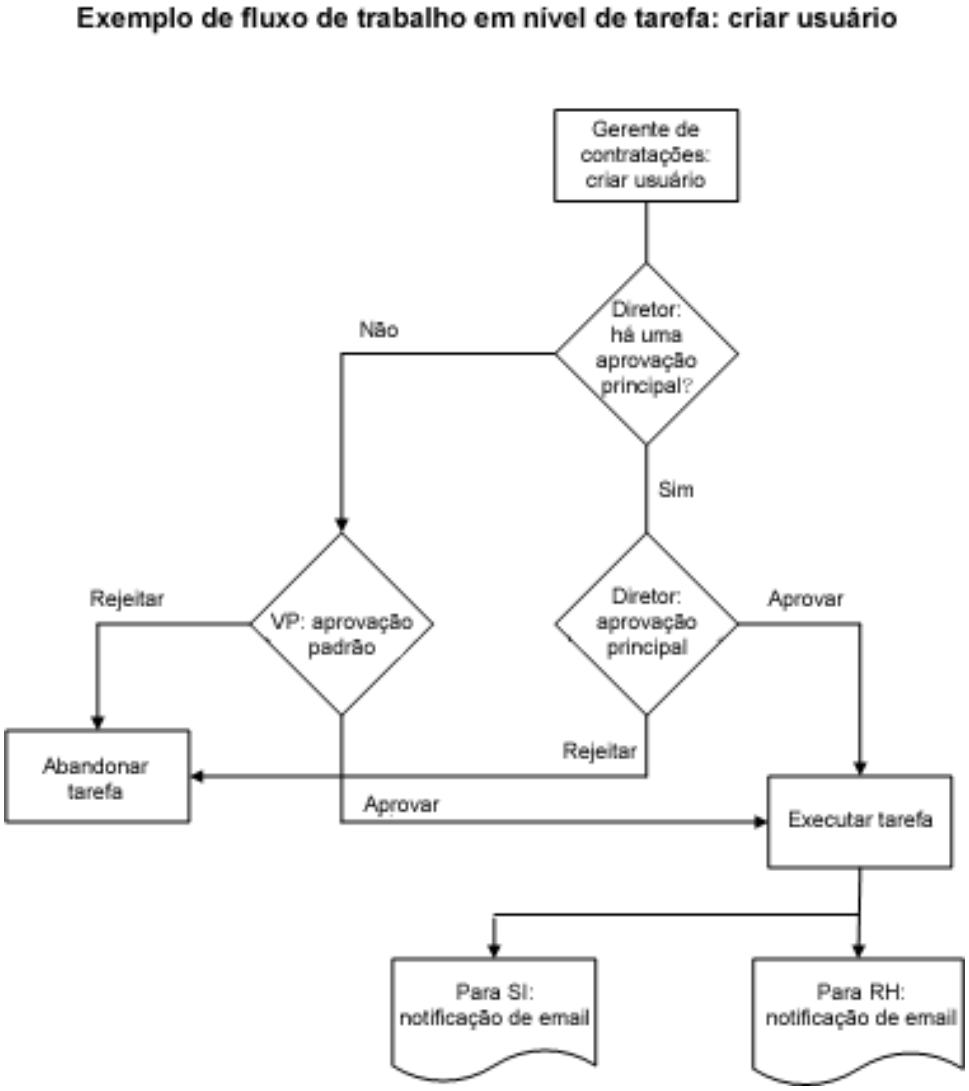
Exemplo de fluxo de trabalho: Criar usuário

O administrador do CA Identity Manager de uma empresa precisa definir um fluxo de trabalho e funções de usuário para lidar com o cenário a seguir:

- O Gerente de vendas da empresa contrata um Representante de vendas. O Gerente de vendas deve conseguir criar um usuário do CA Identity Manager para a nova contratação.
- Para simplificar o processo de contratação, os participantes desejam executar apenas um único item de trabalho para aprovar (ou recusar) a tarefa.
- O Diretor de vendas deve ser o aprovador principal para todos os novos contratados. Se o Diretor de vendas não for encontrado, o VP de vendas deve ser o aprovador padrão.
- Se a nova contratação for aprovada, o CA Identity Manager deverá enviar notificações por email de novo usuário para os departamentos de Recursos Humanos (RH) e Serviços de Informações (IS).

Diagrama de controle de Criar usuário

O diagrama a seguir ilustra o fluxo lógico para o cenário de criação de usuário:



Implementação de exemplo de fluxo de trabalho

Para implementar esse cenário de exemplo, o administrador deve executar as seguintes tarefas:

- Certifique-se de que o iniciador de tarefas seja um integrante da função administrativa exigida.

  O Gerente de vendas deve ser um integrante da função administrativa de Gerenciador de usuários. Essa função fornece ao Gerente de vendas a autoridade necessária para iniciar a tarefa administrativa Criar usuário para o novo Representante de vendas contratado.

- Ative o fluxo de trabalho em nível de tarefa para a tarefa administrativa Criar usuário.

  Os fluxo de trabalho em nível de tarefa garante que apenas um item de trabalho é gerado para concluir a tarefa Criar usuário. Como existem vários eventos individuais associados à tarefa Criar usuário, o fluxo de trabalho em nível de evento geraria vários itens de trabalho e também seria mais difícil de configurar.

- Configure os resolvedores participantes.

  O número de possíveis resolvedores participantes é determinado pelo modelo de processo de fluxo de trabalho selecionado. O modelo SingleStageApproval inclui os aprovadores principal e padrão, sendo que outros modelos permitem mais aprovadores.

  Como este cenário exige somente dois aprovadores individuais, o resolvedor participante Lista de usuários oferece a solução mais simples. Esse resolvedor permite que os aprovadores individuais sejam selecionados pelo nome, em vez de vários usuários serem selecionados por função ou grupo.

- Configure a notificação por email.

  O Management Console permite notificações por email para tarefas e eventos específicos. Neste cenário, o email de tarefa é ativado e notificações por email são enviadas quando a tarefa Criar usuário é concluída.

  Um modelo de email personalizado é necessário para enviar emails aos departamentos de RH e IS com o assunto e o texto da mensagem apropriados.

Mais informações

Notificações por email (na página 353)
Colocar tarefas administrativas em controle de fluxo de trabalho – método de modelos (na página 261)
Como configurar o fluxo de trabalho em nível de tarefa (na página 265)

Como utilizar o método do WorkPoint

O método do WorkPoint é aplicado às releases do CA Identity Manager anteriores a r12. Há 14 processos de fluxo de trabalho predefinidos do WorkPoint que, por padrão, são mapeados para eventos específicos do CA Identity Manager. Você deve utilizar a Interface de desenho do WorkPoint para configurar resolvedores participantes ou modificar os processos de fluxo de trabalho.

O método do WorkPoint também exige que você use o Management Console para mapear um processo de fluxo de trabalho para um evento de aprovação para colocar a tarefa correspondente sob controle do fluxo de trabalho em um nível global dentro do ambiente.

Esta seção apresenta as etapas de alto nível envolvidas na colocação de tarefas administrativas sob controle do fluxo de trabalho usando o método do WorkPoint.

Observação: para obter mais flexibilidade e facilidade de uso, a CA recomenda usar o método de modelos sempre que possível.

Para usar o método do WorkPoint:

1. Configure as ferramentas administrativas do WorkPoint. (na página 282)
2. No Management Console:
   a. Certifique-se de que o fluxo de trabalho esteja ativado para o seu ambiente, marcando a caixa de seleção Ativado em Configurações avançadas, Fluxo de trabalho.

      Observação: os mapeamentos de eventos nessa tela serão aplicados somente se você usar o método do WorkPoint para configurar o fluxo de trabalho. Se você usar o método de modelos (recomendado), não mapeie os eventos para processos usando esse Management Console.

   b. (Opcional) Para mapeamento do evento global, associe um ou mais eventos ao processo de fluxo de trabalho predefinido apropriado.
   c. Se necessário, reinicie o ambiente do CA Identity Manager.
3. No console de usuário:
   a. Para mapeamento do evento de tarefas específicas, associe um ou mais eventos ao processo de fluxo de trabalho predefinido apropriado. (opcional)
4. Na Interface de desenho do WorkPoint:
   a. Associe uma tarefa de aprovação a um processo de fluxo de trabalho (opcional).
   b. Configure resolvedores participantes com um processo de fluxo de trabalho (opcional).

5. No console de usuário:
   a. Depois que o controle do fluxo de trabalho estiver configurado, o usuário com a função apropriada executará a tarefa administrativa.
   b. O participante do fluxo de trabalho designado aprova ou recusa o evento.

Mais informações:

Mapeamento de processos para eventos (na página 288)
Associar uma atividade de fluxo de trabalho com uma tarefa de aprovação (na página 294)
Resolvedores participantes: Método do WorkPoint (na página 295)

Configurar as ferramentas administrativas do WorkPoint

Interface de desenho do WorkPoint é um software da WorkPoint LLC, uma subsidiária da Planet Group, Inc., que é integrado ao CA Identity Manager. A Interface de desenho do WorkPoint permite gerenciar processos e tarefas de fluxo de trabalho. As ferramentas administrativas do WorkPoint incluem a Interface de desenho do WorkPoint e o Arquivamento do WorkPoint. Para configurar as ferramentas administrativas do WorkPoint, instale as ferramentas administrativas do CA Identity Manager. Se você não tiver instalado as ferramentas administrativas do CA Identity Manager, poderá executar o instalador e selecionar a opção Ferramentas administrativas do CA Identity Manager.

Observação: para usar as ferramentas administrativas para fluxo de trabalho, um JDK suportado deve estar instalado no sistema onde as ferramentas administrativas estiverem instaladas. Para obter uma lista completa das versões e plataformas com suporte, consulte a Matriz de suporte do CA Identity Manager no site de suporte do CA Identity Manager.

As ferramentas de cliente de fluxo de trabalho estão localizadas no diretório do WorkPoint nas ferramentas administrativas do CA Identity Manager. As Ferramentas administrativas são colocadas nos seguintes locais padrão:

- **Windows:** <caminho_de_instalação>\tools
- **UNIX:** <caminho_de_instalação2>/tools

As ferramentas desse diretório permitem fazer o seguinte:

- Criar o esquema de banco de dados de fluxo de trabalho
- Carregar os scripts padrão de fluxo de trabalho
- Criar e monitorar os processos e as tarefas do fluxo de trabalho

Configurar as ferramentas administrativas do WorkPoint no JBoss

Para configurar as ferramentas administrativas do WorkPoint no JBoss, edite os arquivos init.bat/sh e workpoint-client.properties.

Editar init.bat/init.sh

Para editar init.bat/init.sh

1. Em um editor de texto, edite um dos seguintes arquivos:
   - **Windows:**

     ferramentas_administrativas\Workpoint\bin\init.bat
   - **UNIX:**

     *ferramentas_administrativas/*Workpoint/bin/init.sh
2. Retire o comentário da linha EJB_CLASSPATH na seção JBoss do arquivo.

   Observação: certifique-se de que todas as seções para outros servidores de aplicativos estejam comentadas.
3. Crie um diretório chamado JBoss em *ferramentas_administrativas*\Workpoint\lib.
4. Copie o conteúdo do diretório jb*oss_home*\client para o diretório *ferramentas_administrativas*\Workpoint\lib\JBoss.

Editarworkpoint-client.properties

Edite o arquivo workpoint-client.properties com base no tipo de servidor de aplicativos selecionado durante a instalação do CA Identity Manager.

Para configurar o arquivo workpoint-client.properties:

1. Abra *ferramentas_administrativas*\Workpoint\conf\ workpoint-client.properties em um editor de texto.

   ferramentas_administrativas é o local de instalação das ferramentas administrativas. As Ferramentas administrativas são colocadas nos seguintes locais padrão:
   - **Windows:** <caminho_de_instalação>\tools
   - **UNIX:** <caminho_de_instalação2>/tools
2. Localize a seção intitulada JBOSS SETTINGS.

3. Retire o comentário de todos os valores de propriedade nessa seção.

   Por exemplo:
   ```
   java.naming.provider.url=localhost
   java.naming.factory.initial=org.jnp.interfaces.NamingContextFactory
   java.naming.factory.url.pkgs=org.jboss.naming
   ```

   Observação: talvez você precise editar o valor de propriedade java.naming.provider.url. Por exemplo, substitua localhost por jnp://*server_name ou ip*:*port*. Certifique-se de usar o número de porta jnp 1099.

4. Salve o arquivo.

Configurar as ferramentas administrativas do WorkPoint no WebLogic

Para configurar as ferramentas administrativas do WorkPoint no WebLogic, edite os arquivos init.bat/sh e workpoint-client.properties.

Editar init.bat/init.sh

Para editar init.bat/init.sh

1. Em um editor de texto, edite um dos seguintes arquivos:

   - **Windows:**

     ferramentas_administrativas\Workpoint\bin\init.bat

   - **UNIX:**

     ferramentas_administrativas/Workpoint/bin/init.sh

2. Retire o comentário de EJB_CLASSPATH na seção WebLogic do arquivo.

   Observação: certifique-se de que todas as seções para outros servidores de aplicativos estejam comentadas.

3. Copie o arquivo wlclient.jar de *weblogic_home*\server\lib para o seguinte local:

   ferramentas_administrativas\Workpoint\lib\

Editarworkpoint-client.properties

Edite o arquivo workpoint-client.properties com base no tipo de servidor de aplicativos selecionado durante a instalação do CA Identity Manager.

Para configurar o arquivo workpoint-client.properties:

1. Abra *ferramentas_administrativas*\Workpoint\conf\ workpoint-client.properties em um editor de texto.

2. Localize a seção WebLogic do arquivo.

3. Retire o comentário de todos os valores de propriedade nessa seção.
4. Salve o arquivo.

   Observação: a propriedade java.naming.provider.url deve apontar para o nome de domínio totalmente qualificado e número de porta do WebLogic do sistema em que você instalou o servidor do CA Identity Manager.

Configurar as ferramentas administrativas do WorkPoint no WebSphere

Para configurar as ferramentas administrativas do WorkPoint no WebSphere, edite os arquivos init.bat/sh e workpoint-client.properties.

Editar init.bat/init.sh

Para editar init.bat/init.sh

1. Em um editor de texto, edite um dos seguintes arquivos:
   - **Windows:**

     ferramentas_administrativas\Workpoint\bin\init.bat
   - **UNIX:**

     ferramentas_administrativas/Workpoint/bin/init.sh
2. Retire o comentário da seção do IBM WebSphere.

   Observação: não comente a entrada WP_CLASSPATH na seção COMMON WP_CLASSPATH.
3. Certifique-se de que todas as seções para outros servidores de aplicativos estejam comentadas.
4. Se necessário, substitua os valores de JAVA_HOME e WAS_HOME pelos devidos caminhos de seu ambiente.

Editarworkpoint-client.properties

Edite o arquivo workpoint-client.properties com base no tipo de servidor de aplicativos selecionado durante a instalação do CA Identity Manager.

Para configurar o arquivo workpoint-client.properties:

1. Abra *ferramentas_administrativas*\Workpoint\conf\ workpoint-client.properties em um editor de texto.

   ferramentas_administrativas é o local de instalação das ferramentas administrativas. As Ferramentas administrativas são colocadas nos seguintes locais padrão:

   - **Windows:** <caminho_de_instalação>\tools
   - **UNIX:** <caminho_de_instalação2>/tools

2. Localize a seção intitulada IBM WEBSPHERE SETTINGS.
3. Retire o comentário de todos os valores de propriedade nessa seção.

   Por exemplo:
   `java.naming.factory.initial=com.ibm.websphere.naming.WsnInitialContextFactory`
   `java.naming.provider.url=iiop://localhost:`*`bootstrap_port`*

   Observação: o número da porta de inicialização deve corresponder ao número da porta especificado no console administrativo do WebSphere. Para localizar o número de porta correto, vá para Servidor, Terminais, Bootstrap server address.

4. Atualize a porta BOOTSTRAP_ADDRESS para o perfil do WebSphere da seguinte maneira:

   a. No console administrativo do WebSphere, vá para Application Servers, server_name, Communications.

   b. Expanda Ports.

   c. Edite o arquivo workpoint-client.properties em iam_im.ear/config.

   d. Altere a porta padrão 2809 na seção do WebSphere da porta do perfil para BOOTSTRAP_ADDRESS.

5. Salve o arquivo.

Iniciando a Interface de desenho do WorkPoint

Para iniciar a Interface de desenho do WorkPoint, execute o seguinte arquivo:

- **Windows:** *ferramentas_administrativas*\WorkPoint\bin\Designer.bat
- **UNIX:** *ferramentas_administrativas*/WorkPoint/bin/Designer.sh

onde *ferramentas_administrativas* é o diretório de instalação das ferramentas administrativas do CA Identity Manager. As Ferramentas administrativas são colocadas nos seguintes locais padrão:

- **Windows:** <caminho_de_instalação>\tools
- **UNIX:** <caminho_de_instalação2>/tools

Observação: os componentes do fluxo de trabalho devem estar instalados e configurados antes que você possa executar a Interface de desenho do WorkPoint. Para obter instruções, consulte a seção "Configurar as ferramentas administrativas do WorkPoint" para o seu servidor de aplicativos.

Mais informações:

Configurar as ferramentas administrativas do WorkPoint no JBoss (na página 283)
Configurar as ferramentas administrativas do WorkPoint no WebLogic (na página 284)
Configurar as ferramentas administrativas do WorkPoint no WebSphere (na página 285)

Processos do WorkPoint

O CA Identity Manager inclui vários processos de fluxo de trabalho que são predefinidos na Interface de desenho do WorkPoint. Você pode usar os processos predefinidos com seus mapeamentos de eventos padrão, mapear os processos de fluxo de trabalho para outros eventos, modificar os processos de fluxo de trabalho, adicionando ou removendo atividades, e criar processos de fluxo de trabalho.

Processo global para mapeamento de eventos

O mapeamento de um processo de fluxo de trabalho para um evento em nível global pode ser com base em políticas ou sem base em políticas.

Para obter mais informações sobre como mapear um evento para um processo de fluxo de trabalho por meio de um fluxo de trabalho com base em políticas, consulte Mapeamento de fluxo de trabalho de evento global com base em políticas.

Esta tabela mostra o processo de fluxo de trabalho global padrão e mapeamentos de eventos especificados no Management Console.

Importante: esses mapeamentos são globais. O processo de fluxo de trabalho mapeado é executado sempre que o evento correspondente for gerado por uma tarefa no ambiente.

Processo de fluxo de trabalho	Evento mapeado
CertifyRoleApproveProcess	CertifyRoleEvent

Processo de fluxo de trabalho	Evento mapeado
CreateGroupApproveProcess	CreateGroupEvent
CreateOrganizationApproveProcess	CreateOrganizationEvent
CreateUserApproveProcess	CreateUserEvent
DeleteGroupApproveProcess	DeleteGroupEvent
DeleteOrganizationApproveProcess	DeleteOrganizationEvent
DeleteUserApproveProcess	DeleteUserEvent
ModifyAccessRoleMembershipApproveProcess	AssignAccessRoleEvent RevokeAccessRoleEvent
ModifyAdminRoleMembershipApproveProcess*	AssignAdminRoleEvent RevokeAdminRoleEvent
ModifyGroupMembershipApproveProcess*	AddToGroupEvent RemoveFromGroupEvent
ModifyOrganizationApproveProcess	ModifyOrganizationEvent
ModifyObjectApproveProcess	ModifyObjectEvent
SelfRegistrationApproveProcess	SelfRegisterUserEvent

Observação: os processos de fluxo de trabalho marcados com um asterisco (*) não são mapeados para os eventos por padrão.

Mais informações:

Mapear um processo para um evento globalmente (na página 289)
Mapear um processo para um evento em uma tarefa específica (na página 290)

Mapeamento de processos para eventos

É possível criar e modificar processos de fluxo de trabalho na Interface de desenho do WorkPoint. Quando você cria um processo de fluxo de trabalho para o CA Identity Manager, isso é feito com uma determinada tarefa do CA Identity Manager em mente. A execução dessa tarefa é controlada pelo processo de fluxo de trabalho.

Além de criar o processo de fluxo de trabalho, você também deve fazer o seguinte:

- Identificar os eventos gerados pela tarefa do CA Identity Manager, descrita em Tarefas administrativas e Eventos. É possível criar um processo de fluxo de trabalho para qualquer tarefa do CA Identity Manager que gera um evento.

- Mapeie o processo de fluxo de trabalho para um evento, executando um dos seguintes procedimentos:
  - Atribua um processo de fluxo de trabalho para um evento globalmente.

    Com esse mapeamento global, o processo do fluxo de trabalho ocorre sempre que o evento é gerado no ambiente, independentemente da tarefa que gera o evento.
  - Atribua um processo de fluxo de trabalho para um evento gerado por uma tarefa específica.

    Com esse mapeamento de tarefas específicas, o processo de fluxo de trabalho ocorre apenas quando a tarefa especificada gera o evento.

  Observação: se você mapear um evento para um processo de fluxo de trabalho globalmente e para uma tarefa específica, o processo de fluxo de trabalho associado à tarefa específica terá precedência.
- Especifique um resolvedor participante para a atividade de fluxo de trabalho no processo de fluxo de trabalho.
- Associe uma atividade de fluxo de trabalho a uma tarefa de aprovação.

Mais informações:

Mapear um processo para um evento globalmente (na página 289)
Mapear um processo para um evento em uma tarefa específica (na página 290)
Atividades de fluxo de trabalho (na página 292)
Resolvedores participantes: Método do WorkPoint (na página 295)

Mapear um processo para um evento globalmente

Você mapeia um processo de fluxo de trabalho para um evento globalmente para que o processo de fluxo de trabalho seja executado quando o evento for gerado por qualquer tarefa no ambiente.

Observação: embora o procedimento a seguir funcione, o procedimento global, com base em políticas e em nível evento (na página 330) é o método recomendado para o mapeamento de um processo para um evento.

Para mapear um processo de fluxo de trabalho sem base em políticas para um evento globalmente:

1. Abra o Management Console inserindo o seguinte URL em um navegador:

   `http://hostname/iam/immanage`

   nome do host

   Define o nome de domínio totalmente qualificado do servidor em que o CA Identity Manager está instalado. Por exemplo, meuservidor.minhaempresa.com:porta.

2. Clique em Ambientes e selecione o nome do ambiente adequado do CA Identity Manager.
3. Clique em Configurações avançadas e, em seguida, clique em Fluxo de trabalho.
4. Faça o seguinte para mapear um evento para um processo de fluxo de trabalho:
   a. Selecione um evento na caixa de listagem Eventos.
   b. Selecione um processo de fluxo de trabalho na caixa de listagem Processo de aprovação.
   c. Clique em Adicionar.
5. Após concluir o mapeamento de eventos para processos de fluxo de trabalho, clique em Salvar.
6. Reinicie o ambiente do CA Identity Manager para que as alterações entrem em vigor.

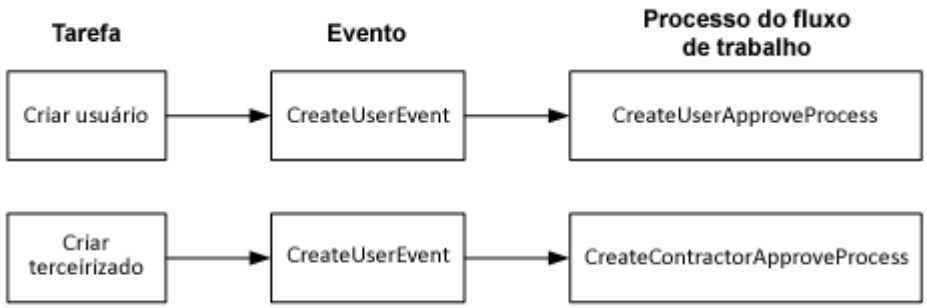
Mais informações:

Processo global para mapeamento de eventos (na página 287)

Mapear um processo para um evento em uma tarefa específica

Você pode atribuir um processo de fluxo de trabalho para um evento gerado por uma determinada tarefa. Nesse caso, o processo de fluxo de trabalho ocorre apenas quando o evento mapeado é gerado pela tarefa especificada.

O mapeamento de tarefas específicas fornece controle variável sobre os processos de fluxo de trabalho que podem ser executados para o mesmo evento. Por exemplo, o diagrama a seguir mostra duas tarefas diferentes que geram o mesmo evento, mas acionam dois processos de fluxo de trabalho diferentes:



Neste diagrama, cada tarefa usa um processo de fluxo de trabalho diferente.

Criar usuário

Especifica a tarefa administrativa padrão que aciona CreateUserEvent, que é mapeado para CreateUserApproveProcess, um processo de fluxo de trabalho padrão.

Criar prestador de serviço

Especifica uma tarefa personalizada com base em Criar usuário. Nesse caso, CreateUserEvent é mapeado para CreateContractorApproveProcess, um processo de fluxo de trabalho personalizado criado para aprovar novas contas de prestadores de serviço.

Para mapear um processo de fluxo de trabalho sem base em políticas para um evento em uma tarefa existente:

1. No console de usuário, selecione Funções e tarefas, Tarefa administrativa, Modificar tarefa administrativa.
2. Procure uma tarefa de administrador.
3. Selecione uma tarefa (por exemplo, a tarefa Modificar usuário ou Criar usuário) e clique em Selecionar.
4. Na guia Eventos, selecione um processo de fluxo de trabalho para o evento na tarefa.

   Observação: para ser exibido nessa guia, o fluxo de trabalho deve ser ativado para os nomes dos eventos e para o menu suspenso do processo de fluxo de trabalho.
5. Clique no botão Editar para exibir a tela de mapeamento de fluxo de trabalho.
6. Usando o menu suspenso do processo de fluxo de trabalho, atribua um processo de fluxo de trabalho para o nome do evento e clique em OK.
7. Clique em Enviar.

Para mapear um processo de fluxo de trabalho sem base em políticas para um evento em uma nova tarefa:

1. No console de usuário, selecione Funções e tarefas, Tarefa administrativa, Criar tarefa administrativa.

   Observação: certifique-se de selecionar uma tarefa de aprovação de fluxo de trabalho existente (como Aprovar Criar grupo ou Aprovar Criar usuário) como o modelo para a nova tarefa de aprovação de fluxo de trabalho.
2. Na guia Perfil, digite as informações nos campos apropriados.
3. Na guia Eventos, selecione um processo de fluxo de trabalho para o evento na tarefa.

   Observação: para ser exibido nessa guia, o fluxo de trabalho deve ser ativado para os nomes dos eventos e para o menu suspenso do processo de fluxo de trabalho.

4. Usando o menu suspenso do processo de fluxo de trabalho, atribua um processo de fluxo de trabalho para o nome do evento e clique em OK.
5. Clique em Enviar.

Observação: para mapear um processo de fluxo de trabalho com base em políticas para um evento, consulte a seção Fluxo de trabalho com base em políticas (na página 314).

Observação: a lista Processo do fluxo de trabalho inclui os processos para uso com o método do modelo e o método do WorkPoint:

- Quando um processo do método do modelo é selecionado (SingleStepApproval, TwoStageApprovalProcess ou EscalationApproval), a página expande para ativar a configuração de resolvedor participante.
- Quando um processo do método do WorkPoint é selecionado, a página não é expandida. Resolvedores participantes são configurados na Interface de desenho do WorkPoint.

Mais informações:

Processo global para mapeamento de eventos (na página 287)

Atividades de fluxo de trabalho

O CA Identity Manager inclui várias atividades de fluxo de trabalho que são predefinidas na Interface de desenho do WorkPoint. Essas atividades são atribuídas a processos de fluxo de trabalho predefinidos.

Os processos de fluxo de trabalho predefinidos são processos de etapa única — isto é, cada processo contém uma única atividade predefinida.

Cada atividade predefinida corresponde a uma tarefa de aprovação de fluxo de trabalho com o mesmo nome, que é predefinida no CA Identity Manager. Você pode usar as atividades predefinidas em outros processos de fluxo de trabalho, além de criar atividades.

Você pode usar os processos de fluxo de trabalho predefinidos sem modificação ou adição de outras atividades. Para obter informações sobre como adicionar uma atividade a um processo de fluxo de trabalho, consulte a documentação do WorkPoint.

Processos, tarefas e atividades

A tabela a seguir lista as atividades de fluxo de trabalho predefinidas e o processo de fluxo de trabalho predefinido para o qual cada atividade é atribuída por padrão.

Observação: as atividades de fluxo de trabalho predefinidas e suas respectivas tarefas de aprovação de fluxo de trabalho têm o mesmo nome.

Processo de fluxo de trabalho	Tarefa/atividade de fluxo de trabalho
CertifyRoleApprovalProcess**	Approvar Certificar função
Processo de consulta*	
CreateGroupApproveProcess	Aprovar Criar grupo
CreateOrganizationApproveProcess	Aprovar Criar organização
CreateUserApproveProcess	Aprovar Criar usuário
DeleteGroupApproveProcess	Aprovar Excluir grupo
DeleteOrganizationApproveProcess	Aprovar Excluir organização
DeleteUserApproveProcess	Aprovar Excluir usuário
ModifyAccessRoleMembershipApproveProcess	Aprovar Modificar associação da função de acesso
ModifyAdminRoleMembershipApproveProcess	Aprovar Modificar associação da função administrativa
ModifyGroupMembershipApproveProcess	Aprovar Modificar associação ao grupo
ModifyIdentityPolicySetApproveProcess	Aprovar Modificar o conjunto de políticas de identidade
ModifyOrganizationApproveProcess	Aprovar Modificar organização
ModifyUserApproveProcess	Aprovar Modificar usuário
SelfRegistrationApproveProcess	Aprovar autorregistro
SingleStepApproval*	
TwoStageApprovalProcess*	

Observação: os processos de fluxo de trabalho marcados com um asterisco (*) são projetados para uso com o método de modelos. São configurados no console de usuário e, por isso, não possuem tarefas ou atividades padrão associadas. O CertifyRoleApprovalProcess (**) é um processo de exemplo que demonstra um resolvedor participante personalizado.

Associar uma atividade de fluxo de trabalho com uma tarefa de aprovação

Para associar uma atividade de fluxo de trabalho com uma tarefa de aprovação de fluxo de trabalho, você pode definir um par de nome/valor na Interface de desenho do WorkPoint.

Observação: se um par de nome/valor não for definido para uma atividade de fluxo de trabalho por padrão, o CA Identity Manager usará uma tarefa com um nome que corresponda à tarefa de aprovação.

Para associar uma atividade de fluxo de trabalho com uma tarefa de aprovação:

1. Inicie a Interface de desenho do WorkPoint.
2. Clique em Arquivo, Abrir, Processo.
3. Selecione um processo de fluxo de trabalho e clique em Abrir.
4. Clique com o botão direito do mouse no nó de atividade no processo e selecione Propriedades.
5. Selecione Texto no menu suspenso Tipo.
6. Digite o seguinte na guia Dados do usuário:
   - **Nome** — TASK_TAG.
   - **Valor** — nome do tag da tarefa de aprovação.
7. Clique em Adicionar.
8. Clique em OK para salvar as alterações.

Criar tarefas de aprovação para terminais

É possível criar tarefas de aprovação para as telas de gerenciamento de contas. Para as tarefas que aprovam modificações de conta, a tela de aprovação deve ser específica para um tipo de terminal, de modo que o aprovador possa ver os valores alterados. Para criar uma tarefa de aprovação para Criar ou Modificar tarefa, siga este procedimento:

Para criar uma tarefa de aprovação para um terminal:

1. No console de usuário, clique em Funções e tarefas, Tarefa administrativa, Criar tarefa administrativa.
2. Selecione Criar cópia de uma tarefa administrativa usada para gerenciar contas no terminal.

   O nome deve começar com criar e indicar o nome do tipo de terminal. Criar conta do Active Directory é um exemplo.
3. Faça as seguintes alterações na guia Perfil.
4. Altere o nome da nova tarefa.
   - Altere o tag da tarefa.
   - Altere a ação para Aprovar evento.
5. Faça as seguintes alterações na guia Guias:
   a. Remova todas as guias de relacionamentos.
   b. Copie e edite as telas de aprovação nas guias, conforme necessário.

      Observação: você pode encontrar problemas ao usar as telas de conta em uma tarefa de aprovação, e talvez alterações precisem ser feitas na tela de conta padrão para que elas funcionem em uma tarefa de aprovação.
6. Clique em Enviar.

Resolvedores participantes: Método do WorkPoint

Para especificar os participantes usando o método do WorkPoint, defina as seguintes propriedades de atividade na Interface de desenho do WorkPoint:

- O nome do script predefinido do CA Identity Manager que permite a comunicação entre o CA Identity Manager e o servidor do fluxo de trabalho. O script emite uma solicitação ao CA Identity Manager para os participantes da atividade e fornece essa lista para o servidor do fluxo de trabalho.
- Referências a um ou mais resolvedores participantes.

Tipos de resolvedor participante

Em vez de inserir uma lista específica de participantes nas propriedades de atividade de fluxo de trabalho, os participantes são referenciados por um nome arbitrário que é mapeado para um *resolvedor participante*.

Para o modelo de processo predefinido, existem quatro tipos de resolvedores participantes:

Resolvedor participante da função

Especifica que os participantes são integrantes de uma determinada função.

Resolvedor participante de grupo

Especifica que os participantes são integrantes de um determinado grupo.

Resolvedor participante personalizado

Especifica que os participantes são determinados por um resolvedor participante personalizado.

Resolvedor participante de filtro

Especifica que os participantes são selecionados por meio de um filtro de pesquisa.

Resolvedores participantes da função

Com os resolvedores participantes de tipo de função, o CA Identity Manager recupera todos os integrantes dessa função e retorna esses integrantes como participantes.

Se nenhum tipo de resolvedor for especificado no parâmetro UserData da caixa de diálogo Atividade, o resolvedor de tipo de função será usado por padrão.

Se você não especificar nenhum resolvedor participante na guia Dados do usuário da caixa de diálogo de propriedades de atividade do WorkPoint, por padrão, o CA Identity Manager localizará todas as funções disponíveis que contêm essa tarefa de aprovação e retornará esses integrantes da função como participantes.

Para configurar resolvedores participantes da função:

1. Inicie a Interface de desenho do WorkPoint.
2. Clique em Arquivo, Abrir, Processo.
3. Selecione um processo de fluxo de trabalho e clique em Abrir.
4. Clique com o botão direito do mouse no nó de atividade no processo e selecione Propriedades.
5. Selecione Texto no menu suspenso Tipo.

6. Digite o seguinte na guia Dados do usuário:
   - **Nome** — APPROVER_ROLE_NAME
   - **Valor** — o nome de uma função do CA Identity Manager (por exemplo, Gerenciador de segurança)
7. Clique em Adicionar.

   Observação: essa função não precisa conter tarefas de aprovação.
8. Selecione Texto no menu suspenso Tipo.
9. Na guia Dados do usuário, insira o seguinte par de nome/valor (opcional):

   Valor — APPROVERS_REQUIRED

   Valor — YES.
10. Clique em Adicionar.

    Observação: a configuração de aprovação padrão é APPROVERS_REQUIRED=NO. Nesse caso, uma atividade será aprovada automaticamente se nenhum participante for localizado.

    Se APPROVERS_REQUIRED=YES e o CA Identity Manager não encontrar participantes, a atividade não será concluída com êxito.
11. Clique em OK para salvar as alterações.

Resolvedores participantes de grupo

Com os resolvedores participantes de tipo de grupo, o CA Identity Manager recupera todos os integrantes desse grupo e retorna esses integrantes como participantes.

Para configurar resolvedores participantes de grupo:

1. Inicie a Interface de desenho do WorkPoint.
2. Clique em Arquivo, Abrir, Processo.
3. Selecione um processo de fluxo de trabalho e clique em Abrir.
4. Clique com o botão direito do mouse no nó de atividade no processo e selecione Propriedades.
5. Selecione Texto no menu suspenso Tipo.
6. Digite o seguinte na guia Dados do usuário:
   - **Nome** — APPROVER_GROUP_UNIQUENAME
   - **Valor** — o nome de um grupo do CA Identity Manager
7. Clique em Adicionar.
8. Selecione Texto no menu suspenso Tipo.

9. Na guia Dados do usuário, insira o seguinte par de nome/valor (opcional):
   - **Nome** — APPROVERS_REQUIRED
   - **Valor** — YES.
10. Clique em Adicionar.

    Observação: a configuração de aprovação padrão é APPROVERS_REQUIRED=NO. Nesse caso, uma atividade será aprovada automaticamente se nenhum participante for localizado.

    Se APPROVERS_REQUIRED=YES e o CA Identity Manager não encontrar participantes, a atividade não será concluída com êxito.
11. Clique em OK para salvar as alterações.

Resolvedores participantes personalizados

O resolvedor participante personalizado é um objeto Java que determina os participantes da atividade de fluxo de trabalho e retorna uma lista no CA Identity Manager, que, em seguida, passa a lista para o mecanismo de fluxo de trabalho. Normalmente, você deve criar um resolvedor participante personalizado somente se as políticas de participante padrão não puderem fornecer a lista de participantes que uma atividade exige.

Observação: você cria um resolvedor participante personalizado usando a API de resolvedor participante. Para obter informações, consulte o *Guia de Programação do Java*.

Para configurar um resolvedor participante personalizado:

1. Abra o Management Console inserindo o seguinte URL em um navegador:

   `http://hostname/iam/immanage`

   nome do host

   Define o nome de domínio totalmente qualificado do servidor em que o CA Identity Manager está instalado. Por exemplo, meuservidor.minhaempresa.com:porta.
2. Clique em Ambientes e selecione o nome do ambiente adequado do CA Identity Manager.
3. Clique em Configurações avançadas, Resolvedor participante do fluxo de trabalho.

4. Na tela do resolvedor participante do fluxo de trabalho, clique em Novo e digite:

   Nome

   Especifica o nome do resolvedor participante personalizado, por exemplo, GroupFinder.

   Descrição

   Especifica uma descrição do resolvedor participante personalizado.

   Classe

   Especifica o nome da classe Java, por exemplo, com.netegrity.samples.GroupFinder

5. Clique em Salvar.
6. Inicie a Interface de desenho do WorkPoint.
7. Clique em Arquivo, Abrir, Processo.
8. Selecione um processo de fluxo de trabalho e clique em Abrir.
9. Clique com o botão direito do mouse no nó de atividade no processo e selecione Propriedades.
10. Selecione Texto no menu suspenso Tipo.
11. Digite o seguinte na guia Dados do usuário:

    Nome

    APPROVER_CUSTOMRESOLVER_NAME

    Valor

    Especifica um nome exclusivo para o resolvedor personalizado. Deve corresponder ao nome que você inseriu na tela do resolvedor participante do tipo personalizado no Management Console, por exemplo, GroupFinder.

12. Clique em Adicionar.

    Observação: a configuração de aprovação padrão é APPROVERS_REQUIRED=NO. Nesse caso, uma atividade será aprovada automaticamente se nenhum participante for localizado.

    Se APPROVERS_REQUIRED=YES e o CA Identity Manager não encontrar participantes, a atividade não será concluída com êxito.

13. Clique em OK para salvar as alterações.

Resolvedores participantes de filtro

Um resolvedor participante de filtro permite que o CA Identity Manager pesquise usuários ou grupos correspondentes aos critérios do filtro. É possível especificar um filtro de pesquisa na Interface de desenho do WorkPoint, e o CA Identity Manager retornará aprovadores correspondentes para a respectiva atividade de fluxo de trabalho.

É possível criar um resolvedor participante de filtro na guia Dados do usuário da caixa de diálogo de propriedades de atividade do WorkPoint.

Sintaxe de resolvedores participantes de filtro

A seguir, há três atributos obrigatórios que são combinados para criar um filtro de pesquisa:

- Atributo de aprovador, como cargo
- Operação de atributo do aprovador, como igual a
- Valor de atributo do aprovador, como gerente

Os atributos obrigatórios do filtro de pesquisa são combinados na seguinte ordem:

atributo operação valor

Por exemplo:

cargo é igual a gerente ou *departamento contém folha de pagamento*

Atributos obrigatórios de filtro do resolvedor participante

Os atributos de filtro do resolvedor participante a seguir são *obrigatórios*.

Observação: para cada filtro, n é um inteiro positivo que indica o número de filtros de pesquisa. O padrão é 1.

APPROVER_FILTER_n_ATTRIBUTE

Especifica o atributo do aprovador. Por exemplo, Cargo, Departamento, ID de usuário. (As sequências de caracteres do nome do atributo do aprovador devem corresponder às sequências de caracteres do nome do atributo do usuário.)

APPROVER_FILTER_n_OP

Especifica a operação associada ao atributo do aprovador. Por exemplo, Igual a, Não é igual a, ou Contém. (As palavras-chave de operação não fazem distinção entre maiúsculas e minúsculas.)

A seguir, estão entradas válidas para este filtro:

- EQUALS
- STARTSWITH
- NOT_EQUALS
- CONTAINS
- ENDS_WITH
- GREATER_THAN
- LESS_THAN
- GREATER_THAN_EQUALS
- LESS_THAN_EQUALS

APPROVER_FILTER_n_VALUE

Especifica o valor associado ao aprovador. Por exemplo, gerente, folha de pagamento, engenharia.

Atributos opcionais de filtro do resolvedor participante

Os atributos de filtro do resolvedor participante a seguir são *opcionais*.

APPROVER_OBJECTTYPE

USUÁRIO ou GRUPO (não faz distinção entre maiúsculas e minúsculas)

O padrão é USUÁRIO.

APPROVER_ORG_UNIQUENAME

Um nome exclusivo para a organização de um aprovador. (As sequências de caracteres do nome da organização devem corresponder às sequências de caracteres do nome da organização do CA Identity Manager.)

O padrão é o usuário raiz.

APPROVER_ORG_AND_LOWER

A organização ou as suborganizações do aprovador:

- 0 significa pesquisar na organização do aprovador.
- 1 significa pesquisar em todas as suborganizações da organização do aprovador.

O padrão é 1.

APPROVER_FILTER_NO

O número de filtros de pesquisa que você está usando. Se você tiver dois filtros, esse número será 2.

O padrão é 1.

Observação: esse filtro é obrigatório se o número de filtros for maior do que um.

APPROVER_FILTER_n_CONJ_TYPE

É possível combinar os filtros de pesquisa usando os tipos de conjunção OR ou AND.

Observação: os filtros separados pela conjunção OR têm precedência sobre aqueles separados por AND.

Por exemplo, você pode especificar o tipo de conjunção AND se estiver pesquisando "cargo é igual a gerente" AND "departamento é igual a desenvolvimento".

Observação: n é um número inteiro positivo maior que 1, indicando o número de filtros de pesquisa.

Adicionar um filtro do resolvedor participante

Para adicionar filtros do resolvedor participante:

1. Inicie a Interface de desenho do WorkPoint.
2. Clique em Arquivo, Abrir, Processo.
3. Selecione um processo de fluxo de trabalho e clique em Abrir.
4. Clique com o botão direito do mouse no nó de atividade no processo e selecione Propriedades.
5. Selecione Texto no menu suspenso Tipo.
6. Digite o seguinte na guia Dados do usuário:
   - **Nome** — APPROVER_FILTER_1_ATTRIBUTE
   - **Valor** — um identificador de função exclusivo (por exemplo, cargo).
7. Clique em Adicionar.
8. Repita as etapas 6 e 7 para cada atributo no filtro de pesquisa.

   Observação: a configuração de aprovação padrão é APPROVERS_REQUIRED=NO. Nesse caso, uma atividade será aprovada automaticamente se nenhum participante for localizado.

   Se APPROVERS_REQUIRED=YES e o CA Identity Manager não encontrar participantes, a atividade não será concluída com êxito.
9. Clique em OK para salvar as alterações.

Exemplo: Resolvedor participante de filtro

O repositório de usuários na tabela a seguir contém quatro usuários — Holly, Sarah, John e Dave — com atributos de ID de usuário, cargo e departamento.

Usuário	ID	Cargo	Departamento
Holly	admin1	sysadmin	administração
Sarah	test1	sysadmin	desenvolvimento
John	admin2	gerente	desenvolvimento
Dave	admin3	sysadmin	contabilidade

O CA Identity Manager aplicará os três filtros definidos na tabela a seguir em relação ao repositório de usuários anterior:

Nome	Valor
APPROVER_FILTER_NO	3
APPROVER_FILTER_1_ATTRIBUTE	uid
APPROVER_FILTER_1_OP	igual a
APPROVER_FILTER_1_VALUE	admin*
APPROVER_FILTER_2_CONJ_TYPE	E
APPROVER_FILTER_2_ATTRIBUTE	departamento
APPROVER_FILTER_2_OP	igual a
APPROVER_FILTER_2_VALUE	administração
APPROVER_FILTER_3_CONJ_TYPE	OU
APPROVER_FILTER_3_ATTRIBUTE	cargo
APPROVER_FILTER_3_OP	igual a
APPROVER_FILTER_3_VALUE	sysadmin

O CA Identity Manager aplicará os filtros na seguinte sequência:

1. Avalia o segundo e o terceiro filtro conectado pela conjunção OR.

   "departamento é igual a administração" OR "cargo é igual a sysadmin"

   Isso exclui John e retorna Holly, Sarah e Dave.

2. Avalia o primeiro e o segundo filtro conectado pela conjunção AND, (onde * é um caractere curinga).

   "uid é igual a admin*" AND "departamento é igual a administração"

   Isso exclui Sarah e retorna Holly e Dave.

Os últimos usuários retornados do repositório de usuários são Holly e Dave.

Ordem de precedência de resolvedores participantes

Se você não especificar nenhum resolvedor participante, por padrão, o CA Identity Manager identificará todas as funções disponíveis que contêm a tarefa de aprovação e retornará os integrantes da função como participantes.

Se você especificar mais de um resolvedor participante, o CA Identity Manager irá avaliá-los usando esta ordem de precedência:

1. Personalizado
2. Função
3. Filtro
4. Grupo

O CA Identity Manager identifica e aplica o primeiro resolvedor nesta ordem de precedência e ignora quaisquer resolvedores subsequentes restantes.

É necessário ter apenas um resolvedor de cada vez. Além disso, certifique-se de que o resolvedor está configurado adequadamente, para que o CA Identity Manager identifique corretamente os participantes.

Especificar script de recurso de fluxo de trabalho

O CA Identity Manager é fornecido com um script, denominado IM Approvers, que passa informações entre o CA Identity Manager e o servidor do fluxo de trabalho.

Quando uma lista de participantes é necessária para uma atividade de fluxo de trabalho, o script passa para o CA Identity Manager o nome da atividade, o identificador do participante fornecido na guia Dados do usuário da caixa de diálogo de propriedades de atividade do WorkPoint e quaisquer outras informações fornecidas na guia Dados do usuário. O CA Identity Manager pesquisa os participantes e devolve a lista para o script. O script, em seguida, fornece a lista para o servidor do fluxo de trabalho.

Quando houver uma nova definição de processo de fluxo de trabalho e a atividade do processo de fluxo de trabalho for uma tarefa de aprovação de fluxo de trabalho do CA Identity Manager, o script IM Approvers deverá ser especificado na guia Recursos da caixa de diálogo de propriedades de atividade do WorkPoint.

Para especificar o script IM Approvers na Interface de desenho do WorkPoint:

1. Na guia Recursos, clique em Selecionar.
2. Na caixa de diálogo Select Resources, selecione Regra na lista suspensa. Essa ação exibe as regras (scripts) que você pode associar a essa atividade.
3. Selecione o nome do script IM Approvers e clique em Adicionar.
4. Clique em OK e, em seguida, clique em Aplicar na caixa de diálogo de propriedades de atividade.

Observação: não modifique o script IM Approvers.

Especificar participantes para tarefas Certificar usuário

As tarefas Certificar usuário geram o evento CertifyRoleEvent. Esse evento pode estar sujeito à aprovação de fluxo de trabalho por meio do processo predefinido CertifyRoleApproveProcess.

O CA Identity Manager também inclui o resolvedor participante predefinido CertifyRoleParticipantResolver, que aparece no seu ambiente por padrão. Os participantes de atividades em um CertifyRoleApprovalProcess são especificados pelo CertifyRoleParticipantResolver.

Para fornecer informações de configuração de participantes:

1. Abra o Management Console inserindo o seguinte URL em um navegador:

   `http://hostname/iam/immanage`

   nome do host

   Define o nome de domínio totalmente qualificado do servidor em que o CA Identity Manager está instalado. Por exemplo, meuservidor.minhaempresa.com:porta.
2. Clique em Ambientes e selecione o nome do ambiente adequado do CA Identity Manager.
3. Clique em Configurações avançadas e, em seguida, clique em Diversos.

4. Defina pares de nome/valor que especificam os aprovadores para cada função a ser certificada:
   - No campo Propriedade, utilize o formato: *role-type.role-name*.

     role-type deve ser uma destas funções: administração, acesso, provisionamento.

     role-name é o nome de qualquer função existente.

     As opções role-name e role-type devem ser separadas por um ponto (.).
   - No campo Valor, especifique as IDs dos aprovadores e separe-as por um ponto-e-vírgula (;).

No exemplo a seguir, a certificação de usuário pode ser aprovada para as funções e pelos participantes a seguir:

- jsmith01 e ajones19 podem aprovar a certificação para a função Gerenciador de usuários
- plewis12 é o único aprovador para a função Gerente do sistema
- rtrevor8 e pkitt3 podem aprovar a certificação da função Meu acesso

Propriedade	Valor
admin.User Manager	jsmith01;ajones19
admin.System Manager	plewis12
access.My Access Role	rtrevor8;pkitt3

Observação: todas as funções não especificadas não terão aprovadores para um CertifyRoleEvent.

Processos na Interface de desenho do WorkPoint

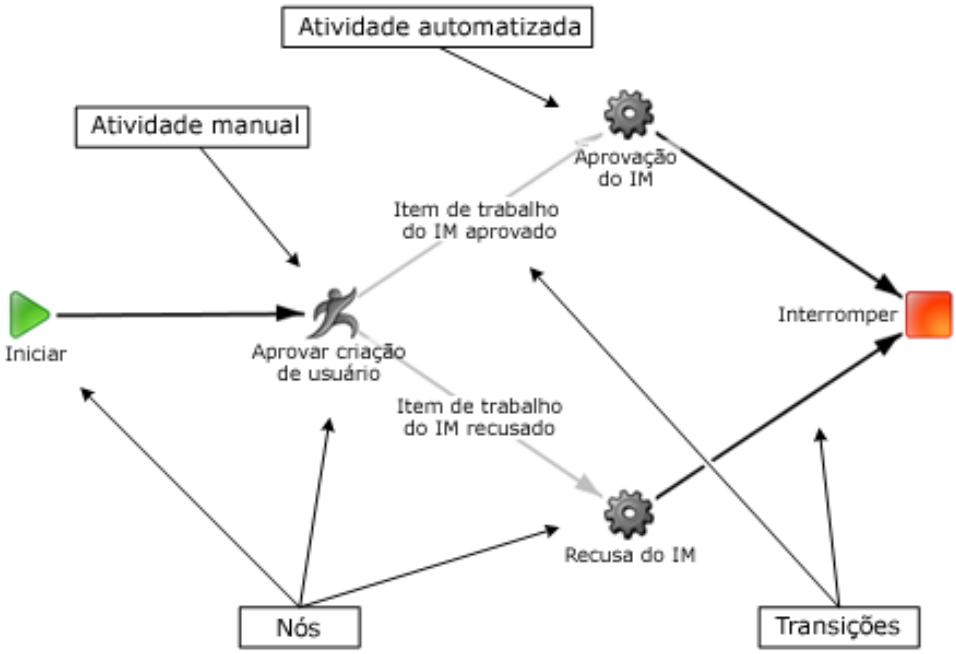
Na Interface de desenho do WorkPoint, você pode personalizar os processos e atividades de fluxo de trabalho padrão fornecidas com o CA Identity Manager e criar outros processos e atividades.

Este documento apresenta informações de fluxo de trabalho do WorkPoint que são específicas para o CA Identity Manager. Para obter informações completas, consulte a documentação da Interface de desenho do WorkPoint.

Observação: ao criar um processo de fluxo de trabalho, considere fazer uma cópia de um processo do CA Identity Manager existente e, em seguida, modificar o novo processo para atender às suas necessidades. Um processo de fluxo de trabalho criado dessa forma inclui elementos e nós específicos do CA Identity Manager padrão, como scripts de transição e atividades automatizadas.

Diagrama de processos do WorkPoint

O diagrama a seguir mostra um típico processo de fluxo de trabalho com o conjunto mínimo de componentes para um processo que controla uma tarefa do CA Identity Manager. O diagrama ilustra o processo predefinido CreateUserApproveProcess, que controla a execução de uma tarefa Criar usuário.



Componentes do processo do WorkPoint

O processo de fluxo de trabalho contém os seguintes nós e transições:

Iniciar

Cada processo de fluxo de trabalho começa com este nó.

Parar

Cada processo do fluxo de trabalho termina com este nó.

Atividades manuais

Uma atividade manual exige a aprovação ou a recusa de uma tarefa do CA Identity Manager por um participante e deve ter o mesmo nome de uma tarefa de aprovação de fluxo de trabalho do CA Identity Manager.

Um processo de fluxo de trabalho que controla uma tarefa do CA Identity Manager deve incluir pelo menos uma atividade manual solicitando aprovação para essa tarefa.

Atividades automatizadas

Um dos dois scripts é atribuído a uma atividade automatizada:

- Notify IM Approve — Informa ao CA Identity Manager para executar a tarefa do CA Identity Manager sob controle do fluxo de trabalho.
- Notify IM Reject — Informa ao CA Identity Manager para cancelar a execução da tarefa do CA Identity Manager.

Em geral, o script Notify IM Approve é ativado se todas as atividades manuais forem aprovadas, e o script Notify IM Reject é ativado se alguma atividade manual for recusada.

Transição incondicional

Uma transição incondicional é um caminho de um nó do processo de fluxo de trabalho para outro, e não está associada a um script de condição.

Transição condicional

Uma transição condicional representa um caminho alternativo de um nó no processo de fluxo de trabalho para outro, e está associada a um script de condição.

Um script de condição determina se a transição ocorre ao avaliar o resultado da atividade associada. Se o script retornar verdadeiro, a transição será executada e o processo passará para o próximo nó indicado.

É possível que dois ou mais scripts de condição retornem verdadeiro. Isso permite que uma atividade seja executada em paralelo, uma vez que cada script está associado a uma transição diferente.

Observação: você pode usar scripts personalizados em transições condicionais. Para obter instruções, consulte o *Guia de Programação do Java*.

Propriedades de atividade manual

As configurações de propriedades específicas para o CA Identity Manager são listadas na tabela a seguir. Essas configurações são definidas nas guias especificadas da caixa de diálogo de propriedades de atividade da Interface de desenho do WorkPoint.

Guia Propriedade	Descrições das propriedades
Recursos	IM Approvers — especificado na lista Incluir. Este script passa informações entre o CA Identity Manager e o servidor do fluxo de trabalho.
Agentes	Nobody Auto Complete — especificado na lista assíncrona e associado ao estado Disponível. Esse script determina se uma atividade deve ser considerada aprovada se não existir nenhum participante da atividade.
Dados do usuário	Definir pares de nome/valor que o CA Identity Manager usa para recuperar participantes da atividade. Opcionalmente, você também pode definir os dados a serem passados para um resolvedor participante personalizado.

Propriedades da transição condicional

Os scripts padrão a seguir são exibidos na guia Condição da caixa de diálogo de propriedades da transição:

IM WorkItem Approved

Retorna verdadeiro se a atividade associada for aprovada. O processo de fluxo de trabalho é transferido para o próximo nó indicado pela transição.

IM WorkItem Rejected

Retorna verdadeiro se a atividade associada for recusada. O processo de fluxo de trabalho é transferido para o próximo nó indicado pela transição.

Tarefas e instâncias de processo

Um *processo fluxo de trabalho* define as etapas que devem ocorrer antes que o CA Identity Manager possa concluir uma tarefa específica. Uma *tarefa* é uma instância de tempo de execução de um processo de fluxo de trabalho.

Por exemplo, o processo de fluxo de trabalho padrão CreateUserApproveProcess define as etapas que devem ocorrer para que um novo usuário seja aprovado. Quando um usuário é realmente criado no CA Identity Manager e a tarefa é enviada para aprovação, uma instância de tarefa de CreateUserApproveProcess é criada na Interface de desenho do WorkPoint.

É possível abrir, exibir e modificar tarefas na Interface de desenho do WorkPoint usando uma interface que é muito semelhante à usada para editar processos de fluxo de trabalho.

Várias tarefas com base no mesmo processo podem existir ao mesmo tempo.

Filtrando tarefas

A Interface de desenho do WorkPoint inclui a filtragem, que permite pesquisar tarefas com base em vários critérios. Por exemplo, é possível pesquisar tarefas que:

- Têm como base um ou mais processos de fluxo de trabalho selecionados
- Têm uma referência de tarefa definida pelo usuário ou uma ID de tarefa exclusiva
- Estão em um determinado estado (como ativo, concluído ou suspenso)
- Foram criadas ou iniciadas dentro de um intervalo de datas especificado

Observação: para obter instruções e informações de referência sobre a filtragem de tarefas, consulte a documentação da Interface de desenho do WorkPoint.

Status e propriedades da tarefa

Quando você abre uma tarefa, o diagrama de fluxo de trabalho da tarefa é exibido. Os nós e transições de atividade de fluxo de trabalho são processados em cor, indicando se foram executados.

Você pode exibir e, em alguns casos, modificar:

- Propriedades de uma tarefa, incluindo informações de participantes e histórico de tarefas
- O estado de uma tarefa aberta, por exemplo, se foi concluída
- Propriedades de nós individuais e transições em uma tarefa

Propriedades de atividade e item de trabalho

Você pode exibir e, em alguns casos, modificar as propriedades da atividade da tarefa e da atividade do processo, incluindo as seguintes:

- Informações de estado de atividades
- Informações de aprovação de atividades
- Tarefa de aprovação (chamada de *item de trabalho* na Interface de desenho do WorkPoint), por exemplo:
  - Se nenhum participante tiver o item de trabalho reservado (o que remove o item das listas de tarefas de outros aprovadores), o estado será Disponível e a ID de usuário de nenhum participante é exibida.
  - Se um participante tiver reservado, mas ainda não tiver concluído o item de trabalho, o estado será Aberto e a ID de usuário do participante e a hora de reserva serão exibidas.
  - Se o item de trabalho tiver sido concluído, o estado será Concluído. A ID de usuário do participante que aprovou ou recusou a tarefa sob controle do fluxo de trabalho será exibida, juntamente com a hora de conclusão.

As propriedades específicas de item de trabalho incluem:

- O nome e o estado atual do item de trabalho
- Informações de histórico de estado, incluindo as IDs de usuário dos participantes responsáveis por determinados estados
- Informações de participantes do item de trabalho autorizados

Observação: para obter mais informações sobre propriedades de tarefa, atividade e item de trabalho, consulte a documentação da Interface de desenho do WorkPoint.

Executando atividades de fluxo de trabalho

Em um processo de fluxo de trabalho, uma atividade manual é executada por uma pessoa designada como um participante da atividade, que aprova ou recusa um evento associado a uma tarefa de aprovação. Os participantes executam essa atividade no CA Identity Manager.

As seguintes operações ocorrem quando uma atividade associada a uma tarefa de aprovação do CA Identity Manager é executada:

1. O CA Identity Manager notifica os participantes.
2. Um participante aprova ou recusa a tarefa.
3. O servidor do fluxo de trabalho conclui a atividade.

Localizar e notificar os participantes

Quando uma atividade de fluxo de trabalho associada a uma tarefa de aprovação do CA Identity Manager é iniciada, o servidor do fluxo de trabalho passa informações sobre participantes da atividade ao CA Identity Manager. Essas informações são definidas nas propriedades da atividade. O CA Identity Manager usa essas informações para recuperar os participantes da atividade e alertá-los de que uma tarefa de aprovação está pendente.

Após identificar os participantes, o CA Identity Manager adiciona um novo item de trabalho (a tarefa de aprovação) a cada lista de tarefas do participante. Como opção, o CA Identity Manager também envia uma notificação por email sobre o novo item de trabalho para cada participante.

Observação: se a propriedade de atividade AAPPROVERS_REQUIRED estiver definida como falsa e nenhum participante for encontrado, a tarefa será considerada como aprovada por padrão.

Observação: um círculo na coluna Status indica que a tarefa de aprovação está disponível para solicitação de qualquer participante. Uma marca de seleção indica que o proprietário da lista de tarefas aceitou a tarefa de aprovação, mas ainda não a concluiu.

Aceitar e executar a tarefa de aprovação

Quando os participantes são encontrados, a atividade não pode ser concluída até que um participante aceite a tarefa de aprovação e aprove ou recuse a tarefa sob controle do fluxo de trabalho.

Um participante aceita uma tarefa de aprovação clicando no nome do item de trabalho no console de atividade de fluxo de trabalho e, em seguida, clicando em Reservar item. (Reservar um item o remove das listas de tarefas de outros aprovadores.)

Uma vez que um participante aceita uma tarefa de aprovação, ele se compromete em tomar a decisão de aprovação ou recusa para a tarefa sob controle do fluxo de trabalho. E, já que vários participantes não podem aceitar a mesma tarefa de aprovação, ela é removida das listas de tarefas de outros participantes.

Depois que um participante aceita uma tarefa de aprovação, uma tela de aprovação é exibida, na qual o participante pode executar uma destas ações:

- Aprovar ou recusar a tarefa sob controle do fluxo de trabalho imediatamente.
- Liberar a tarefa de aprovação para torná-la disponível para outros participantes.
- Fechar a caixa de diálogo e concluir a atividade mais tarde. Para reabrir a caixa de diálogo Aprovar Criar usuário mostrada acima, o participante clica no nome da tarefa de aprovação em sua lista de tarefas.

Além disso, o participante pode atualizar um ou mais campos que podem ser modificados, se houver algum, na tela de aprovação. Você pode permitir a modificação dos campos dessa tela durante a criação da tarefa.

Depois que o participante aprova ou recusa a tarefa sob controle do fluxo de trabalho, a atividade é concluída, e o processo de fluxo de trabalho pode continuar no caminho determinado pelo resultado da atividade, conforme descrito na próxima seção.

O servidor do fluxo de trabalho conclui a atividade

Uma atividade manual é exibida na janela da Interface de desenho com duas ou mais transições condicionais a partir dela.

Cada transição condicional está associada a um script. Quando um participante conclui a atividade, os scripts avaliam o resultado da atividade. O resultado dessas avaliações determina a direção do fluxo do processo.

A ilustração a seguir mostra a atividade Aprovar Criar usuário na Interface de desenho e a respectiva tarefa de aprovação com o mesmo nome no CA Identity Manager.

Quando o participante (ou aprovador) da atividade clica no botão Aprovar ou Recusar no CA Identity Manager:

1. A atividade Aprovar Criar usuário na instância da tarefa do processo termina. Os scripts associados às transições condicionais avaliam o resultado da atividade.

2. A instância da tarefa continua, dependendo de qual transição condicional é avaliada como verdadeira:
   - Se a atividade for aprovada, o script IM WorkItem Approved retornará verdadeiro. O fluxo de trabalho leva a transição IM WorkItem Approved para o próximo nó. Essa atividade automatizada, IM Approve, notificará o CA Identity Manager para executar a tarefa Criar usuário.
   - Se a atividade for recusada, o script IM WorkItem Rejected retornará verdadeiro. O fluxo de trabalho leva a transição IM WorkItem Rejected para o próximo nó de fluxo de trabalho. Essa atividade automatizada, IM Reject, notificará o CA Identity Manager para cancelar a tarefa Criar usuário.

Exibição de tarefa do WorkPoint

É possível exibir o status de tempo de execução de tarefas do WorkPoint no console de usuário a partir de:

- Tarefas de aprovação
- Exibir tarefas enviadas.

Em novos ambientes, todas as tarefas de aprovação incluem a guia Exibir tarefa por padrão. Somente os eventos criados nesta release oferecem suporte à exibição de imagens da tarefa para todas as definições de processo chamadas para o evento ou a tarefa selecionada em Exibir tarefas enviadas. Eventos criados em releases anteriores não oferecem suporte para o recurso Exibição de tarefa do fluxo de trabalho.

Adicionar a guia Exibir tarefa a guias de aprovação existentes

Para tarefas de aprovação, é necessário adicionar a nova guia Exibir tarefa a todas as tarefas existentes para exibir a imagem da tarefa para esse item de trabalho.

Observação: novos ambientes contêm essa guia para todas as tarefas de aprovação.

Para adicionar a guia Exibir tarefa a uma tarefa existente:

1. Na categoria Tarefas administrativas e Função, execute ModifyAdminTask, selecionando Tarefa administrativa, Modificar tarefa administrativa.
2. Clique em Pesquisar e selecione uma tarefa de aprovação (por exemplo, Aprovar Criar usuário) e clique em Selecionar.

   A caixa de diálogo Modificar tarefa administrativa: Aprovar Criar usuário é exibida.
3. Clique na guia Guias e, no menu suspenso, selecione Exibir tarefa (JobView) e clique em Enviar.

   A guia Exibir tarefa é adicionada à tarefa de aprovação.

   Repita a operação para todas as tarefas de aprovação existentes.

Fluxo de trabalho com base em políticas

O fluxo de trabalho com base em políticas permite colocar um evento ou uma tarefa administrativa sob controle do fluxo de trabalho com base na avaliação de uma regra. Isso significa que, em vez de um evento ou uma tarefa administrativa sempre iniciar um processo de fluxo de trabalho, o processo de fluxo de trabalho é executado e gera um item de trabalho somente se uma regra associada ao evento ou uma tarefa administrativa for verdadeira.

Uma *regra de aprovação* é uma condição que determina se um processo de fluxo de trabalho deve ser iniciado. Se for iniciado, o processo de fluxo de trabalho coloca o evento ou uma tarefa administrativa sob controle do fluxo de trabalho, adicionando um item de trabalho à lista de tarefas de um aprovador.

Uma *política de aprovação* é a combinação da regra de aprovação, do tipo de avaliação de regra, da ordem das políticas, da descrição da política e do processo de fluxo de trabalho.

Por exemplo, ao criar um grupo, você pode definir uma política de aprovação que coloca o CreateGroupEvent sob controle do fluxo de trabalho e cria um item de trabalho somente se o novo grupo fizer parte de uma determinada organização pai. Se o novo grupo não fizer parte da organização, o processo de fluxo de trabalho não será executado e nenhum item de trabalho será criado.

Se o evento contiver várias regras, todos os processos de fluxo de trabalho associados ao evento deverão ser aprovados para que o evento seja aprovado. De forma semelhante para uma tarefa administrativa, você pode definir uma política de aprovação que coloca o CreateGroupTask sob controle do fluxo de trabalho e cria um item de trabalho somente se o nome do novo grupo começar com Vendas. Se o nome do novo grupo não começar com Vendas, o processo de fluxo de trabalho não será executado e nenhum item de trabalho será criado.

Você pode criar uma regra de política que é avaliada sempre ou apenas quando um determinado atributo de um objeto gerenciado é alterado, por exemplo, o valor do salário de um funcionário.

Observação: em versões anteriores do fluxo de trabalho com base em políticas, se algum aprovador fizesse qualquer alteração nos atributos, eles eram enviados novamente para aprovação. Com aprovação ou recusa em nível de atributo, alterações em qualquer estágio são aprovadas apenas uma vez. O item de trabalho nunca é enviado novamente para aprovação, mesmo que o atributo contido na regra seja modificado. Depois que um aprovador aprovar uma mudança, só verá o item de trabalho novamente quando uma nova mudança for enviada ou a tarefa for reenviada.

Mais informações:

Fluxo de trabalho em nível de evento (na página 266)
Fluxo de trabalho em nível de tarefa (na página 263)
Ordem das políticas (na página 318)
Avaliação de regra (na página 316)

Objetos de regras

Um administrador do CA Identity Manager pode criar políticas de aprovação para um evento ou tarefa administrativa com base nos seguintes objetos. Os seguintes são os objetos para um evento caso eles se apliquem a um determinado evento e estejam presentes durante a execução do evento:

- **Iniciador da tarefa** - O administrador do CA Identity Manager que executa a tarefa.
- **Objeto principal do evento** - O objeto principal associado ao evento.
- **Objeto secundário do evento** - O objeto secundário associado ao evento relativo ao objeto principal.

Os seguintes são os objetos para uma tarefa administrativa:

- **Objeto principal da tarefa** - O objeto principal associado à tarefa.
- **Iniciador da tarefa** - O administrador do CA Identity Manager que executa a tarefa.
- **Violações da política de identidade** - Para as violações da política de identidade, as regras têm como base o nome da política de identidade que ocasionou a violação, por exemplo, Nome da política EQUALS TitlePolicy. A mensagem de violação será exibida na guia Detalhes da tarefa da tela de aprovação, que é a mesma guia Detalhes da tarefa de Exibir tarefas enviadas. A mensagem de violação de segregação de tarefas é exibida em um novo cabeçalho de seção denominado Violação da política de identidade. Um aprovador pode exibir essas mensagens e decidir se deseja aprovar ou recusar a tarefa.

  Observação: se uma regra tiver como base a Violação da política de identidade, a avaliação será diferente da avaliação normal. Uma vez aprovada, a violação de segregação de tarefas não chama nenhum outro processo de fluxo de trabalho, mesmo que existam outras regras que possam ser avaliadas como verdadeiras para essa determinada violação de segregação de tarefas. Com a avaliação normal, todos os processos de fluxo de trabalho serão chamados um por um, mesmo que a mesma alteração tenha sido aprovada por outros aprovadores.

Avaliação de regra

As regras de políticas podem ser avaliadas para um evento nas duas maneiras a seguir:

- Sempre

  Uma política com o tipo de avaliação Sempre é chamada se a política for avaliada como verdadeira, independentemente de quaisquer atributos contidos na política forem alterados ou não. Na tela de aprovação de um item de trabalho que foi gerado como resultado do tipo de avaliação de política Sempre, um aprovador pode alterar qualquer atributo editável na tela de aprovação.

  Observação: se o aprovador clicar no botão Recusar, o evento será recusado.

  Para Sempre, o comportamento do tipo de avaliação é o mesmo para tarefas e eventos.

- Somente se um atributo especificado na condição de aprovação for alterado

  Uma política com o tipo de avaliação OnChange é chamada apenas quando a política é avaliada como verdadeira ou quando algum dos atributos contidos na política for alterado. Na tela de aprovação de um item de trabalho que foi gerado como resultado de uma política com o tipo de avaliação OnChange, o aprovador pode alterar o valor desses atributos contidos na política apenas se eles tiverem uma permissão de leitura/gravação para a tela de aprovação. Todos os outros atributos que existem na tela de aprovação têm permissões somente leitura.

  Observação: para o fluxo de trabalho em nível de evento, caso o aprovador clique no botão Recusar, somente as alterações feitas nos atributos contidos na política de aprovação serão recusadas, e a próximo política de aprovação na ordem será avaliada.

  Para o fluxo de trabalho em nível de tarefa, se o aprovador clicar no botão Recusar, o evento será recusado.

  Observação: para os dois tipos de regra OnChange e Sempre, quando um aprovador desfaz todas as alterações e clica em Aprovar, as alterações são recusadas e auditadas de maneira correspondente.

Mais informações:

Ordem das políticas (na página 318)
Objetos de regras (na página 315)

Exemplo de avaliação de regra

Considere as seguintes políticas, todas para ModifyUserEvent na tarefa administrativa Modificar usuário:

Diretiva	Regra	Avaliação
Policy1	Usuário onde (ID de usuário = Smith01)	Sempre
Policy2	Usuário onde (Cargo = Gerente)	Quando o atributo Cargo é alterado
Policy3	Usuário onde (Salário >= 80.000)	Quando o atributo Salário é alterado

A Policy1 é avaliada sempre que o administrador chama a tarefa Modificar usuário para o usuário Smith01, independentemente de qual atributo foi alterado.

A Policy2 é avaliada quando o administrador chama a tarefa Modificar usuário para alterar o atributo Cargo para qualquer objeto de usuário. A Policy2 será verdadeiro se Cargo for alterado para Gerente.

A Policy3 é avaliada quando o administrador chama a tarefa Modificar usuário para alterar o atributo Salário para qualquer objeto de usuário. A Policy3 será verdadeiro se Salário for alterado para 80.000 ou mais.

Neste exemplo, se um administrador usar a tarefa Modificar usuário para alterar o atributo Cargo para Gerente para o usuário Smith01, a Policy1 e a Policy2 serão avaliadas como verdadeiras, e seus respectivos processos de fluxo de trabalho serão iniciados. Neste caso, a ordem de prioridade padrão se aplica.

A avaliação de regra condicional permite que um aprovador de um item de trabalho altere um atributo que afeta outro item de trabalho do mesmo evento enquanto o evento ainda estiver pendente. Isso só é possível em políticas de aprovação com um tipo de avaliação Sempre. No exemplo anterior, se um administrador alterar um atributo para o usuário Smith01, Policy1 será verdadeiro e gerará um item de trabalho. Ao aprovar o item de trabalho gerado pela Policy1, esse aprovador pode, na mesma tela de aprovação, alterar o atributo Salário de Smith01. Nesse caso, o novo valor de Salário para Smith01 determina se Policy3 gerará um item de trabalho para a mesma instância de ModifyUserEvent. Se o aprovador alterar o salário para 90.000, Policy3 gerará um novo item de trabalho que deverá ser aprovado antes que o evento seja aprovado. A ordem de prioridade padrão se aplica.

Ordem das políticas

Todas as políticas de aprovação contêm um campo Ordem das políticas no qual um valor inteiro positivo, ordenado do mais baixo para o mais alto, especifica a prioridade. A prioridade de cada política determina o seguinte:

- A ordem na qual as regras de aprovação são avaliadas
- Para regras avaliadas como verdadeiras, a ordem em que os processos de fluxo de trabalho são iniciados

Uma política com um valor de número inteiro menor tem uma prioridade mais alta e sua regra é avaliada antes de uma política com um valor de número inteiro maior. Para todas as políticas de um evento ou tarefa administrativa que forem avaliadas como verdadeiras, a política com a prioridade mais alta inicia seu processo de fluxo de trabalho primeiro.

Exemplo de ordem das políticas

Esse exemplo simples demonstra como funciona a ordenação de políticas. Neste exemplo, suponha que as regras de política são sempre avaliadas.

Se o evento contiver várias políticas que são sempre avaliadas, para que o evento seja aprovado, todas as políticas devem ser aprovadas. No entanto, se uma política associada ao evento que tiver um tipo de avaliação de política ALWAYS for recusada, o evento será recusado.

Observação: se uma política associada ao evento tiver um tipo de avaliação OnChange, apenas as alterações associadas aos atributos contidos nessa política serão recusadas. O evento em si não será recusado e a próximo política na fila será avaliada.

Neste exemplo, Policy1, Policy2 e Policy3 têm o tipo de avaliação de política ALWAYS. Policy1 é avaliada como falsa, o processo de fluxo de trabalho chamado Process1 não é executado e nenhum item de trabalho é gerado para o User1. O controle do evento passa imediatamente para a Policy2. A Policy2 e a Policy3 são avaliadas como verdadeiras. Devido à sua prioridade mais alta, o Process2 de fluxo de trabalho é executado primeiro e gera um item de trabalho para o User2.

Se o User2 aprovar o item de trabalho, o Process3 de fluxo de trabalho é executado e gera um item de trabalho para o User3, que deve aprovar o item de trabalho para o evento para ser aprovado. Essas ações são mostradas na seguinte tabela:

Prioridade	Diretiva	Resultado	Fluxo de trabalho	Aprovador	Ação
1	Policy1	Falso	Process1	User1	—
2	Policy2	Verdadeiro	Process2	User2	Aprovado

Prioridade	Diretiva	Resultado	Fluxo de trabalho	Aprovador	Ação
3	Policy3	Verdadeiro	Process3	User3	Aprovado

No entanto, se o User2 recusar o item de trabalho, o evento será recusado e nenhum item de trabalho será gerado para o User3, conforme mostrado na seguinte tabela:

Prioridade	Diretiva	Resultado	Fluxo de trabalho	Aprovador	Ação
1	Policy1	Falso	Process1	User1	—
2	Policy2	Verdadeiro	Process2	User2	Recusado
3	Policy3	Verdadeiro	Process3	User3	—

Em seguida, Policy1, Policy2 e Policy3 têm o tipo de avaliação de política ONCHANGE. Se o User2 recusar o item de trabalho, apenas as alterações associadas aos atributos contidos na Policy2 serão recusadas. A Policy3 será avaliada e o Process3 de fluxo de trabalho será executado e gerará um item de trabalho para o User3. Se o User3 recusar o item de trabalho, o evento será recusado, pois todas as alterações feitas nesse evento foram recusadas. Se o User3 aprovar o item de trabalho, o evento será aprovado e as alterações de atributo contidas na Policy3 serão mantidas.

Prioridade	Diretiva	Resultado	Fluxo de trabalho	Aprovador	Ação
1	Policy1	Falso	Process1	User1	—
2	Policy2	Verdadeiro	Process2	User2	Recusado
3	Policy3	Verdadeiro	Process3	User3	Aprovado

Descrição da diretiva

Um atributo de descrição de sequência de caracteres opcional e não pesquisável foi adicionado ao objeto gerenciado da Política de aprovação e aparece nos itens de trabalho resultantes.

Número máximo de caracteres suportados: 255 caracteres

Você pode inserir informações de pacote/chave no formato a seguir para a descrição:

```
$ (bundle=<fully qualified resource bundles name> : key=<key>)
```

Políticas de aprovação e atributos com vários valores

Se uma regra tivesse sido definida para um atributo com vários valores, não era possível dizer que essa regra deveria se aplicar apenas em valores adicionados ou removidos recentemente do atributo com vários valores. Ao examinar o tipo de avaliação de política de uma regra com base em um atributo com vários valores, isso é possível agora. Se o tipo de avaliação de regra for OnChange, essa regra só poderá ser aplicada em valores adicionados ou removidos recentemente do atributo com vários valores e não em todos os valores desse atributo.

Se a regra precisar ter como base todos os valores do atributo com vários valores, independentemente de terem sido adicionados ou removidos recentemente, o tipo de avaliação para essa regra deve ser Sempre.

As alterações feitas nos atributos com vários valores estão realçadas na tela de perfil com um ícone Desfazer. Se uma regra tiver sido avaliada como verdadeira, pois um novo valor foi adicionado ou removido de um atributo com vários valores, o aprovador que aprova essa alteração verá TODOS os valores contidos no atributo com vários valores. Clicar no ícone Desfazer reverte o valor desse atributo para seu valor original. Se um aprovador desejar ver os valores removidos, clicar no ícone Desfazer mostra o conjunto de valores originais.

Clicar no ícone Refazer mostra o novo conjunto de valores, permitindo ao aprovador diferenciar quais foram os valores removidos e quais foram os valores adicionados. Clicar no botão Aprovar aprova todas as alterações nesse atributo com vários valores. Clicar no botão Recusar recusa todas as alterações feitas nesse atributo com vários valores. Todas as outras regras referentes a esse atributo com vários valores não são avaliadas, a não ser que exista um novo delta de valores para esse atributo com vários valores.

Observação: no caso de regras com base em atributos com vários valores, os valores contidos nesse atributo são os valores reais e não os valores de exibição. Por exemplo, o valor de exibição para o Estado MA é Massachusetts. Ao criar uma política de aprovação que se baseia no atributo de Estado, a regra deve se parecer com Estado = MA.

Considere as seguintes políticas de exemplo, todas para ModifyUserEvent na tarefa administrativa Modificar usuário:

Diretiva	Regra	Avaliação
Policy1	Usuário onde (Estado = MA)	OnChange
Policy2	Usuário onde (Estado = DC)	Sempre

Policy1 é avaliada sempre que um administrador chama a tarefa ModifyUser para alterar o atributo de Estado e retorna verdadeiro se o valor MA tiver sido adicionado ou removido do atributo de Estado.

Policy2 é avaliada sempre que o administrador chama a tarefa Modificar usuário para um usuário cujo Estado contém o valor DC.

Atributos realçados como alterados nas telas de aprovação de fluxo de trabalho

Em uma tela de aprovação, atributos adicionais podem aparecer realçados como alterados, mesmo que um administrador não tenha feito alterações neles na tarefa original. Isso ocorre porque a tela pode conter scripts que podem alterar os valores de vários atributos contidos na tela como parte da inicialização ou validação de tela para uma alteração de algum outro atributo.

Exemplos de políticas

Os seguintes exemplos de casos de uso de negócios a seguir demonstram como é possível aplicar políticas de aprovação de fluxo de trabalho a um evento:

Exemplo 1:

Caso de uso - Um administrador modifica uma conta de um banco de dados relacional pertencente a um funcionário.

Tarefa administrativa – ModifyMSSQLAccount

Evento – ModifyMSSQLAccountEvent

Regra de aprovação - Usuário onde (Cargo = RDBAcctManager)

Processo de fluxo de trabalho - ModAcctApproval (processo de fluxo de trabalho personalizado)

Objeto - Iniciador da tarefa

Avaliação - Sempre avalia a regra

Exemplo 2:

Caso de uso - Um administrador modifica o salário de um funcionário para refletir um novo aumento.

Tarefa administrativa - Modificar usuário

Evento - ModifyUserEvent

Regra de aprovação - Usuário onde (Salário >= 100.000)

Processo de fluxo de trabalho - SalaryChangeApproval (processo de fluxo de trabalho personalizado)

Objeto - Objeto principal do evento (usuário)

Avaliação – Avaliar apenas quando o atributo Salário for alterado

Exemplo 3:

Caso de uso - Um administrador adiciona um usuário ao grupo Prestadores de serviço quando o cargo desse usuário é alterado para Prestador de serviço. Esse exemplo pode ser dividido nas duas políticas de aprovação a seguir:

Política 1:

Tarefa administrativa - Modificar usuário

Evento - ModifyUserEvent

Regra de aprovação - Usuário onde (Cargo = Prestador de serviço)

Processo de fluxo de trabalho - SingleStepApproval (modelo de processo padrão)

Objeto - Objeto principal do evento (usuário)

Avaliação – Avaliar apenas quando o atributo Cargo for alterado

Política 2:

Tarefa administrativa - Modificar grupo (ou Modificar associação ao grupo)

Evento - AddToGroup

Regra de aprovação - Grupo onde (Nome do grupo = Prestadores de serviço)

Processo de fluxo de trabalho - SingleStepApproval (modelo de processo padrão)

Objeto - Objeto secundário do evento (grupo)

Avaliação - Sempre avalia a regra

Os seguintes exemplos de casos de uso de negócios a seguir demonstram como é possível aplicar políticas de aprovação de fluxo de trabalho a uma tarefa:

Exemplo 1:

Caso de uso - Um administrador modifica uma conta do Active Directory que pertence a um funcionário.

Tarefa administrativa – ModifyActiveDirectoryAccount

Objeto - Iniciador da tarefa

Regra de aprovação - Usuário onde (Cargo = ActiveDirectoryManager)

Processo de fluxo de trabalho - Aprovação de etapa única

Avaliação - Sempre avalia a regra

Exemplo 2:

Caso de uso - Um administrador modifica um usuário cujo código de funcionário é HighSecurity.

Tarefa administrativa - Modificar usuário

Objeto - Objeto principal da tarefa

Regra de aprovação - Usuário onde (Número do funcionário = HighSecurity)

Processo de fluxo de trabalho - Aprovação de etapa única

Avaliação - Sempre avalia a regra

Exemplo 3:

Caso de uso - Um administrador modifica um usuário para atribuir as funções administrativas CheckApprover e CheckSigner.

Tarefa administrativa - Modificar usuário

Objeto - Violação da política de identidade

Regra de aprovação - IdentityPolicy onde (Nome = CheckRoles)

Processo de fluxo de trabalho - Aprovação de etapa única

Avaliação - Sempre avalia a regra

Como configurar o fluxo de trabalho com base em políticas para eventos

O procedimento para configurar o fluxo de trabalho com base em políticas é semelhante ao processo de configuração do fluxo de trabalho em nível de evento, com as etapas adicionais de definir as políticas de aprovação que determinam se o fluxo de trabalho será executado.

Para configurar o fluxo de trabalho com base em políticas:

1. No console de usuário, selecione Funções e tarefas, Tarefa administrativa, Modificar (ou Criar) tarefa administrativa.

   Uma tela Selecionar tarefa administrativa é exibida.

2. Pesquise a tarefa que desejada sob controle do fluxo de trabalho e clique em Selecionar.

   A tela Modificar (ou Criar) tarefa administrativa é exibida.

3. Na guia Perfil, verifique se Ativar fluxo de trabalho está marcada.

4. Na guia Eventos, selecione um evento para mapear para um modelo de processo.

   A tela de mapeamento do fluxo de trabalho é exibida.

5. Selecione o botão de opção Com base na política e, em seguida, clique em Adicionar.

   A tela Política de aprovação é exibida.

6. Configure uma política de aprovação (na página 327).

7. Configure resolvedores participantes, conforme exigido pelo seu processo de fluxo de trabalho selecionado.

   As solicitações do participante são adicionadas ao processo.

8. Clique em OK.

   O CA Identity Manager salva a configuração do fluxo de trabalho em nível de evento.

9. Clique em Enviar.

   O CA Identity Manager processa a modificação da tarefa.

Observação: a lista Processo do fluxo de trabalho inclui os processos para uso com o método do modelo e o método do WorkPoint:

- Quando um processo do método do modelo é selecionado (SingleStepApproval, TwoStageApprovalProcess ou EscalationApproval), a página expande para ativar a configuração de resolvedor participante.
- Quando um processo do método do WorkPoint é selecionado, a página não é expandida. Resolvedores participantes são configurados na Interface de desenho do WorkPoint.

Mais informações:

Resolvedores participantes: Método do WorkPoint (na página 295)
Como configurar uma política de aprovação (na página 327)

Como configurar o fluxo de trabalho com base em políticas para tarefas

O procedimento para configurar o fluxo de trabalho com base em políticas para tarefas é semelhante ao processo de configuração do fluxo de trabalho em nível de tarefa, com as etapas adicionais de definir as políticas de aprovação que determinam se o fluxo de trabalho será executado.

Para configurar o fluxo de trabalho com base em políticas:

1. No console de usuário, selecione Funções e tarefas, Tarefa administrativa, Modificar (ou Criar) tarefa administrativa.

   Uma tela Selecionar tarefa administrativa é exibida.

2. Pesquise a tarefa que desejada sob controle do fluxo de trabalho e clique em Selecionar.

   A tela Modificar (ou Criar) tarefa administrativa é exibida.

3. Na guia Perfil, verifique se Ativar fluxo de trabalho está marcada

4. Na guia Perfil, clique no ícone em forma de lápis ao lado do campo Processo de fluxo de trabalho

   A tela de mapeamento do fluxo de trabalho é exibida.

5. Selecione o botão de opção Com base na política e, em seguida, clique em Adicionar.

   A tela Política de aprovação é exibida.

6. Configure uma política de aprovação (na página 327).

7. Configure resolvedores participantes, conforme exigido pelo seu processo de fluxo de trabalho selecionado.

   As solicitações do participante são adicionadas ao processo.

8. Clique em OK.

   O CA Identity Manager salva a configuração do fluxo de trabalho em nível de tarefa.

9. Clique em Enviar.

   O CA Identity Manager processa a modificação da tarefa.

Observação: a lista Processo de fluxo de trabalho inclui os processos para uso com o método de modelos para o fluxo de trabalho com base em políticas em nível de tarefa:

- Quando um processo do método de modelos é selecionado (SingleStepApproval ou TwoStageApprovalProcess), a página expande para ativar a configuração de resolvedor participante.

Mais informações

Como configurar uma política de aprovação (na página 327)

Como configurar uma política de aprovação

A configuração de uma política de aprovação para um evento ou tarefa envolve as etapas a seguir.

1. Selecione um objeto para testar.
2. Defina uma regra de aprovação para o objeto.
3. Para os objetos principais, decida se essa é uma avaliação condicional.
4. Especifique a ordem da avaliação da política.
5. Configure um processo de fluxo de trabalho para executar se a regra for avaliada como verdadeira.

Para configurar uma política de aprovação:

1. Na tela Política de aprovação, selecione um objeto para que a regra teste na lista suspensa.

   A tela é alterada para refletir sua seleção.
2. Na nova lista suspensa ao lado do nome do objeto, selecione um modelo de expressão de condição.

   A tela é alterada para refletir sua seleção.
3. Crie e edite a expressão de condição, conforme necessário.
4. Selecione o botão de opção Avaliação de regra para indicar se a regra é avaliada sempre ou apenas se um atributo na condição de aprovação for alterado.
5. Digite um valor inteiro positivo para especificar a ordem de avaliação das políticas (caso haja várias políticas para o evento).
6. Selecione e configure o processo de fluxo de trabalho que é executado quando a regra é avaliada como verdadeira.
7. Clique em OK para salvar a política de aprovação.

Mais informações:

Como configurar o fluxo de trabalho em nível de evento (na página 268)
Como configurar o fluxo de trabalho com base em políticas para eventos (na página 324)
Como configurar o fluxo de trabalho com base em políticas para tarefas (na página 326)

Status do fluxo de trabalho com base em políticas

Os administradores do CA Identity Manager podem exibir o status de tarefas que contêm políticas de aprovação de fluxo de trabalho usando as seguintes ferramentas padrão do sistema:

- Guia Exibir tarefas enviadas
- Guia Histórico do usuário
- Relatórios e logs

As informações de tarefa enviada e do histórico da tarefa incluem:

- Informações de tarefas e eventos
- Informações do fluxo de trabalho e da regra de aprovação
- Resultados da avaliação da regra de aprovação

Consulte a documentação da guia Sistema para obter as descrições do histórico de tarefas enviadas.

Mais informações:

Descrição do status do evento (na página 572)
Status da tarefa no CA Identity Manager (na página 565)

Mapeamento de fluxo de trabalho global com base em políticas em nível de evento

Um evento pode ser mapeado para um processo de fluxo de trabalho no Management Console, ou ser associado a políticas de aprovação de fluxo de trabalho com base em políticas em uma tarefa específica. A nova tarefa Configurar política global para o fluxo de trabalho com base em eventos permite que os administradores configurem o mapeamento de fluxo de trabalho com base em políticas para eventos em nível de ambiente. Ao contrário de configurar um fluxo de trabalho com base em políticas para um evento em uma tarefa administrativa, os mapeamentos configurados de fluxo de trabalho com base em políticas são aplicados a todas as tarefas que geram o evento.

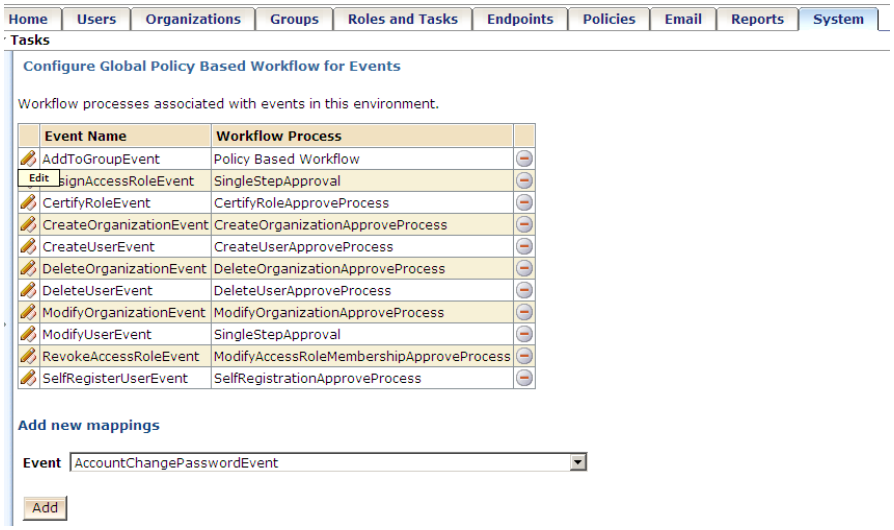
Observação: a tarefa Configurar política global para o fluxo de trabalho com base em eventos funciona somente quando o fluxo de trabalho está ativado. Se essa tarefa for executada quando o fluxo de trabalho estiver desativado, um erro será gerado.

Essa tarefa foi adicionada à guia Sistema. Quando uma tarefa é enviada, o processo de fluxo de trabalho de cada evento nesta tarefa é recuperado da seguinte forma:

Qualquer fluxo de trabalho configurado para o evento dessa tarefa administrativa terá precedência. Um evento pode ser configurado para o fluxo de trabalho com base em políticas ou sem base em políticas. Se o fluxo de trabalho com base em políticas for configurado para o evento dessa tarefa administrativa, o processo de fluxo de trabalho associado à política será chamado. Se nenhuma regra for correspondente, nenhum fluxo de trabalho será chamado para o evento. Da mesma forma, se o fluxo de trabalho sem base em políticas for configurado para o evento dessa tarefa administrativa, o processo de fluxo de trabalho associado à política será chamado. Se nenhum fluxo de trabalho tiver sido configurado para o evento dessa tarefa administrativa, a configuração do fluxo de trabalho global para esse evento terá precedência.

Tela de tarefa Configurar política global para o fluxo de trabalho com base em eventos

A tarefa de Configurar política global para o fluxo de trabalho com base em eventos permite que um administrador configure um fluxo de trabalho com base em política ou que não se baseia em nenhuma política para todos os eventos no ambiente atual. Clicar na tarefa exibe o mapeamento do evento padrão para definições de processo do fluxo de trabalho. Cada mapeamento do evento pode ser modificado ou excluído, e novos mapeamentos de eventos podem ser adicionados para eventos que não foram configurados.



Os campos nessa tela são os seguintes:

Processos de fluxo de trabalho associados aos eventos neste ambiente.

Especifica os processos de fluxo de trabalho associados a políticas de aprovação.

Adicionar novos mapeamentos

Especifica uma política de aprovação para mapear para um processo de fluxo de trabalho.

Botão Adicionar

Adiciona o novo mapeamento.

Adicionar ou modificar um mapeamento abre a tela Mapeamento de fluxo de trabalho, em que você pode selecionar os mapeamentos de processo e as políticas de aprovação. O comportamento é o mesmo que o da configuração do fluxo de trabalho em nível de evento. Clicar no botão Adicionar na página Mapeamento de fluxo de trabalho exibe uma outra página, na qual é possível configurar uma política de aprovação.

Mais informações

Como configurar o fluxo de trabalho com base em políticas para eventos (na página 324)
Como configurar uma política de aprovação (na página 327)

Solicitações online

O CA Identity Manager permite criar tarefas de solicitação online de finalidade geral. A implementação de solicitação online padrão é composta por um conjunto de tarefas relacionadas para solicitações de automodificação e solicitações de modificação de usuário administrativo. No entanto, o recurso de solicitação online pode ser facilmente implementado para outras tarefas de solicitação do CA Identity Manager.

Uma solicitação de modificação de usuário aciona um processo de fluxo de trabalho que gera um item de trabalho. Os participantes do fluxo de trabalho podem aprovar e implementar o item de trabalho, ou recusá-lo. O usuário que inicia a tarefa insere uma descrição da solicitação no editor de histórico, uma área do texto que o CA Identity Manager usa para manter um histórico da solicitação. Esse editor de histórico pode ser configurado para permitir que os participantes deixem comentários sobre a ação que executam no item de trabalho. Esses comentários tornam-se parte do histórico cumulativo do item de trabalho.

Ações novas além (ou no lugar) das ações de aprovação ou recusa padrão também são possíveis. Por exemplo, um participante corporativo pode esclarecer ou comentar sobre a solicitação, e um participante técnico pode implementar a solicitação. Essas novas atividades podem ser representadas por novos botões de ação de fluxo de trabalho como Esclarecer e Implementar, que você pode adicionar aos botões padrão Aprovar e Recusar na tarefa de aprovação.

Tarefas de solicitação online

Há cinco tarefas que trabalham juntas para formar a implementação padrão de solicitação online. Essas tarefas demonstram o uso de solicitações personalizadas, histórico e botões de ação do fluxo de trabalho:

Observação: as tarefas administrativas (Alterar minha conta e Criar solicitação online) são configuradas por padrão para o fluxo de trabalho em nível de evento usando o modelo de processo de consulta.

Alterar minha conta

Esta é uma tarefa administrativa de automodificação que cria uma solicitação de alteração de conta de usuário. Possui uma guia Solicitação com um editor de histórico para descrever a solicitação e uma guia Perfil com detalhes de usuário somente leitura.

Criar solicitação online

Esta é uma tarefa administrativa de modificação de usuário que cria uma solicitação de alteração de conta para um determinado usuário. Possui uma guia Solicitação com um editor de histórico para descrever a solicitação e uma guia Perfil da entidade com detalhes de usuário somente leitura.

Aprovar solicitação online

Esta é uma tarefa de aprovação que permite ao participante corporativo aprovar ou recusar a tarefa, ou solicitar o esclarecimento da tarefa. Esta tarefa possui uma guia Solicitação com uma exibição de histórico e um editor de histórico para consultas ou comentários, uma guia Perfil da entidade somente leitura e uma guia Destinatários.

Esclarecer solicitação online

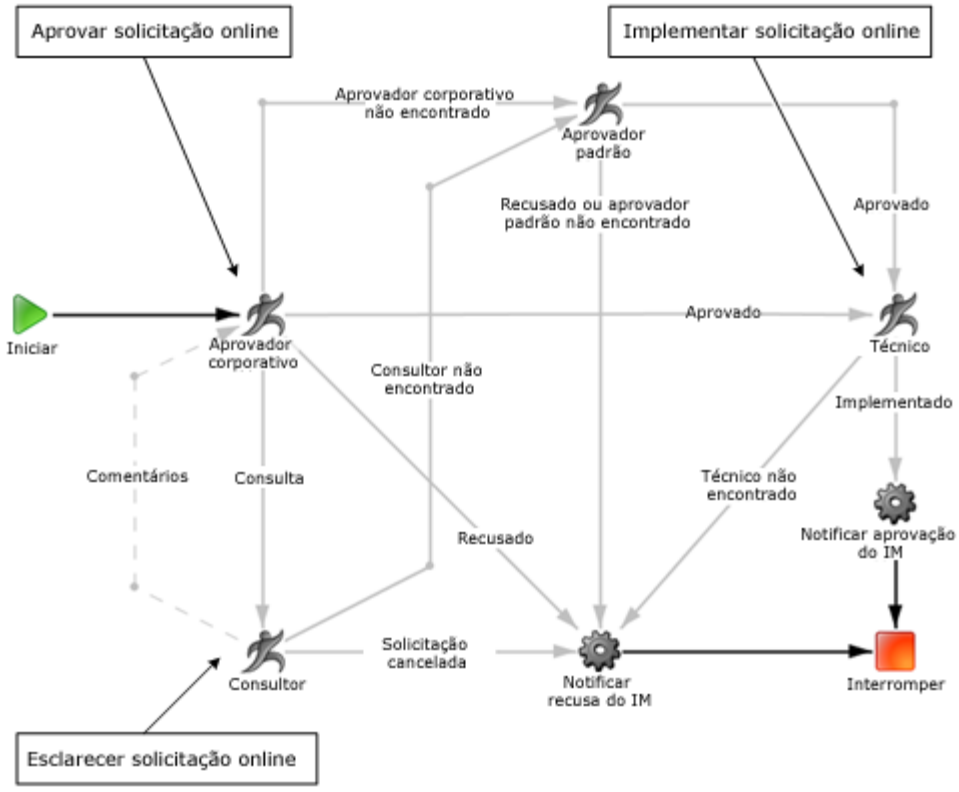
Esta é uma tarefa de aprovação que permite ao participante de esclarecimento responder a uma solicitação de esclarecimento, e devolve a tarefa para o participante corporativo para aprovação. Possui uma guia Solicitação com uma exibição de histórico e um editor de histórico para comentários e uma guia Perfil da entidade somente leitura.

Implementar a solicitação online

Esta é uma tarefa de aprovação que permite ao participante técnico implementar a tarefa e adicionar um comentário ao histórico de tarefas. Possui uma guia Implementar solicitação com uma exibição de histórico e um editor de histórico para comentários, uma guia Perfil da entidade somente leitura e uma guia Destinatários.

Processar da solicitação online

As tarefas da solicitação online são controladas por um modelo de processo de fluxo de trabalho chamado Processo de consulta, mostrado como é exibido na Interface de desenho do WorkPoint:



O Processo de consulta inclui quatro atividades manuais que correspondem às tarefas de aprovação na implementação da solicitação online:

- Uma atividade para o aprovador corporativo, que recusa, aprova e transmite o item de trabalho ao técnico ou solicita o esclarecimento do consultor.
- Uma atividade para o consultor, que esclarece o item de trabalho e o envia de volta ao aprovador corporativo.
- Uma atividade para um aprovador padrão, que assume a responsabilidade caso o aprovador corporativo ou o consultor não possa ser contatado.
- Uma atividade para o técnico, que implementa a solicitação e conclui o item de trabalho.

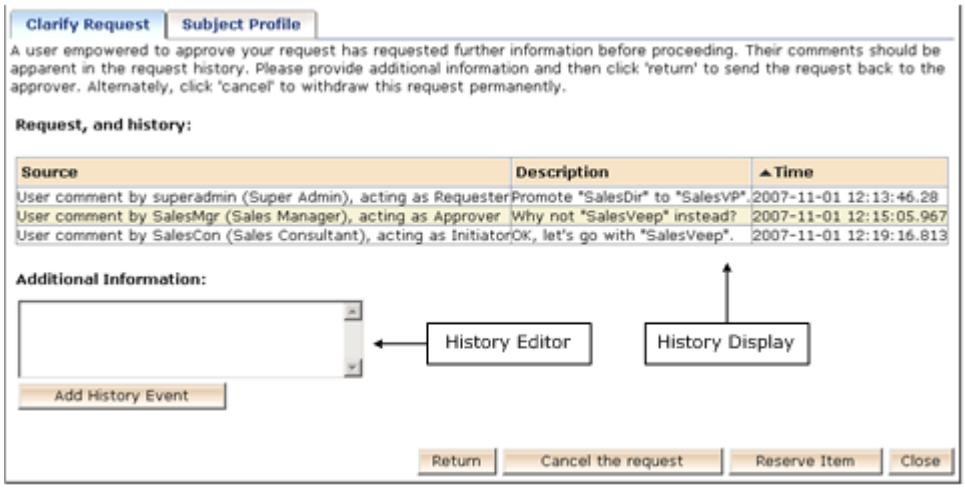
Histórico da solicitação online

O recurso de histórico da solicitação online permite aos participantes criar um registro de ações dos itens de trabalho. Como a responsabilidade pelo item de trabalho passa de um participante para outro, o novo participante pode revisar o histórico do item de trabalho antes de executar qualquer ação.

Dois controles são usados para implementar o histórico da solicitação online:

- A exibição de histórico é uma tabela somente leitura que contém detalhes de entradas anteriores no histórico em ordem cronológica.
- O editor de histórico é uma caixa de texto para a criação de entradas no histórico. Também possui um botão opcional para adicionar várias entradas sem enviar o item de trabalho.

Por padrão, o editor de histórico e a exibição de histórico são exibidos na guia Solicitação para todas as tarefas associadas à implementação da solicitação online. A tela a seguir mostra os controles do histórico na tarefa Esclarecer solicitação online:



Usando solicitações online

As etapas a seguir descrevem o processo de fluxo de trabalho da solicitação online. Em cada etapa, a tarefa IM gerada é exibida entre parênteses. Em cada etapa do processo, o participante pode adicionar um comentário no editor de histórico. Esse comentário é exibido na exibição de histórico para o próximo participante no processo de fluxo de trabalho.

1. O iniciador de tarefas solicita uma modificação para um usuário do CA Identity Manager (Criar solicitação online).
2. O aprovador corporativo recebe um item de trabalho e executa uma das ações a seguir:
   - Aprova o item de trabalho (Aprovar solicitação online).
   - Recusa o item de trabalho e encerra o processo de fluxo de trabalho. Nenhuma nova tarefa é gerada.
   - Solicita um esclarecimento do consultor (Esclarecer solicitação online).
3. O consultor recebe um item de trabalho e executa uma das ações a seguir:
   - Adiciona um esclarecimento e retorna o item de trabalho para o aprovador corporativo. Nenhuma nova tarefa é gerada.
   - Cancela o item de trabalho e encerra o processo de fluxo de trabalho. Nenhuma nova tarefa é gerada.
4. O técnico recebe um item de trabalho e implementa a solicitação (Implementar a solicitação online).

Botões de ação do fluxo de trabalho

As tarefas de aprovação no CA Identity Manager historicamente possuem os botões de ação Aprovar e Recusar que são exibidos nas telas correspondentes de item de trabalho. Os botões de ação do fluxo de trabalho permitem aos administradores ampliar a funcionalidade das tarefas e fluxos de trabalho do CA Identity Manager adicionando botões de ação a tarefas de aprovação e removendo ou modificando os botões existentes. (Os botões padrão Aprovar e Recusar são implementados da mesma forma que os botões de ação do fluxo de trabalho personalizados).

Por exemplo, um processo de fluxo de trabalho pode exigir uma ação que permite aos participantes de nível médio escalonar alguns casos para um participante mais sênior para aprovação ou recusa final. Esses participantes de nível médio podem adicionar um comentário ou recomendação usando o editor de histórico e, em seguida, enviar o item de trabalho para que o participante sênior revise e aprove ou recuse.

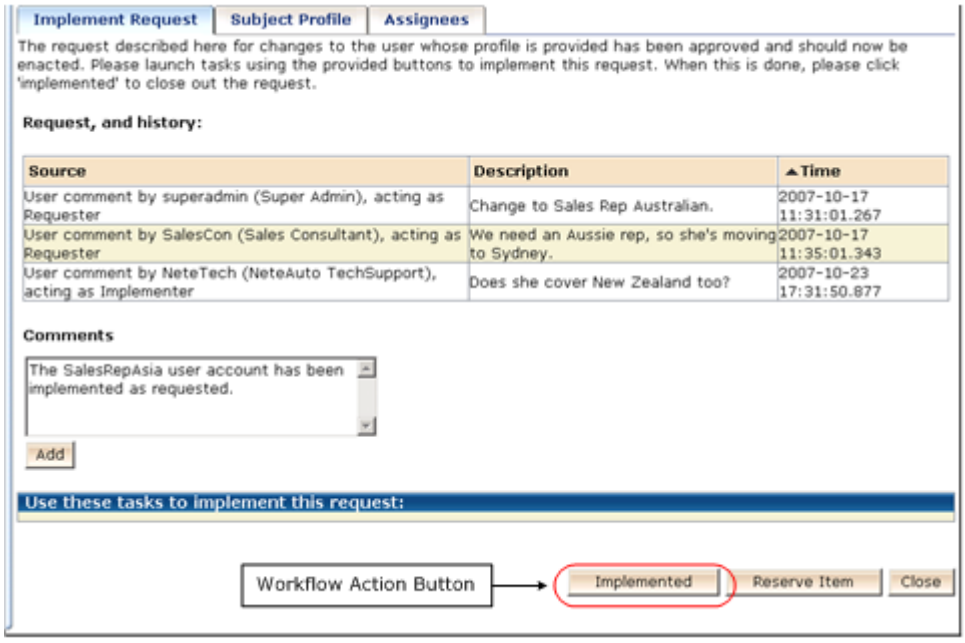
A adição ou remoção de botões de ação do fluxo de trabalho exige alterações apropriadas no processo de fluxo de trabalho do WorkPoint que fornece a lógica de negócios para lidar com essas novas ações.

Mais informações:

Configuração de botões no CA Identity Manager (na página 336)
Botões de fluxo de trabalho em tarefas de aprovação (na página 336)
Configuração de botões na Interface de desenho do WorkPoint (na página 339)

Botões de fluxo de trabalho em tarefas de aprovação

Os botões de ação do fluxo de trabalho correspondem a nós de transição que não apontam para os nós de atividade manual em um diagrama de processos do WorkPoint. Por exemplo, no Processo de consulta, o nó de atividade Técnico tem uma transição única chamada Implementado. Corresponde ao botão Implementado na tarefa de aprovação Implementar a solicitação online, mostrado na figura a seguir:



Observação: os botões Reservar item e Fechar são governados pelas lógicas de programação do CA Identity Manager e não estão sob controle do fluxo de trabalho.

Mais informações:

Botões de ação do fluxo de trabalho (na página 335)
Configuração de botões no CA Identity Manager (na página 336)

Configuração de botões no CA Identity Manager

Para configurar um botão de ação do fluxo de trabalho, clique no botão chamado Botões de ação do fluxo de trabalho na guia Perfil de uma tarefa de aprovação.

A guia Perfil do botão tem uma tabela com uma linha para cada botão de ação do fluxo de trabalho. Cada linha do botão possui as seguintes quatro propriedades, que correspondem a colunas da tabela:

Nome de exibição

O nome que aparece no botão na tela de aprovação. O nome é um valor localizado condicionalmente, que pode ser uma sequência de caracteres ou uma chave para uma sequência de caracteres localizada em um arquivo de recurso.

Ação

O valor que é passado de volta para o processo de fluxo de trabalho quando a opção é selecionada. Esse valor é um atributo do nó de transição correspondente no diagrama de processos do WorkPoint. O valor é uma sequência de caracteres não localizada. As configurações padrão são aprovadas ou recusadas.

Dica de ferramenta

Uma descrição curta (ou dica de ferramenta) da ação do botão que é exibida quando um usuário passa o cursor do mouse sobre o botão. A dica de ferramenta é um valor localizado condicionalmente, que pode ser uma sequência de caracteres ou uma chave para uma sequência de caracteres localizada em um arquivo de recurso.

Descrição longa

Uma descrição mais longa da ação do botão que adiciona uma mensagem que descreve a ação na tela Exibir tarefas enviadas. Se a descrição for deixada em branco, a mensagem que é exibida na tela Exibir tarefas enviadas será o nome do botão. O nome é um valor localizado condicionalmente, que pode ser uma sequência de caracteres ou uma chave para uma sequência de caracteres localizada em um arquivo de recurso.

Mais informações:

Configuração de botões na Interface de desenho do WorkPoint (na página 339)

Adicionando botões de ação do fluxo de trabalho

Para adicionar um novo botão a um processo de fluxo de trabalho existente, siga as seguintes etapas de alto nível:

1. Adicione um botão de fluxo de trabalho no CA Identity Manager.

   Para obter instruções, consulte o tópico Como adicionar um botão de ação do fluxo de trabalho (na página 338).

2. Se necessário, adicione chaves de localização.

   Para obter instruções, consulte o *Guia de Configuração*.

3. Adicione novos nós necessários na Interface de desenho do WorkPoint.

   Para obter instruções, consulte a ajuda online da Interface de desenho do WorkPoint.

4. Defina um script no nó de transição da Interface de desenho do WorkPoint.

   Para obter instruções, consulte o tópico Configuração de botões na Interface de desenho do WorkPoint (na página 339).

Mais informações:

Configuração de botões na Interface de desenho do WorkPoint (na página 339)
Como adicionar um botão de ação do fluxo de trabalho (na página 338)

Como adicionar um botão de ação do fluxo de trabalho

ou é possível adicionar botões de ação do fluxo de trabalho a tarefas de aprovação no CA Identity Manager.

Para adicionar um botão de ação do fluxo de trabalho a uma tarefa administrativa:

1. No console de usuário, selecione Funções e tarefas, Tarefa administrativa, Modificar tarefa administrativa.

   A tela Selecionar tarefa administrativa é exibida.

2. Pesquise a tarefa de aprovação e clique em Selecionar.

   A tela Modificar tarefa administrativa é exibida.

3. Na guia Perfil, clique no botão chamado Botões de ação do fluxo de trabalho.

   A guia Perfil do botão de ação do fluxo de trabalho é exibida.

4. Clique em Adicionar botão para adicionar um novo botão à tarefa de aprovação.

5. Digite as informações de propriedade do botão.

6. Clique em OK.

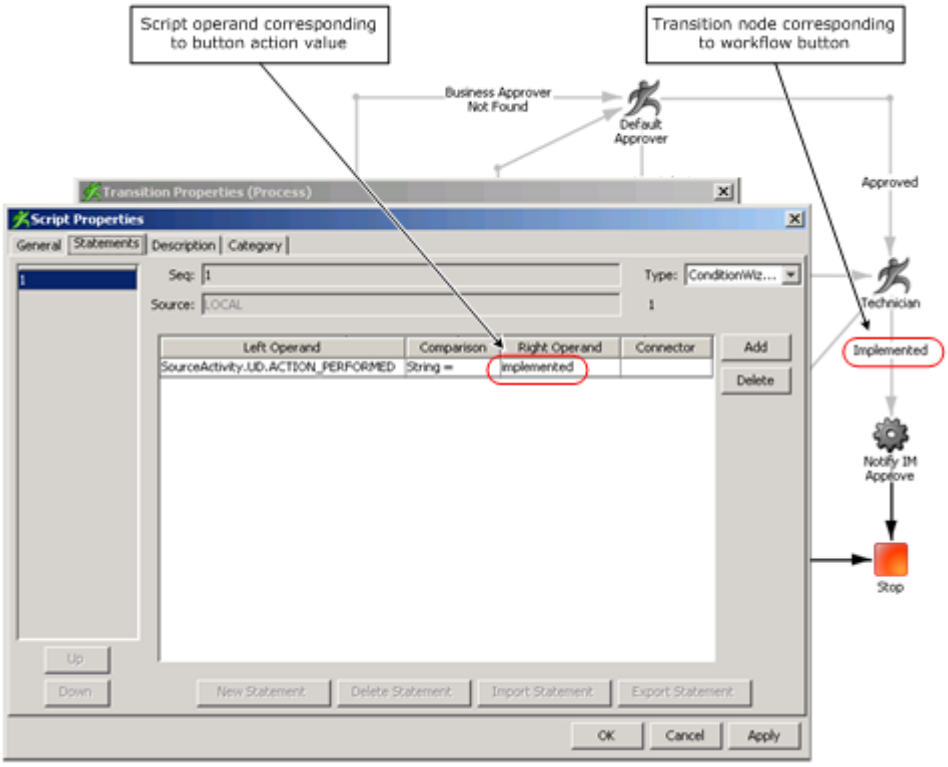
   O CA Identity Manager salva as informações do novo botão.

7. Clique em Enviar.

   O CA Identity Manager processa a modificação da tarefa.

Configuração de botões na Interface de desenho do WorkPoint

Na Interface de desenho do WorkPoint, botões de ação do fluxo de trabalho são configurados usando propriedades de script do nó de transição, conforme mostrado na figura a seguir:



Por padrão, botões de ação do fluxo de trabalho usam as seguintes propriedades de script para executar uma comparação de sequências de caracteres:

- Left Operand - ACTION_PEFORMED, que é definido nas propriedades de Dados do usuário do nó de atividade manual anterior.
- Right Operand - O valor de ação do botão, que é definido na guia Perfil do botão do console de usuário.

Observação: consulte a ajuda online da Interface de desenho do WorkPoint para obter informações sobre os scripts e as propriedades do nó de atividade e do nó de transição.

Mais informações:

Configuração de botões no CA Identity Manager (na página 336)

Listas de tarefas e itens de trabalho

Uma *lista de tarefas* é uma lista de itens de trabalho (ou tarefas de aprovação) que é exibida no console de usuário do participante autorizado a aprovar a tarefa. Os itens de trabalho correspondem às atividades manuais de um processo de fluxo de trabalho. São representados como linhas na lista de tarefas.

Os itens de trabalho podem ser adicionados a uma lista de tarefas das seguintes formas:

- Um resolvedor participante determinando uma lista de aprovadores.
- Recebendo itens de trabalho delegados de outro usuário.
- Reatribuindo itens de trabalho para outro usuário.

Os itens de trabalho podem ser removidos de uma lista de tarefas das seguintes formas:

- Concluindo (aprovando ou recusando) o item de trabalho.
- Reatribuindo itens de trabalho para outro usuário.
- Reservando o item de trabalho. Isso o remove da lista de tarefas de todos os outros participantes.

Observação: quando você aceita ou recusa um item de trabalho, a alteração não tem efeito imediato. Por exemplo, se você recusar um item de trabalho, esse item ainda aparecerá em sua lista de tarefas até que o processo de fluxo de trabalho registre as informações e avance o processo para o próximo nó.

As guias de informações que são exibidas em um item de trabalho variam se o item de trabalho tiver sido gerado pelo fluxo de trabalho sob controle em nível de tarefa ou em nível de evento:

- **Perfil** — Fornece informações de perfil sobre o objeto afetado pelo evento (somente em nível de evento).
- **Detalhes da tarefa** — Fornece informações detalhadas sobre todos os eventos dentro da tarefa (somente em nível de tarefa).
- **Aprovadores** — Lista todos os aprovadores individuais e os delegantes para a tarefa ou evento (em nível de tarefa e em nível de evento)

Exibindo uma lista de tarefas

Sua lista de tarefas será exibida automaticamente quando você efetuar logon no console de usuário se tiver sido atribuído como um participante para aprovar tarefas (ou itens de trabalho) iniciados por outros usuários.

Para exibir sua lista de tarefas manualmente:

1. No console de usuário, selecione Principal, Exibir minha lista de tarefas.

   A lista de tarefas é exibida.

2. Clique no nome de um item de trabalho para exibi-lo.

   O item de trabalho selecionado é exibido.

Os administradores podem gerenciar os itens de trabalho para os usuários sobre os quais têm escopo.

Observação: o gerenciamento de itens de trabalho de um usuário permite que os administradores reservem um item de trabalho. A exibição da lista de tarefas de um usuário não permite alterações de nenhum tipo em itens de trabalho.

Para exibir a lista de tarefas de outro usuário:

1. No console de usuário, selecione Usuários, Gerenciar itens de trabalho, Exibir a lista de tarefas do usuário.

   A tela Selecionar usuário é exibida.

2. Pesquise o usuário cuja lista de tarefas você deseja exibir e clique em Selecionar.

   A tela da lista de tarefas do usuário é exibida.

Para gerenciar itens de trabalho para outro usuário:

1. No console de usuário, selecione Usuários, Gerenciar itens de trabalho, Gerenciar os itens de trabalho do usuário.

   A tela Selecionar usuário é exibida.

2. Pesquise o usuário cujos itens de trabalho você deseja gerenciar e clique em Selecionar.

   A tela da lista de tarefas do usuário é exibida.

3. Clique no nome de um item de trabalho para exibi-lo.

   O item de trabalho selecionado é exibido.

Ativando a tela de pesquisa da lista de tarefas

É possível ativar as telas de pesquisa predefinidas para localizar itens de tarefas.

1. No Management Console, vá para Home, Environments, <ambiente>, Roles.
2. Clique em Import. Importe o arquivo worklistsearch.xml a partir de: `<LOCAL_DA_INSTALAÇÃO>\CA\IdentityManager\IAM Suite\Identity Manager\tools\worklistsearch`
3. Clique em Finish.
4. Efetue logon no ambiente do CA Identity Manager.
5. No console de usuário, selecione Funções e tarefas, Tarefa administrativa, Modificar tarefa administrativa.
6. Procure e selecione a tarefa Exibir minha lista de tarefas.
7. Selecione a guia Pesquisar. Clique em Procurar.

   Uma lista de definições de tela é exibida.
8. Clique em Novo.

   Uma lista de novos tipos de tela é exibida.
9. Selecione Tela de pesquisa da lista de tarefas e clique em OK.
10. Digite os detalhes para configurar a tela de pesquisa da lista de tarefas e clique em OK.

    A tela de nova pesquisa é adicionada à lista de definições de tela

Reservando itens de trabalho

Você pode reservar um item de trabalho para verificá-lo e removê-lo da lista de tarefas de outros participantes. A reserva de um item de trabalho o mantém para o usuário que está executando a reserva.

Se o usuário da reserva liberar o item de trabalho, ele volta a ficar disponível na lista de tarefas de outros participantes. Se o usuário da reserva aprovar ou recusar o item de trabalho, ele será concluído e não ficará mais disponível para outros participantes.

Mais informações:

Delegação e itens de trabalho reservados (na página 343)
Reatribuição e itens de trabalho reservados (na página 343)

Reatribuição e itens de trabalho reservados

Se um usuário tiver um item de trabalho reservado enquanto ele for reatribuído, o usuário o manterá reservado. No entanto, se o usuário liberar esse item de trabalho, perderá o acesso a ele.

Um administrador pode reatribuir, reservar ou liberar o item de trabalho de outro usuário, mas não pode aprovar ou recusar o item de trabalho de outro usuário. Somente o participante do item de trabalho atribuído pode fazer isso.

Mais informações:

Reatribuindo itens de trabalho (na página 349)

Delegação e itens de trabalho reservados

Enquanto uma delegação estiver ativa, o representante ou o delegante pode reservar um item de trabalho. Um item de trabalho reservado por um usuário não pode ser exibido na lista de tarefas de outro usuário.

Por exemplo, se um representante tiver um item de trabalho reservado quando a delegação for removida, ele manterá o item de trabalho reservado. No entanto, se o representante liberar esse item de trabalho, perderá o acesso a ele.

Se um usuário que é representante for excluído enquanto tiver um item de trabalho reservado, ainda manterá o item de trabalho. Se o representante aprovar o item de trabalho, a auditoria não poderá mais determinar quem o delegou.

Se um representante tiver um item de trabalho reservado quando a delegação for removida, ele manterá o acesso até que o item de trabalho seja concluído ou liberado.

Mais informações:

Delegando itens de trabalho (na página 344)
Reservando itens de trabalho (na página 342)

Como reservar ou liberar um item de trabalho

Você pode reservar um item de trabalho para verificá-lo e removê-lo da lista de tarefas de outros participantes.

Você libera um item de trabalho reservado para torná-lo disponível na lista de tarefas de outros participantes.

Observação: a única maneira de liberar um item de trabalho reservado é liberá-lo explicitamente.

Para reservar ou liberar um item de trabalho:

1. No console de usuário, selecione Principal, Exibir minha lista de tarefas.

   A lista de tarefas é exibida.

2. Selecione o item de trabalho que deseja reservar ou liberar.

   A tela expandida do item de trabalho é exibida.

3. Clique em Reservar item ou Liberar item.

   O CA Identity Manager confirma sua ação.

Delegando itens de trabalho

A *delegação* do item de trabalho permite que um usuário (o delegante) especifique que outro usuário (o representante) tem a permissão de aprovar tarefas na lista de tarefas do delegante. Um delegante pode atribuir itens de trabalho para outro aprovador durante os períodos em que o delegante estiver ausente. Os delegantes mantêm acesso completo aos seus itens de trabalho durante o período de delegação.

Os itens de trabalho delegados não são alterados de nenhuma maneira. A geração de log indica se um item de trabalho foi delegado.

A delegação permite que o representante personifique o delegante e exiba os itens na lista de tarefas do delegante. Ao exibir uma lista de tarefas, os representantes veem seus próprios itens de trabalho, bem como os itens de trabalho do delegante.

A delegação não é transitiva. Um representante pode ver apenas os itens de trabalho que o delegante tiver atribuído diretamente. Por exemplo, se o usuário A delegar itens de trabalho para o usuário B, e o usuário B delegar itens de trabalho para o usuário C, o usuário C poderá ver apenas os itens de trabalho pertencentes ao usuário B, mas nenhum item de trabalho que possa ter sido delegado para o usuário B pelo usuário A.

Mais informações:

Delegação e itens de trabalho reservados (na página 343)

Atributo conhecido de delegação

A delegação usa o seguinte atributo conhecido:

%DELEGATORS%

Esse atributo conhecido armazena os nomes de usuários que estão sendo delegados ao usuário com o atributo, assim como o horário em que a delegação foi criada.

Como ativar a delegação

Você deve ter ativado a delegação de aprovação de fluxo de trabalho para que possa delegar itens de trabalho a outro usuário. Por padrão, a delegação fica desativada.

Para ativar a delegação de aprovação de fluxo de trabalho:

1. Abra o Management Console inserindo o seguinte URL em um navegador:

   `http://hostname/iam/immanage`

   nome do host

   Define o nome de domínio totalmente qualificado do servidor em que o CA Identity Manager está instalado. Por exemplo, meuservidor.minhaempresa.com:porta.

2. Clique em Ambientes e selecione o nome do ambiente adequado do CA Identity Manager.
3. Clique em Configurações avançadas e, em seguida, clique em Workflow Approval Delegation.
4. Selecione a caixa de seleção Ativado e, em seguida, clique em Salvar.

Mais informações:

Como delegar para si mesmo (na página 345)
Como delegar para outro usuário (na página 348)

Como delegar para si mesmo

Você pode delegar itens de trabalho a outro usuário durante os períodos em que estiver ausente. Os delegantes ainda têm acesso completo a seus itens de trabalho durante o período de delegação.

Para delegar itens de trabalho para si mesmo:

1. No console de usuário, selecione Principal, Assistente de ausência temporária.

   A tela Assistente de ausência temporária é exibida.

2. Clique em Adicionar usuário.

   A tela Selecionar usuário é exibida.

3. Procure e selecione um ou mais usuários para atuar como representantes.

   Os usuários são adicionados à lista de representantes.

4. Clique em Enviar.

   A tarefa é enviada e a delegação é salva.

Observação: os usuários que já forem representantes não serão exibidos nos resultados da pesquisa ao adicionar um representante.

Mais informações:

Como ativar a delegação (na página 345)

Delegação de itens de trabalho com base em tempo

Nas releases anteriores, era possível especificar a hora de início, mas não a hora de término para as delegações. As delegações criadas recentemente têm suas datas para delegação definidas como verdadeiras, com a hora de início padrão definida como Agora.

Na hora de modificação, as datas de início e término podem ser alteradas. A hora de término padrão é uma semana a partir da data de início.

Para alterar as datas de início ou de término, faça o seguinte:

1. Na guia Principal do console de usuário, selecione Assistente de ausência temporária.
2. Clique no ícone em forma de lápis ao lado da ID do usuário cujas informações de delegação deseja alterar.

   A tela Editar detalhes de delegação é exibida.
3. Clique no calendário ao lado da data de início para alterar a data de início da delegação.

   Observação: uma mensagem de erro será exibida quando a data de início da delegação selecionada for anterior à data atual.
4. Se desejar selecionar uma data de término, marque a caixa de seleção Possui data de término.

   O campo Data de término fica disponível para definir a data de término.
5. Clique no calendário ao lado do campo Data final para definir uma data de término para a delegação.
6. Uma vez que as datas forem definidas, clique em OK.

Como alternativa, é possível fazer o mesmo na guia Delegar itens de trabalho, durante a criação ou modificação de um usuário.

Ativar a delegação de itens de trabalho com base em tempo

Para ativar a delegação de item de trabalho com base no tempo em um ambiente existente na atualização, faça o seguinte:

No Management Console:

1. Navegue até a página Ambiente.
2. Faça uma busca detalhada no ambiente selecionado, Configurações avançadas, Work Item Delegation.
3. Desmarque a caixa de seleção Ativado.
4. Salve as alterações e reinicie o ambiente.
5. Faça uma busca detalhada em Configurações avançadas, Work Item Delegation.
6. Marque a caixa de seleção Ativado.
7. Salve as alterações e reinicie o ambiente.

Observação: esse procedimento pode ser usado apenas em ambientes existentes. A delegação de itens de trabalho com base em tempo é ativada para novos ambientes.

Tela Assistente de ausência temporária

Você usa a seguinte tela Assistente de ausência temporária para adicionar e remover representantes para si mesmo:

A tela Assistente de ausência temporária exibe uma lista de seus representantes atuais. Além das colunas que identificam o representante, três colunas adicionais serão incluídas na lista:

Data de início

Exibe a data em que a delegação foi criada.

Data de término

Exibe a data em que a delegação deve terminar.

Possui representantes

Indica se o representante delegou itens de trabalho para outro usuário.

Ao clicar no ícone em forma de lápis próximo à ID de usuário selecionada, a tela Editar detalhes de delegação é exibida, onde é possível alterar o campo Data de início e especificar a Data de término para a delegação.

Como delegar para outro usuário

Os administradores podem delegar itens de trabalho de um usuário (delegante) para outro. Por exemplo, um usuário pode ficar ausente de forma inesperada ou um administrador pode precisar atribuir uma grande carga de trabalho a vários usuários.

Os administradores podem delegar itens de trabalho apenas para os usuários sobre os quais têm escopo. Da mesma forma, eles só podem adicionar ou remover usuários que gerenciam na lista de representantes.

Para delegar itens de trabalho para outro usuário:

1. No console de usuário, selecione Usuários, Gerenciar itens de trabalho, Delegar itens de trabalho.

   A tela Selecionar usuário é exibida.

2. Pesquise o usuário cujos itens de trabalho você deseja delegar (o delegante) e clique em Selecionar.

   Uma tela de delegação de itens de trabalho é exibida.

3. Clique em Adicionar usuário.

   A tela Selecionar usuário é exibida.

4. Procure e selecione um ou mais usuários para atuar como representantes.

   Os usuários são adicionados à lista de representantes.

5. Clique em Enviar.

   A tarefa é enviada e a delegação é salva.

Observação: os usuários que já forem representantes não serão exibidos nos resultados da pesquisa ao adicionar um representante.

Mais informações:

Como ativar a delegação (na página 345)

Como remover uma delegação

Se um usuário efetuar logon no CA Identity Manager com delegações em vigor, o CA Identity Manager exibirá o seguinte lembrete:

```
Você tem delegações em vigor. Verifique se elas ainda são necessárias.
```

Para remover uma delegação para si mesmo:

1. No console de usuário, selecione Principal, Assistente de ausência temporária.

   A tela Assistente de ausência temporária é exibida.

2. Clique no sinal de menos (-) para os representantes que deseja remover.

   Os representantes desaparecem da lista.

3. Clique em Enviar.

   A tarefa é enviada e a delegação é removida.

Para remover uma delegação para outro usuário:

1. No console de usuário, selecione Usuários, Gerenciar itens de trabalho, Delegar itens de trabalho.

   Uma tela de pesquisa de usuário é exibida.

2. Procure e selecione o usuário cujas delegações você deseja remover.

   A lista de representantes é exibida.

3. Clique no sinal de menos (-) para os representantes que deseja remover.

   Os representantes desaparecem da lista.

4. Clique em Enviar.

   A tarefa é enviada e a delegação é removida.

Observação: é possível remover um representante apenas se tiver escopo sobre esse usuário.

Reatribuindo itens de trabalho

A reatribuição permite que usuários e administradores alterem os responsáveis por um item de trabalho após sua criação. Um administrador pode:

- Exibir a lista de tarefas de outro usuário
- Adicionar e remover responsáveis pelo item de trabalho
- Alterar o status de reserva de itens de trabalho

Por exemplo, um administrador pode reatribuir um item de trabalho ou liberar um item de trabalho reservado de um usuário que não estiver executando ações nele.

Se um usuário tiver um item de trabalho reservado enquanto ele for reatribuído, o usuário o manterá reservado. No entanto, se o usuário liberar esse item de trabalho, perderá o acesso a ele.

Se um representante tiver um item de trabalho reservado quando a delegação for removida, ele manterá o acesso até que o item de trabalho seja concluído ou liberado.

Mais informações:

Reatribuição e itens de trabalho reservados (na página 343)

A guia Aprovadores

Você executa a reatribuição na guia Aprovadores do item de trabalho, que exibe uma lista dos aprovadores atuais do item de trabalho (ou responsáveis). Quando você executa a reatribuição, atribui o item de trabalho aberto para todos os aprovadores na lista. Portanto, para reatribuir um item de trabalho para um novo responsável, você também deve remover o responsável atual.

Como reatribuir itens de trabalho

A reatribuição de um item de trabalho de um usuário para outro é um processo de duas etapas:

- Selecionar um novo aprovador.
- Remover o aprovador atual.

Observação: é preciso ter escopo sobre os usuários para os quais deseja reatribuir o item de trabalho.

Para reatribuir seu próprio item de trabalho

1. Selecione Principal, Exibir minha lista de tarefas.

   A lista de tarefas é exibida.

2. Selecione um item de trabalho para expandi-lo.
3. Selecione a guia Aprovadores.

   A lista de todos os aprovadores atuais é exibida, incluindo o usuário cuja lista de tarefas você está gerenciando.

4. Clique em Adicionar responsáveis.

   A tela Selecionar usuário é exibida.

5. Procure e selecione um ou mais usuários para os quais deseja reatribuir o item de trabalho.

   Observação: para os modos de aprovação ALL e SUBSET, apenas é possível atribuir um item de trabalho a um *único* usuário.

6. Clique no sinal de menos (-) para excluir a si mesmo como um responsável.
7. Clique em Executar reatribuição.

   O item de trabalho é exibido nas listas de tarefas dos usuários reatribuídos.

Observação: um administrador pode reatribuir, reservar ou liberar o item de trabalho de outro usuário, mas não pode aprovar ou recusar o item de trabalho de outro usuário. Somente o proprietário do item de trabalho pode fazer isso.

Para reatribuir outro item de trabalho do usuário

1. Selecione Usuários, Gerenciar itens de trabalho, Gerenciar os itens de trabalho do usuário.

   A tela Selecionar usuário é exibida.

2. Pesquise o usuário cujos itens de trabalho você deseja reatribuir e clique em Selecionar.

   A página Gerenciar os itens de trabalho do usuário é exibida.

3. Selecione um item de trabalho para expandi-lo.

4. Selecione a guia Aprovadores.

   A lista de todos os aprovadores atuais é exibida, incluindo o usuário cuja lista de tarefas você está gerenciando.

5. Clique em Adicionar responsáveis.

   A tela Selecionar usuário é exibida.

6. Procure e selecione um ou mais usuários para os quais deseja reatribuir o item de trabalho.

7. Clique no sinal de menos (-) para remover o responsável atual.

8. Clique em Executar reatribuição.

   O item de trabalho é exibido nas listas de tarefas dos usuários reatribuídos.

Operações em massa em itens de trabalho

Com esta release do CA Identity Manager, as seguintes operações em massa podem ser executadas nos itens de trabalho:

- Aprovar
- Recusar
- Reservar
- Liberar

No console de usuário, a configuração da guia Lista de tarefas foi aprimorada para incluir uma nova caixa de seleção Oferece suporte a operações de fluxo de trabalho em massa. Quando essa caixa de seleção estiver ativada, o usuário poderá aprovar, recusar, liberar e reservar em massa os itens de trabalho que possuem ou de qualquer delegante. Os administradores somente podem executar essas operações em massa nos itens de trabalho usando a tarefa Gerenciar os itens de trabalho do usuário.

Observação: as operações em massa não podem ser ativadas para qualquer tarefa do tipo Exibir, como Exibir minha lista de tarefas.

Configurar a guia Lista de tarefas para operações em massa

Para configurar a guia Lista de tarefas, a fim de oferecer suporte a operações em massa nos itens de trabalho, siga o procedimento a seguir.

Na guia Funções e tarefas no console de usuário:

1. Selecione uma das seguintes opções:
   - Funções e tarefas.
   - Tarefas, Funções e Tarefas.
2. Selecione Tarefas administrativas, Gerenciar tarefas administrativas.
3. Clique em Pesquisar.
4. Selecione Gerenciar os itens de trabalho do usuário.
5. Na guia Guias, clique no ícone em forma de lápis ao lado de Lista de tarefas.

   A tela de configuração da Lista de tarefas é exibida.
6. Selecione Oferece suporte a operações de fluxo de trabalho em massa.
7. Salve as alterações e envie a tarefa.

   As operações em massa em itens de trabalho ficam disponíveis.

Capítulo 12: Notificações por email

Esta seção contém os seguintes tópicos:

Notificações por email no CA Identity Manager

As notificações por email informam ao CA Identity Manager os usuários de tarefas e eventos no sistema. Por exemplo, o CA Identity Manager pode enviar um email aos aprovadores quando um evento ou uma tarefa exigir uma aprovação.

O CA Identity Manager oferece os seguintes métodos para configuração de notificações por email:

- **Políticas de notificação por email**

  As políticas de notificação por email permitem que os administradores de negócios criem, exibam, modifiquem e excluam notificações por email usando tarefas no console de usuário. Nenhuma codificação é necessária para a criação de notificações por email.

  Os administradores podem definir o conteúdo de um email, quando ele será enviado e quem o receberá. O conteúdo do email, que é definido em um editor de HTML, pode conter informações dinâmicas, como a data atual ou informações de eventos, que o CA Identity Manager preenche quando o email é enviado. Por exemplo, você pode configurar uma notificação por email que é enviada para um aprovador quando um usuário é criado. O email pode conter as informações de logon do usuário, a data de contratação e o gerente.

  Observação: as regras de notificação por email são políticas Policy Xpress (na página 485) que são criadas e gerenciadas por um conjunto separado de tarefas.

- **Modelos de email**

  Nesse método, as notificações por email são geradas dos modelos de email. O CA Identity Manager fornece modelos de email padrão que podem ser usados como instalados ou que podem ser personalizados pelos administradores de sistema. Esses administradores usam uma API de modelo de email para especificar o conteúdo dinâmico, como a lista de destinatários e informações sobre o evento que aciona o email.

O CA Identity Manager pode gerar notificações por email quando ocorre o seguinte:

- Um evento que exige aprovação ou recusa por um aprovador de fluxo de trabalho estiver pendente

  Observação: se você tiver um processo de aprovação do WorkPoint com mais de uma atividade de aprovação, a notificação por email configurada nas tarefas do console de usuário enviará uma notificação para cada atividade. Se você usar os modelos de email para a mesma notificação, somente um email será enviado aos aprovadores (quando o evento chegar ao estado pendente).

- Um aprovador aprovar um evento ou tarefa
- Um aprovador recusar um evento ou tarefa

- Um evento ou uma tarefa for iniciada, falhar ou for concluída
- Um usuário for criado ou modificado

Para usar as notificações por email do CA Identity Manager, defina as configurações de SMTP (na página 356). Se estiver usando o método de modelo de email, você também ativa as notificações por email no CA Identity Manager.

Como selecionar um método de notificação por email

A tabela a seguir resume as diferenças entre as políticas de notificação por email e os modelos de email:

Atividade	Tarefas de gerenciamento de emails	Modelos de email
Configurando notificações por email	Os administradores usam tarefas administrativas no Console de usuário para criar, modificar, exibir e excluir as notificações por email.	Os administradores modificam modelos padrão nas Ferramentas administrativas do CA Identity Manager.
Configurando quando emails são enviados	O CA Identity Manager pode gerar notificações por email quando determinados eventos ou tarefas ocorrem. As tarefas de gerenciamento de emails e os modelos de email oferecem suporte aos mesmos eventos e tarefas, no entanto, as tarefas de gerenciamento de emails fornecem mais granularidade em alguns casos. As notificações por email são suportadas para os seguintes eventos e tarefas: ■ Um evento que exige aprovação ou recusa por um aprovador de fluxo de trabalho estiver pendente ■ **Observação:** se você tiver um processo de aprovação do Workpoint que tenha mais de uma atividade de aprovação, a notificação por email configurada usando as tarefas de gerenciamento de emails envia uma notificação para cada atividade. Se você usar os modelos de email para a mesma notificação, somente um email será enviado aos aprovadores (quando o evento chegar ao estado pendente). ■ Um aprovador aprovar um evento ou tarefa ■ Um aprovador recusar um evento ou tarefa ■ Um evento ou uma tarefa for iniciada, falhar ou for concluída ■ Um usuário for criado ou modificado	

Atividade	Tarefas de gerenciamento de emails	Modelos de email
Adicionando conteúdo dinâmico aos emails	Os administradores adicionam conteúdo dinâmico ao corpo de uma mensagem de email selecionando em uma lista de opções na guia Conteúdo das tarefas Criar email ou Modificar email. O CA Identity Manager preenche automaticamente o conteúdo dinâmico com base nas informações do evento ou da tarefa que aciona a notificação.	Os administradores usam a API de modelo de email para personalizar os modelos de email padrão, que são usados para gerar notificações por email.
Oferecendo suporte às notificações por email existentes	As notificações por email que são configuradas usando as tarefas de gerenciamento de emails têm como base as políticas Policy Xpress. Se você tiver atualizado do CA Identity Manager Option Pack 1 para o CA Identity Manager 12.6.5, as notificações por email que você configurou no Policy Xpress continuarão funcionando. No entanto, você gerencia essas notificações por email usando as tarefas de gerenciamento de emails, e não o Policy Xpress.	As notificações por email que você criou usando o método de modelo de email nas versões anteriores do CA Identity Manager continuarão funcionando no CA Identity Manager 12.6.5.

Definir configurações de SMTP

Antes de ativar notificações por email, defina as configurações de SMTP. Consulte as seções a seguir para definir as configurações de SMTP para o seu servidor de aplicativos.

Definir configurações de SMTP no JBoss

1. Em um editor de texto, abra o descritor de implantação do serviço de email como se segue:

   Único nó: *base_do_jboss*\server\default\deploy\mail-service.xml

   Cluster: *base_do_jboss*\server\all\deploy\mail-service.xml

2. Modifique a propriedade mail.smtp.host com o nome do servidor SMTP, como segue:

   ```
   <-- Change to the SMTP gateway server -->
   <property name="mail.smtp.host" value="seu_servidor_smtp "/>
   ```

   Por exemplo:

   ```
   <property name="mail.smtp.host" value="smtp.mailserver.company.com"/>
   ```

3. Salve o arquivo mail-service.xml.

4. Em um editor de texto, abra o arquivo de propriedades de email a seguir:

   Único nó:
   base_do_jboss\server\default\deploy\iam_im.ear\config\com\netegrity\config\email.properties

   Cluster:*base_do_jboss*\server\all\deploy\iam_im.ear\config\com\netegrity\config\email.properties

5. Para definir o endereço de retorno de email que o email gerado pelo fluxo de trabalho usa, localize a propriedade admin.email.address e defina o valor para o endereço de email adequado. Por exemplo:
   `admin.email.address=admin@company.com`

6. Se você estiver usando o método de modelo de email, ative as notificações por email no Management Console.

   Você não precisa ativar as notificações por email no Management Console se estiver usando as políticas de notificação por email.

Definir configurações de SMTP no WebLogic

Defina as configurações de email no Console de administração do servidor do WebLogic e em um arquivo email.properties.

Para definir configurações de email para o WebLogic

1. No Console de administração do servidor do WebLogic, crie uma sessão de email com as propriedades a seguir:
   - propriedade **mail.smtp.host**: defina esse valor para seu servidor SMTP. Por exemplo, mail.smtp.host=mymailserver.company.com
   - propriedade **mail.transport.protocol**: defina esse valor para SMTP. Por exemplo, mail.transport.protocol=smtp
   - **Nome JNDI**: nete/Mail
   - **Destino**: o nome do servidor do WebLogic

2. Em um editor de texto, abra o arquivo de propriedades de email a seguir para o CA Identity Manager:

   domínio_do_weblogic\applications\iam.ear\config\com\netegrity\config\email.properties

3. Defina o endereço de retorno de email usado pelos emails gerados pelo fluxo de trabalho localizando a propriedade admin.email.address e configurando o valor para o endereço de email adequado. Por exemplo:
   `admin.email.address=admin@company.com`

4. Ative a notificação por email no Management Console.

   Observação: você não precisa ativar as notificações por email no Management Console se estiver usando as políticas de notificação por email.

Definir configurações de SMTP no WebSphere

O utilitário imsSetup que você executa depois de instalar os componentes do CA Identity Manager configura um novo objeto de sessão de email chamado mailMail.

Para que o recurso de notificação por email funcione corretamente, especifique o servidor ao qual o WebSphere se conecta ao enviar email no campo Mail Transport Host da sessão mailMail.

A sessão mailMail está localizada em Resources, Mail Providers, Built-in Mail Provider, Mail Sessions, mailMail no Console administrativo do WebSphere.

Observação: para exibir o objeto mailMail, altere o Escopo para Servidor na tela Mail Session. Se você não alterar o escopo para Servidor, o objeto mailMial não será exibido.

Para obter mais informações sobre como configurar um provedor de email do WebSphere, consulte a documentação do WebSphere.

Se você estiver usando o método de modelo de email, ative a notificação por email no Management Console depois de definir as configurações de SMTP.

Observação: você não precisa ativar as notificações por email no Management Console se estiver usando as políticas de notificação por email.

Como configurar um endereço de email do administrador exclusivo para cada ambiente

É possível configurar um endereço de email do administrador exclusivo para cada ambiente do CA Identity Manager.

Siga estas etapas::

1. No Management Console, clique em Environments.

   Uma lista de ambientes do CA Identity Manager é exibida.
2. Selecione um ambiente do CA Identity Manager.
3. Vá para Advanced Settings, E-mail.
4. Em Administrator Email address, especifique um endereço de email para esse ambiente.
5. Clique em Save.
6. Clique em Restart environment.

   Você agora pode segregar os emails de diferentes ambientes do CA Identity Manager dos quais você receber notificações por email, de um endereço de email diferente para cada ambiente do CA Identity Manager.

Como criar políticas de notificação por email

Você pode usar o console de usuário para criar políticas de notificação por email que enviam emails quando determinadas ações ocorrem. Por exemplo, você pode criar uma política de notificação por email que envia um email para notificar os aprovadores quando um novo usuário é criado.

Siga estas etapas:

1. Selecione Sistema, Email, Criar Email.
2. Selecione uma das opções a seguir:
   - Criar um objeto do tipo email gerenciado
   - Criar uma cópia de um objeto do tipo email gerenciado

     Usa uma política de notificação por email existente como modelo para criar uma política.
3. Forneça informações básicas sobre a política de notificação por email na guia Perfil.
4. Especifique quando o CA Identity Manager envia o email na guia Quando enviar.

   A guia Quando enviar fornece várias opções para especificar as ações que acionam notificações por email.
5. Especifique os destinatários do email na guia Destinatários.
6. Defina o assunto e o conteúdo do email na guia Conteúdo.

   Você pode especificar um conteúdo dinâmico, como a data, o nome da tarefa ou do evento, e os atributos do usuário no conteúdo do email.

Mais informações:

Guia Quando enviar (na página 362)
Guia Destinatários (na página 363)
Conteúdo (na página 365)
Guia Perfil de notificação por email (na página 360)

Guia Perfil de notificação por email

A guia Perfil nas tarefas de gerenciamento de emails permite especificar as informações básicas sobre uma política de notificação por email. Essa guia inclui os seguintes campos:

Nome do email

Identifica a política de notificação por email no console de usuário.

Observação: o nome do email não é exibido quando o email é enviado. O nome é usado somente para gerenciar a política de notificação por email no console de usuário.

Categoria

Agrupa as políticas de notificação por email para simplificar o gerenciamento.

Especifique uma categoria existente, selecionando-a na lista suspensa, ou selecione o botão de segunda opção e digite o nome de uma nova categoria.

Descrição

Descreve a política de notificação por email para os administradores.

A descrição não é exibida quando o email é enviado.

Ativado

Especifica que o CA Identity Manager enviará o email quando as condições definidas na guia Quando enviar forem atendidas.

Dados personalizados

Cria um elemento de dados personalizado do Policy Xpress que pode ser usado para configurar destinatários personalizados ou conteúdo personalizado.

Elementos de dados personalizados também podem ser usados como parâmetros em outros elementos de dados.

Observação: Dados (na página 492) fornece mais informações sobre elementos de dados.

Quando você clica em Dados personalizados, o CA Identity Manager abre uma tela na qual é possível adicionar novos elementos de dados.

Regras de entrada

Define regras para quando o CA Identity Manager envia notificações por email em casos em que as regras padrão na guia Quando enviar não são granulares o bastante.

Por exemplo, a guia Quando enviar fornece uma regra padrão que envia um email quando qualquer atributo de um perfil de usuário é modificado. Se desejar que o CA Identity Manager envie um email somente quando o departamento de um usuário for alterado, você poderá criar uma regra de entrada personalizada. (Nesse caso, crie um elemento de dados personalizado que identifica quando o departamento é alterado e, em seguida, crie uma regra de entrada que usa o elemento de dados personalizado que você criou.)

Observação: a seção Regras de entrada (na página 495) fornece mais informações.

Mais informações:

Elementos de dados (na página 492)
Regras de entrada (na página 495)

Guia Quando enviar

O CA Identity Manager fornece várias opções padrão que determinam quando o email é enviado. Algumas dessas opções exigem informações adicionais, tais como o nome da tarefa ou do evento. Por exemplo, para enviar um email quando uma tarefa for iniciada é preciso selecionar a tarefa que aciona o email.

Você pode selecionar uma ou mais das seguintes opções da guia Quando enviar:

Criado pelo usuário

Envia um email quando um usuário tiver sido criado. O email é enviado quando o evento CreateUserEvent for concluído.

Modificado pelo usuário

Envia um email quando um usuário tiver sido modificado. O email é enviado quando o evento ModifyUserEvent for concluído.

Fluxo de trabalho pendente

Envia um email quando um processo de fluxo de trabalho atribui um aprovador. Ao selecionar essa opção, especifique o processo de fluxo de trabalho aplicável. O email definido com essa política envia emails aos aprovadores em cada etapa do processo de fluxo de trabalho selecionado.

Email pendente do fluxo de trabalho

Envia um email quando um processo de fluxo de trabalho atinge uma determinada atividade. Ao selecionar essa opção, especifique o processo de fluxo de trabalho aplicável. O email definido com essa política envia uma notificação por email para cada etapa de aprovação.

Evento iniciado

Envia um email quando um evento atinge o estado Antes. Ao selecionar essa opção, especifique o evento.

Observação: se você especificar Evento iniciado e ocorrer uma falha no envio do email, o evento associado à notificação não será executado.

Evento concluído

Envia um email quando um evento atinge o estado Após. Ao selecionar essa opção, especifique o evento.

Evento aprovado

Envia um email quando um evento atinge o estado Aprovado. Ao selecionar essa opção, especifique o evento.

Evento recusado

Envia um email quando um evento atinge o estado Recusado. Ao selecionar essa opção, especifique o evento.

Falha no evento

Envia um email quando um evento falha. Ao selecionar essa opção, especifique o evento.

Tarefa enviada

Envia um email quando a tarefa inicia o processamento. Ao selecionar essa opção, especifique a tarefa.

Tarefa concluída

Envia um email quando a tarefa é concluída. Ao selecionar essa opção, especifique a tarefa.

Tarefa com falha

Envia um email se ocorrer falha na tarefa. Ao selecionar essa opção, especifique a tarefa.

Guia Destinatários

É possível configurar vários destinatários para os campos Para, CC ou CCO do email. A lista de destinatários pode ser estática ou depender do tipo de ação que aciona o email e dos usuários envolvidos.

Para especificar os destinatários, selecione o ícone Editar próximo aos campos Para, CC ou CCO na guia Destinatários. Em seguida, selecione uma das opções a seguir, que permitem configurar a lista de destinatários:

Aprovadores do fluxo de trabalho

Envia o email para todos os aprovadores no processo de fluxo de trabalho. Essa opção é aplicável apenas se o email for enviado para um evento pendente do fluxo de trabalho.

Gerente

Envia o email para o gerente do usuário no qual a tarefa foi executada.

Observação: para usar a opção de destinatário Gerente, configure o atributo de gerente para o ambiente. Para configurar o atributo de gerente, vá para Ambiente, *EnvironmentName*, Configurações avançadas, Diversos no Management Console. Defina managerattribute para o nome do atributo físico que armazena o nome exclusivo do gerente de um usuário.

Para bancos de dados relacionais, especifique o atributo usando o seguinte formato:

tablename.attribute

Integrantes do grupo

Envia o email a todos os integrantes de um grupo. A seleção dessa opção abre uma lista suspensa com os nomes dos grupos disponíveis.

Integrantes da função

Envia o email a todos os integrantes de uma função administrativa. A seleção dessa opção abre uma lista suspensa com os nomes das funções disponíveis.

Endereço estático

Envia o email para um endereço de email selecionado. Você pode especificar o endereço de email na área de texto adicional disponível.

Observação: não especifique mais de um endereço na área de texto.

Usuário

Envia o email para o usuário no qual a tarefa foi executada.

Iniciador

Envia o email para a pessoa que fez a solicitação.

Personalizado

Permite que você selecione um elemento de dados personalizado para definir os destinatários.

Quando você seleciona a opção personalizada, uma lista suspensa é exibida com os elementos de dados personalizados que estão disponíveis para uso.

Observação: a seção Dados (na página 492) fornece mais informações sobre elementos de dados.

Conteúdo

Você pode definir o assunto e o corpo de um email usando texto simples, ou adicioná-los com conteúdo dinâmico que é calculado quando o email é enviado.

A linha de assunto é um campo de texto sem formatação onde você pode escrever a mensagem. Essa mensagem é o assunto do email.

O corpo é exibido em um editor de HTML. É possível inserir e formatar qualquer texto para criar o corpo do email.

Para incluir conteúdo dinâmico, selecione opções na lista suspensa. O editor adiciona indicadores de conteúdo dinâmico, que são semelhantes aos seguintes, onde o cursor está localizado:

{*type*}

type representa um dos tipos de conteúdo dinâmico com suporte.

Por exemplo, quando você seleciona o tipo de conteúdo dinâmico Atributo e especifica o atributo FirstName, o editor de HTML exibe o seguinte na guia Conteúdo:

{'Attribute: FirstName'}

Observação: para adicionar conteúdo dinâmico à linha de assunto, use a lista suspensa abaixo da linha de assunto. Para adicionar conteúdo dinâmico no corpo do email, use a lista suspensa abaixo da caixa de conteúdo.

Quando a mensagem de email é enviada, o CA Identity Manager substitui o conteúdo dinâmico pelo texto apropriado. O texto mantém a formatação, como caracteres em negrito, especificada no editor de HTML.

Os tipos de conteúdo dinâmico incluem o seguinte:

Data

Especifica a data atual no formato especificado.

Tarefa

Especifica a tarefa para a qual o email é enviado.

Nome do objeto

Especifica o nome do objeto no evento que aciona o email. Se o evento for um evento do usuário, esse campo é o nome de logon do usuário.

O objeto pode ser um item diferente de um usuário. Por exemplo, pode ser qualquer objeto gerenciado, como um grupo, função administrativa e assim por diante.

Atributo

Especifica o valor de um dos atributos do usuário. O usuário é o assunto da tarefa. Essa opção exige a seleção do atributo na lista suspensa.

Atributo do gerenciador

Especifica o valor de um dos atributos do gerenciador do usuário. O usuário é o assunto da tarefa. Essa opção exige a seleção do atributo na lista suspensa.

Observação: para usar a opção de destinatário Gerente, configure o atributo de gerente para o ambiente. Para configurar o atributo de gerente, vá para Ambiente, *EnvironmentName*, Configurações avançadas, Diversos no Management Console. Defina managerattribute para o nome do atributo físico que armazena o nome exclusivo do gerente de um usuário.

Para bancos de dados relacionais, especifique o atributo usando o seguinte formato:

tablename.attribute

Personalizado

Permite que você selecione um elemento de dados personalizado para definir os destinatários.

Quando você seleciona a opção personalizada, uma lista suspensa é exibida com os elementos de dados personalizados que estão disponíveis para uso.

Observação: a seção Dados (na página 492) fornece mais informações sobre elementos de dados.

Modificar políticas de notificação por email

Você modifica uma política de notificação por email existente para atender às suas necessidades de negócios.

Para modificar uma política de notificação por email:

1. Selecione Sistema, Email, Criar Email.

   O CA Identity Manager exibe uma tela de pesquisa.

2. Procure e selecione a política de notificação por email que deseja modificar.
3. Altere as configurações nas guias Perfil, Quando enviar, Destinatários e Conteúdo, conforme necessário.

Desativar políticas de notificação por email

Você pode ativar ou desativar as políticas de notificação por email usando a caixa de seleção Ativado na guia Perfil quando você cria ou modifica uma política de notificação por email. Quando uma política de notificação por email é desativada, o email selecionado não fica ativo e nenhum email é enviado.

Observação: as políticas de notificação por email são ativadas por padrão.

Caso de Uso: enviando um email de boas-vindas

Quando um novo funcionário é contratado, a Forward, Inc. deseja enviar um email a esse usuário para dar as boas-vindas. O email precisa fornecer informações importantes para o novo funcionário, como links para a página inicial de funcionário e informações sobre seu gerente e departamento.

Para criar o email, o administrador de Recursos Humanos usa a tarefa Criar email no console de usuário para definir as seguintes configurações:

- Na guia Quando enviar, selecione Criado pelo usuário.
- Na guia Destinatários, execute estas etapas:
  - Clique no ícone Editar próximo ao campo Para.

    Selecione Usuário e, em seguida, clique no sinal de mais. Selecione o Gerente usando o mesmo método e, em seguida, clique em OK.
  - Clique no ícone Editar próximo ao campo CC.

    Selecione Iniciador, clique no sinal de mais e, em seguida, clique em OK para enviar uma cópia do email para o usuário que criou o funcionário no CA Identity Manager.
- Na guia Conteúdo, execute estas etapas:
  - No campo Assunto, insira o seguinte texto: Bem-vindo,

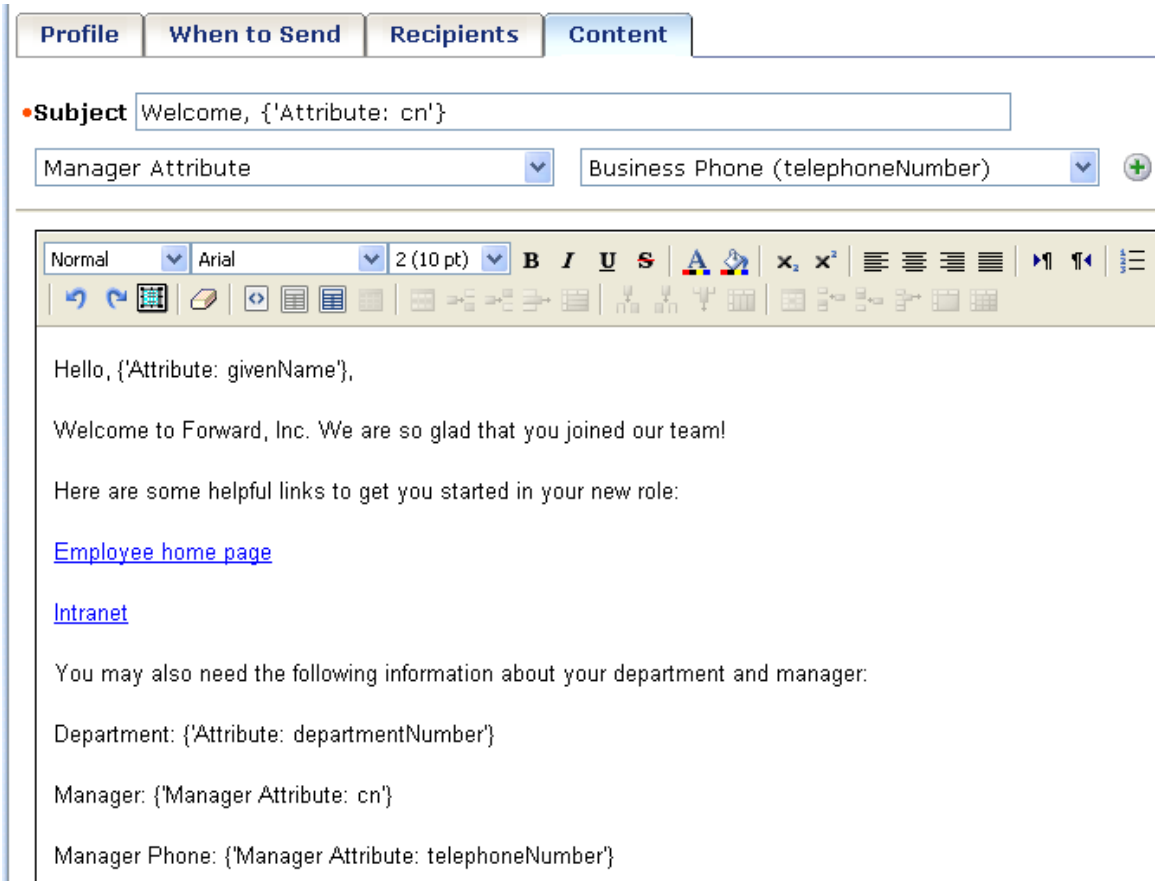
    Com o cursor no fim do texto digitado, selecione o atributo na lista suspensa. Em seguida, selecione Nome completo na segunda lista suspensa e clique no sinal de mais.

    A linha de assunto é semelhante à seguinte:

    Bem-vindo, {'Attribute: eTFullName'}

    Observação: o nome do atributo depende do repositório de usuários e do atributo que você estiver usando.
  - No campo Conteúdo, adicione qualquer texto de boas-vindas. Inclua links para o portal do funcionário e use as opções de conteúdo dinâmico abaixo da caixa de conteúdo para exibir o departamento e o gerente do usuário, além do telefone do gerente, da seguinte maneira:

Equation 1: A tela mostra a guia Conteúdo



Como usar modelos de email

O CA Identity Manager inclui modelos de email padrão que podem ser usados para gerar mensagens de email. É possível usar os modelos padrão como instalados ou personalizá-los para atender às suas necessidades de negócios.

Para usar modelos de email

1. Defina as configurações de SMTP para permitir que o CA Identity Manager envie notificações por email.
2. Ative a notificação por email no Management Console (na página 370).
3. Configure um evento ou uma tarefa para enviar um email. (na página 370)
4. (Opcional) Personalize os modelos padrão (na página 376), conforme a necessidade.

Ativar notificação por email

Você pode ativar ou desativar a notificação por email para o ambiente do CA Identity Manager. Ao ativar as notificações por email, o CA Identity Manager enviará notificações por email sobre eventos e tarefas que você especificar.

Observação: para usar o recurso de senha esquecida, ative a notificação por email.

Antes de ativar as notificações por email do CA Identity Manager, defina as configurações de SMTP (na página 356) para o seu servidor de aplicativos.

Para ativar as notificações por email

1. No Management Console, clique em Environments.

   Uma lista de ambientes do CA Identity Manager é exibida.
2. Clique no ambiente do CA Identity Manager apropriado.
3. Vá para Advanced Settings, Email.
4. Marque a caixa de seleção Enabled.
5. Configure os eventos e as tarefas que acionam o email (na página 370).
6. Clique em Salvar.
7. Reinicie a instância do servidor de aplicativos na qual o CA Identity Manager está instalado.

Configurar um evento ou uma tarefa para enviar um email

Se as notificações por email estiverem ativadas, você poderá especificar uma lista de eventos e tarefas que acionam notificações por email. Por exemplo, talvez você queira que emails sejam enviados nas seguintes circunstâncias:

- Para um administrador de sistema, na conclusão de uma tarefa de redefinição de senha do usuário.
- Para um novo gerente de funcionário, na conclusão de uma tarefa de criação de usuário. Além disso, quando o AddToGroupEvent gerado na tarefa Criar usuário é aprovado, outro email pode ser enviado a todos os integrantes de um grupo ao qual o novo usuário está sendo adicionado.

Para especificar eventos e tarefas que acionam notificações por email

1. No Management Console, clique em Environments.

   Uma lista de ambientes do CA Identity Manager é exibida.
2. Clique no ambiente do CA Identity Manager apropriado.

3. Vá para Advanced Settings, Email.

   A tela Propriedades de email é aberta.

4. Marque as caixas de seleção Ativar a seguir que se aplicarem:

   - Email de eventos ativado

     Ativa a notificação por email para eventos do CA Identity Manager

   - Email de tarefas ativado

     Ativa a notificação por email para tarefas do CA Identity Manager

5. Insira o local dos modelos de email que o CA Identity Manager usa para criar as mensagens de email.

   Os modelos de email estão localizados em um subdiretório no seguinte local:

   iam_im.ear\custom\emailTemplates

   Observação: quando você cria um arquivo de modelo de email com um nome de arquivo usando um idioma diferente, a sessão do sistema operacional deve estar operando em um idioma que ofereça suporte ao conjunto de caracteres.

6. Especifique os eventos para os quais as notificações por email são enviadas, como se segue:

   - Para adicionar um evento, selecione o evento na caixa de listagem Evento e clique em Adicionar.

     O CA Identity Manager adiciona o evento selecionado à lista de eventos para os quais as notificações por email são enviadas.

     Observação: se você selecionar um evento que não esteja associado a um processo de fluxo de trabalho, o CA Identity Manager enviará uma notificação por email quando o evento for concluído.

   - Para excluir um evento, marque a caixa de seleção do evento e clique em Excluir.

7. Especifique as tarefas para as quais as notificações por email são enviadas, como se segue:

   - Para adicionar uma tarefa, procure-a selecionando uma condição no primeiro campo e inserindo um nome de tarefa no segundo campo. Clique em Pesquisar.

     É possível digitar um nome de tarefa parcial usando o caractere curinga (*). Por exemplo, para procurar Criar tarefa, insira Criar*.

     Selecione uma ou mais tarefas nos resultados da pesquisa. Clique em Adicionar.

     Observação: as notificações por email em nível de tarefa não estão disponíveis para tarefas que tenham o tipo de ação Exibir ou Autoexibição. Para ver o tipo de ação de uma tarefa, vá para Modificar tarefa administrativa, selecione uma tarefa e marque o campo de ação no perfil da tarefa.

   - Para excluir uma tarefa, marque a caixa de seleção da tarefa e clique em Excluir.

     A exclusão de uma tarefa a remove da tabela de tarefas. A tarefa não é excluída.

8. Quando terminar de configurar as tarefas e os eventos que acionam notificações por email, clique em Salvar.
9. Reinicie o servidor de aplicativos no qual o CA Identity Manager está instalado.

Conteúdo do email

As notificações por email consistem em um modelo genérico mais detalhes específicos da tarefa que são adicionados ao email por meio da API de email. Por exemplo, as informações a seguir podem ser inseridas em um email para uma tarefa de criação de usuário:

- O nome do administrador que está executando a tarefa
- O nome do novo usuário
- O endereço de email do usuário, nome do departamento e outros dados do atributo
- A organização onde o usuário está sendo criado
- Tempo e status de aprovação do fluxo de trabalho
- O nome da tarefa e os nomes dos eventos na tarefa

Modelos de email

As notificações por email são geradas dos modelos de email. O CA Identity Manager fornece modelos de email padrão que você pode usar como instalados ou que pode usar para criar seus próprios modelos de email.

Cada modelo de email contém o seguinte:

- **Informações de entrega** - uma lista de destinatários de email. O CA Identity Manager gera automaticamente a lista de destinatários, com base nos usuários envolvidos na tarefa. Por exemplo, um email de aprovação é enviado a todos os Aprovadores da tarefa.
- **Assunto** - o texto usado na linha de assunto da mensagem.
- **Conteúdo** - o corpo da mensagem. Geralmente, o corpo contém texto estático e variáveis, que o CA Identity Manager resolve com base na tarefa ou no evento que aciona o email.

Os modelos de email padrão estão localizados em um diretório emailTemplates onde as ferramentas administrativas do CA Identity Manager estão instaladas. O local de instalação padrão das ferramentas administrativas é:

- Para Windows - C:\Arquivos de programas\CA\IAM Suite\Identity Manager \tools\emailtemplates
- Para UNIX - <diretório_inicial>/CA/IAM Suite/Identity Manager/tools/emailtemplates

O diretório emailTemplates contém cinco pastas. Cada pasta está associada a um estado de evento ou tarefa:

Diretório	Conteúdo
Aprovado	defaultEvent.tmpl - informa os destinatários que um evento foi aprovado

Diretório	Conteúdo
Concluído	■ CertificationNonCertifiedActionCompletedNotification.tmpl - informa o gerente que uma ação fora de conformidade foi aplicada a um funcionário. ■ CertificationNonCertifiedActionPendingNotification.tmpl - informa o gerente que uma ação fora de conformidade será aplicada a um funcionário. ■ CertificationRequiredFinalNotification.tmpl - lembrete final para um gerente que a tarefa de certificação do usuário deve ser concluída para um funcionário. ■ CertificationRequiredNotification.tmpl - informa o gerente que um processo de certificação teve início para um funcionário. O gerente deve concluir um a tarefa de certificação do usuário para esse funcionário. ■ CertificationRequiredReminderNotification.tmpl - lembra o gerente que a tarefa de certificação do usuário deve ser concluída para um funcionário. ■ Certify Employee.tmpl - informa um administrador que o processo de certificação para um funcionário foi concluído. ■ CreateProvisioningUserNotificationEvent.tmpl - envia uma senha temporária a um usuário quando a conta desse usuário é criada no diretório de provisionamento. ■ defaultTask.tmpl - informa os destinatários que o CA Identity Manager concluiu uma tarefa. ■ ForgottenPassword.tmpl - envia uma senha temporária aos usuários que usaram o recurso de senha esquecida. ■ ForgottenUserID.tmpl - envia uma ID aos usuários que usaram o recurso de ID de usuário esquecida. ■ Self Registration.tmpl - informa um usuário que a tarefa de autorregistro foi concluída com êxito.
Inválido	■ AssignProvisioningRoleEvent.tmpl - informa os destinatários que uma solicitação para adicionar um usuário a uma função de provisionamento falhou ■ DefaultEvent.tmpl - informa os destinatários que um evento falhou ■ DefaultTask.tmpl - informa os destinatários que uma tarefa do CA Identity Manager falhou
Pendente	■ defaultEvent.tmpl - informa os aprovadores que um item da lista de tarefas requer atenção ■ ModifyUserEvent.tmpl - igual ao modelo padrão, mas inclui métodos para recuperar os atributos do objeto gerenciado pelo usuário
Recusado	defaultEvent.tmpl - informa os destinatários que um evento foi rejeitado

Use os modelos e a estrutura do diretório de modelos do CA Identity Manager que estão instalados no diretório *<dir_ferramentas_administrativas_im>*\Identity Manager\tools\
emailTemplates como uma base para criar modelos de email personalizados.

Diretórios de modelo

Cada diretório de modelo descrito em Modelos de email (na página 373) está associado a um estado específico de tarefa ou evento. Por exemplo, se um email deve ser enviado para um evento que foi recusado em um processo de fluxo de trabalho, o CA Identity Manager procura pelo modelo a ser usado em um diretório recusado implantado. Em seguida, o CA Identity Manager gera o email usando o modelo adequado no diretório.

Modelos de email em um diretório

Cada diretório de modelos implantado contém um ou mais modelos de email. Quando ocorrer uma tarefa ou um evento para o qual o email estiver ativado, o CA Identity Manager buscará o diretório de modelos apropriado para obter um nome de modelo que seja igual ao nome da tarefa ou do evento. Se tal modelo não puder ser encontrado, o CA Identity Manager usará o modelo padrão no diretório. Os nomes de modelo padrão estão listados em Modelos de email (na página 373). Por exemplo, o CA Identity Manager usa defaultEvent.tmpl no diretório Pendente para informar os aprovadores que eles têm um novo item de lista de tarefas.

Conjuntos de diretórios de modelos

Um conjunto de diretórios de modelos contém um diretório aprovado, concluído, pendente e recusado. Você pode implantar vários conjuntos de diretórios de modelos e especificar um conjunto a ser usado para um determinado ambiente do CA Identity Manager.

A Implantação de modelo de email (na página 395) fornece informações sobre como implantar conjuntos de diretórios de modelos.

Para obter informações sobre como configurar diretórios de modelos de email para que o CA Identity Manager use o conjunto correto para um determinado ambiente, consulte o *Guia de Configuração do CA Identity Manager*.

Criar modelos de email

Para criar mensagens de email personalizadas

1. Abra o modelo que você deseja modificar.

   Por exemplo, se você deseja criar uma mensagem de email para um evento pendente Criar usuário, abra defaultEvent.tmpl no diretório Pendente.

2. Salve o modelo no mesmo diretório com um novo nome. O nome deve corresponder ao nome do evento ao qual o email se aplica e ter a extensão .tmpl.

   Por exemplo, o nome da mensagem para o evento pendente Criar usuário é:

   CreateUserEvent.tmpl

   Observação: quando você cria um arquivo de modelo de email com um nome de arquivo usando um idioma diferente, a sessão do sistema operacional deve estar operando em um idioma que ofereça suporte ao conjunto de caracteres.

3. Modifique o modelo de mensagem de acordo com as necessidades, conforme descrito na próxima seção, Modelos de email personalizados (na página 376).

Modelos de email personalizados

Um modelo de email é um arquivo dinâmico que oferece suporte ao HTML e JavaScript do lado do servidor incorporado. Um modelo permite que você insira os valores de variável em texto estático, o que, por sua vez, permite que as mensagens específicas do caso sejam geradas de um único modelo.

O mesmo modelo pode ser usado inúmeras vezes para imprimir texto estático clichê (como a frase que foi aprovada) juntamente com o texto variável específico a um determinado contexto (como o nome do evento que está sendo aprovado).

Por exemplo, veja a seguir um modelo para relatar a aprovação de um evento:

```
<!-- Define the E-mail Properties --->
<%
   _to = _util.getNotifiers("ADMIN");
   _cc = "" ;
   _bcc = "";
   _subject = _eventContextInformation.getEventName() + " approved";
%>
<!--- Start of Body --->
<html>
<body text="Navy">
```

```
Event: <b> <%=_eventContextInformation.getEventName()%> </b><br>
<%=_eventContextInformation.getPrimaryObjectTypeName()%>:
<b><%=_eventContextInformation.getPrimaryObjectName()%></b><br>
In <%=_eventContextInformation.getSecondaryObjectTypeName()%>:
<b><%=_eventContextInformation.getSecondaryObjectName()%></b><br>
Status: <b>Approved</b>
</body>
</html>
```

Observação: objects _util e _eventContextInformation do CA Identity Manager usados no exemplo acima são descritos em API de modelo de email (na página 379).

Se uma aprovação for gerada para o evento CreateUserEvent, e o usuário John Jones for criado na organização RH, o corpo da notificação de email gerada do modelo de aprovação poderá ter esta aparência:

```
Event: CreateUserEvent
USER: John Jones
In ORGANIZATION: HR
Status: Approved
```

As seções a seguir descrevem a sintaxe e os objetos do CA Identity Manager que tornam possíveis as mensagens de email dinâmicas.

Elementos do modelo

Os modelos de email do CA Identity Manager oferecem suporte a:

- Tags HTML padrão.
- JavaScript do lado do servidor.
- Um ou mais objetos implícitos que o CA Identity Manager disponibiliza a uma instância do modelo, isto é, a uma mensagem de email.
- As tags do CA Identity Manager que permitem incorporar o JavaScript no modelo, chamar os métodos nos objetos implícitos do CA Identity Manager e inserir valores de variável no texto estático do modelo.

Extensões de tag do CA Identity Manager

Os modelos de email oferecem suporte às seguintes tags:

<% %>

Incorpora JavaScript em um modelo de email.

<%= %>

Insere um valor de variável em texto estático.

As tags são descritas nas seções a seguir.

<% %>

Essa tag permite que você incorpore JavaScript para execução em linha em um modelo de email.

Você pode usar qualquer objeto JavaScript dentro do JavaScript incorporado. Também é possível chamar métodos de objeto implícito do CA Identity Manager no JavaScript incorporado.

Por exemplo, o código a seguir modifica o corpo do modelo de aprovação mostrado em Personalizar modelos de email (na página 376). O JavaScript é usado para determinar se um objeto secundário é envolvido no evento (como um objeto ORGANIZATION quando um objeto principal USER é adicionado). Se não houver nenhum objeto secundário, o texto relacionado ao objeto secundário é omitido da mensagem:

```
Event: <b> <%=_eventContextInformation.getEventName()%> </b><br>
<%=_eventContextInformation.getPrimaryObjectTypeName()%>:
<b><%=_eventContextInformation.getPrimaryObjectName()%></b><br>
<%
var secondaryType =        _eventContextInformation.getSecondaryObjectTypeName();
if (secondaryType != "") {
   template.add("In " + secondaryType + ": ");
   template.add("<b> "+_eventContextInformation.getSecondary
                                    ObjectName()+" </b><br>");
   }
%>
Status: <b>Approved</b>
```

<%= %>

Essa tag permite que você insira um valor de variável em texto estático. O valor pode ser:

- Uma variável definida em algum JavaScript executado anteriormente no modelo. Por exemplo:

  ```
  <%
  var secondaryType =
       _eventContextInformation.getSecondaryObjectTypeName();
  ...          // More JavaScript processing
  %>
  ...          // More HTML
  The primary object was created in <%=secondaryType%>.
  ```

- Um valor retornado de um método em um objeto implícito do CA Identity Manager. Por exemplo:

  ```
  Event <%=_eventContextInformation.getEventName()%> is approved.
  ```

API de modelo de email

Quando uma mensagem é gerada de um modelo, o CA Identity Manager disponibiliza os objetos implícitos abaixo para a mensagem. Esses objetos permitem que você insira informações específicas da instância em uma mensagem chamando métodos na API de modelo de email.

Um modelo pode chamar os métodos em qualquer um dos seguintes objetos:

- _contentType. Especifica o contentType do email.
- _priority. Especifica a prioridade do email.
- _to. Adiciona os destinatários ao campo Para da mensagem.
- _cc. Adiciona os destinatários ao campo cc (com cópia para) da mensagem.
- _bcc. Adiciona os destinatários ao campo cco (com cópia oculta para) da mensagem.
- _subject. Especifica o assunto do email.
- _encoding. Especifica a codificação do email.
- _additionalHeaders. Permite especificar os atributos extras do cabeçalho do email no modelo de email.
- template. Permite adicionar uma sequência de caracteres de texto a uma mensagem das linhas de código JavaScript.
- _util. Um objeto utilitário.
- _eventContextInformation. Contém informações sobre o evento gerado pela tarefa atual, como nome do evento e status de aprovação.
- _taskContextInformation. Contém um conjunto de informações sobre a tarefa atual, como o nome da tarefa, o nome da organização e eventos constituintes.

Esses objetos são descritos nas seções a seguir:

contentType

Especifica o contentType do email.

Se nenhum contentType for especificado por meio da variável _contentType, será aplicado o padrão "text/html" de contentType.

Métodos: nenhum.

Exemplo:

```
<% _contentType = "text/html"; %>
```

priority

Especifica a prioridade do email. Especifique 0 para nenhuma prioridade (padrão) e 1 para prioridade alta.

Métodos: nenhum.

Exemplo:

```
<% _priority = "1"; %>
```

to

Adiciona os destinatários ao campo Para da mensagem.

O valor da variável _to é uma sequência de caracteres JavaScript. Vários destinatários são permitidos, mas a sequência de caracteres deve estar de acordo com a sintaxe do JavaScript, como mostrado no exemplo a seguir.

Métodos: nenhum.

Exemplo:

```
<%
_to =
_util.getNotifiers("USER") + ',' +
_util.getNotifiers("USER_MANAGER","ManagerLookup=managerattribute");
_cc = "" ;
_bcc = "" ;
_subject = "Your new password ";
%>
```

Observação: quando os emails alertam os participantes que uma tarefa está no estado Pendente e sob o controle de fluxo de trabalho, o objeto _to é preenchido previamente com os endereços dos participantes. Não é possível usar o objeto _to em um modelo Pendente.

cc

Adiciona os destinatários ao campo cc (com cópia para) da mensagem.

O valor da variável _to é uma sequência de caracteres JavaScript. Vários destinatários são permitidos, mas a sequência de caracteres deve estar de acordo com a sintaxe do JavaScript, como mostrado no exemplo a seguir.

Métodos: nenhum.

Exemplo:

```
<%
_cc =
_util.getNotifiers("USER") + ',' +
_util.getNotifiers("USER_MANAGER","ManagerLookup=managerattribute");
%>
```

bcc

Adiciona os destinatários ao campo cco (com cópia oculta para) da mensagem.

Endereços de email especificados nesse campo não aparecem no email.

O valor da variável _to é uma sequência de caracteres JavaScript. Vários destinatários são permitidos, mas a sequência de caracteres deve estar de acordo com a sintaxe do JavaScript, como mostrado no exemplo a seguir.

Métodos: nenhum.

Exemplo:

```
<%
_bcc =
_util.getNotifiers("USER") + ',' +
_util.getNotifiers("USER_MANAGER","ManagerLookup=managerattribute");
%>
```

subject

Especifica o assunto do email.

Métodos: nenhum.

Exemplo:

```
<% _subject=_eventContextInformation.getEventName()+" approved";%>
```

encoding

Especifica a codificação do email.

Se nenhuma codificação for especificada por meio de _encoding or pela variável LANG, os caracteres no email podem não ser exibidos corretamente. Certifique-se de definir _encoding ou LANG para a localidade apropriada.

Métodos: nenhum.

Exemplo:

```
<% _encoding = "UTF-8"; %>
```

additionalHeaders

_additionalHeaders

Especifica atributos extras de cabeçalho de email no modelo de email.

Você deve atribuir um HashMap() a esse atributo. Os nomes e valores armazenados no HashMap devem ser sequências de caracteres.

Exemplo: Adicionar atributos de cabeçalho personalizados

O exemplo a seguir mostra como adicionar dois atributos de cabeçalho personalizados, "X-TCCCSWD" e "myheader":

```
<!-- Define the E-mail Properties --->
<%
_to = "siteadmin@ca.com";
_cc = "" ;
_bcc = "" ;
_subject = _eventContextInformation.getEventName() +" completed";
var additionalHeaders = new java.util.HashMap();
additionalHeaders.put("header_a","1");
additionalHeaders.put("header_b","foo");
_additionalHeaders = additionalHeaders;
%>
```

template

Permite adicionar uma sequência de caracteres de texto a uma mensagem usando as linhas de código JavaScript (isto é, as linhas dentro da tag <% %>). A sequência de caracteres pode conter tags HTML, texto estático e/ou valores de variável retornados pelos métodos nos objetos implícitos do CA Identity Manager.

Observação: o objeto de modelo não é precedido pelo caractere sublinhado (_).

Método:

- add(String)

  O argumento deve ser avaliado para uma sequência de caracteres, incluindo todas as chamadas aos métodos em um objeto implícito do CA Identity Manager. No exemplo abaixo, veja _eventContextInformation.getSecondaryObjectName().

Exemplo:

```
<%
var secondaryType =        _eventContextInformation.getSecondaryObjectTypeName();
if (secondaryType != "") {
   template.add("In " + secondaryType + ": ");
   template.add("<b> "+_eventContextInformation.getSecondary
                                    ObjectName()+" </b><br>");
   }
%>
```

util

Objeto utilitário.

Método:

- getNotifiers(String [,String])

  Retorna IDs de email com base em uma regra de notificação.

  O primeiro argumento oferece suporte às seguintes regras de notificação predefinidas, entre aspas:

  - "ADMIN". Envia o email ao administrador que iniciou a tarefa.
  - "USER". Envia email ao usuário no contexto atual.
  - "USER_MANAGER". Envia o email ao gerente do usuário no contexto atual.

Você também pode fazer referência a uma regra de notificação personalizada que você cria com a API de regra de notificação. Para obter informações, consulte o *Guia de Programação do Java*.

O segundo argumento é opcional. Você pode usá-lo para passar um ou mais pares de nome/valor definidos pelo usuário a uma regra de notificação personalizada. Separe cada par de nome/valor com uma vírgula, no seguinte formato: *"nome1=valor1,nome2=valor2,..."*

Exemplos:

```
<%

_to = _util.getNotifiers("ADMIN");_cc = "";
%>
<%
_to = _util.getNotifiers("MYRULE","type=loan,district=3");
_cc = "";
%>
```

Notificando um gerenciador de usuários

Você pode usar a regra de notificação USER_MANAGER para enviar email a gerenciador de usuário. O CA Identity Manager usa essa regra no modelos de email que ofereçam suporte à certificação dos direitos dos usuários.

Observação: a Regra de notificação USER_MANAGER se aplica somente a eventos ou tarefas que criam ou gerenciam um único usuário.

Como existem várias maneiras de especificar uma relação entre usuário e gerenciador em um diretório de usuários, o Adaptador de notificação de gerenciador de usuários padrão resolve essa relação com base em uma expressão de atributo especificada no segundo parâmetro do método getNotifiers ().

Exemplo:

```
<%
_to = _util.getNotifiers("USER_MANAGER","ManagerLookup=managerattribute");
_cc = "";
%>
```

O Adaptador de notificação de gerenciador de usuários oferece suporte a duas opções de pesquisa:

- managerattribute **=<***Nome_do_atributo do gerenciador***>**- onde o objeto User mantém um atributo que indica o DN ou UserID do gerenciador do usuário
- commonattribute **= <***Nome_do_atributo***>** - onde o usuário e o gerenciador do usuário compartilham um valor de atributo comum, como "departamento"

É possível configurar essas opções de pesquisa em Miscellaneous Properties de um ambiente no Management Console do CA Identity Manager.

Para configurar a regra de notificação USER_MANAGER:

1. No Management Console do CA Identity Manager, selecione Environment do CA Identity Manager. Em seguida, selecione o ambiente para o qual você está configurando a notificação por email.
2. Selecione Advanced Settings>Miscellaneous Properties.
3. Na página Miscellaneous Properties, conclua as etapas de configuração para a opção de pesquisa que deseja usar:
   - Para usar a opção de pesquisa managerattribute=<Nome_do_atributo do gerenciador>:
     a. No campo Property, digite managerattribute.
     b. No campo Value, insira o atributo que armazena o DN ou a ID de usuário do gerenciador.
     c. Clique em Adicionar.
     d. Clique em Salvar.
   - Para usar a opção de pesquisa commonattribute=<Nome_do_atributo>:
     a. No campo Property, digite commonattribute.
     b. No campo Value, insira o atributo que o usuário e o gerenciador de usuários têm em comum.
     c. Clique em Adicionar.
     d. No campo Property, digite ismanagerfilter.
     e. No campo Value, insira uma expressão de pesquisa usando a seguinte sintaxe:

        <atributo> <operador> <filtro>

        Por exemplo, título EQUALS gerenciador
     f. Clique em Adicionar.
     g. Clique em Salvar.

Você também pode criar um adaptador personalizado e suas próprias regras para notificar um gerenciador de usuários. Consulte o *Guia de Programação do Java*.

eventContextInformation

Contém informações sobre o evento gerado pela tarefa atual, como nome do evento e status de aprovação. Essas informações são chamadas de informações de *contexto* do evento.

O objeto _eventContextInformation é criado a partir da classe ExposedEventContextInformation no pacote com.netegrity.imapi.

Esse objeto está disponível para mensagens de email com base em modelos Aprovados, Pendentes e Recusados. Para obter informações sobre esses modelos, consulte Modelos de email (na página 373).

Métodos: todos os métodos a seguir retornam uma sequência de caracteres.

Método	Descrição
getAdminName()	Retorna o nome da pessoa que enviou a tarefa que gerou o evento. Substituído no CA Identity Manager 5.6. Use um dos seguintes métodos herdados: ■ getAdministrator() ■ getAdminFriendlyName()
getApprovalStatus()	Retorna o status de aprovação do evento. Um destes valores: APPROVAL_STATUS_APPROVED APPROVAL_STATUS_REJECTED
getApprovalTime()	Retorna a hora em que o evento foi aprovado.
getEventName()	Retorna o nome do evento. Para obter uma lista de nomes de eventos, consulte Eventos do CA Identity Manager.
getOrgName()	Retorna o nome amigável da organização na qual a tarefa está sendo executada. Substituído no CA Identity Manager 5.6. Use o método herdado getObjectOrganizationFriendlyName().
getPassword()	Se os objetos principais forem do tipo USER, retorna a senha do usuário.

Método	Descrição
getPrimaryObjectTypeName()	Retorna o tipo de objeto principal. Tipos de objeto principal retornados: ACCESSROLE ACCESSTASK ADMINROLE ADMINTASK GROUP ORGANIZATION USER
getPrimaryObjectName()	Retorna o nome do objeto principal afetado pelo evento. Um *objeto principal* é o objeto afetado diretamente pelo evento. Um *objeto secundário* é o objeto ao qual o objeto principal está vinculado, se houver. Por exemplo: ■ O tipo de objeto principal para CreateUserEvent é USER. O objeto secundário é o objeto em que o usuário foi criado, isto é, ORGANIZATION. ■ O tipo de objeto principal para CreateAdminRoleEvent é ADMINROLE. Esse objeto não está vinculado a outros objetos, portanto, não há objeto secundário. Com um objeto principal do tipo USER, getPrimaryObjectName() pode retornar John Jones.
getSecondaryObjectTypeName()	Se um objeto secundário foi afetado pelo evento, retorna o tipo de objeto. Tipos de objeto secundário retornados: ACCESSROLE ACCESSTASK ADMINROLE ADMINTASK GROUP ORGANIZATION USER

Método	Descrição
getSecondaryObjectName()	Se um objeto secundário foi afetado pelo evento, retorna o nome do objeto. Consulte getPrimaryObjectName() para obter informações sobre objetos principal e secundário. Com um objeto secundário do tipo ORGANIZATION, o método getSecondaryObjectName() pode retornar RH.

Observação: os métodos em _eventContextInformation são fornecidos por meio da interface ExposedEventContextInformation. Como ExposedEventContextInformation herda métodos na API principal do CA Identity Manager, _eventContextInformation também pode chamar esses métodos de um modelo de email, juntamente com os métodos na tabela acima. Para obter mais informações sobre esses métodos herdados, consulte Métodos adicionais (na página 392).

Exemplo - notificação por email sobre um evento Pendente:

```
<%

_cc = "" ;_bcc = "";
_subject = _eventContextInformation.getEventName() +
                                                " Approval Request";
%>
<!--- Start of Body --->
<html>
<body text="Navy">

The following item has been added to your work list for approval:
<br><br><br>
Event: <b><%=_eventContextInformation.getEventName()%></b> <br>
<%=_eventContextInformation.getPrimaryObjectTypeName()%>:
<b><%=_eventContextInformation.getPrimaryObjectName()%></b><br>
In <%=_eventContextInformation.getSecondaryObjectTypeName()%>:
<b><%=_eventContextInformation.getSecondaryObjectName()%></b><br>
</body>
</html>
```

Possível corpo do email:

De: lsmith@security.com [mailto:lsmith@security.com]
Para: vimperioso@security.com
Assunto: CreateUserEvent Approval Request

The following item has been added to your work list for approval:

Event: **CreateUserEvent**
USER: **Richard Ferrigamo**
In ORGANIZATION: **Mortgages & Loans**

Observação: o valor do campo De é derivado do arquivo email.properties. Para alterar o valor, edite o seguinte arquivo:

<*iam_im.ear*>\config\com\netegrity\config\email.properties

onde <*iam_im.ear*> é o local de instalação do CA Identity Manager no domínio do servidor de aplicativo. Por exemplo:

Para WebLogic:

<*base_do_WebLogic*>\user_projects\<domain>\applications\iam_im.ear

Para JBoss:

<*base_do_Identity Manager*>\jboss-3.2.2\server\default\deploy\iam_im.ear

Para WebSphere:

<*dir_ferramentas_administrativas_im*>\WebSphere-ear\iam_im.ear

Para adicionar mais informações sobre o usuário afetado pelo evento ao email no exemplo anterior, adicione texto semelhante ao seguinte:

```
<% user = _eventContextInformation.getEvent().getUser(); %>
<b>User information:</b><br>
Last Name: <b><%=user.getAttribute("%LAST_NAME%")%></b><br>
First Name: <b><%=user.getAttribute("%FIRST_NAME%")%></b><br>
Full Name: <b><%=user.getAttribute("%FULL_NAME%")%></b><br>
Email: <b><%=user.getAttribute("%EMAIL%")%></b><br>
Organization Membership: <b><%=user.getAttribute("%ORG_MEMBERSHIP%")%></b><br>
```

Possível corpo do email:

De: lsmith@security.com [mailto:lsmith@security.com]
Para: vimperioso@security.com
Assunto: CreateUserEvent Approval Request

The following item has been added to your work list for approval:

Event: **CreateUserEvent**
USER: **Richard Ferrigamo**
In ORGANIZATION: **Mortgages & Loans**
User information:
Last Name: Ferrigamo
First Name: Richard
Full Name: Richard Ferrigamo
Email: rferrigamo@mybank.org
Organization Membership: **Mortgages & Loans**

taskContextInformation

Contém um conjunto de informações sobre a tarefa atual, como o nome da tarefa, o nome da organização e eventos constituintes. Essas informações são chamadas de informações de *contexto* da tarefa.

Esse objeto está disponível para mensagens de email com base em modelos Concluídos. Para obter informações sobre esse modelo, consulte Modelos de email (na página 373).

Métodos: todos os métodos abaixo retornam uma sequência de caracteres, exceto para o método getExposedEventContexts(), que retorna um Java Vector.

Método	Descrição
getAdminName()	Retorna o nome da pessoa que está enviando a tarefa. Substituído no CA Identity Manager 5.6. Use um dos seguintes métodos herdados: ■ getAdministrator() ■ getAdminFriendlyName()

Método	Descrição
getExposedEventContexts()	Retorna um Java Vector de todos os eventos associados à tarefa. Cada objeto no Vector é um objeto de contexto do evento. É possível usar os métodos listados em _eventContextInformation para recuperar informações de contexto para um determinado objeto de evento. O objeto de retorno é um objeto padrão Java Vector. Você pode usar qualquer um métodos do objeto Vector. Por exemplo, get() e size(), para gerenciar os elementos no Vector.
getOrgName()	Retorna o nome da organização na qual a tarefa está sendo executada. Substituído no CA Identity Manager 5.6. Use o método herdado getObjectOrganizationFriendlyName().
getTaskName()	Retorna o nome da tarefa que está sendo executada. Substituído no CA Identity Manager 5.6. Use um dos seguintes métodos herdados: ■ getAdminTask() ■ getTaskFriendlyName()

Observação: os métodos em _taskContextInformation são fornecidos por meio da interface ExposedTaskContextInformation. Como ExposedEventContextInformation herda métodos na API principal do CA Identity Manager, _taskContextInformation também pode chamar esses métodos de um modelo de email, juntamente com os métodos na tabela acima. Para obter mais informações sobre esses métodos herdados, consulte Métodos adicionais (na página 392).

Exemplo - corpo de um modelo de notificação por email para uma alteração de senha:

```
<%
var imsEventContexts =
            _taskContextInformation.getExposedEventContexts();
if(imsEventContexts != null)
   {
   for(var i=0;i<imsEventContexts.size();i++)
      {
      var eventContext = imsEventContexts.get(i);
      template.add("Hi "+ eventContext.getPrimaryObjectName()
                                                        + ",");
      template.add("<br>Your new password is: <b>"+
                           eventContext.getPassword());</br>
      template.add("<hr>");
      }
   }
%>
```

Possível corpo do email:

Olá Victor Imperioso,
A sua nova senha é: LFH7F1226

Métodos adicionais

Os métodos _taskContextInformation e _eventContextInformation são fornecidos por meio dos objetos do CA Identity Manager ExposedTaskContextInformation e ExposedEventContextInformation, respectivamente.

Esses objetos herdam métodos na API principal do CA Identity Manager. Consequentemente, os métodos herdados também estão disponíveis para _taskContextInformation and _eventContextInformation.

Os seguintes métodos herdados do objeto TaskInfo são particularmente úteis para um modelo de email:

- getAdministrator(). Recupera um objeto User para o administrador que está executando a tarefa atual.
- getAdminTask(). Recupera um objeto AdminTask para a tarefa atual.

Esses objetos recuperados permitem inserir informações específicas de administrador e específicas de tarefa em um email. Por exemplo:

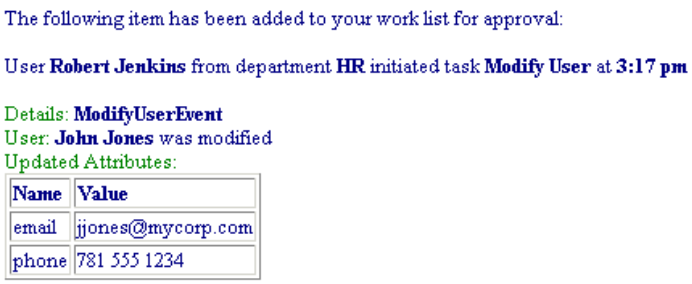
```
<!-- Define the E-mail Properties --->

<%
   _cc = "" ;
   _bcc = "" ;
   _subject = _eventContextInformation.getEventName() +
                                                 " Approval Request";
%>
<!--- Start of Body --->
<html>
<body text="Navy">

The following item has been added to your work list for approval:<br>
<br>
User <b><%= _eventContextInformation.getAdministrator().
               getAttribute(Packages.com.netegrity.llsdk6,imsapi.
                managedobject.User.PROPERTY_FRIENDLY_NAME)%> </b>
               from department <b><%= _eventContextInformation.
               getAdministrator().getOrg(null).getFriendlyName()
               %></b> initiated task <b><%= _eventContextInformation.
               getAdminTask().getFriendlyName() %></b>at <b><%=
               _eventContextInformation.getSessionCreateTime() %></b>
<br><br>
<font color="green">Details: </font><b><%=_eventContextInformation.
                                          getEventName()%></b><br>
<font color="green"><%=_eventContextInformation.
                               getPrimaryObjectTypeName()%>:</font>
<b><%=_eventContextInformation.getPrimaryObjectName()%></b>
                                                        was modified
<br>
<font color="green">Updated Attributes:</font>
<table border="1">
<tr>
  <td><b>Name</b></td>
  <td><b>Value</b></td>
</tr>
```

```
<%
   var event = _eventContextInformation.getEvent();
   if(event instanceof Packages.com.netegrity.imapi.UserEvent) {
      var user = event.getUser();
      var attributes = user.getAttributes().keys();
      while(attributes.hasMoreElements()) {
         var attr = attributes.nextElement();
         var value = user.getAttribute(attr);
         if(user.hasAttributeChanged(attr)) {
            template.add("<tr><td>" + attr +"</td>");
            template.add("<td>" + value +"</td></tr>");
         }
      }
   }
%>
</table>
<br>
</body>
</html>
```

Possível corpo do email:


The following item has been added to your work list for approval:

User **Robert Jenkins** from department **HR** initiated task **Modify User** at **3:17 pm**

Details: **ModifyUserEvent**
User: **John Jones** was modified
Updated Attributes:

Name	Value
email	jjones@mycorp.com
phone	781 555 1234

Para obter mais informações sobre os métodos herdados disponíveis para a API de modelo de email, consulte os objetos ExposedTaskContextInformation e ExposedEventContextInformation no Javadoc do CA Identity Manager.

Fluxo de saída padrão do Java

Uma mensagem de email também pode fazer chamadas para o fluxo de saída padrão do Java de dentro da tag do JavaScript (<% %>). Por exemplo, a chama a seguir envia a mensagem Concluído para o console do servidor:

```
<%
...       // JavaScript processing
out.println("Done.");
%>
```

Referência ao Javadoc

Para obter informações sobre os objetos ExposedTaskContextInformation e ExposedEventContextInformation, incluindo os métodos que eles herdam da API principal do CA Identity Manager, consulte o Javadoc do CA Identity Manager.

As páginas do Javadoc são integradas a uma versão HTML do Guia de Programação do Java, que está disponível na Biblioteca do CA Identity Manager.

Implantação do modelo de email

Quando o CA Identity Manager estiver prestes a enviar emails, ele irá procurar modelos dos quais gerar o email no seguinte local raiz no seu servidor de aplicativos:
iam_im.ear\custom\emailTemplates

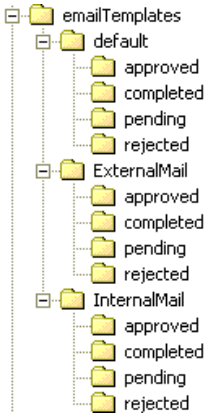
Os modelos de email implantados nessa raiz estão contidos nos conjuntos de modelos que têm a mesma estrutura de diretório, isto é, há um diretório aprovado, concluído, pendente e recusado em cada conjunto.

Conjuntos de modelos

É possível implantar vários conjuntos de modelos de email em emailTemplates. Por exemplo, durante a instalação, o seguinte conjunto de modelos de email é criado em iam_im.ear\custom \emailTemplates:

```
default\approved
default\completed
default\pending
default\rejected
```

O conjunto de modelos de email padrão contém os modelos instalados que são descritos em Modelos de email (na página 373). Você pode adicionar modelos personalizados ao conjunto padrão. Também é possível implantar outros conjuntos de modelos de email em estruturas de diretório que você define no mesmo nível que o conjunto padrão. Por exemplo, iam_im.ear\custom pode conter os seguintes modelos de email implantados:



Observação: para obter informações sobre como o CA Identity Manager escolhe um determinado modelo de email dentro de um conjunto de modelos, consulte Diretórios de modelos (na página 375).

Como especificar um conjunto de modelos de um ambiente

Ao configurar o email para um ambiente do CA Identity Manager, você especifica o conjunto de modelos de email que deseja usar para o ambiente. Para obter informações sobre como configurar email para um ambiente do CA Identity Manager, consulte o *Guia de Configuração do CA Identity Manager*.

Nomes do modelo

Os diretórios em um conjunto de modelos personalizados devem conter modelos padrão com o mesmo nome daqueles que foram instalados no conjunto de modelos padrão. Os nomes padrão são listados em Modelos de email (na página 373). O CA Identity Manager usa os modelos padrão quando não for possível encontrar nenhum outro modelo com um nome que corresponda à tarefa ou ao evento que está sendo executado.

Como opção, você pode adicionar outros modelos para um ou mais diretórios em um conjunto de modelos se desejar que um email seja gerado de um modelo específico. Para fazer isso:

- Atribua ao modelo o mesmo nome da tarefa ou do evento para o qual o email será gerado.
- Coloque o modelo no diretório associado ao estado da tarefa ou do evento para o qual o email será gerado.

Por exemplo, se desejar que os emails sejam gerados de um modelo específico quando um CreateUserEvent for recusado, coloque um modelo denominado CreateUserEvent.tmpl no diretório recusado do conjunto de modelos do ambiente.

Capítulo 13: Geração de relatórios

Esta seção contém os seguintes tópicos:

Visão geral da configuração

No CA Identity Manager, é possível executar dois tipos diferentes de relatório:

Relatórios de instantâneo

Inclui dados do banco de dados de instantâneos, que contém informações do armazenamento de objetos do CA Identity Manager e do armazenamento de usuários do CA Identity Manager. Um exemplo de um relatório de instantâneo é o relatório de perfil de usuário. Você define os dados que serão adicionados ao banco de dados de instantâneos usando Definições de instantâneo, que especificam as informações a serem incluídas.

Relatórios do Non-Snapshot

Incluem dados de outras origens de dados, como o banco de dados de auditoria. Por exemplo, o CA Identity Manager inclui relatórios de auditoria padrão. (Esses relatórios têm o prefixo "Audit - " em seu nome no console de usuário). Por padrão, o CA Identity Manager inclui apenas relatórios do Audit, mas você pode criar seus próprios relatórios personalizados que incluem dados de qualquer origem de dados, como bancos de dados de persistência de tarefas ou do fluxo de trabalho.

Cada relatório do CA Identity Manager exige configuração inicial para que seja possível executá-lo. As etapas de configuração dependem do tipo de relatório que você deseja executar.

As etapas a seguir resumem os procedimentos deste capítulo.

Para Relatórios de instantâneos

1. Crie uma definição do instantâneo para definir os dados que serão adicionados ao banco de dados de instantâneos.
2. Capture dados do instantâneo para o relatório.

3. Modificar a tarefa de relatório no console de usuário e executar as seguintes ações:
   a. Associe uma definição do instantâneo com a tarefa.
   b. Adicione o objeto de conexão rptParamConn à tarefa.
4. Solicite o relatório usando um dos seguintes métodos:
   - Executar o relatório imediatamente
   - Programar o relatório
5. Exibir o relatório no console de usuário

Para relatórios que não são de instantâneo:

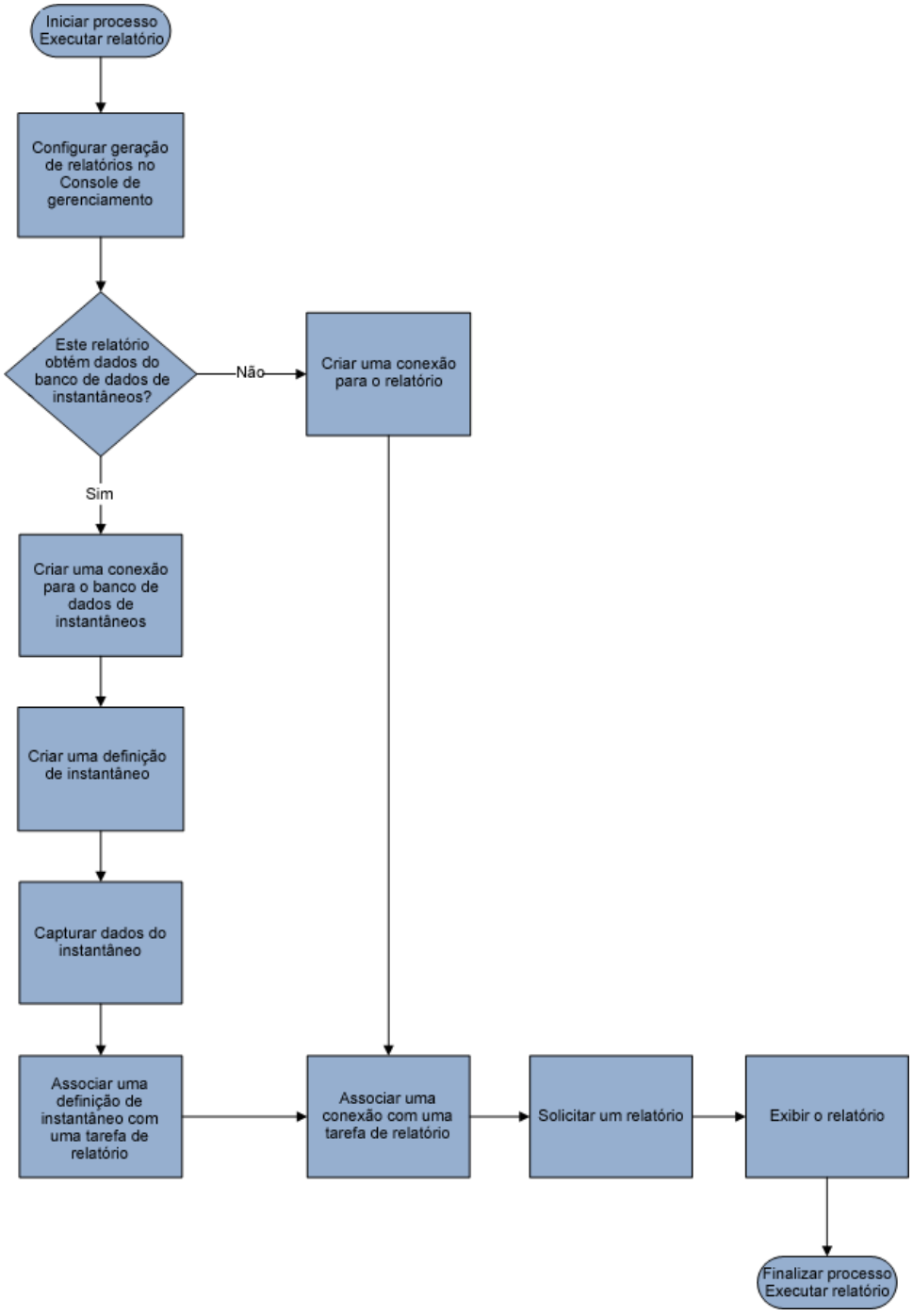
1. Crie um objeto de conexão com as informações da origem de dados para o relatório.
2. Modifique a tarefa de geração de relatório no CA Identity Manager e adicione o objeto de conexão à tarefa.
3. Solicite o relatório usando um dos seguintes métodos:
   - Executar o relatório imediatamente
   - Programar o relatório
4. Exibir o relatório no console de usuário

Depois que a configuração inicial para o relatório estiver concluída, você poderá solicitar um relatório no CA Identity Manager. Você pode executar um relatório imediatamente ou programar um relatório para ser executado posteriormente. Você também pode criar uma programação recorrente para o relatório no CA Identity Manager.

Por fim, você pode exibir o relatório no console de usuário, ou exportar o relatório para vários formatos.

O processo de relatório

O gráfico a seguir detalha o processo exigido para executar e exibir relatórios:



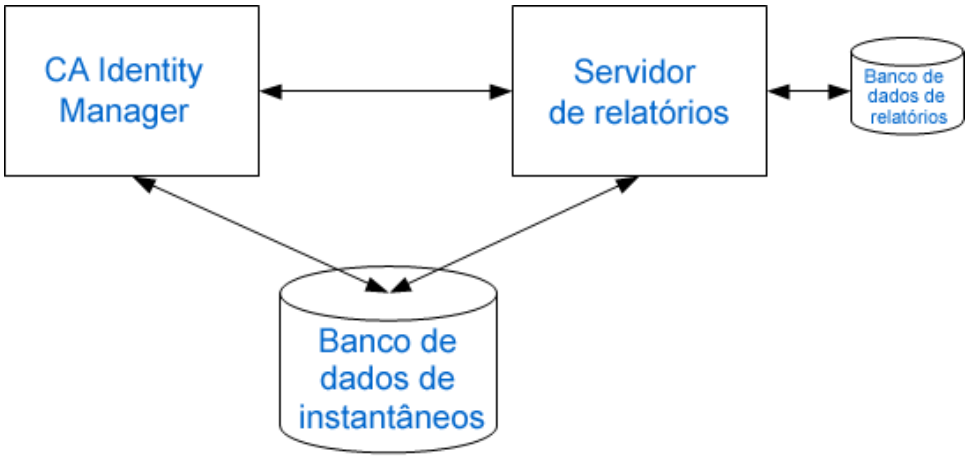
Como executar um relatório de instantâneo

Os relatórios do CA Identity Manager permitem ver o estado atual de um ambiente do CA Identity Manager. Você pode usar essas informações para assegurar a conformidade com as políticas de negócios internas ou com os regulamentos externos.

Gere relatórios do CA Identity Manager usando os dados de gerenciamento que descrevem o relacionamento entre objetos no ambiente do CA Identity Manager. Seguem alguns exemplos de dados de gerenciamento:

- Atributos de perfil dos usuários
- Lista de funções que contêm uma determinada tarefa
- Os integrantes de uma função ou de um grupo
- As regras que compõem uma função

No CA Identity Manager, a configuração de relatórios requer os três componentes principais a seguir:



Observação: o banco de dados de instantâneos neste gráfico ilustrado também poderia ser o banco de dados de auditoria ou o banco de dados de fluxo de trabalho.

Servidor de relatórios

Também conhecido como CA Business Intelligence, este servidor gera relatórios, comunicando-se diretamente com o CA Identity Manager e o banco de dados de instantâneos.

Banco de dados de relatórios

O banco de dados em que o servidor de relatórios da CA (Business Objects) armazena seus próprios dados.

CA Identity Manager

O CA Identity Manager permite exportar dados do objeto do CA Identity Manager para o banco de dados de relatórios.

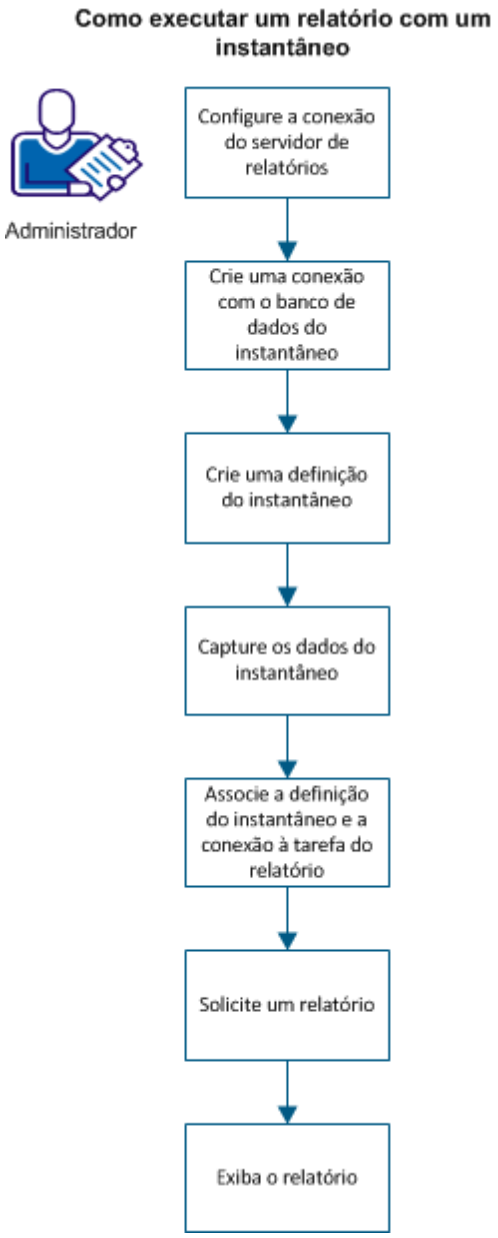
Banco de dados de instantâneos

Um banco de dados separado que contém os dados de instantâneos de objetos do CA Identity Manager

Importante: O servidor de relatórios usa o Business Objects Enterprise. Se você já tiver um servidor de relatórios em seu ambiente e você desejar usá-lo com o CA Identity Manager, a versão mínima exigida pelo CA Identity Manager é o CA Business Intelligence 3.2 SP5.

Um relatório de instantâneo inclui dados do banco de dados de instantâneos, que contém informações do armazenamento de objetos e do armazenamento de usuários do CA Identity Manager. Um exemplo de um relatório de instantâneo é o Relatório de perfis de usuário. Defina os dados de instantâneo que serão adicionados ao banco de dados de instantâneos e, usando as definições de instantâneo, especifique as informações a serem incluídas.

O gráfico a seguir ilustra o processo para executar um relatório de instantâneo:



Para executar o relatório de instantâneo, execute as seguintes etapas:

1. Configurar a conexão com o servidor de relatórios (na página 420).
2. Criar uma conexão com o banco de dados de instantâneos.
3. Criar uma definição do instantâneo.
4. Capturar os dados do instantâneo.
5. Associar uma definição do instantâneo e uma conexão com a tarefa de relatório.
6. Solicitar um relatório.

7. Exibir o relatório (na página 424).

Configurar a conexão do servidor de relatórios

Configure a conexão entre o CA Identity Manager e o servidor de relatórios.

Observação: é recomendável que todos os sistemas envolvidos na geração de relatórios sejam definidos com o mesmo fuso horário e hora.

Para definir a geração de relatórios:

1. No console de usuário, clique em Tarefas, Sistema, Geração de relatórios, Conexão com o servidor de relatórios.
2. Digite as configurações do servidor de relatórios. Observe o seguinte:
   - Nome do host e porta – o nome do host e o número da porta do URL HTTP do sistema em que o servidor de relatórios está instalado.
   - Nome da pasta de relatórios — Local dos relatórios padrão do CA Identity Manager.
   - ID de usuário — Usuário criado para o servidor de relatórios.
   - Senha — Senha para o usuário criado no servidor de relatórios.
   - Conexão segura — Marque a caixa de seleção para ativar a conexão Secure Sockets Layer (SSL) entre o CA Identity Manager e o servidor de relatórios.

     Observação: antes de marcar a caixa de seleção Conexão segura, verifique se você instalou o certificado do BOServer. Para obter mais informações sobre como configurar o SSL, consulte o capítulo Instalação do servidor de relatórios, no *Guia de Instalação*.
   - Servidor web — Definido como não IIS para o Tomcat
3. Clique em Testar conexão para verificar a conexão.
4. Clique em Enviar.

A conexão de geração de relatórios é estabelecida.

Criar uma conexão com o banco de dados de instantâneos

O CA Identity Manager precisa saber para onde deve exportar os dados do instantâneo. Crie uma conexão com o banco de dados do CA Identity Manager com o banco de dados de instantâneos.

Para criar uma conexão com o banco de dados de instantâneos:

1. No console de usuário, clique em Tarefas, Relatórios, Tarefas de instantâneo, Gerenciar conexão com o banco de dados de instantâneos, Criar conexão com o banco de dados de instantâneos.
2. Crie uma conexão com o banco de dados de instantâneos, preenchendo todos os campos necessários.
3. Clique em Enviar.

   Uma conexão com o banco de dados de instantâneos é criada.

Criar uma definição de instantâneo

Um instantâneo reflete o estado dos objetos no CA Identity Manager em um determinado momento. Você deverá usar esses dados de instantâneos para criar um relatório. Para capturar os dados do objeto do CA Identity Manager, crie uma definição do instantâneo que exporte os dados para o banco de dados de instantâneos. Usando a definição do instantâneo, você define as regras para carregar usuários, terminais, funções administrativas, funções de provisionamento, grupos e organizações.

Siga estas etapas:

1. No console de usuário, vá para Tarefas, Relatórios, Tarefas de instantâneo, Gerenciar definição de instantâneo, Criar definição de instantâneo.
2. Selecione Criar ou Copiar um objeto do Tipo de instantâneo.
3. Clique em OK.
4. Na guia Perfil, preencha os campos a seguir para criar um perfil de definição do instantâneo:

   Nome da definição do instantâneo

   Identifica o nome exclusivo que é especificado para a definição do instantâneo.

   Descrição da definição do instantâneo

   Exibe todas as informações adicionais que você desejar para descrever o instantâneo.

   Ativado

   Especifica que o CA Identity Manager cria um instantâneo com base na definição do instantâneo atual no horário programado.

   Observação: se essa opção não estiver selecionada, a definição do instantâneo não será capturada no horário programado. Além disso, a definição do instantâneo não é listada na tela de captura de dados do instantâneo.

   Número de instantâneos retidos

   Especifica o número de instantâneos bem-sucedidos retidos no banco de dados de instantâneos.

   Observação: se você não especificar um valor para esse campo, o CA Identity Manager armazena um número ilimitado de instantâneos.
5. Na guia Políticas de instantâneo, selecione os objetos que estão relacionados às políticas para exportação.
6. Na guia Configurações da função, selecione um ou mais componentes de função e atributos disponíveis para o instantâneo para exportação.

   Observação: na guia Políticas de instantâneo, se você selecionar o objeto Função de acesso, Função administrativa ou Função de provisionamento, selecione os atributos na guia Configurações da função.

7. Na guia Detalhes dos atributos de usuário, selecione um ou mais atributos do usuário para o instantâneo para exportação.

   Observação: na guia Políticas de instantâneo, se você selecionar apenas um objeto de usuário, por padrão, todos os dados relacionados a atributos de usuário serão exportados.

8. Na guia Atributos da conta do terminal, selecione um ou mais atributos de conta para um tipo de terminal.

   Observação: para um tipo de terminal selecionado, por padrão, todos os dados relacionados aos atributos da conta do terminal serão exportados. Para capturar dados relacionados a um atributo específico, selecione o atributo adequado. Para obter mais informações sobre a seleção de atributos que são necessários para exportação para um tipo de terminal, consulte a seção Relatórios padrão no *Guia de Configuração*.

9. (Opcional) Marque a caixa de seleção Exportar contas órfãs para incluir contas do terminal sem usuário global no servidor de provisionamento.

   Observação: para exportar dados do relatório para relatórios de contas fora padrão, com tendências fora do padrão e órfãs, selecione o atributo exceptionAccount e a caixa de seleção Exportar contas órfãs.

10. Clique em Enviar.

    O CA Identity Manager é configurado para criar instantâneos dos objetos mencionados na definição do instantâneo.

Agora que você já criou uma definição do instantâneo, é possível capturar dados do instantâneo imediatamente ou programar a exportação de dados do instantâneo mais tarde. O tópico Capturar dados de instantâneo fornece mais informações.

Mais informações:

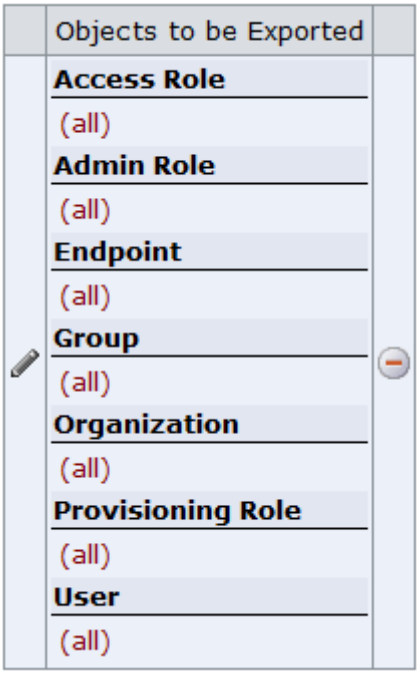
Guia Recorrência (na página 411)

Exemplo: criando uma definição de instantâneo para dados de direitos de um usuário

O exemplo a seguir ilustra o processo para criar uma definição de instantâneo de um relatório de direitos do usuário:

1. No console de usuário, vá para Tarefas, Relatórios, Tarefas de instantâneo, Gerenciar definição de instantâneo, Criar definição de instantâneo.
2. Selecione Criar um novo objeto do tipo Tipo de instantâneo.
3. Insira o nome, a descrição e o número de instantâneos retidos da Definição de instantâneo.
4. Na guia Definição de política de instantâneo, clique em Adicionar.

   No menu suspenso, selecione o usuário e selecione Todas. Da mesma maneira, adicione Terminal, Função de provisionamento, Função administrativa, Função de acesso, Organização e Grupo, conforme mostrado na tela a seguir:



5. Na guia Configuração da função, marque todas as caixas de seleção de função do usuário.
6. Na guia Atributos do usuário, selecione os atributos necessários na lista Valores disponíveis e mova-os para a lista Valores atuais.
7. Clique em Enviar.

Gerenciar instantâneos

O CA Identity Manager permite exibir, modificar e excluir suas definições de instantâneo. Ao exibir ou modificar uma definição de instantâneo, as guias Perfil e Manutenção são exibidas. A guia Manutenção é exibida apenas depois de capturar um instantâneo uma vez. Na guia Manutenção, você pode excluir os instantâneos (mesmo que o status do instantâneo seja com falha).

Para exibir, modificar ou excluir uma definição de instantâneo, vá para Relatórios, Tarefas de instantâneo, Gerenciar definição de instantâneo e clique na tarefa que deseja executar.

Observação: se uma definição de instantâneo estiver sendo usada para exportar dados para o banco de dados de instantâneos, não será possível excluir a definição de instantâneo. Ao excluir uma definição de instantâneo em uso, a exportação dos dados para o banco de dados de instantâneos é interrompida, mas a definição de instantâneo permanece disponível.

Capturar dados do instantâneo

Se desejar capturar os dados do instantâneo imediatamente ou programar a exportação dos dados do instantâneo mais tarde, ou com base em uma programação recorrente, execute a tarefa Capturar dados do instantâneo. Esta tarefa exporta os dados imediatamente (definida pela definição do instantâneo) para o banco de dados de instantâneos.

Importante: exportar dados do instantâneo pode levar muito tempo se houver uma grande quantidade de dados para exportação. Recomendamos que você programe os instantâneos para a exportação de vários dados.

Para capturar dados de instantâneo

1. No console de usuário, vá para Tarefas, Relatórios, Tarefas de instantâneo, Capturar dados do instantâneo.
2. Selecione Executar agora para executar a exportação de dados imediatamente, ou selecione Programar nova tarefa (na página 411) para executar a exportação de dados mais tarde ou em uma programação recorrente.
3. Clique em Avançar.
4. Escolha uma definição de instantâneo.
5. Clique em Enviar.

   Dados do instantâneo são exportados para o banco de dados de instantâneos.

Observação: se a tarefa Capturar dados do instantâneo parecer estar demorando demais, você pode verificar o andamento da tarefa na guia Sistema, clicando em Exibir tarefas enviadas.

Guia Recorrência

Use essa guia para programar sua tarefa. Os campos nesta guia são os seguintes:

Executar agora

Executa a tarefa imediatamente.

Programar nova tarefa

Programa uma nova tarefa.

Modificar a tarefa existente

Especifica que você deseja modificar uma tarefa que já existe.

Observação: esse campo aparece apenas se uma tarefa já tiver sido programada para essa tarefa.

Nome da tarefa

Especifica o nome da tarefa que você deseja criar ou modificar.

Fuso horário

Especifica o fuso horário do servidor.

Observação: se o seu fuso horário for diferente do fuso horário do servidor, uma caixa suspensa será exibida para que você possa escolher entre o seu fuso horário ou o do servidor ao programar uma nova tarefa. Não é possível alterar o fuso horário ao modificar uma tarefa existente.

Programação diária

Especifica que a tarefa é executada a cada número determinado de dias.

A cada (número de dias)

Define o número de dias entre as execuções da tarefa.

Programação semanal

Especifica que a tarefa é executada em um ou mais dias e hora específicos durante uma semana.

Dia da semana

Especifica os dias da semana em que a tarefa é executada.

Programação mensal

Especifica um dia da semana ou dia do mês em que a tarefa é executada mensalmente.

Programação anual

Especifica um dia da semana ou dia do mês em que a tarefa é executada anualmente.

Programação avançada

Especifica informações adicionais de programação.

Expressão cron

Para obter informações sobre como preencher esse campo, consulte o seguinte:

http://quartz-scheduler.org/api/2.1.0/org/quartz/CronExpression.html

Hora da execução

Especifica a hora do dia, no formato de 24 horas, em que a tarefa é executada. Por exemplo, 14h15.

Associar uma definição de instantâneo a uma tarefa de geração de relatório

Atribua uma definição de instantâneo para uma tarefa de geração de relatório, de forma que o CA Identity Manager saiba quais definições de instantâneo devem ser usadas para executar o relatório. Além disso, as informações de relatórios do CA Identity Manager podem ser provenientes de várias origens, e cada relatório deve ser associado a uma origem de dados específica, de acordo com as informações que deseja ver no relatório.

Para associar uma definição de instantâneo e uma conexão com uma tarefa de geração de relatório:

1. No console de usuário, vá para Tarefas, Funções e tarefas, Tarefas administrativas, Modificar tarefa administrativa.
2. Pesquise a tarefa de geração de relatório com a qual deseja associar uma definição de instantâneo.
3. Vá para a guia Guias e clique no botão Editar ao lado da guia Associar definições de instantâneo.
4. Clique em Adicionar.
5. Pesquise a definição de instantâneo a ser associada à tarefa de geração de relatório e clique em Selecionar.

   Ao associar uma definição de instantâneo a uma tarefa de geração de relatório, observe o seguinte:

   - Um relatório pode ser associado a uma ou mais definições de instantâneo.
   - Uma definição de instantâneo pode ser associada a mais de um relatório.
   - Vários instantâneos associados a uma única tarefa de geração de relatório não devem usar a mesma hora de recorrência.
6. Clique em OK.
7. Vá para a guia Pesquisar e clique em Procurar para localizar as telas de pesquisa.

8. Edite a tela de pesquisa da tarefa de geração de relatório e escolha rptParamConn em Objeto de conexão para o relatório.
9. Clique em OK.
10. Clique em Selecionar.
11. Clique em Enviar.

Sincronizar contas do terminal com modelos de conta

Essa tarefa sincroniza uma conta do terminal após a modificação de um modelo de conta associado. Por exemplo, uma conta do Active Directory não tem grupos, mas o modelo de conta associado está definido para incluir grupos.

Siga estas etapas:

1. Efetue logon no console de usuário.
2. Selecione Tarefas, Terminais, Gerenciar terminais, Verificar sincronização de contas de terminais.
3. Selecione um terminal.

   Uma tela é exibida mostrando as contas no terminal em questão, os modelos de conta associados e quais atributos não estão sincronizados.
4. Clique em Sincronizar para fazer com que os atributos para essas contas correspondam ao que está definido no modelo de conta.

   As alterações que você fizer nos modelos de conta afetam as contas existentes da seguinte maneira:

   - Se você alterar o valor de um atributo de recurso, o atributo da conta correspondente será atualizado para ser sincronizado com o valor do atributo do modelo de conta. Consulte a descrição de sincronização fraca e forte.
   - Alguns atributos de conta são designados pelo conector como não sendo atualizados após alterações no modelo de conta. Os exemplos incluem determinados atributos que o tipo de terminal permite que sejam definidos apenas durante a criação da conta, e o atributo Senha.

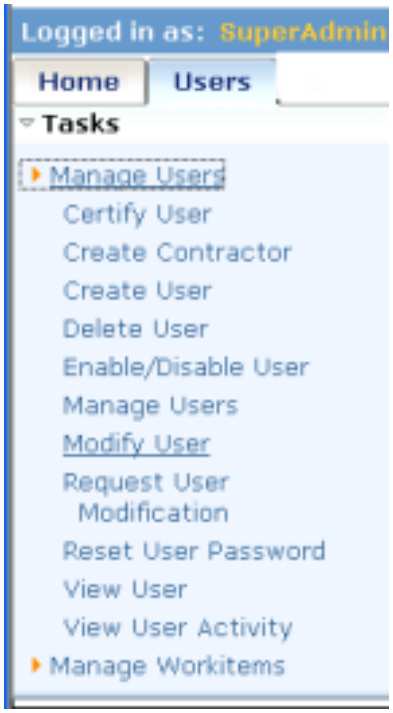
Um exemplo de tarefa administrativa

Ao criar uma tarefa administrativa, você define o conteúdo e o layout das telas na tarefa, incluindo:

- O nome da tarefa
- A categoria na qual a tarefa é exibida

- As guias e os campos a serem usados na tarefa, bem como as propriedades de exibição do campo
- Os campos que um administrador pode usar em uma consulta de pesquisa e os campos exibidos nos resultados da pesquisa

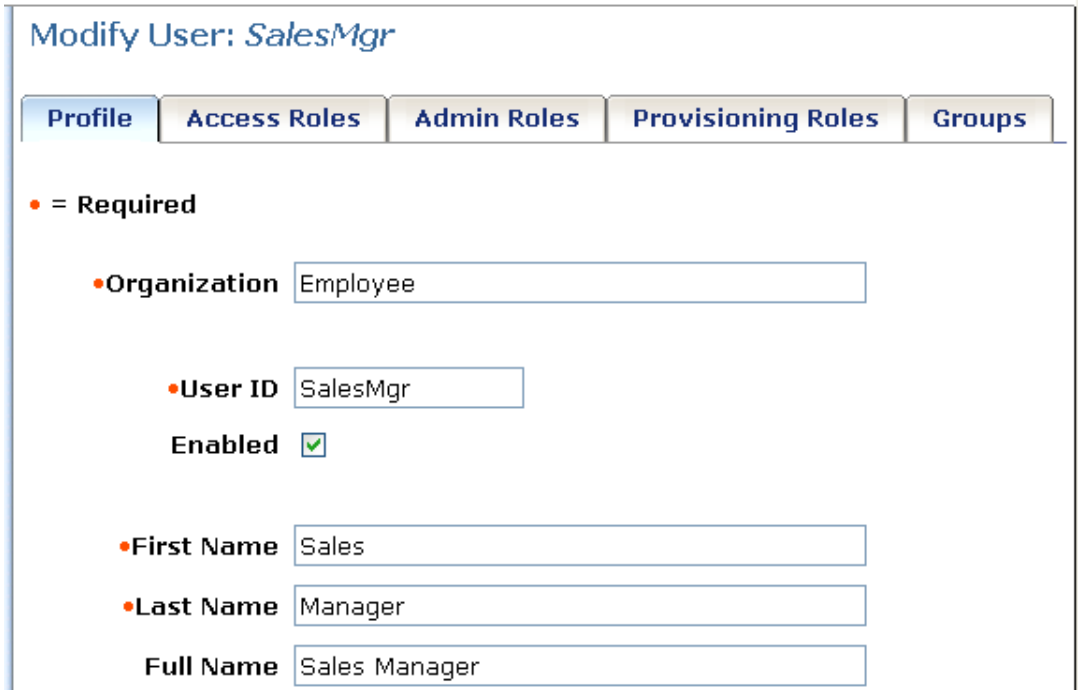
Para compreender os elementos de uma tarefa, considere a tarefa Modificar usuário. Nesse caso, Usuários é a categoria, Gerenciar usuários é uma subcategoria e Modificar usuário é a tarefa. Você cria os nomes da categoria e da tarefa quando cria uma tarefa.



Quando você seleciona Modificar usuário, uma tela de pesquisa é exibida. Uma *tela de pesquisa* contém opções para localizar o objeto a ser exibido ou modificado. Cada opção é chamada de *filtro*, que é um limite para os objetos encontrados pela pesquisa.

Após preencher a tela de pesquisa, uma tela com guias será exibida. Por exemplo, a figura a seguir mostra as guias para a tarefa Modificar usuário. A guia Perfil é exibida primeiro e mostra os atributos do usuário; as outras guias mostram a função e os privilégios de grupo do usuário.

Para a tarefa criada, você decide quais guias incluir e determina a ordem e o conteúdo de cada uma delas.

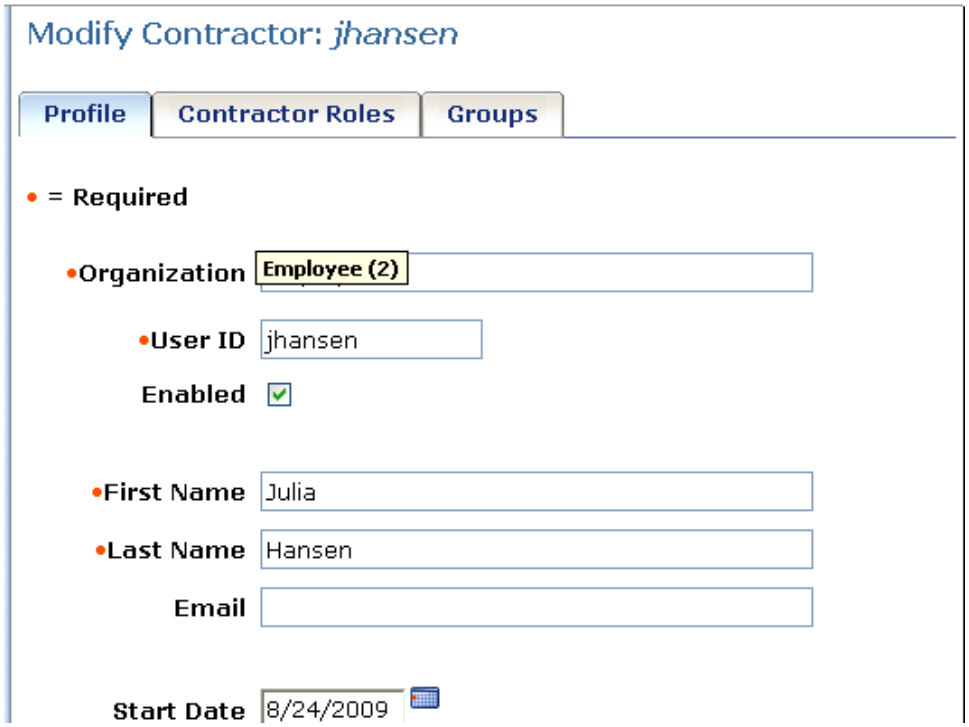


Por exemplo, usando a tarefa Modificar usuário como um modelo, você pode criar uma tarefa Modificar contratante cujas alterações foram feitas:

- Nos campos da guia Perfil
- Nas guias a serem incluídas na tarefa e seu conteúdo
- Na categoria sob a qual a tarefa é exibida

  Você pode criar essa tarefa sob uma nova categoria: Contratante.

A tarefa Modificar contratante inclui alguns dos campos da guia Perfil na tarefa Modificar usuário, além de outros campos, como a data de início do contrato e a empresa do contratante. Os administradores podem procurar um contratante pesquisando por nome do contratante, empresa e data de início.



A nova tarefa também inclui a guia Funções do contratante, onde é possível adicionar funções para contratantes.

Solicitar um relatório

Para exibir o relatório, solicite um relatório para um usuário com privilégios de administração de relatório. A aprovação é obrigatória, pois alguns relatórios podem exigir muito tempo ou recursos significativos do sistema para que sejam executados. Se a solicitação de relatório exigir uma aprovação, o sistema enviará um alerta de email.

Siga estas etapas:

1. Efetue logon no console de usuário com privilégios de usuário de tarefas de geração de relatório.
2. Selecione Tarefas, Relatórios, Tarefas de geração de relatórios e Solicitar um relatório.

   Uma lista de relatórios será exibida.

3. Selecione o relatório que deseja solicitar.

   Uma tela de parâmetros é exibida.

   Forneça qualquer informação referente aos parâmetros que julgar necessária.

   Observação: se estiver executando um relatório de instantâneo e nenhum instantâneo estiver disponível para esse relatório, você deve primeiro capturar um instantâneo.

   - Alguns relatórios mostram o status do sistema em um horário específico. Ao solicitar esse tipo de relatório, você seleciona de que momento deseja ver os dados do relatório. Esse momento é chamado de um *instantâneo*.

     Observação: as datas e horários do instantâneo que você pode escolher são pré-determinados. Normalmente, o administrador do sistema, ou outro usuário com privilégios de administração de relatório, configura instantâneos. Se nenhum instantâneo estiver disponível para o relatório que deseja solicitar, entre em contato com o administrador do sistema.

   - Alguns relatórios mostram atividade durante um período de tempo. Os títulos desses relatórios geralmente começam com a palavra *Auditoria*. Ao solicitar esse tipo de relatório, você especifica de que período deseja ver os dados do relatório. Por exemplo, você pode executar o relatório de Auditoria - Redefinir senha dos últimos 30 dias.

4. Clique em Programar relatório e selecione uma programação para o relatório.

   Agora

   Especifica que o relatório é executado imediatamente.

   Uma vez

   Especifica que o relatório é executado uma vez, durante um período específico. Selecione a data de início, a data de término, a hora de início e a hora de término quando desejar gerar o relatório.

   Observação: considere selecionar essa opção se o relatório que você estiver solicitando exigir uma grande quantidade de dados. Para economizar recursos do sistema, escolha um momento em que há menos atividades no sistema.

5. Clique em Enviar.

   A solicitação de relatório é enviada. Dependendo da configuração do ambiente, a solicitação será executada imediatamente, ou após a aprovação de um administrador.

   Normalmente, um administrador do sistema ou outro usuário com privilégios de administração de relatório deve aprovar uma solicitação de relatório antes que ela seja executada pelo sistema. A aprovação é obrigatória, pois alguns relatórios podem exigir muito tempo ou recursos significativos do sistema para que sejam executados. Se a solicitação de relatório exigir uma aprovação, o sistema enviará um alerta de email.

Exibir o relatório

Dependendo da configuração do ambiente, um relatório ficará disponível para exibição quando um administrador aprovar a solicitação para aquele relatório. Se a solicitação de relatório tiver uma aprovação pendente, o sistema enviará um alerta de email. O relatório que você deseja exibir não aparecerá na lista de pesquisa até que seja aprovado.

Observação: para exibir relatórios no CA Identity Manager usando a tarefa Exibir meus relatórios, ative os cookies de sessão de terceiros no navegador.

Siga estas etapas:

1. No console de usuário, vá para Tarefas, Relatórios, Tarefas de geração de relatórios, e clique em Exibir meus relatórios.
2. Procure o relatório gerado que deseja exibir.

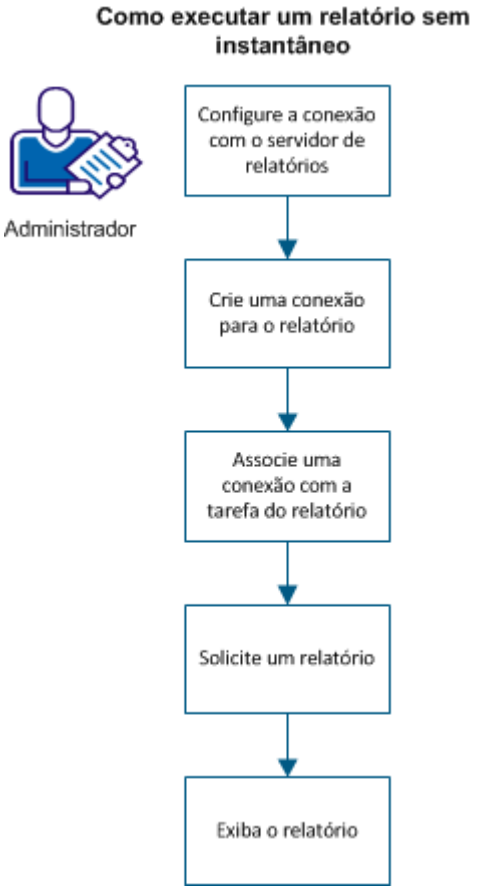
   As instâncias de relatórios de recorrência gerados e de relatórios sob demanda são exibidas.

   Observação: se o status do relatório for Pendente/recorrente, o relatório não será gerado e poderá levar algum tempo para ser concluído.
3. Selecione o relatório que deseja exibir.
4. (Opcional) Clique em Exportar esse relatório (canto superior esquerdo) para exportar o relatório para os seguintes formatos:
   - Crystal Report
   - PDF
   - Microsoft Excel (97-2003)
   - Microsoft Excel (97-2003) – somente dados
   - Microsoft Excel (97-2003) – editável
   - RTF (Rich Text Format – Formato Rich Text)
   - CSV (Comma Separated Values – Valores Separados por Vírgulas)
   - XML

Como executar um relatório que não é de instantâneo

Um relatório que não é de instantâneo inclui dados de outras origens dos dados, como os bancos de dados de auditoria, de fluxo de trabalho ou de persistência de tarefas. O CA Identity Manager inclui relatórios de auditoria padrão com o prefixo "Auditoria-" em seu nome, no console do usuário. Por padrão, o CA Identity Manager inclui apenas relatórios de auditoria, mas é possível criar seus próprios relatórios personalizados, que podem incluir dados de qualquer origem de dados.

Esse cenário descreve como um super administrador configura uma conexão com o banco de dados de relatórios e executa um relatório que não é de instantâneo.



O diagrama a seguir ilustra o processo executando um relatório de instantâneo:

Para executar o relatório que não é de instantâneo, execute as seguintes etapas:

1. Configurar a conexão com o servidor de relatórios. (na página 420)
2. Criar uma conexão para o relatório.
3. Associe uma conexão à tarefa de geração de relatório.

4. Solicitar um relatório.
5. Exibir o relatório. (na página 424)

Configurar a conexão do servidor de relatórios

Para coletar dados do servidor de relatórios, é necessário configurar a conexão com o servidor de relatórios. Antes de iniciar o procedimento, reúna as informações a seguir sobre o servidor de relatórios:

Nome	Descrição
Nome do host	O nome do host do computador em que o servidor de relatórios está instalado
Porta	O nome da porta do computador em que o servidor de relatórios está instalado
Nome da pasta de relatórios	O local dos relatórios padrão do CA Identity Manager.
ID do usuário	Especifica o usuário criado para o servidor de relatórios.
Senha	Especifica a senha do usuário criado no servidor de relatórios.
Conexão segura	Especifica a conexão segura para o servidor de relatórios. Marque a caixa de seleção para ativar a conexão SSL (Secure Sockets Layer) entre o CA Identity Manager e o servidor de relatórios. **Observação:** antes de marcar a caixa de seleção Conexão segura, verifique se você instalou o certificado do BOServer. Para obter mais informações sobre como configurar o SSL, consulte o capítulo Instalação do servidor de relatórios, no *Guia de Instalação*.
Servidor web	Especifica o servidor web. Defina como Não IIS para o Tomcat.

Observação: é recomendável que todos os sistemas envolvidos na geração de relatórios sejam definidos com o mesmo fuso horário e hora.

Siga estas etapas:

1. No console de usuário, clique em Sistema, Geração de relatórios, Conexão com o servidor de relatórios.
2. Digite as configurações do servidor de relatórios.
3. Clique em Testar conexão para verificar a conexão.
4. Clique em Submit.

A conexão de geração de relatórios é estabelecida.

Criar uma conexão para o relatório

As informações de relatórios do CA Identity Manager podem ser provenientes de várias origens. Para especificar os detalhes da conexão de uma origem de dados adicional para o relatório, crie uma conexão JDBC no CA Identity Manager.

Siga estas etapas:

1. No console de usuário, vá para Tarefas, Sistema, Gerenciamento de conexão JDBC, Criar conexão JDBC.
2. Crie um objeto de conexão ou escolha um objeto de conexão com base em uma origem de dados específica do JNDI.
3. Preencha todos os campos necessários e clique em Enviar.

   Uma conexão JDBC é criada.

Importante: recomendamos que você *não* utilize o banco de dados de repositório de objetos do CA Identity Manager para a geração de relatórios.

Associar uma conexão a uma tarefa de geração de relatório

As informações de relatórios do CA Identity Manager são captadas de várias origens, e cada relatório deve ser associado a uma origem de dados específica, de acordo com as informações que você deseja exibir no relatório.

Para associar uma conexão a uma tarefa de geração de relatório:

1. No console de usuário, vá para Tarefas, Funções e tarefas, Tarefas administrativas, Modificar tarefa administrativa.
2. Pesquise a tarefa de geração de relatório com a qual deseja associar uma conexão.
3. Vá para a guia Pesquisar e clique em Procurar para localizar as telas de pesquisa.
4. Edite a tela de pesquisa da tarefa de geração de relatório e escolha uma conexão em Objeto de conexão para o relatório.
5. Clique em OK.
6. Clique em Selecionar.
7. Clique em Enviar.

Solicitar um relatório

Para exibir o relatório, solicite um relatório para um usuário com privilégios de administração de relatório. A aprovação é obrigatória, pois alguns relatórios podem exigir muito tempo ou recursos significativos do sistema para que sejam executados. Se a solicitação de relatório exigir uma aprovação, o sistema enviará um alerta de email.

Siga estas etapas:

1. Efetue logon no console de usuário com privilégios de usuário de tarefas de geração de relatório.
2. Selecione Tarefas, Relatórios, Tarefas de geração de relatórios e Solicitar um relatório.

   Uma lista de relatórios será exibida.
3. Selecione o relatório que deseja solicitar.

   Uma tela de parâmetros é exibida.

   Forneça qualquer informação referente aos parâmetros que julgar necessária.

   Observação: se estiver executando um relatório de instantâneo e nenhum instantâneo estiver disponível para esse relatório, você deve primeiro capturar um instantâneo.

   - Alguns relatórios mostram o status do sistema em um horário específico. Ao solicitar esse tipo de relatório, você seleciona de que momento deseja ver os dados do relatório. Esse momento é chamado de um *instantâneo*.

     Observação: as datas e horários do instantâneo que você pode escolher são pré-determinados. Normalmente, o administrador do sistema, ou outro usuário com privilégios de administração de relatório, configura instantâneos. Se nenhum instantâneo estiver disponível para o relatório que deseja solicitar, entre em contato com o administrador do sistema.
   - Alguns relatórios mostram atividade durante um período de tempo. Os títulos desses relatórios geralmente começam com a palavra *Auditoria*. Ao solicitar esse tipo de relatório, você especifica de que período deseja ver os dados do relatório. Por exemplo, você pode executar o relatório de Auditoria - Redefinir senha dos últimos 30 dias.

4. Clique em Programar relatório e selecione uma programação para o relatório.

   Agora

   Especifica que o relatório é executado imediatamente.

   Uma vez

   Especifica que o relatório é executado uma vez, durante um período específico. Selecione a data de início, a data de término, a hora de início e a hora de término quando desejar gerar o relatório.

   Observação: considere selecionar essa opção se o relatório que você estiver solicitando exigir uma grande quantidade de dados. Para economizar recursos do sistema, escolha um momento em que há menos atividades no sistema.

5. Clique em Enviar.

   A solicitação de relatório é enviada. Dependendo da configuração do ambiente, a solicitação será executada imediatamente, ou após a aprovação de um administrador.

   Normalmente, um administrador do sistema ou outro usuário com privilégios de administração de relatório deve aprovar uma solicitação de relatório antes que ela seja executada pelo sistema. A aprovação é obrigatória, pois alguns relatórios podem exigir muito tempo ou recursos significativos do sistema para que sejam executados. Se a solicitação de relatório exigir uma aprovação, o sistema enviará um alerta de email.

Exibir o relatório

Dependendo da configuração do ambiente, um relatório ficará disponível para exibição quando um administrador aprovar a solicitação para aquele relatório. Se a solicitação de relatório tiver uma aprovação pendente, o sistema enviará um alerta de email. O relatório que você deseja exibir não aparecerá na lista de pesquisa até que seja aprovado.

Observação: para exibir relatórios no CA Identity Manager usando a tarefa Exibir meus relatórios, ative os cookies de sessão de terceiros no navegador.

Siga estas etapas:

1. No console de usuário, vá para Relatórios, Tarefas de geração de relatórios, e clique em Exibir meus relatórios.
2. Procure o relatório gerado que deseja exibir.

   As instâncias de relatórios de recorrência gerados e de relatórios sob demanda são exibidas.

   Observação: se o status do relatório for Pendente/recorrente, o relatório não será gerado e poderá levar algum tempo para ser concluído.
3. Selecione o relatório que deseja exibir.
4. (Opcional) Clique em Exportar esse relatório (canto superior esquerdo) para exportar o relatório para os seguintes formatos:
   - Crystal Report
   - PDF
   - Microsoft Excel (97-2003)
   - Microsoft Excel (97-2003) – somente dados
   - Microsoft Excel (97-2003) – editável
   - RTF (Rich Text Format – Formato Rich Text)
   - CSV (Comma Separated Values – Valores Separados por Vírgulas)
   - XML

Definir opções de geração de relatórios

Configure o número de instâncias de relatório que um usuário pode gerar para um relatório específico.

Para modificar as opções de geração de relatórios:

1. Selecione Tarefas, Relatórios, Tarefas de geração de relatórios, Definir opções de geração de relatórios.

   O CA Identity Manager se conecta ao servidor de relatórios do IAM e recupera uma lista de todos os relatórios.

2. Selecione um relatório e clique em Modificar.

   O painel de atributos do relatório é exibido.

3. Edite os seguintes campos:

   Nome

   Especifica o nome de exibição para o relatório selecionado.

   Número de instâncias

   Especifica o número de instâncias permitidas que podem ser geradas por um usuário para esse relatório.

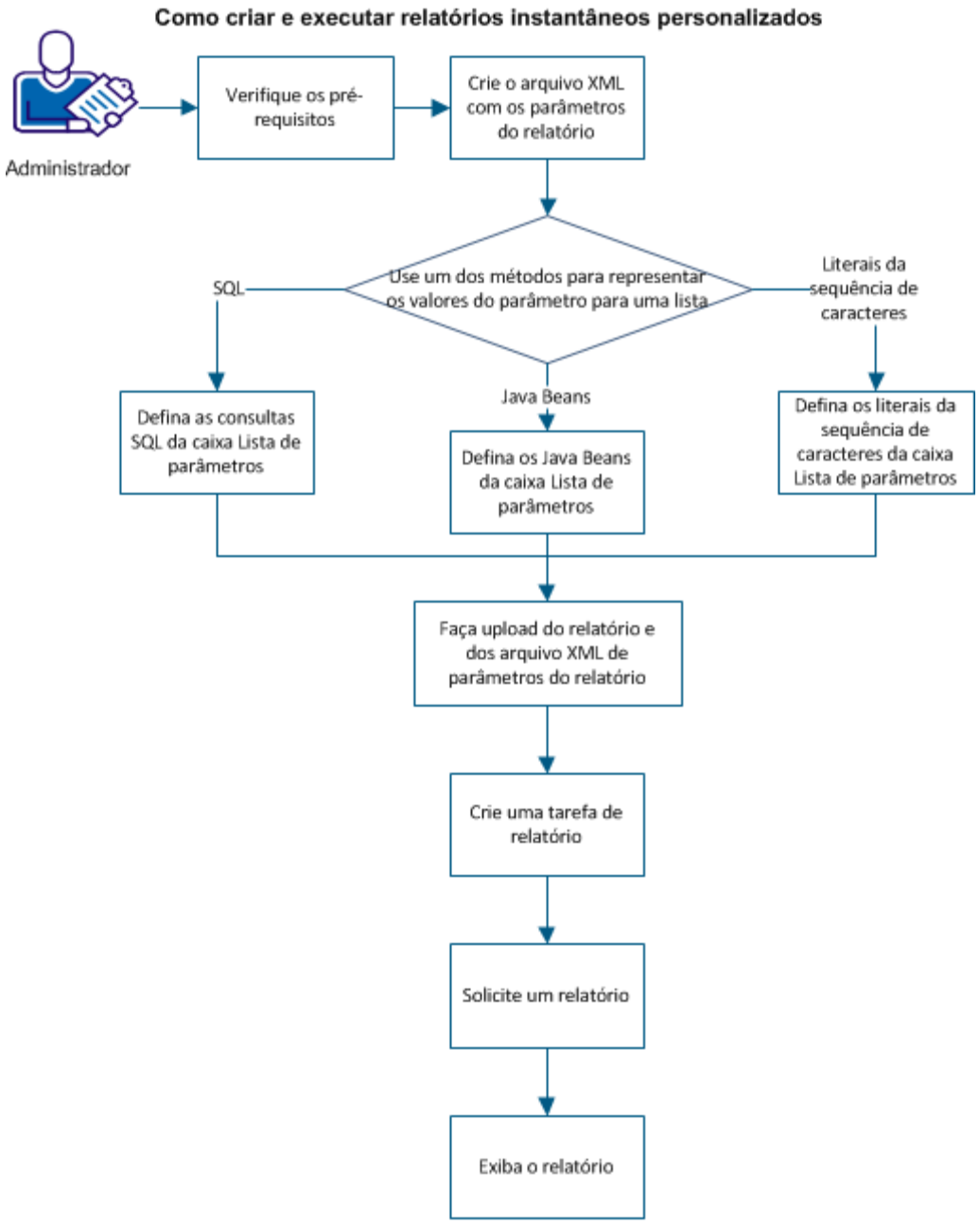
4. Clique em OK.

   Os atributos de geração de relatórios são alterados.

Como criar e executar um relatório de instantâneo personalizado

O CA Identity Manager permite criar e personalizar relatórios para atender às suas necessidades de negócios. O CA Identity Manager fornece um arquivo XML de parâmetros de relatório que inclui todos os parâmetros relacionados aos atributos de relatórios. De acordo com as suas necessidades de negócios, é possível escolher os atributos necessários para preencher dados do relatório a partir da origem de dados do instantâneo.

O gráfico a seguir ilustra o processo para criar e executar um relatório de instantâneo personalizado:



Como administrador do sistema, execute as seguintes etapas:

1. Verificar os pré-requisitos (na página 428)
2. Criar o arquivo XML de parâmetro de relatório (na página 428)
3. Use um dos métodos a seguir para representar os valores de parâmetro de uma lista:
   - Definir Consultas do SQL para a caixa de listagem Parâmetro (na página 431)

- Definir Java Beans para a caixa de listagem Parâmetro (na página 432)
- Definir Literais de sequência de caracteres para a caixa de listagem Parâmetro (na página 432)

4. Fazer upload do relatório e do arquivo XML de parâmetro de relatório (na página 432)
5. Criar a tarefa de relatório
6. Solicitar um relatório
7. Exibir um relatório (na página 424)

Criar um relatório no Crystal Reports

Para usar os relatórios personalizados no CA Identity Manager, crie um relatório (arquivo RPT) no Desenvolvedor do Crystal Reports. Para obter mais informações sobre como criar um relatório no Crystal Reports, consulte a documentação do Crystal Reports.

Observação: para consultar o esquema do CA Identity Manager para criar relatórios personalizados, o esquema de banco de dados do CA Identity Manager está no seguinte local:

```
<caminho_de_instalação>\db\objectstore
```

Criar o arquivo XML de parâmetro de relatório

Um parâmetro é um dos campos em um relatório que pode ser usado para filtrar relatórios. Você pode gerar um relatório filtrando os dados usando parâmetros. Para permitir a personalização da tela de pesquisa do relatório, cada relatório (arquivo RPT) é associado a um arquivo XML de parâmetro de relatório. No CA Identity Manager, é possível criar tarefas de relatório e criar tela de pesquisa para que um usuário possa inserir ou selecionar os dados necessários durante a geração de um relatório.

Observação: você só precisará de um arquivo XML de parâmetro de relatório se o relatório consultar atributos no objeto.

O arquivo XML de parâmetro de relatório deve ter o mesmo nome do relatório (arquivo RPT) com uma extensão .xml. Por exemplo, se você fizer upload de um relatório denominado test1.rpt no Servidor de relatórios, o seu arquivo XML deve ser denominado test1.xml.

O arquivo XML de parâmetro de relatório tem os seguintes elementos:

<product>

Identifica o produto para o qual os parâmetros são usados. Você pode criar parâmetros diferentes para diversos produtos usando o mesmo arquivo XML de parâmetro.

<screen>

Define os parâmetros que são exibidos em uma tela. É possível usar o elemento de tela para vincular os parâmetros a uma tela específica. A ID da tela é alfanumérica e exclusiva e é usada para identificar as telas e seus parâmetros.

<parameters>

Especifica a coleção de parâmetros de uma tela.

<param>

Define o elemento de parâmetro que passa pelos dados especificados para o relatório. Os atributos a seguir são usados no elemento <param>:

id

Define à qual parâmetro se associar no relatório.

Observação: a ID deve ter o mesmo nome que o parâmetro do Crystal Report.

nome

Esse campo não é usado atualmente pelo CA Identity Manager. Defina esse atributo com o mesmo valor de id.

displaytext

Especifica o texto amigável ao usuário a ser exibido na tela para o parâmetro.

type

Define o tipo de parâmetro. A exibição da tela muda com base nesse atributo. Os tipos de parâmetro suportados são os seguintes:

- **Caixa de texto**

  Exemplo: <param id="param1" displaytext="First Name" name="param1" type="string"/>

- **Data e hora**

  Exemplo: <param id="dateVal" displaytext="Date" name="dateVal" type="date_str"/>

  <param id="timeVal" displaytext="Time" name="timeVal" type="time_str"/>

  <param id="datetimeVal" displaytext="Date & Time" name="datetimeVal" type="date_time_str"/>

- **Lista suspensa**

  Exemplo: <param id="lastname1" displaytext="Name" name="lastname1" type="dropdown" default="key1%1FMy Value1%1Ekey2%1FMy Value2" selected_value="My Value2"/>

- **Caixa de listagem**

  Exemplo: <param id="lstlastname1" displaytext="Name" name="lstlastname1" type="listbox" rows="10" default="key1%1FSuper%1Ekey2%1Fsql2kSuser01%1E key1F%Super"/>

- **Caixa de opção**

  Exemplo: <param id="optionslist" displaytext="Option 1" name="optionslist" type="radiobox" value="option1"/>

  <param id="optionslist" displaytext="Option 2" name="optionslist" type="radiobox" value="option2"/>

  <param id="optionslist" displaytext="Option 3" name="optionslist" type="radiobox" value="option3"/>

- **Caixa de seleção**

  Exemplo: <param id="enabled" displaytext="Enabled" name="enabled" type="checkbox"/>

row

Define quantas linhas são visíveis em uma caixa de listagem.

Padrão: 5

default

Define o valor padrão exibido na tela para um determinado parâmetro. Esse atributo pode ser usado com a sequência de caracteres, a caixa de listagem e os tipos de lista suspensa.

Definir Consultas do SQL para a caixa de listagem Parâmetro

É possível definir consultas SQL como parte de uma caixa de listagem ou caixa suspensa no arquivo XML de parâmetro de relatório. Ao associar um parâmetro ao relatório e criar uma tarefa de relatório, o parâmetro é exibido na caixa de listagem ou caixa suspensa para o usuário. Para usar SQL no parâmetro de caixa suspensa ou caixa de listagem, forneça uma instrução SQL válida no atributo sql.

Exemplo:

```
<param id="lstlastname2" displaytext="Name" name="lstlastname2" type="sqlstr"
multiselect="true" sql="select lastname, lastname from tblusers where firstname
like 'S%/>
```

No exemplo anterior, todos os sobrenomes dos usuários com um nome que começa com *S* são fornecidos ao relatório.

No entanto, a condição do nome que comece com *S* é uma condição estática. Esta consulta não é flexível o suficiente para que um usuário carregue o valor com base no valor do parâmetro inserido em uma das telas anteriores, que foi usado no mesmo grupo de parâmetros de relatório. Para usar um valor anterior que foi inserido em outra tela, a instrução SQL pode ser aumentada com *##<id do parâmetro>##*.

Por exemplo, se você tiver um parâmetro com id=User, que era do tipo Sequência de caracteres:

```
<param id="User" displaytext="First Name" name="firstname" type="string"/>
```

Se desejar usar o valor de entrada para esse parâmetro no SQL, a instrução SQL pode ser a seguinte:

```
<param id="lstlastname2" displaytext="Name" name="lstlastname2" type="sqlstr"
multiselect="true" sql="select lastname, lastname from tblusers where firstname
like '##User##'/>
```

O CA Identity Manager substitui ##User## pelo valor inserido para o parâmetro com a id=User.

Observação: o valor do parâmetro a ser substituído não pode estar na mesma tela que o parâmetro do SQL. Por exemplo, se *lstlastname2* estiver na tela 3, o parâmetro Usuário deverá estar em uma das telas anteriores.

Definir Java Beans para a caixa de listagem Parâmetro

Se usar o SQL não for ideal, você poderá usar o java beans para calcular os valores e fornecer a lista de pares <chave, valor> ao CA Identity Manager. O java beans deve estar no caminho de classe do CA Identity Manager.

Exemplo:

```
<param id="lastname2" displaytext="Name using Javabean" name="lastname2"
type="dropdown" class="com.ca.ims.reporting.unittests.TestDataCollector"/>
```

No exemplo anterior, o TestDataCollector recupera os valores da sua própria maneira e envia os dados para a lista suspensa do relatório. Os pares <chave, valor> são separados por %1F.

Certifique-se de que o java beans esteja no diretório iam_im.ear\custom.

Observação: para obter mais informações sobre como implementar o java beans, consulte a documentação do Business Objects.

Definir Literais de sequência de caracteres para a caixa de listagem Parâmetro

A maneira mais simples de representar os valores de parâmetro de uma lista ou caixa suspensa é usando literais de sequência de caracteres. O valor da chave é delimitado por %1F e cada par <chave, valor> é separado por %1E.

Exemplo:

```
<param id="lastname1" displaytext="Name" name="lastname" type="dropdown"
default="key1%1FMy Value1%1Ekey2%1FMy Value2" selected_value="My Value2"/>
```

Fazer upload do relatório e do arquivo XML de parâmetro de relatório

Depois de criar o relatório (RPT) e o arquivo XML de parâmetro de relatório correspondente, faça upload de ambos os arquivos no Servidor de relatórios (Business Objects).

Siga estas etapas:

1. Efetue logon no Management Console central do Business Objects.
2. Clique em Pastas.
3. Selecione a pasta IM Reports.
4. Crie um pacote de objetos.
5. No novo pacote de objetos, navegue para adicionar o Crystal Report.

6. Procure o novo relatório (RPT) que você criou.

   Observação: certifique-se de que a pasta de relatórios do IM está selecionada como a pasta na qual salvar o relatório.

7. Clique em OK.

   O arquivo Crystal Report é adicionado.

8. No novo pacote de objetos, adicione um novo documento local e navegue até o novo arquivo XML de parâmetro de relatório.

9. Selecione o tipo de arquivo como *Texto*.

10. Clique em OK.

O relatório e o arquivo xml de parâmetro de relatório agora estão carregados. Para verificar, vá para a pasta de relatórios do IM e certifique-se de que os dois arquivos novos estão disponíveis.

Criar a tarefa de relatório

As tarefas de relatório são usadas para criar, gerenciar, exibir e excluir os modelos para os relatórios gerados no Console de usuário.

Siga estas etapas:

1. No console de usuário, vá para Tarefas, Funções e tarefas, Tarefas administrativas, Criar tarefa administrativa.
2. Selecione Criar uma tarefa administrativa e clique em OK.
3. Na guia Perfil, preencha os seguintes campos:

   Nome

   Define o nome do relatório. O nome de cada tarefa de relatório deve ser exclusivo.

   Marcação

   Define um identificador exclusivo para a tarefa. É usado em um URL, um serviço web ou em arquivos de propriedades. Deve conter letras, números e/ou sublinhados, começando com uma letra ou sublinhado.

   Categoria

   Especifica a categoria à qual a tarefa atual pertence.

   Observação: selecione a categoria Relatórios.

   Categoria 2

   Especifica a subcategoria à qual a tarefa atual pertence. Insira qualquer sequência de caracteres neste campo.

   Objeto principal

   Especifica o objeto sobre o qual a tarefa atua.

   Observação: selecione Instância de relatório como o objeto principal.

   Ação

   Especifica a ação que é executada no objeto principal.

   Observação: selecione Criar como a ação.
4. Para criar uma nova tela de pesquisa para a tarefa de relatório, execute as seguintes etapas:
   a. Na guia Pesquisar, clique em Procurar para localizar as telas de pesquisa.

      A lista de telas de pesquisa disponíveis é exibida.

   b. Clique em Novo.

      O painel Criar tela é exibido.

   c. Selecione Tela de seleção de modelos de relatório na lista e clique em OK.

O CA Identity Manager se conecta ao Servidor de relatórios e exibe todos os relatórios.

d. Preencha os seguintes campos:

Nome

Define o nome do relatório. O nome de cada tarefa de relatório deve ser exclusivo.

Marcação

Atua como um identificador exclusivo em uma tarefa. Ele pode conter caracteres ASCII (a-z, A-Z), números (0-9) ou caracteres de sublinhado, começando com uma letra ou sublinhado.

Cargo

Define o título da nova tela de pesquisa. O título deve ser exclusivo.

Modelo de relatório

Identifica o relatório a ser associado à tela de pesquisa.

Observação: escolha um dos relatórios que adicionou ao Servidor de relatórios.

Objeto de conexão para o relatório

Define os detalhes da conexão da origem dos dados a ser usada no relatório.

5. Clique em OK.

A nova tela de pesquisa agora está criada para os relatórios.

6. Ao criar uma guia Guias para a tarefa de relatório, execute as seguintes etapas:

a. Clique em Guias.

As guias que são visíveis para o usuário são exibidas.

b. Selecione o Controlador de guias padrão.

c. Se o seu relatório usar uma definição de instantâneo, execute as seguintes etapas:

a. As guias De qual devem aparecer nesta tarefa?, selecione Associar definições de instantâneo.

A guia Associar definições de instantâneo é adicionada à lista de guias.

b. Clique em  para editar a guia Associar definições de instantâneo.

c. Clique em Adicionar para associar a tarefa de relatório a uma definição de instantâneo.

Uma lista de definições de instantâneo disponíveis é exibida.

d. Selecione uma Definição de instantâneo e clique em OK.

A tarefa de relatório é associada a uma definição de instantâneo.

d. Clique em Enviar.

   A tarefa de relatório é criada.

e. Atribua a nova tarefa de relatório a uma função administrativa.

   Os usuários com a função administrativa do CA Identity Manager podem usar a nova tarefa de relatório.

A tarefa de relatório agora está pronta para ser usada pelo administrador.

Observação: um relatório (arquivo RPT) pode ser associado apenas a *uma* tarefa de relatório.

Solicitar um relatório

Para exibir o relatório, solicite um relatório para um usuário com privilégios de administração de relatório. Normalmente, um administrador do sistema ou outro usuário com privilégios de administração de relatório deve aprovar uma solicitação de relatório antes que ela seja executada pelo sistema. A aprovação é obrigatória, pois alguns relatórios podem exigir muito tempo ou recursos significativos do sistema para que sejam executados. Se a solicitação de relatório exigir uma aprovação, o sistema enviará um alerta de email.

Siga estas etapas:

1. Efetue logon no console de usuário como um usuário que tem acesso às tarefas de relatório.
2. No menu de navegação, selecione Tarefas, Relatórios, Tarefas de geração de relatórios, Solicitar um relatório.

   Uma lista de relatórios será exibida.
3. Selecione o relatório que deseja solicitar.

   Uma tela de parâmetros é exibida.
4. Forneça qualquer informação referente aos parâmetros que julgar necessária.

   Observação: se estiver executando um relatório de instantâneo e nenhum instantâneo estiver disponível para esse relatório, você deve primeiro capturar um instantâneo.

   - Alguns relatórios mostram o status do sistema em um horário específico. Ao solicitar esse tipo de relatório, você seleciona de que momento deseja ver os dados do relatório. Esse momento é chamado de um *instantâneo*.

     Observação: as datas e horários do instantâneo que você pode escolher são pré-determinados. Normalmente, o administrador do sistema, ou outro usuário com privilégios de administração de relatório, configura instantâneos. Se nenhum instantâneo estiver disponível para o relatório que deseja solicitar, entre em contato com o administrador do sistema.
   - Alguns relatórios mostram atividade durante um período de tempo. Os títulos desses relatórios geralmente começam com a palavra *Auditoria*. Ao solicitar esse tipo de relatório, você especifica de que período deseja ver os dados do relatório. Por exemplo, você pode executar o relatório de Auditoria - Redefinir senha dos últimos 30 dias.
5. Clique em Programar relatório e selecione uma programação para o relatório.

   Agora

   Especifica que o relatório é executado imediatamente.

   Uma vez

Especifica que o relatório é executado uma vez, durante um período específico. Selecione a data de início, a data de término, a hora de início e a hora de término quando desejar gerar o relatório.

Observação: considere selecionar essa opção se o relatório que você estiver solicitando exigir uma grande quantidade de dados. Para economizar recursos do sistema, escolha um momento em que há menos atividades no sistema.

6. Clique em Enviar.

   A solicitação de relatório é enviada. Dependendo da configuração do ambiente, a solicitação será executada imediatamente, ou após a aprovação de um administrador.

Exibir o relatório

Dependendo da configuração do ambiente, um relatório ficará disponível para exibição quando um administrador aprovar a solicitação para aquele relatório. Se a solicitação de relatório tiver uma aprovação pendente, o sistema enviará um alerta de email. O relatório que você deseja exibir não aparecerá na lista de pesquisa até que seja aprovado.

Observação: para exibir relatórios no CA Identity Manager usando a tarefa Exibir meus relatórios, ative os cookies de sessão de terceiros no navegador.

Siga estas etapas:

1. No console de usuário, vá para Tarefas, Relatórios, Tarefas de geração de relatórios, e clique em Exibir meus relatórios.
2. Procure o relatório gerado que deseja exibir.

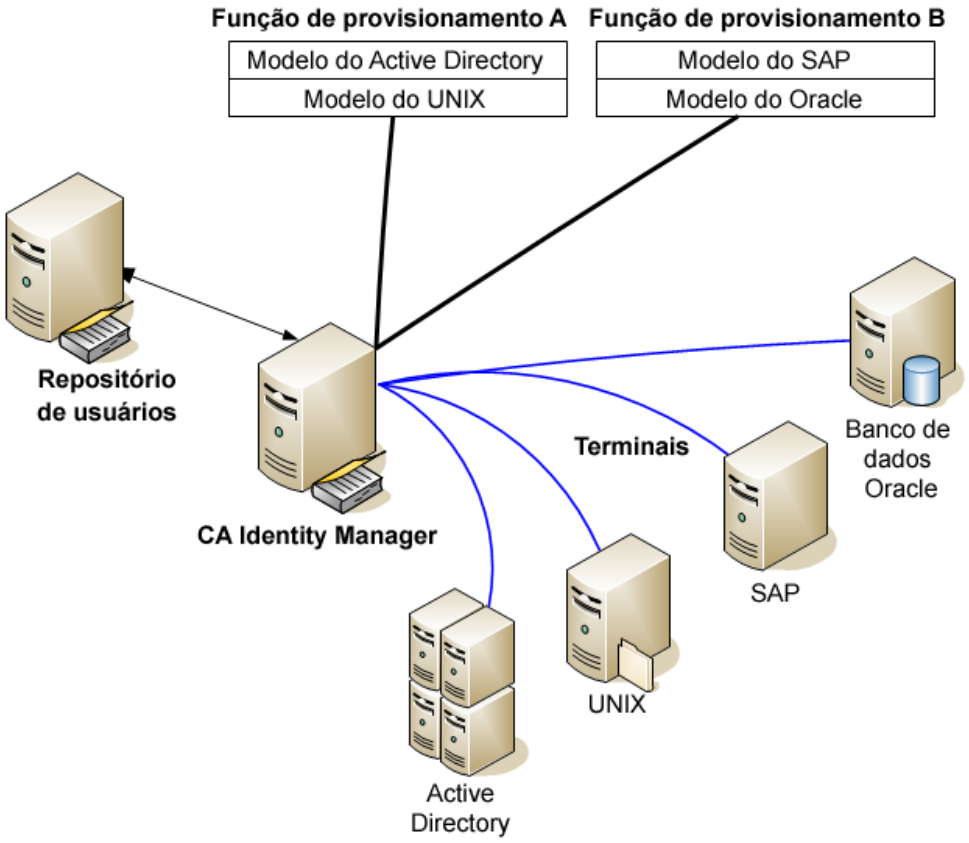
   As instâncias de relatórios de recorrência gerados e de relatórios sob demanda são exibidas.

   Observação: se o status do relatório for Pendente/recorrente, o relatório não será gerado e poderá levar algum tempo para ser concluído.
3. Selecione o relatório que deseja exibir.
4. (Opcional) Clique em Exportar esse relatório (canto superior esquerdo) para exportar o relatório para os seguintes formatos:
   - Crystal Report
   - PDF
   - Microsoft Excel (97-2003)
   - Microsoft Excel (97-2003) – somente dados
   - Microsoft Excel (97-2003) – editável
   - RTF (Rich Text Format – Formato Rich Text)
   - CSV (Comma Separated Values – Valores Separados por Vírgulas)
   - XML

Sincronizando usuários, contas e funções

A integração de vários terminais e contas em um único sistema de gerenciamento de usuários pode resultar na perda de sincronização. As funções de provisionamento ou os modelos de conta que são atribuídos a um usuário podem ser diferentes das contas reais que existem para esse usuário.

Por exemplo, considere uma situação com duas funções de provisionamento, uma com modelos de conta do Active Directory e UNIX e outra função com modelos do SAP e Oracle. O usuário joão_silva tem a Função de provisionamento A, que contém modelos de conta do Active Directory e UNIX, mas esse usuário tem apenas uma conta do Active Directory. Possivelmente, o modelo de conta do UNIX foi adicionado à função depois que ela havia sido atribuída ao usuário. Portanto, o administrador deve sincronizar o usuário com a definição da função atual.



As situações a seguir são outros motivos pelos quais os usuários perdem a sincronização com funções de provisionamento ou modelos de conta:

- As tentativas anteriores de criar as contas necessárias falharam devido a problemas de software ou hardware na rede, resultando em contas ausentes.
- Funções de provisionamento e modelos de conta mudam, criando contas extras ou ausentes.
- Contas foram atribuídas a modelos de conta após a criação, portanto, as contas existentes, mas não estão sincronizadas com seus modelos de conta.
- A criação de uma conta foi atrasada porque a conta foi especificada para ser criada posteriormente.
- Um novo terminal foi adquirido. Durante a exploração e a correlação, o servidor de provisionamento não atribuiu funções de provisionamento para os usuários automaticamente. Você atualiza a função para indicar os usuários que precisam de contas no terminal. Qualquer conta que estava correlacionada a um usuário é listada como uma conta extra quando o usuário é sincronizado.
- Uma conta existente foi atribuída a um usuário, copiando a conta para o usuário.
- Uma conta foi criada para um usuário sem atribuir o usuário a uma função. Por exemplo, você copiou um usuário para um modelo de conta que não está em uma função de provisionamento para esse usuário. A conta é listada como uma conta extra ou como uma conta com um modelo de conta extra. Se você copiar o usuário para um terminal para criar uma conta usando o modelo de conta padrão, essa pode ser uma conta extra.

As seções a seguir explicam como realizar os três tipos de sincronização:

1. Sincronizar usuários com funções (na página 169).
2. Sincronizar usuários com modelos de conta (na página 169).
3. Sincronizar contas de terminal com modelos de conta (na página 171).

Sincronizar usuários com funções

Essa tarefa cria, atualiza ou exclui contas, de forma que elas estejam de acordo com as funções de provisionamento atribuídas a um usuário. Por exemplo, os administradores usam ferramentas nativas em um terminal para adicionar ou excluir contas, mas você não explorou novamente esse terminal para atualizar o diretório de provisionamento. Portanto, os usuários têm contas extras ou ausentes. Essa tarefa também garante que cada conta pertence aos modelos de conta corretos.

Siga estas etapas:

1. Efetue logon no console de usuário.
2. Selecione Usuários, Sincronização, Verificar sincronização de funções.
3. Selecione um usuário.

   Uma tela é exibida, mostrando as contas esperadas, extras e ausentes.
4. Clique em Sincronizar para fazer com que as contas correspondam ao modelo nessa função.

   a. É possível marcar uma caixa de seleção para criar a conta no terminal. Se mais de um modelo de conta para o usuário indicar a mesma conta, a conta será criada, mesclando todos os modelos de conta relevantes.

      Essa conta é atribuída aos modelos de conta que, no momento, não estão sincronizados com a conta.

   b. É possível marcar uma caixa de seleção para excluir as contas extras. No entanto, os usuários podem ter motivos válidos para ter essas contas. Se for esse o caso, deixe essa opção desmarcada.

      Em determinados terminais, a função de exclusão da conta está desativada; portanto, a conta não será excluída.

Sincronizar usuário com modelos de conta

Essa tarefa sincroniza os atributos para as contas do terminal com os modelos de conta associados a um usuário. No entanto, a sincronização completa depende destes fatores:

- A sincronização completa da conta ocorre em duas situações. Um modelo de conta usa a sincronização forte (na página 172), ou dois ou mais modelos de conta foram adicionados a uma conta.
- Se um modelo de conta usa a sincronização fraca (na página 172), essa tarefa inicia uma sincronização de conta que envolve apenas esse modelo. Se a conta estava fora da sincronização de conta com outros modelos de conta antes dessa atualização, também poderá estar fora da sincronização de conta posteriormente.

Siga estas etapas:

1. Efetue logon no console de usuário.
2. Selecione Usuários, Sincronização, Verificar sincronização de modelos de conta.
3. Selecione um usuário.

   Uma tela é exibida, mostrando as contas esperadas, extras e ausentes.
4. Clique em Sincronizar para fazer com que as contas correspondam ao modelo.
   a. É possível marcar uma caixa de seleção para criar a conta no terminal. Se mais de um modelo de conta para o usuário indicar a mesma conta, a conta será criada, mesclando os modelos de conta relevantes.

      Essa conta é atribuída aos modelos de conta que não estão sincronizados com a conta. A sincronização de conta não é necessária em contas recém-criadas.
   b. É possível marcar uma caixa de seleção para excluir as contas extras. No entanto, os usuários podem ter motivos válidos para ter essas contas. Se for esse o caso, deixe essa opção desmarcada.

      Em determinados terminais, a função de exclusão da conta está desativada; portanto, a conta não será excluída.

Sincronizar contas do terminal com modelos de conta

Essa tarefa sincroniza uma conta do terminal após a modificação de um modelo de conta associado. Por exemplo, uma conta do Active Directory não tem grupos, mas o modelo de conta associado está definido para incluir grupos.

Siga estas etapas:

1. Efetue logon no console de usuário.
2. Selecione Terminais, Manage Endpoints, Verificar sincronização de contas de terminal.
3. Selecione um terminal.

   Uma tela é exibida mostrando as contas no terminal em questão, os modelos de conta associados e quais atributos não estão sincronizados.
4. Clique em Sincronizar para fazer com que os atributos para essas contas correspondam ao que está definido no modelo de conta.

   As alterações que você fizer nos modelos de conta afetam as contas existentes da seguinte maneira:

   - Se você alterar o valor de um atributo de recurso, o atributo da conta correspondente será atualizado para ser sincronizado com o valor do atributo do modelo de conta. Consulte a descrição de sincronização fraca e forte.

- Alguns atributos de conta são designados pelo conector como não sendo atualizados após alterações no modelo de conta. Os exemplos incluem determinados atributos que o tipo de terminal permite que sejam definidos apenas durante a criação da conta, e o atributo Senha.

Quais atributos são atualizados

Quando você altera os atributos de capacidade em um modelo de conta, o atributo correspondente nas contas é alterado. Essa alteração tem um impacto nos atributos da conta. O impacto tem como base os seguintes fatores:

- Se o modelo de conta está definido para usar sincronização fraca ou forte.
- Se a conta pertence a vários modelos de conta.

Sincronização fraca

A *sincronização fraca* garante que os usuários tenham o mínimo de atributos de capacidade para suas contas. A sincronização fraca é o padrão na maioria dos tipos de terminal. Se você atualizar um modelo que usa sincronização fraca, o CA Identity Manager atualizará os atributos de capacidade da seguinte maneira:

- Se um campo de número for atualizado em um modelo de conta e o número novo for maior do que o número na conta, o CA Identity Manager alterará o valor na conta para corresponder ao novo número.
- Se uma caixa de seleção não tiver sido marcada em um modelo de conta e você marcá-la depois, o CA Identity Manager atualizará a caixa de seleção em qualquer conta em que a caixa de seleção não estiver marcada.
- Se uma lista for alterada em um modelo de conta, o CA Identity Manager atualizará todas as contas para incluir qualquer valor da nova lista que não foi incluído na lista de valores da conta.

Se uma conta pertencer a outros modelos de conta (se esses modelos usarem sincronização fraca ou forte), o CA Identity Manager consultará apenas o modelo que está sendo alterado. Essa ação é mais eficiente do que a verificação de todos os modelos de conta. Como a sincronização fraca apenas adiciona capacidades às contas, geralmente não é necessário consultar os outros modelos de conta.

Observação: quando se propaga a partir de um modelo de conta de sincronização fraca, as alterações que poderiam remover ou reduzir as capacidades podem deixar algumas contas não sincronizadas. Lembre-se de que, com a sincronização fraca, as capacidades nunca são removidas ou reduzidas. Sem consultar outros modelos para uma conta, a propagação não considera se a sincronização fraca é suficiente.

Nessa situação, use Sincronizar usuários com modelos de conta para sincronizar a conta com seus modelos de conta.

Sincronização forte

A sincronização forte garante que as contas possuam exatamente os atributos de conta que são especificados no modelo de conta.

Por exemplo, suponhamos que você adicione um grupo a um modelo de conta do UNIX existente. Originalmente, o modelo de conta tornou as contas integrantes do grupo Equipe. Agora, você deseja tornar as contas integrantes dos grupos Equipe e Sistema. Todas as contas associadas ao modelo de conta são consideradas sincronizadas quando cada conta é integrante dos grupos Equipe e Sistema (e de nenhum outro grupo). Qualquer conta que não fizer parte do grupo Equipe é adicionada aos dois grupos.

Alguns outros fatores a serem considerados incluem as seguintes situações:

- Se o modelo de conta usar a sincronização forte, qualquer conta que pertencer a grupos que não sejam Equipe e Sistema será removida dos grupos adicionais.
- Se o modelo de conta usar a sincronização fraca, as contas serão adicionadas aos grupos Equipe e Sistema. Qualquer conta que tiver grupos adicionais que estiverem definidos para ela permanecerá um integrante desses grupos.

Observação: sincronize as contas com seus modelos regularmente para garantir que as contas permaneçam sincronizadas com seus modelos de conta.

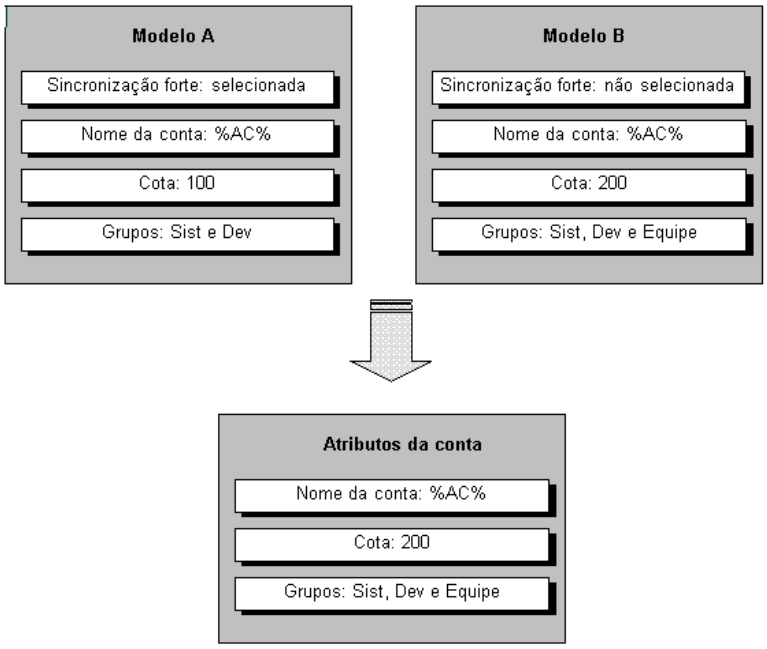
Contas com vários modelos

A sincronização depende também se a conta pertence a mais de um modelo de conta. Se a conta tiver apenas um modelo de conta e esse modelo usar a sincronização forte, cada atributo é atualizado para corresponder exatamente ao valor de atributo de modelo de conta. O resultado é o mesmo de quando o atributo for um atributo inicial.

Uma conta pode pertencer a vários modelos de conta, como seria o caso se um usuário pertencer a várias funções de provisionamento, cada uma delas com algum nível de acesso no mesmo terminal gerenciado. Quando isso acontecer, o CA Identity Manager combina esses modelos de conta em um modelo de conta em vigor que indica o superconjunto de recursos a partir dos modelos de conta. Esse modelo de conta é considerado para usar a sincronização fraca se todos os modelos de contas forem fracos, ou a sincronização forte se qualquer um dos modelos de conta for forte.

Observação: muitas vezes, você usa apenas a sincronização fraca ou apenas a sincronização forte para os modelos de conta que controlam uma conta, dependendo se as funções da empresa definem completamente os acessos que seus usuários precisam. Se os usuários não se encaixarem em funções claras e você precisar da flexibilidade para conceder recursos adicionais para as contas de usuário, use a sincronização fraca. Se for possível definir as funções para especificar exatamente os acessos que seus usuários precisam, use a sincronização forte.

O exemplo a seguir demonstra como vários modelos de conta são combinados em um único modelo de conta em vigor. Neste exemplo, um modelo de conta será marcado para sincronização fraca e o outro para sincronização forte. Portanto, o modelo de conta em vigor criado pela combinação dos dois modelos de conta será tratado como um modelo de conta de sincronização forte. O atributo inteiro Cota assume o maior valor dos dois modelos de conta, e o atributo Grupo com vários valores assume a união de valores das duas políticas.



Atributos somente para novas contas

Em um modelo de conta, determinados atributos são aplicados somente ao criar a conta. Por exemplo, o atributo Senha é uma expressão de regra, que define a senha para novas contas. Essa expressão de regra nunca atualiza a senha de uma conta. As alterações feitas na expressão de regra de senha só afetam as contas criadas após a definição da expressão de regra.

Da mesma forma, uma expressão de regra de modelo para um atributo da conta somente leitura afeta somente as contas criadas após a definição da expressão de regra. A alteração não terá efeito em contas existentes.

Solução de problemas

A seção a seguir detalha tópicos sobre solução de problemas de relatórios.

Exibindo um relatório que redireciona para a página de logon do Infoview

Ao exibir um relatório no CA Identity Manager, você pode ser redirecionado para a página de logon do InfoView do Business Objects.

Exibir o relatório, caso seja redirecionado

1. Verifique se você está usando o nome de domínio totalmente qualificado do Servidor de relatórios da CA (Business Objects).
2. Clique com o botão direito do mouse na página de logon do InfoView e selecione View Source.
3. Localize o URL para o relatório.
4. Copie e cole o URL em uma nova janela do navegador.
5. Se você não visualizar o relatório, use uma ferramenta de rastreamento de HTTP para fornecer mais informações.
6. Se você encontrar o relatório, tente o seguinte para corrigir as configurações do navegador:
   - Aceite cookies de terceiros.
   - Permita cookies de sessão.
   - Remova as configurações de alta segurança.

Gerando contas de usuário para mais de 20.000 registros

Se existirem mais de 20.000 registros, algumas etapas extras serão necessárias para gerar o relatório de contas de usuário.

Para gerar um relatório de contas de usuário para mais de 20.000 registros

1. Abra o Management Console central do Business Objects.
2. Clique em Servers e selecione *nome_do_servidor*.pageserver.
3. Selecione Unlimited records para a entrada Database Records To Read When Previewing Or Refreshing a Report.
4. Usando um designer do Crystal Reports, abra o relatório de contas de usuário.
5. Usando Database, Set Datasource Location, defina o local do banco de dados para seu banco de dados de instantâneos.

6. Salve essa alteração.
7. Usando Database, Datasource Expert, clique com o botão direito do mouse em Command na janela do lado direito.

   Ela mostra a sintaxe SQL no lado esquerdo e a lista de parâmetros.
8. Insira o nome do parâmetro como encontrado nos campos de parâmetros no modelo de relatório.
9. Altere a consulta no lado esquerdo e adicione esse parâmetro nela.

   Por exemplo, se você tiver o parâmetro reportid, a consulta será:

```
Select *  from endPointAttributes, endpointview, imreport6
where endPointAttributes.imr_endpointid = endpointview.imr_endpointid and
endPointAttributes.imr_reportid = endpointview.imr_reportid
 endpointview.imr_reportid = imreport6,imr_reportid and
imreport6,imr_reportid = {?reportid}
```

10. Salve o relatório.

Capítulo 14: Políticas de identidade

Esta seção contém os seguintes tópicos:

Políticas de identidade

Uma diretiva de identidade é um conjunto de alterações nos negócios que ocorrem quando um usuário atende a uma determinada condição ou uma regra. É possível usar conjuntos de políticas de identidade para:

- Automatizar determinadas tarefas de gerenciamento de identidade, como a atribuição de funções e associação ao grupo, alocação de recursos ou modificação dos atributos de perfil do usuário.
- Aplicar a segregação de tarefas. Por exemplo, você pode criar um conjunto de políticas de identidade que proíbe os integrantes da função de Signatário de cheques de ter a função de Aprovador de cheques, e impedir que qualquer pessoa na empresa preencha um cheque de mais US$ 10.000.
- Aplicar conformidade. Por exemplo, você pode auditar usuários que tenham um determinado cargo e ganhem mais de US $100.000.

  As políticas de identidade que aplicam conformidade são chamadas de *políticas de conformidade*.

As mudanças nos negócios associadas a uma política de identidade incluem:

- A atribuição ou revogação de funções, incluindo funções de provisionamento (se você estiver usando um diretório de provisionamento apenas).
- A atribuição ou revogação de associação de grupo.
- A atualização de atributos de um perfil de usuário.

Por exemplo, uma empresa pode criar uma política de identidade que declara que todos os vice-presidentes pertencem ao grupo Integrante do clube campestre e têm a função de Aprovador de salários. Quando o cargo de um usuário muda para vice-presidente e esse usuário é sincronizado com a política de identidade, o CA Identity Manager adiciona o usuário ao grupo e função apropriados. Quando um vice-presidente é promovido a CEO, deixa de atender à condição na política de identidade de vice-presidente, portanto, as alterações aplicadas por essa política são revogadas, e novas alterações com base na política do CEO são aplicadas.

As ações de alteração que ocorrem com base em uma política de identidade contêm eventos que podem ser colocados sob controle de fluxo de trabalho e auditados. No exemplo anterior, a função de Aprovador de salários concede privilégios significativos aos integrantes. Para proteger a função de Aprovador de salários, a empresa pode criar um processo de fluxo de trabalho que exige um conjunto de aprovações antes de atribuir a função e configurar o CA Identity Manager para auditar a atribuição de função.

Para simplificar o gerenciamento de políticas de identidade, estas são agrupadas em um conjunto de políticas de identidade. Por exemplo, o vice-presidente e o CEO podem fazer parte do conjunto de políticas de identidade de Privilégios executivos.

Observação: o CA Identity Manager inclui um tipo de política de identidade adicional, chamado *política de identidade preventiva* (na página 472). Essas políticas, que são executadas antes que uma tarefa seja enviada, permitem que um administrador verifique violações de políticas antes de atribuir privilégios ou alterar atributos do perfil. Se uma violação existir, o administrador pode removê-la antes de enviar a tarefa.

Planilha de planejamento do conjunto de políticas de identidade

Um conjunto de políticas de identidade contém uma ou mais políticas de identidade. Antes de criar um conjunto de políticas de identidade, use a planilha a seguir para planejar cada política de identidade no conjunto.

Pergunta	Sua resposta
Que nome você deseja dar à política de identidade?	
A quais usuários a política de identidade se aplica?	
Quando uma política de identidade é aplicada a um usuário, quais ações o CA Identity Manager deve executar?	
Quando uma política de identidade que se aplicava a um usuário não for mais aplicável, quais ações o CA Identity Manager deve executar?	
O CA Identity Manager deve aplicar as alterações em uma política de identidade várias vezes ou apenas na primeira vez em que um usuário atender às condições da política?	

Depois que preencher essa planilha para cada política de identidade em um conjunto de políticas, certifique-se de que as políticas não estão em conflito com outras políticas. Por exemplo, verifique se uma política não concede um privilégio que outra política revoga.

Criar um conjunto de políticas de identidade

Para criar um conjunto de políticas de identidade, é preciso ter a função de Gerente do sistema ou uma função que inclui a tarefa Criar conjunto de políticas de identidade.

Para criar um conjunto de políticas de identidade, execute as seguintes etapas:

1. Definir o perfil para o conjunto de políticas de identidade (na página 451)
2. Criar uma regra de integrante do conjunto de políticas (na página 452)
3. Criar uma política de identidade (na página 452)
4. Especificar proprietários para o conjunto de políticas de identidade (na página 461)

Observação: para usar as políticas para o ambiente do CA Identity Manager, ative as políticas de identidade no Management Console do CA Identity Manager. Consulte o *Guia de Configuração* para obter mais informações.

Definir o perfil para o conjunto de políticas de identidade

A guia Perfil permite definir propriedades básicas para um conjunto de políticas de identidade.

Para definir um perfil de conjunto de políticas de identidade:

1. Selecione Políticas, Gerenciar políticas de identidade, Criar conjunto de políticas de identidade no console de usuário.

   Você deve estar conectado ao CA Identity Manager como um usuário com privilégios para gerenciar políticas de identidade. A função de Gerente do sistema padrão inclui esses privilégios.
2. Escolha a opção de criar um conjunto de políticas de identidade ou criar uma cópia de um conjunto de políticas de identidade existente.
3. Digite um nome para o conjunto de políticas de identidade.
4. Digite uma categoria para o conjunto de políticas de identidade.

   A categoria agrupa os conjuntos de políticas de identidade com fins semelhantes para a geração de relatórios. O campo Categoria é obrigatório.
5. Opcionalmente, digite uma descrição para o conjunto de políticas de identidade.
6. Se não desejar deixar o conjunto de políticas de identidade disponível para o uso, desmarque a caixa de seleção Ativado.
7. Quando tiver preenchido a guia Perfil, selecione a guia Políticas para criar as políticas de identidade para o conjunto de políticas de identidade.

Mais informações:

Criar uma política de identidade (na página 452)
Criar uma regra de integrante do conjunto de políticas (na página 452)

Criar uma regra de integrante do conjunto de políticas

Você pode criar uma regra de integrante para um conjunto de políticas, de modo que o conjunto de regras se aplique apenas a determinados usuários. A regra é avaliada antes da avaliação de políticas de identidade do conjunto, o que pode economizar muito tempo. Por exemplo, se uma regra de integrante limitar a avaliação de políticas de identidade para 10% dos usuários, economiza 90% do tempo de avaliação.

Para criar uma regra de integrante do conjunto de políticas:

1. Selecione a guia Políticas.
2. Clique no símbolo de Editar em Regra do integrante do conjunto de políticas.
3. Insira uma regra para aplicar a política a apenas determinados usuários.
4. Clique em OK.

Mais informações:

Criar uma política de identidade (na página 452)

Criar uma política de identidade

Depois de definir o perfil e a regra de integrante do conjunto de políticas de identidade, você pode definir as políticas de identidade desse conjunto de políticas.

Observação: em grandes implementações, a tarefa de avaliar as regras de políticas de identidade pode demorar um tempo significativo. Para reduzir o tempo de avaliação para regras que incluem atributos de usuário, você pode ativar a opção de avaliação em memória. Para obter mais informações, consulte o *Guia de Configuração*.

Para criar uma política de identidade:

1. Selecione a guia Políticas.
2. Clique em Adicionar.
3. Digite um nome para a política de identidade.
4. Marque a caixa de seleção Aplicar uma vez se desejar aplicar a política somente quando um usuário atender à política pela primeira vez.

5. Marque a caixa de seleção Conformidade para indicar que essa política é uma política de conformidade.

   Se essa caixa de seleção estiver marcada:

   - O CA Identity Manager pode gerar relatórios para usuários que não estão sincronizados com políticas de conformidade.
   - A ação Violação de conformidade é visível na caixa de listagem Ação ao aplicar a política/Ação ao remover a política.

6. Identifique os usuários aos quais a política se aplica na seção Condição da política.
7. Na seção Ação ao aplicar a política, defina as ações que o CA Identity Manager executa quando a política de identidade é aplicada a um usuário.
8. Na seção Ação ao remover a política, defina as ações que o CA Identity Manager executa quando um usuário não atender mais às condições para a política de identidade.
9. Clique em OK.

Observação: antes que seja possível usar o conjunto de políticas de identidade que você criou, ative as políticas de identidade no Management Console. Consulte o *Guia de Configuração* para obter mais informações.

A configuração Aplicar uma vez

O CA Identity Manager aplica uma política de identidade de forma diferente, com base na configuração Aplicar uma vez.

Ativando a configuração Aplicar uma vez

Se a configuração Aplicar uma vez estiver ativada, o CA Identity Manager aplica as alterações associadas à política de identidade quando um usuário atender à condição definida na política pela *primeira vez*. As ações de alteração associadas à política ocorrem uma única vez. Portanto, o CA Identity Manager não aplica atualizações de políticas aos usuários se a política tiver sido aplicada anteriormente.

Quando um usuário deixa de atender à condição definida na política, o CA Identity Manager executa as ações de remoção da política.

A configuração Aplicar uma vez é geralmente usada durante o provisionamento de recursos. Por exemplo, você pode ter uma política que atribui um celular aos gerentes. Quando um usuário se torna um gerente, um celular é atribuído a esse usuário. O CA Identity Manager atribui o celular apenas uma vez, não cada vez que a política é avaliada. Se a política de celular for atualizada para incluir um modelo de celular mais novo, o CA Identity Manager não atribui novos celulares aos gerentes existentes.

Observação: o provisionamento de recursos fica disponível quando o CA Identity Manager integra-se ao servidor de provisionamento.

Desativando a configuração Aplicar uma vez

Se a configuração Aplicar uma vez não estiver ativada, as ações de alteração associadas à política de identidade são aplicadas cada vez que uma política de identidade é avaliada. Isso significa que o CA Identity Manager aplica as ações de alteração a todos os usuários que atenderem à condição na política, independentemente se as ações de alteração tiverem sido aplicadas anteriormente.

Normalmente, você deve desativar a configuração Aplicar uma vez em uma política de identidade que aplica conformidade. Por exemplo, você pode criar uma política de identidade que restringe a autoridade de gastos dos gerentes para US$ 5.000. Se o CA Identity Manager encontrar um gerente cuja autoridade de gastos estiver definida como US$ 10.000, redefinirá a autoridade de gastos para US$ 5.000. Cada vez que um gerente for sincronizado com a política de identidade, o CA Identity Manager verifica se a autoridade de gastos está definida corretamente.

Se uma alteração manual que estiver em conflito com uma ação de alteração for feita em um perfil de usuário, o CA Identity Manager substituirá a alteração quando o usuário for sincronizado com a política.

No exemplo anterior, se alguém aumentar manualmente uma autoridade de gastos de um gerente para US$ 10.000, o CA Identity Manager redefinirá a autoridade de gastos para US$ 5.000 quando o gerente for sincronizado com a política.

A tabela a seguir resume os efeitos de ativar ou desativar a configuração Aplicar uma vez.

Se Aplicar uma vez for...	Faça o seguinte...
Ativado	■ As ações de alteração associadas à política de identidade são aplicadas apenas uma vez ■ As alterações manuais feitas após a aplicação da política de identidade são mantidas ■ As atualizações não são aplicadas a usuários que atendem à condição em uma política de identidade se o CA Identity Manager tiver aplicado a política anteriormente ■ Quando um usuário deixar de atender à condição em uma política de identidade, o CA Identity Manager executa as ações de remoção

Se Aplicar uma vez for...	Faça o seguinte...
Desabilitado	■ As ações de alteração associadas à política de identidade são aplicadas cada vez que um usuário é sincronizado com a política ■ As alterações manuais são substituídas quando a política de identidade é aplicada ■ As atualizações na política são aplicadas quando um usuário é sincronizado ■ Quando um usuário deixar de atender à condição em uma política de identidade, o CA Identity Manager executa as ações de remoção

Condições da política

As condições da política são as regras que determinam o conjunto de usuários ao qual uma política de identidade se aplica.

A tabela a seguir descreve as opções disponíveis.

Sintaxe	Condição	Exemplo
(tudo)	A política de identidade é aplicada a todos os usuários.	
com <filtro-de-usuário>	O usuário deve corresponder a um ou mais valores de atributo.	Usuários com cargo=gerente e localidade=leste
em <regra-de-org>	O usuário deve pertencer a organizações nomeadas. **Observação:** quando você seleciona essa opção, o CA Identity Manager exibe uma nova caixa de listagem na qual você pode selecionar as seguintes opções: ■ Organização <organização> [e inferior] - Use uma tela de pesquisa de organização para selecionar uma organização e, opcionalmente, incluir as organizações filho. ■ Organizações com <filtro-de-org> [e inferior] - Especifica um filtro que selecione uma ou mais organizações.	Usuários na organização de vendas e inferior

Sintaxe	Condição	Exemplo
com <filtro-de-usuário> e que estiver em <regra-de-org>	O usuário deve corresponder a atributos de usuários específicos e pertencer a uma organização específica.	cargo=gerente e organização=vendas*
que são os integrantes de <função-de-integrante-do-grupo>	O usuário deve pertencer a um grupo que atenda a uma condição especificada pelos atributos do grupo. **Observação:** quando você seleciona essa opção, o CA Identity Manager exibe uma nova caixa de listagem na qual você pode selecionar as seguintes opções: ■ grupo <grupo> - Utilize uma tela de pesquisa de grupo para selecionar um grupo. ■ grupo com <filtro-de-grupo> - Especifica um filtro que seleciona um ou mais grupos.	Usuários que são integrantes de grupos com proprietário=CIO
que são os integrantes de <regra-de-função>	O usuário deve ser integrante de uma função. A função pode ser uma: ■ função de acesso ■ função administrativa ■ função de provisionamento **Observação:** para usar as funções de provisionamento, o CA Identity Manager deve se integrar a um servidor de provisionamento. Consulte o *Guia de Instalação* para obter mais informações.	Usuários que são integrantes da função de central de atendimento
que são os administradores de <regra-de-função>	O usuário deve ser um administrador de uma função. A função pode ser uma: ■ função de acesso ■ função administrativa ■ função de provisionamento **Observação:** para usar as funções de provisionamento, o CA Identity Manager deve se integrar a um servidor de provisionamento. Consulte o *Guia de Instalação* para obter mais informações.	Usuários que são administradores da função de Gerente de vendas

Sintaxe	Condição	Exemplo
que são os proprietários de <regra-de-função>	O usuário deve ser um proprietário de uma função. A função pode ser uma: ■ função de acesso ■ função administrativa ■ função de provisionamento **Observação:** para usar as funções de provisionamento, o CA Identity Manager deve se integrar a um servidor de provisionamento. Consulte o *Guia de Instalação* para obter mais informações.	Usuários que são proprietários da função de Gerenciador de usuários
retornado pela consulta <consulta-LDAP>	O usuário deverá atender a uma condição com base em uma consulta LDAP.	Usuário que atende às condições de uma consulta LDAP. Por exemplo: (departmentNumber=Accounts)
em <restrição-de-união-administrativa>	O usuário deverá atender a pelo menos uma das condições em uma lista de condições. É possível incluir os seguintes tipos de filtro em uma restrição de união administrativa: ■ Integrante da função de acesso/administrativa/de provisionamento ■ Administrador da função de acesso/administrativa/de provisionamento ■ Proprietário da função de acesso/administrativa/de provisionamento ■ Integrante de um grupo	Usuários que são integrantes da função de Gerenciador de certificação *ou* que são proprietários da função de Gerenciador de certificação.

Sintaxe	Condição	Exemplo
em <restrição-de-intersecção-administrativa>	O usuário deve atender a todas as condições em uma lista de condições. É possível incluir os seguintes tipos de filtro em uma restrição de união administrativa: ■ Integrante da função de acesso/administrativa/de provisionamento ■ Administrador da função de acesso/administrativa/de provisionamento ■ Proprietário da função de acesso/administrativa/de provisionamento ■ Integrante de um grupo	Usuários que são integrantes da função de Iniciador de contratos *e* da função de Aprovador de contratos.

Ações ao aplicar/remover políticas

Você pode definir ações de alteração que o CA Identity Manager executa quando avalia as políticas de identidade. As ações incluem:

Ações ao aplicar a política

Um conjunto de ações que o CA Identity Manager executa quando um usuário atende às condições da política.

Ações ao remover a política

Um conjunto de ações que o CA Identity Manager executa quando um usuário deixa de atender às condições da política.

Essas ações que o CA Identity Manager pode executar quando as políticas de identidade são aplicadas ou removidas são as mesmas. Consulte a tabela a seguir para obter mais informações:

Ação de alteração	Descrição
Adicionar ao grupo <nome-do-grupo> [...]	Adiciona usuários a um grupo. Quando essa opção é selecionada, o CA Identity Manager exibe uma tela onde você pode procurar o grupo desejado.
Adicionar ao grupo <nome-do-grupo> na organização do usuário	Adiciona usuários a um grupo local. Quando essa opção é selecionada, o CA Identity Manager apresenta uma caixa de texto onde você pode inserir o nome do grupo que deseja.

Ação de alteração	Descrição
Definir <atributo-de-usuário-de-valor-único> como valor	Define o valor de um atributo em um perfil de usuário. Caso exista um valor, o CA Identity Manager irá substituí-lo pelo valor especificado na ação de alteração.
Adicionar <valor> a <atributo-de-usuário-de-vários-valores>	Adiciona um valor a um atributo de usuário de vários valores. Essa opção não substitui os valores existentes.
Transformar em integrante da função de acesso	Atribui os usuários a uma função de acesso.
Transformar em administrador da função de acesso	Torna usuários os administradores de uma função de acesso
Transformar em integrante da função administrativa	Torna os usuários integrantes de uma função administrativa
Transformar em administrador da função administrativa	Torna os usuários administradores de uma função administrativa
Transformar em integrante da função de provisionamento	Torna os usuários integrantes de uma função de provisionamento, o que cria contas do terminal associadas. **Observação:** para usar as funções de provisionamento, o CA Identity Manager deve se integrar a um servidor de provisionamento. Consulte o *Guia de Instalação* do servidor de aplicativos.
Transformar em administrador da função de provisionamento	Torna os usuários administradores de uma função de provisionamento. **Observação:** para usar as funções de provisionamento, o CA Identity Manager deve se integrar a um servidor de provisionamento. Consulte o *Guia de Instalação* do servidor de aplicativos.
Remover do grupo <nome-do-grupo> [...]	Remove usuários de um grupo. Quando essa opção é selecionada, o CA Identity Manager exibe uma tela onde você pode procurar o grupo desejado.
Remover do grupo <nome-do-grupo> na organização do usuário	Remove usuários de um grupo local. Quando essa opção é selecionada, o CA Identity Manager apresenta uma caixa de texto onde você pode inserir o nome do grupo que deseja.
Remover <valor> de <atributo-de-usuário-de-vários-valores>	Remove um valor de um atributo de usuário de vários valores.
Remover integrante da função de acesso	Revoga uma função de acesso.

Ação de alteração	Descrição
Remover administrador da função de acesso	Revoga privilégios de administrador de uma determinada função de acesso
Remover integrante da função administrativa	Revoga uma função administrativa.
Remover administrador da função administrativa	Revoga privilégios de administrador de uma determinada função administrativa
Remover integrante da função de provisionamento	Revoga uma função de provisionamento.
Remover administrador da função de provisionamento	Revoga privilégios de administrador de uma determinada função de provisionamento.
Enviar mensagem de auditoria	Envia uma mensagem que você criar para o banco de dados de auditoria. Essa mensagem poderá ser exibida em um relatório que você criar.
Violação de conformidade	Envia uma mensagem que você criar para o banco de dados de auditoria. Se você criar um relatório de conformidade, a mensagem será exibida toda vez que a política de identidade for aplicada/removida de um usuário. Consulte o *Guia de Configuração* para obter mais informações sobre auditoria. **Observação:** você deve ativar a caixa de seleção Conformidade na guia Perfil para que o conjunto de políticas de identidade use a opção Violação de conformidade.
Aceitar (Somente ação ao aplicar políticas)	Permite que a tarefa seja enviada quando houver uma violação de política de identidade preventiva. Quando você selecionar essa ação, deve fornecer uma mensagem que o CA Identity Manager grava no banco de dados de auditoria e exibe em Exibir tarefas enviadas na ocorrência de uma violação.
Recusar (Somente ação ao aplicar políticas)	Impede que a tarefa seja enviada quando ocorre uma violação na política de identidade. Essa ação é usada com políticas de identidade preventivas, para impedir que os usuários recebam privilégios que podem resultar em um conflito de interesses ou fraudes. Quando você seleciona essa ação, também fornece uma mensagem que o CA Identity Manager exibe na ocorrência de uma violação. A mensagem é armazenada no banco de dados de auditoria e exibida no console de usuário.

Ação de alteração	Descrição
Aviso (Somente ação ao aplicar políticas)	Aciona um processo de fluxo de trabalho quando ocorre uma violação de política de identidade preventiva, caso você associe essa violação a uma política de aprovação de fluxo de trabalho. O CA Identity Manager permite que a tarefa seja enviada independentemente se o fluxo de trabalho tiver sido configurado. **Observação:** para obter informações sobre como associar um processo de fluxo de trabalho a uma política de identidade preventiva, consulte Fluxo de trabalho e políticas de identidade preventivas (na página 478). Quando você seleciona essa ação, também fornece uma mensagem que o CA Identity Manager exibe na ocorrência de uma violação. A mensagem é armazenada no banco de dados de auditoria e exibida em Exibir tarefas enviadas.

Mais informações:

Políticas de identidade preventivas (na página 472)
Fluxo de trabalho e políticas de identidade preventivas (na página 478)

Especificar proprietários para o conjunto de políticas de identidade

Na guia Proprietários, defina as regras sobre quem pode ser o proprietário do conjunto de políticas de identidade. Um proprietário do conjunto de políticas de identidade pode modificar as informações básicas sobre o conjunto de políticas e adicionar, alterar ou remover políticas de identidade do conjunto.

Para preencher a guia Proprietários:

1. Defina as regras de proprietário, que determinam os usuários que podem modificar o conjunto de políticas de identidade.
2. Clique em Enviar.

Gerenciar um conjunto de políticas de identidade

O CA Identity Manager inclui as seguintes tarefas de gerenciamento de um conjunto de políticas de identidade:

- Exibir conjunto de políticas de identidade
- Modificar conjunto de políticas de identidade
- Excluir conjunto de políticas de identidade

Por padrão, quando um administrador usa uma dessas tarefas, o CA Identity Manager exibe uma lista de todos os conjuntos de políticas de identidade dos quais o administrador é um proprietário. Em seguida, o administrador poderá escolher o conjunto de políticas que precisa na lista.

Em um ambiente do CA Identity Manager que inclui vários conjuntos de políticas de identidade, é possível personalizar as tarefas de Exibir, Modificar e Excluir conjunto de políticas de identidade, para permitir que os administradores procurem um conjunto de políticas de identidade em vez de exibi-los em uma lista.

Para personalizar essas tarefas:

1. No console de usuário, selecione Funções e tarefas, Funções administrativas, Modificar tarefa administrativa.

   A tela Modificar tarefa administrativa é exibida.

2. Procure e selecione a tarefa que deseja personalizar.
3. Na guia Escopo, selecione Todos os conjuntos de políticas de identidade.

   Quando essa opção é selecionada, o CA Identity Manager usa a definição de tela de pesquisa de conjunto de políticas de identidade padrão.

4. Clique em Enviar.

Como usuários e políticas de identidade são sincronizados

Ao usar políticas de identidade, é importante compreender como o CA Identity Manager avalia e aplica as políticas aos usuários. Sem um entendimento completo do processo de sincronização de usuário, você poderá configurar conjuntos de políticas de identidade que geram resultados inesperados.

O procedimento a seguir descreve como o CA Identity Manager avalia e aplica políticas de identidade:

1. O processo de sincronização de usuário é iniciado:
   - **Automaticamente** — É possível configurar as tarefas do CA Identity Manager para acionar automaticamente a sincronização de usuário
   - **Manualmente** — Use a tarefa Sincronizar usuário no console de usuário para sincronizar um usuário.
2. O CA Identity Manager determina o conjunto de políticas de identidade que se aplicam a um usuário.
3. O CA Identity Manager compara o conjunto de políticas de identidade que se aplica a um usuário com a lista de políticas que já foram aplicadas a esse usuário.

   Observação: a lista de políticas que já foram aplicadas a um usuário é armazenada no conhecido atributo %IDENTITY_POLICY% no perfil de usuário. Para obter informações sobre como configurar esse atributo, consulte o *Guia de Configuração*.
   - Se uma política de identidade estiver na lista de políticas aplicáveis, *e* a política *não* tiver sido aplicada ao usuário anteriormente, o CA Identity Manager adicionará a política a uma lista de alocação.
   - Se uma política de identidade estiver na lista de políticas aplicáveis, a política tiver sido aplicada ao usuário anteriormente e a configuração Aplicar uma vez para a política estiver desativada, o CA Identity Manager adicionará a política a uma lista de realocação.
   - Se uma política de identidade não estiver na lista de políticas aplicáveis, a política tiver sido aplicada ao usuário e o usuário deixar de corresponder à condição da política. O CA Identity Manager adicionará essas políticas a uma lista de desalocação.
4. Depois que o CA Identity Manager avaliar todas as políticas para um usuário, aplicará as políticas na seguinte ordem:
   a. Políticas de identidade da lista de desalocação
   b. Políticas de identidade da lista de alocação
   c. Políticas de identidade da lista de realocação

5. Depois que as políticas de identidade tiverem sido aplicadas, o CA Identity Manager reavaliará as políticas para ver se outras alterações serão necessárias com base nas alterações que ocorreram no primeiro processo de sincronização (etapas de 2 a 4).

   Isso é feito para garantir que as alterações realizadas através da aplicação de políticas de identidade não acionem outras políticas de identidade.

6. O CA Identity Manager continua a reavaliar e aplicar políticas de identidade até que o usuário seja sincronizado com todas as políticas aplicáveis, ou até que o CA Identity Manager atinja o nível máximo de recursão, que é definido no Management Console.

   Por exemplo, uma política de identidade pode alterar o departamento de um usuário quando o usuário recebe uma função. O novo departamento dispara outra política de identidade. No entanto, se o nível de recursão for definido como 1, a alteração subsequente não será feita até que o usuário seja sincronizado novamente.

   Para obter mais informações sobre como definir o nível de recursão, consulte a Ajuda online do Management Console.

Configurar a sincronização de usuário automática

O CA Identity Manager pode sincronizar automaticamente as contas de usuário com as políticas de identidade em diferentes pontos durante o ciclo de vida de uma tarefa.

Uma tarefa do CA Identity Manager gera *eventos*, que são atividades detectáveis que ocorrem durante o processamento da tarefa. Por exemplo, a tarefa Criar usuário padrão gera CreateUserEvent, AddUserToGroupEvent e AssignAccessRoleEvent. É possível configurar o CA Identity Manager para sincronizar usuários após a conclusão de uma tarefa, ou quando cada evento for concluído.

Observação: a seção Sincronizar usuários com políticas de identidade (na página 462) fornece mais informações sobre o processo de sincronização de usuário.

Para configurar uma tarefa para acionar a sincronização de usuário:

1. Efetue logon no CA Identity Manager como um usuário que pode modificar tarefas administrativas.
2. Selecione Funções e tarefas, Tarefa administrativa, Modificar tarefa administrativa.

   O CA Identity Manager exibe uma tela de pesquisa.

3. Procure e selecione a tarefa administrativa que acionará a sincronização de usuário.

4. Selecione uma das seguintes opções no campo Sincronização de usuário na guia Perfil da tarefa:

   - **Desativado** — Essa tarefa não acionará a sincronização de usuário.
   - **Ao concluir a tarefa** — O CA Identity Manager iniciará o processo de sincronização de usuário após a conclusão de todos os eventos. Essa configuração é a opção de sincronização padrão para as tarefas Criar usuário, Modificar usuário e Excluir usuário. A configuração padrão para todas as outras tarefas é Desativado.

     Observação: se você selecionar a opção Ao concluir a tarefa de uma tarefa que inclui vários eventos, o CA Identity Manager não sincronizará os usuários até que todos os eventos da tarefa sejam concluídos. Se um ou mais desses eventos exigirem uma aprovação de fluxo de trabalho, esse procedimento pode levar vários dias. Para evitar que o CA Identity Manager espere para aplicar as políticas de identidade após a conclusão de todos os eventos, selecione a opção Em cada evento.
   - **Em cada evento** — O CA Identity Manager inicia o processo de sincronização de usuário quando cada evento em uma tarefa for concluído.

     Para tarefas com um evento principal e um secundário para o mesmo usuário, a configuração da sincronização de usuário como Em cada evento pode resultar em mais avaliações de políticas de identidade para um usuário do que na opção Ao concluir a tarefa.

Sincronizar usuários manualmente

Você pode optar por sincronizar manualmente um usuário com um conjunto de políticas de identidade para garantir que uma conta de usuário tenha os privilégios certos ou esteja de acordo com uma política de conformidade.

É possível sincronizar manualmente um usuário por meio da tarefa Sincronizar usuário no console de usuário do CA Identity Manager.

Observação: para que a tarefa Sincronizar usuário funcione corretamente, a opção Sincronização de usuário deve ser definida como Desativado e a opção Sincronização de conta deve ser definida como Ao concluir a tarefa ou Em cada evento. Para melhorar o desempenho, selecione a opção Ao concluir a tarefa. Essas opções são definidas na guia Perfil da tarefa Sincronizar usuário.

A tarefa Sincronizar usuário inclui as seguintes guias:

- **Políticas correspondentes atuais** — Exibe uma lista de políticas de identidade que o CA Identity Manager aplicará ao usuário quando a tarefa Sincronizar usuário for enviada.

  Observação: a guia Políticas correspondentes atuais exibe somente as políticas de identidade que se aplicam ao usuário no momento em que você acessa a tarefa Sincronizar usuário. Quando o usuário é sincronizado com essas políticas, podem ocorrer alterações que acionam outras políticas de identidade. Para evitar que o CA Identity Manager aplique as novas políticas até que elas tenha sido verificadas, defina o nível de recursão de conjuntos de políticas de identidade para 1 no Management Console do CA Identity Manager. Após enviar a tarefa Sincronizar usuário, acesse-a novamente para verificar as políticas.

- **Políticas já aplicadas** — Exibe uma lista de políticas de identidade que já foram aplicadas ao usuário.

- **Resumo da sincronização** — Exibe todas as políticas de identidade que se aplicam ao usuário e as ações de alteração para essas políticas.

Para sincronizar uma conta de usuário:

1. Efetue logon no CA Identity Manager como um usuário que pode usar a tarefa Sincronizar usuário. (Por padrão, os usuários com a função de Gerente do sistema podem usar essa tarefa.)
2. Selecione Políticas, Sincronizar usuário.

   A tarefa Sincronizar usuário será aberta.
3. Selecione a guia Resumo da sincronização.
4. Verifique as políticas e as ações associadas que o CA Identity Manager aplicará ao usuário e, em seguida, clique em Enviar.

Verificar a sincronização de usuário

Para confirmar se as alterações apropriadas serão executadas quando um usuário for sincronizado com as políticas de identidade, verifique a guia Políticas já aplicadas na tarefa Sincronizar usuário.

1. Efetue logon no CA Identity Manager como um usuário que pode usar a tarefa Sincronizar usuário. (Por padrão, os usuários com a função de Gerente do sistema podem usar essa tarefa.)
2. Selecione Políticas, Sincronizar usuário.

   A tarefa Sincronizar usuário será aberta.
3. Selecione a guia Políticas já aplicadas.
4. Verifique as políticas e as ações associadas que o CA Identity Manager aplicará ao usuário.

Conjuntos de políticas de identidade em um ambiente do CA Identity Manager

As seções a seguir descrevem as diferentes maneiras de usar as políticas de identidade:

- Exemplo: Preenchendo automaticamente os atributos do usuário (na página 467)
- Exemplo: Alocando recursos e direitos (na página 468)
- Exemplo: Aplicando conformidade (na página 469)
- Exemplo: Aplicando segregação de tarefas (na página 470)

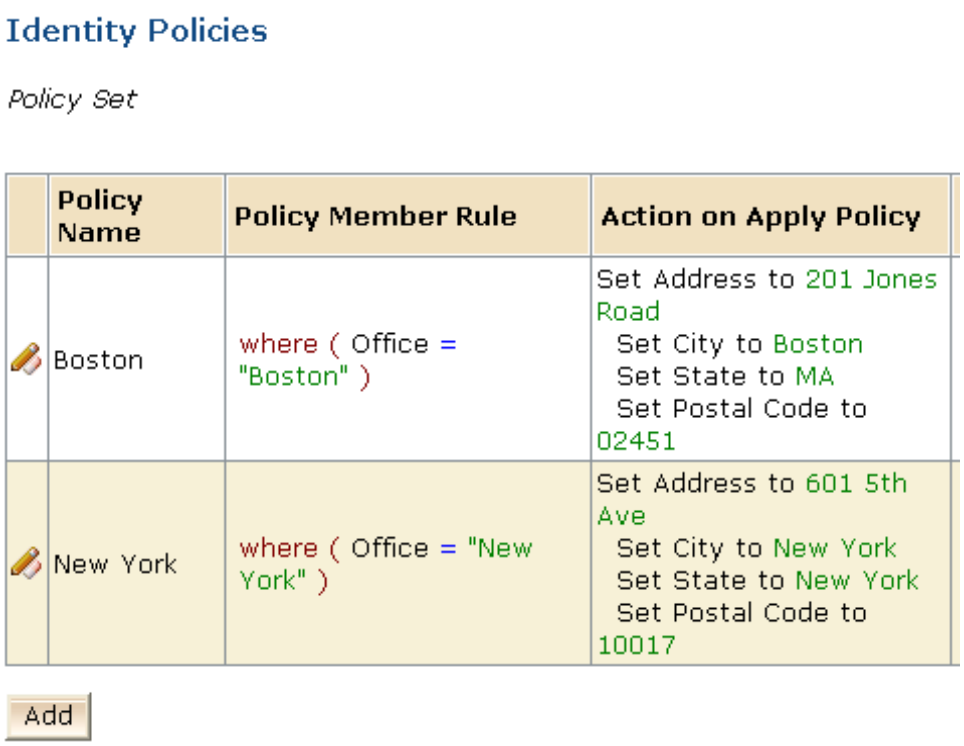
Exemplo: Preenchendo automaticamente os atributos do usuário

Você pode usar um conjunto de políticas de identidade para atribuir automaticamente valores de atributos do usuário com base em outro valor de atributo ou direitos de usuário. Por exemplo, você pode criar um conjunto de políticas de identidade que preenche automaticamente um endereço para correspondência do usuário com base no escritório doméstico do usuário.

Para configurar um conjunto de políticas de identidade para endereços de funcionários, crie uma política de identidade com as configurações a seguir para cada escritório:

Configuração	Valor
Condições da política	escritório = <localização_do_escritório>
Ação ao aplicar a política	definir Rua = <alguma_rua> definir Cidade = <alguma cidade> Definir Estado/província = <algum estado ou província> Definir Código postal = <algum código postal>

A figura a seguir mostra exemplos de políticas no conjunto de políticas de identidade Endereços de funcionários.



Exemplo: Alocando recursos e direitos

Políticas de identidade podem atribuir automaticamente recursos, como contas de domínio, ou conceder direitos, como tornar um usuário integrante de uma função, quando os usuários atendem à condição da política. Por exemplo, você pode criar um conjunto de políticas de identidade que atribuem recursos e funções com base no cargo de um usuário.

Para criar um conjunto de políticas de identidade para alocação de recursos e funções, crie uma política de identidade com as configurações a seguir para cada um dos cargos em sua organização:

Configuração	Valor
Condições da política	cargo = <algum _cargo>

Configuração	Valor
Ação ao aplicar a política	Qualquer ação que alocar recursos ou direitos a usuários que atendem à condição da política, por exemplo: ■ transformar em integrante de <algum_grupo> ■ transformar em integrante da função administrativa <alguma_função_administrativa> ■ transformar em integrante da função de provisionamento <alguma_função_de_provisionamento>
Ação ao remover a política	Qualquer ação que remover recursos ou direitos quando um usuário deixar de atender à condição da política. Por exemplo, se o CA Identity Manager tiver transformado o usuário em integrante de uma função quando a política de identidade foi aplicada, convém configurar o CA Identity Manager para revogar a função quando o usuário deixar de atender à condição da política.

A figura a seguir ilustra políticas de amostra no conjunto de políticas de identidade Recursos de funcionários:

Identity Policies

Policy Set

	Policy Name	Policy Member Rule	Action on Apply Policy	Action on Remove Policy
	Managers	where (Title = "Manager")	Make member of admin role User Manager Make member of provisioning role Corporate NT Domain Role	Remove member from admin role User Manager
	Human Resources	where (Title = "HR Administrator")	Make member of admin role User Manager Add to group HR Department Make member of provisioning role Corporate NT Domain Role	Remove from group HR Department Remove member from admin role User Manager Remove member from provisioning role Corporate NT Domain Role

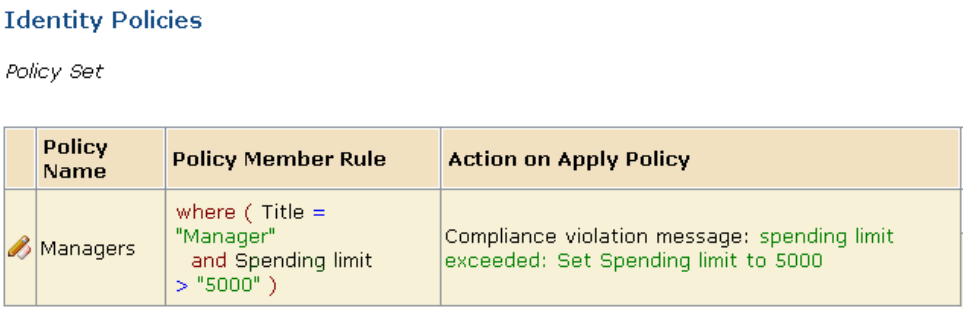
Exemplo: Aplicando conformidade

Você pode configurar políticas de identidade para definir as condições que devem ou não devem existir, e para executar determinadas ações com base na avaliação dessas condições. Por exemplo, você pode definir uma política de conformidade que declara que os gerentes devem ter um limite de gastos de US$ 5.000. Se um gerente tiver um limite de gastos de US$ 10.000, o CA Identity Manager pode redefinir o limite de gastos do gerente e registrar uma violação de conformidade para fins de auditoria.

Para criar um conjunto de políticas de conformidade para aplicar limites de gastos, crie uma política de identidade com as seguintes configurações:

Configuração	Valor
Aplicar uma vez	Não ativado
Conformidade	Ativado
Condições da política	Todas as condições que definem a conformidade ou uma violação de conformidade, por exemplo: cargo = <algum_cargo> AND Limite de gastos > <algum limite de gastos>
Ação ao aplicar a política	As ações que o CA Identity Manager deve executar quando a condição da política se aplica, por exemplo: ■ Mensagem de violação de conformidade: limite de gastos excedido ■ Definir limite de gastos para <algum_valor>

A figura a seguir mostra a política de conformidade de amostra descrita neste exemplo.



Exemplo: Aplicando segregação de tarefas

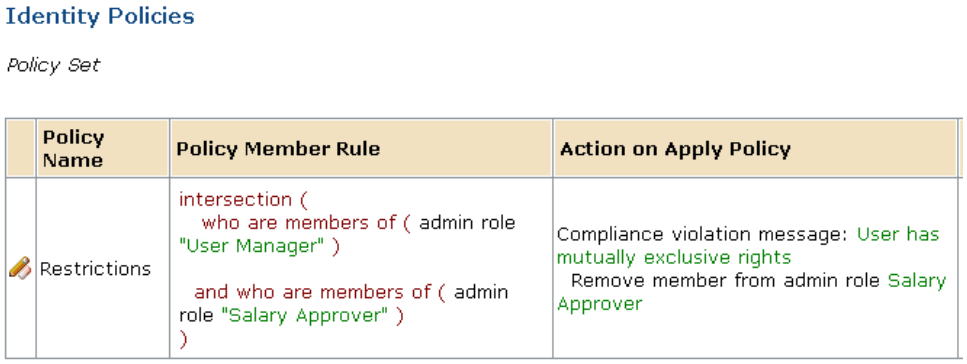
As políticas de identidade podem definir funções que são mutuamente exclusivas e não podem ser concedidas para o mesmo usuário ao mesmo tempo. Por exemplo, você pode impedir que um gerenciador de usuários que pode conceder aumentos também seja um Aprovador de salários.

Para criar um conjunto de políticas de identidade que aplica a segregação de tarefas, crie uma política de identidade com as seguintes configurações:

Configuração	Valor
Aplicar uma vez	Não ativado

Configuração	Valor
Conformidade	Ativado
Condições da política	Use a opção "em <restrição-de-intersecção-administrativa>" para definir um conjunto de condições que violam uma política de negócios. Se um usuário atender a todas as condições, o CA Identity Manager executará as ações no campo Ação ao aplicar a política. Por exemplo, defina a condição da política da seguinte maneira: interseção (que são os integrantes de <alguma_função>) e que são os integrantes de <alguma_outra_função>)
Ação ao aplicar a política	As ações que o CA Identity Manager deve executar quando a condição da política se aplica, por exemplo: ■ Mensagem de violação de conformidade: O usuário possui funções que se excluem mutuamente ■ Remover integrante de <alguma_função>

A figura a seguir ilustra a política de identidade neste exemplo.



Políticas de identidade preventivas

Uma *política de identidade preventiva* é um tipo de política de identidade que impede que os usuários recebam privilégios que possam resultar em um conflito de interesses ou fraude. Essas políticas apoiam os requisitos de segregação de tarefas de uma empresa.

Políticas de identidade preventivas, que são executadas antes que uma tarefa seja enviada, permitem que um administrador verifique violações de políticas antes de atribuir privilégios ou alterar atributos do perfil. Se uma violação existir, o administrador pode removê-la antes de enviar a tarefa.

Por exemplo, uma empresa pode criar uma política de identidade preventiva que proíba que os usuários que tenham a função Gerenciador de usuários também tenham a função Aprovador de usuários. Se um administrador usar a tarefa Modificar usuário para fornecer a um gerenciador de usuários a função de Aprovador de usuários, o CA Identity Manager exibirá uma mensagem sobre a violação. O administrador pode alterar as atribuições de função para remover a violação antes de enviar a tarefa.

Você pode criar políticas de identidade preventivas para as seguintes alterações:

- **Associação da função**

  Impede que os usuários tenham determinadas funções ao mesmo tempo.

  Por exemplo, os usuários não podem ter as funções de Gerenciador de usuários e de Aprovador de usuários ao mesmo tempo.

- **Administradores da função**

  Impede que os usuários sejam administradores de determinadas funções se forem administradores de outras funções.

  Por exemplo, os usuários não podem ser administradores das funções de Gerenciador de usuários e de Aprovador de usuários ao mesmo tempo.

- **Atributos do usuário**

  Impede que os usuários tenham determinados atributos de perfil ao mesmo tempo.

  Por exemplo, os usuários não podem ter o cargo de Contador sênior e pertencer ao departamento de TI.

- **Atributos de organização**

  Impede que perfis de usuário sejam criados em uma determinada organização.

  Por exemplo, os administradores não podem criar perfis de funcionário na organização Fornecedores.

- **Atributos do grupo**

  Impede que os usuários sejam integrantes de determinados grupos.

  Por exemplo, os usuários não podem ser integrantes do grupo de Equipe do projeto e do grupo de Contabilidade.

Mais informações:

Ações para violações da política de identidade preventiva (na página 473)

Ações para violações da política de identidade preventiva

Quando uma política de identidade preventiva aplica-se a uma mudança nos negócios, a CA executará determinadas ações para resolver a violação.

Quando você especifica uma dessas ações em uma política de identidade, especifica uma mensagem que descreve a violação. Essa mensagem é registrada no banco de dados de auditoria. Dependendo do tipo de ação, a mensagem também poderá ser exibida para os usuários no console de usuário e registrada em Exibir tarefas enviadas.

É possível configurar as seguintes ações para uma política de identidade preventiva:

Aceitar

O CA Identity Manager exibe uma mensagem em Exibir tarefas enviadas que descreve a violação, mas permite que a tarefa seja enviada.

Recusar

O CA Identity Manager exibe uma mensagem no console de usuário e impede o envio da tarefa.

Aviso

O CA Identity Manager exibe uma mensagem no console de usuário e em Exibir tarefas enviadas. Essa ação pode, opcionalmente, acionar um processo de fluxo de trabalho que exige uma aprovação de um usuário apropriado antes que o CA Identity Manager execute a tarefa.

Para acionar um processo de fluxo de trabalho, você deve associar a política de identidade preventiva a um processo de fluxo de trabalho com base em políticas (na página 479) a tarefas que possam causar a violação.

Por exemplo, se a violação ocorrer quando um usuário receber determinadas funções ao mesmo tempo, configure o processo de fluxo de trabalho para todas as tarefas que atribuem essas funções a usuários.

Observação: ao configurar o processo de fluxo de trabalho com base em políticas para a tarefa, a regra de aprovação deve fazer referência ao nome da política de identidade preventiva.

Como funcionam as políticas de identidade preventivas

O processo de exemplo a seguir ilustra como as políticas de identidade preventivas funcionam:

1. Um administrador de políticas de identidade cria uma política de identidade preventiva que proíbe que os usuários que possuem o cargo de Contador sênior estejam no departamento de TI.

   Ao definir essa política de identidade, o administrador especifica que o CA Identity Manager deve recusar quaisquer alterações que violem essa política.

2. Um administrador de RH usa a tarefa Criar usuário para criar um perfil de usuário para um novo Contador sênior. O administrador de RH seleciona corretamente o cargo do usuário, mas seleciona acidentalmente o departamento de TI.

3. O administrador de RH preenche os demais campos da tarefa Criar usuário e clica em Enviar.

4. O CA Identity Manager detecta que a tarefa abrange alterações que estão definidas em uma política de identidade e avalia se há violações nas alterações.

5. O CA Identity Manager detecta a violação, exibe uma mensagem ao administrador de RH e impede o envio da tarefa.

   O CA Identity Manager também registra a mensagem no banco de dados de auditoria.

6. O administrador de RH vê os detalhes da violação na mensagem e altera o departamento do usuário para Finanças. Em seguida, o administrador envia novamente a tarefa.

7. O CA Identity Manager avalia as alterações propostas em relação a todas as políticas de identidade aplicáveis e, em seguida, permite que a tarefa Criar usuário seja enviada.

Observações importantes sobre políticas de identidade preventivas

Antes de implementar políticas de identidade preventivas, observe o seguinte:

- As políticas de identidade preventivas impedem apenas as violações que poderiam ocorrer devido a alterações propostas na tarefa atual. Elas não impedem violações existentes.

  Por exemplo, uma empresa cria uma política de identidade preventiva que impede que os usuários tenham as funções de Gerenciador de usuários e Aprovador de usuários ao mesmo tempo. Um administrador atribui a função de Gerenciador do grupo a um usuário que já possui as funções de Gerenciador de usuários e Aprovador de usuários. O CA Identity Manager permite que a nova atribuição seja bem-sucedida, pois essa alteração não causa diretamente uma violação da política.

- Se várias políticas de identidade preventivas se aplicarem a um conjunto de alterações propostas, o CA Identity Manager aplicará primeiro as políticas com ações Recusar.

- Não especifique grupos dinâmicos nas condições de políticas de identidade preventivas. (As condições da política determinam o conjunto de usuários ao qual a política de identidade preventiva se aplica.)

  Por exemplo, uma empresa tem um grupo dinâmico que inclui todos os usuários que possuem o cargo de Gerente. A empresa também cria uma política de identidade preventiva que proíbe que os integrantes do grupo Gerentes tenham a função de prestador de serviço.

  Um administrador altera o cargo de um usuário que possui a função de prestador de serviço para Gerente. Essa alteração fará com que o usuário se torne um integrante do grupo Gerentes *depois* que a tarefa tiver sido enviada com êxito. No entanto, o cargo do usuário não é Gerente no momento em que o CA Identity Manager avalia a política, portanto, nenhuma violação é detectada.

- O filtro de proprietário da função e o filtro de consulta LDAP não são suportados em condições da política para políticas de identidade preventivas.

Criar uma política de identidade preventiva

Antes de criar uma política de identidade preventiva, você deve criar um conjunto de políticas de identidade, que agrupa logicamente um conjunto de políticas de identidade.

Observação: consulte o tópico Observações importantes sobre políticas de identidade preventivas (na página 475) antes de começar.

Para criar um conjunto de políticas de identidade preventivas:

1. Abra Políticas, Criar conjunto de políticas de identidade no console de usuário.

   Crie um conjunto de políticas de identidade ou use um existente como modelo.
2. Defina o perfil do conjunto de políticas de identidade (na página 451) na guia Perfil.
3. Crie uma regra de integrante do conjunto de políticas (na página 452) na guia Políticas.
4. Crie uma política de identidade preventiva da seguinte maneira:
   a. Clique em Adicionar.
   b. Digite um nome para a política de identidade.

      Observação: as configurações Aplicar uma vez e Conformidade não se aplicam a políticas de identidade preventivas.
   c. Identifique os usuários aos quais a política se aplica na seção Condição da política.

      Observação: o filtro de proprietário da função e o filtro de consulta LDAP não são suportados em políticas de identidade preventivas.
   d. No campo Ação ao aplicar a política, defina as ações que o CA Identity Manager executa quando detecta uma violação de política:

      Aceitar

      O CA Identity Manager exibe uma mensagem em Exibir tarefas enviadas que descreve a violação, mas permite que a tarefa seja enviada.

      Recusar

      O CA Identity Manager exibe uma mensagem no console de usuário e impede o envio da tarefa.

      Aviso

      O CA Identity Manager exibe uma mensagem no console de usuário e em Exibir tarefas enviadas. Essa ação pode, opcionalmente, acionar um processo de fluxo de trabalho (na página 478).

      Ao selecionar uma dessas ações, o CA Identity Manager exibe uma caixa de texto onde você pode especificar a mensagem que é exibida na ocorrência de uma violação.

e. Especifique a mensagem na caixa de texto.

Observação: caso esteja localizando o console de usuário, pode especificar uma chave de recurso em vez de texto no campo de mensagens. Consulte o *Guia de Design do Console de Usuário* para obter mais informações sobre chaves de recurso.

f. Adicione outras ações, se necessário, e clique em OK.

5. Especifique proprietários para o conjunto de políticas de identidade (na página 461).

Observação: antes de usar o conjunto de políticas de identidade que você criou, certifique-se de que as políticas de identidade estão ativadas no Management Console. Consulte o *Guia de Configuração* para obter mais informações.

Caso de uso: impedindo que os usuários tenham funções conflitantes

A Forward, Inc. deseja impedir que seus funcionários tenham as funções de Gerenciador de usuários e Aprovador de usuários ao mesmo tempo. Os funcionários que tiverem essas duas funções podem modificar atributos de usuário, como salário, e aprová-los de maneira inadequada.

Para evitar essa situação, a Forward, Inc. cria uma política de identidade preventiva que se aplica aos usuários que têm as funções de Gerenciador de usuários e Aprovador de usuários. Se um administrador tentar atribuir essas funções a um usuário, o CA Identity Manager recusa o envio da tarefa e exibe uma mensagem que explica a violação.

Configure uma política de identidade preventiva para oferecer suporte a esse caso de uso, da seguinte maneira:

- Crie um conjunto de políticas de identidade para a política que deseja criar.
- Crie uma política de identidade preventiva com as seguintes configurações:
  - Condição da política:

  - Ação ao aplicar a política:
    - Recusar com a mensagem: O usuário não pode ser integrante das funções de Aprovador de usuários e Gerenciador de usuários.

Fluxo de trabalho e políticas de identidade preventivas

Quando uma política de identidade preventiva estiver configurada para emitir um aviso, você pode definir um processo de fluxo de trabalho em nível de tarefa com base em políticas, que está associado à política de identidade, para tarefas que podem acionar uma violação. Por exemplo, se uma política de identidade proíbe que contadores seniores sejam integrantes do departamento de TI, você define um processo de fluxo de trabalho em nível de tarefa com base em políticas nas tarefas Criar usuário e Modificar usuário.

Todos os itens de trabalho que são gerados como resultado do fluxo de trabalho em nível de tarefa com base em políticas devem ser aprovados antes que o CA Identity Manager execute a tarefa. Os aprovadores veem um item da lista de tarefas quando efetuam logon no console de usuário. Quando o aprovador clica no item da lista de tarefas, uma tarefa de aprovação, que inclui a mensagem de aviso que descreve a violação, é exibida. O aprovador pode aprovar ou recusar a tarefa, com base na violação.

Os processos de fluxo de trabalho com base em políticas são associados às políticas de identidade preventivas pelo nome da política.

Mais informações:

Fluxo de trabalho com base em políticas (na página 314)

Violações da política de identidade em tarefas de aprovação

Quando uma política de identidade preventiva está associada a um processo de fluxo de trabalho de uma tarefa, o CA Identity Manager gera um item da lista de tarefas para os aprovadores apropriados. Esses aprovadores usam uma tarefa de aprovação para aprovar ou recusar a mudança que acionou a violação de política.

A tarefa de aprovação padrão inclui uma seção que lista as violações de políticas de identidade. Pode haver mais de uma violação se as alterações propostas acionarem várias políticas de identidade preventivas.

Cada violação pode ter um dos seguintes status:

- **Avaliação pendente**

  O CA Identity Manager ainda não começou a avaliação das regras de aprovação para a tarefa. Esse é o estado inicial.

- **Aguardando aprovação**

  O CA Identity Manager localizou uma correspondência para a política de identidade definida nas regras de aprovação e acionou o processo de fluxo de trabalho associado.

- **Aprovado**

  Um aprovador aprovou as alterações propostas. O CA Identity Manager faz as alterações que acionaram as violações da política de identidade preventiva.

- **Recusado**

  Um aprovador recusou a mudança proposta. A tarefa foi recusada.

- **Nenhum fluxo de trabalho configurado**

  Não há processo de fluxo de trabalho configurado para essa violação. A tarefa é executada sem nenhuma aprovação necessária.

Como configurar o fluxo de trabalho para políticas de identidade preventivas

Configure o fluxo de trabalho para políticas de identidade preventivas nas tarefas administrativas que englobam alterações que podem acionar uma violação de política de identidade.

Por exemplo, se a política de identidade preventiva proíbe que os usuários tenham determinadas funções administrativas ao mesmo tempo, configure tarefas que atribuam funções administrativas para oferecer suporte ao fluxo de trabalho para políticas de identidade preventivas.

Observação: antes de configurar o fluxo de trabalho, crie uma política de identidade preventiva com as seguintes configurações:

- Um nome de política exclusivo

  O nome da política deve ser exclusivo entre todos os conjuntos de políticas de identidade, pois os processos de fluxo de trabalho são associados às políticas de identidade preventivas pelo nome da política.

  Se várias políticas de identidade preventivas tiverem o mesmo nome, vários processos de fluxo de trabalho podem ser aplicados.

- Aviso no campo Ação ao aplicar a política

  Aviso é a única ação que pode acionar um processo de fluxo de trabalho.

Depois de configurar a política de identidade preventiva, determine as tarefas que podem acionar a violação de política. Em seguida, crie uma política de aprovação de fluxo de trabalho (na página 480) para essas tarefas.

Criar uma política de aprovação de fluxo de trabalho para políticas de identidade preventivas

Você pode configurar um processo de fluxo de trabalho em nível de tarefa com base em políticas para uma tarefa administrativa. Esse processo de fluxo de trabalho inclui uma ou mais políticas de aprovação que podem associar uma política de identidade preventiva a um fluxo de trabalho. O CA Identity Manager executa o fluxo de trabalho quando ocorre uma violação da política de identidade preventiva associada.

Observação: para obter mais informações sobre os processos de fluxo de trabalho em nível de tarefa com base em políticas, consulte Fluxo de trabalho com base em políticas (na página 314).

Para criar uma política de aprovação de fluxo de trabalho para políticas de identidade preventivas:

1. Modifique as tarefas administrativas que permitem alterações que possam acionar uma violação de uma política de identidade preventiva.

   Por exemplo, se uma violação de política de identidade ocorrer porque o usuário possui as funções de Gerenciador de usuários e Aprovador de usuários, modifique as tarefas administrativas que permitem aos administradores atribuir funções, como Criar usuário, Modificar usuário e Modificar integrantes/administradores da função administrativa.

2. Clique no ícone Editar ao lado do campo Processo de fluxo de trabalho na guia Perfil da tarefa para adicionar um processo de fluxo de trabalho.

   O CA Identity Manager exibe a tela Configuração do fluxo de trabalho em nível de tarefa.

3. Selecione Com base na política e, em seguida, clique em Adicionar.

4. Na seção Regra de aprovação, selecione o objeto Violação da política de identidade.

5. No campo Política de identidade, selecione um filtro que determina quais políticas de identidade acionam o fluxo de trabalho associado à política de aprovação.

   No filtro, inclua o nome da política de identidade, *não* o nome do conjunto de políticas de identidade.

6. Configure os campos Avaliação de regra, Ordem das políticas e Descrição da política, conforme necessário.

7. Selecione um processo de fluxo de trabalho e, em seguida, clique em OK.

   Quando você seleciona um processo de fluxo de trabalho, o CA Identity Manager exibe campos adicionais.

8. Especifique as tarefas de aprovação e os aprovadores, conforme necessário.

   O CA Identity Manager associa o processo de fluxo de trabalho com a política de identidade preventiva.

Caso de uso: aprovando cargos

A Forward, Inc. tem uma política de empresa que declara que todos os gerentes devem ser funcionários de tempo integral. No entanto, recentemente a Forward, Inc. contratou vários prestadores de serviço para projetos específicos. Para executar esses projetos específicos de maneira eficiente, alguns dos prestadores de serviço receberão o cargo de Gerente. A Forward, Inc. deseja exigir a aprovação do diretor de Recursos Humanos antes de permitir que os administradores atribuam o cargo de Gerente a um prestador de serviço.

Para automatizar o processo de aprovação nessas situações, a Forward, Inc. cria uma política de identidade preventiva, chamada Cargos de gerente para prestadores de serviço, que detecta quando um cargo do usuário é Gerente e a organização do usuário é Prestador de serviço. A Forward, Inc. também configura um processo de aprovação com base em políticas na tarefa Modificar usuário. Esse processo de aprovação é acionado quando a política Cargos de gerente para prestadores de serviço é violada.

Quando um administrador altera o cargo de um prestador de serviço para Gerente, o CA Identity Manager exibe uma mensagem de aviso e envia um item de trabalho ao diretor de Recursos Humanos para aprovação. O CA Identity Manager não altera o cargo do prestador de serviço até que o item de trabalho seja aprovado.

Para configurar o suporte para esse caso de uso, execute as seguintes etapas no CA Identity Manager:

- Criar uma política de identidade preventiva chamada Cargos de gerente para prestadores de serviço com as seguintes configurações:
  - Condição da política: usuários com (Cargo = Gerente e Organização = Prestador de serviço)
  - Ação ao aplicar a política: aviso com a mensagem Os gerentes devem ser funcionários de tempo integral.
- Modificar a tarefa Modificar usuário para incluir um processo de fluxo de trabalho com as seguintes configurações:
  - Processo de fluxo de trabalho: com base em políticas
  - Objeto de regra de aprovação: violação da política de identidade
  - Política de identidade: com (Nome = Cargos de gerente para prestadores de serviço)
  - Processo de fluxo de trabalho: SingleStepApproval

Combinando políticas de identidade e políticas de identidade preventivas

É possível combinar políticas de identidade e políticas de identidade preventivas para atender aos requisitos de segregação de tarefas. Nesse caso, as políticas de identidade resolvem as violações de segregação de tarefas existentes e as políticas de identidade preventivas proíbem novas violações.

Para oferecer suporte a esse caso de uso, você pode configurar um conjunto de políticas de identidade com dois tipos de ação:

- Ações que ocorrem durante a sincronização de usuário

  Essas ações resultam em alterações nos atributos de usuário, integrantes, administradores e proprietários de grupos e funções. Por exemplo, uma ação desse tipo pode remover um usuário de uma função quando uma violação for detectada.

  Essas ações são diferentes das ações preventivas, pois não são aplicadas quando uma tarefa é enviada. São aplicadas somente durante a sincronização de usuário (na página 462).

- Ações preventivas

  Essas ações determinam o que o CA Identity Manager faz quando ocorre uma violação da política de identidade preventiva *antes* que uma tarefa seja enviada. O CA Identity Manager pode permitir o envio da tarefa, emitir um aviso e acionar um processo de fluxo de trabalho, ou impedir o envio da tarefa.

  Em cada um desses casos, a violação é registrada no banco de dados de auditoria.

Considere uma empresa que queira impedir que os usuários tenham as funções de Administrador de RH e Aprovador de salários ao mesmo tempo. Essa empresa cria uma política de identidade com duas ações Ação ao aplicar a política:

- Remover o usuário da função de Aprovador de salários

  Essa ação ocorre quando o CA Identity Manager sincroniza os usuários com as políticas de identidade.

  Nesse caso, essa empresa configurou a sincronização de usuário para a tarefa Modificar usuário. Quando um administrador modifica um usuário, o CA Identity Manager avalia todas as políticas de identidade aplicáveis e aplica as ações. Nesse exemplo, o CA Identity Manager remove os usuários com as funções de Administrador de RH e Aprovador de salários da função de Aprovador de salários.

- Recusar a tarefa

  Essa ação preventiva proíbe os administradores de atribuir essas duas funções a uma pessoa, não permitindo que o administrador envie a tarefa.

Observação: ao configurar uma política de identidade com esses dois tipos de ação, verifique se as ações não entram em conflito. Por exemplo, você pode configurar uma política de identidade que impede que os usuários tenham as funções de gerente e prestador de serviço. Na política, você especifica duas ações:

- Um aviso que aciona um processo de fluxo de trabalho, que exige uma aprovação antes de atribuir as funções.
- Uma ação que remove um usuário da função de gerente.

Um aprovador aprova a atribuição de função para as funções de gerente e prestador de serviço, mas a segunda ação remove o usuário da função de gerente quando a sincronização de usuário ocorre.

Capítulo 15: Policy Xpress

Esta seção contém os seguintes tópicos:

Visão geral do Policy Xpress

O Policy Xpress permite criar lógicas de negócios complexas (políticas) no CA Identity Manager sem a necessidade de desenvolvimento de código personalizado. No entanto, os conceitos envolvidos na criação de políticas do Policy Xpress são complexos e exigem atenção e planejamento cuidadoso. Um administrador que usa as telas do portal do CA Identity Manager pode configurar uma política no Policy Xpress para implementar até mesmo as mais sofisticadas lógicas de negócios necessárias. À medida que as políticas de negócios mudam, um administrador pode modificá-las usando as telas de configuração dentro do CA Identity Manager sem precisar que um programador faça alterações de código subjacente ou, mais importante — com os procedimentos adequados de gerenciamento de mudanças —, sem reiniciar os serviços do CA Identity Manager.

Observação: para obter informações mais detalhadas sobre o Policy Xpress, consulte o Policy Xpress Wiki.

Como criar uma política

Para criar uma política com o Policy Xpress, defina os seguintes elementos básicos de uma política.

Perfil

Define o tipo de política e a prioridade, e permite o agrupamento de políticas semelhantes, para facilitar o gerenciamento.

Eventos

Define quando uma política é executada.

Observação: certifique-se de definir o parâmetro Eventos com cuidado. A lógica de negócios deve ser executada em horários específicos para impedir que os dados sejam corrompidos e aumentar o desempenho. Por exemplo, a definição de um usuário como ativado deve ocorrer quando ele for criado. A execução dessa lógica em todos os momentos pode fazer com que as contas de usuários que devem ficar desativadas sejam ativadas novamente. Outro exemplo é fornecer ao usuário uma função de provisionamento que concede acesso a um determinado sistema. Essa função deve ser atribuída para o usuário apenas depois que uma função diferente tiver sido atribuída e aprovada. O Policy Xpress permite a ativação da lógica de negócios durante o processamento de eventos e do manipulador de tarefas de lógica de negócios, de maneira muito parecida com adaptadores personalizados. Portanto, ao contrário das políticas de identidade, a lógica pode ser iniciada a qualquer momento, e não apenas no início de uma tarefa.

Dados (Elementos de dados)

Especifica os dados usados pela política. Todos os tipos de lógica de negócios exigem alguns dados para funcionar. Esses dados podem ser usados para tomar decisões ou para criar dados mais complexos. O Policy Xpress fornece muitos componentes individuais para coletar dados. Esses componentes são chamados de *Elementos de dados*. Um exemplo de um elemento de dados é um valor de atributo do usuário. Por exemplo, o Policy Xpress pode obter o nome do usuário e armazená-lo como um elemento de dados para uso posterior.

Regras de entrada

Define os requisitos que devem ser atendidos antes da execução. A definição das regras de entrada permite especificar quando o Policy Xpress avalia políticas, o que pode simplificar as políticas e melhorar o desempenho. Um exemplo de regra de entrada é executar uma política Set Full Name *apenas* se o nome ou o sobrenome tiver sido alterado.

Regras de ação

Define a ação executada com base nas informações coletadas. Por exemplo, com base no nome do departamento de um usuário, o Policy Xpress pode atribuir um usuário a diferentes funções ou especificar outros valores de conta.

Ações

Especifica a ação a ser executada. No final do processo, o Policy Xpress executa as ações necessárias para a lógica de negócios. O Policy Xpress funciona por meio de uma regra de ação vinculada a várias ações. Desse modo, quando a regra é atingida, as ações são realizadas. As ações podem incluir atribuir valores de atributo a um usuário ou a uma conta, executar uma linha de comando, executar um comando SQL ou gerar um novo evento.

Perfil

A guia do perfil para uma política do Policy Xpress contém campos que gerenciam políticas e refinam recursos de políticas.

Observação: uma política se aplica somente ao ambiente na qual foi criada. Por exemplo, se você criar uma política enquanto estiver conectado ao ambiente neteauto, a política será executada apenas para o ambiente neteauto.

Forneça as seguintes informações do perfil ao criar uma política:

Nome da diretiva

Fornece um nome exclusivo e amigável para a política.

Tipo de diretiva

Define os ouvintes (na página 489) que acionam a política. Cada tipo de política tem uma configuração diferente.

Observação: não é possível alterar esse campo depois que a política for salva.

Categoria

Define um grupo de políticas relacionadas. Esse campo permite agrupar políticas para facilitar o gerenciamento.

Descrição

Especifica uma descrição da política.

Prioridade

Se houver várias políticas que são executadas em um único evento, esse campo especifica quando a política é executada. As políticas são executadas com base nas respectivas prioridades. Quanto menor o número, maior a prioridade (a prioridade 1 é executada em primeiro lugar, 10 é executada em segundo lugar, 50 é executada em terceiro lugar e assim por diante).
Definir a prioridade é útil para políticas que dependem umas das outras, ou dividir uma política complexa em duas simples, que são executadas uma após a outra. Por exemplo, existem três políticas que são executadas se houver um valor específico no banco de dados. Em vez de solicitar que cada uma das políticas verifique o valor no banco de dados, você pode criar uma política que é executada antes das outras três políticas e verifica o valor. Se a nova política corresponder ao valor obrigatório, o Policy Xpress pode definir uma variável. As outras três políticas são executadas apenas se essa variável estiver definida, o que impede o acesso redundante ao banco de dados.

Ativado

Especifica se a política está ativa no CA Identity Manager. É possível desmarcar esta caixa de seleção se desejar desativar uma política sem excluí-la.

Executar uma vez

Especifica se a política é executada apenas uma vez. Algumas políticas podem precisar ser executadas sempre que atenderem aos critérios, e outras podem precisar ser executadas apenas uma vez. Este valor determina se as regras de ação que já foram executadas no passado devem ser executadas novamente.

Por exemplo, a adição de uma função SAP a um usuário com base no departamento é uma ação que só deve ocorrer na primeira vez em que o usuário corresponder a esse departamento. Como alternativa, uma política que define o nível salarial do usuário com base no cargo *não* será definida para ser executada uma vez, para garantir que não ocorram alterações não autorizadas.

Observação: a opção Executar uma vez se aplica a um objeto; não se aplica globalmente.

Ouvintes

As políticas do Policy Xpress são acionadas por algo que acontece no sistema. Para implementar essa funcionalidade, os ouvintes que se integram ao sistema notificam o Policy Xpress quando um evento ocorre e fornecem detalhes sobre o evento que ocorreu.

Os ouvintes a seguir estão disponíveis:

Evento

Verifica todos os eventos do sistema e todos os estados associados ao evento (antes, aprovado, recusado e assim por diante). Esse ouvinte também relata o nome do evento para o Policy Xpress. Estes estados estão disponíveis para o ouvinte de eventos:

- Antes
- Recusado
- Aprovado
- Depois
- Com falha

UI

Verifica diferentes tarefas em execução no sistema durante o estado sincronizado, ou seja, enquanto um usuário ainda tiver a interface de usuário para a tarefa aberta. Estes estados estão disponíveis para o ouvinte UI:

- Iniciar — quando a tarefa é iniciada
- Definir a entidade — quando o objeto principal é encontrado
- Validar mediante alteração (na página 490) — quando um atributo definido com o sinalizador Validar mediante alteração é alterado
- Validar mediante envio — quando clicar no botão de envio
- Envio — quando a tarefa é enviada

Fluxo de trabalho

Verifica os processos de fluxo de trabalho que encontraram aprovadores. Esse ouvinte é útil para execução com base na lógica em aprovadores, como enviar um email ao aprovador.

Tarefa enviada

Verifica se há tarefas enviadas que não estão sendo executadas em segundo plano. Esse ouvinte é semelhante ao ouvinte de eventos, no entanto, considera a tarefa como um todo, em vez dos eventos da tarefa. Estes estados estão disponíveis para o ouvinte de tarefas enviadas:

- Tarefa iniciada
- Tarefa concluída
- Tarefa com falha

Sincronização reversa

Verifica se há notificações no sistema que estão relacionadas à funcionalidade Explorar do CA Identity Manager.

Validação de atributo na tela

Além dos disparadores definidos (tipos de política), o Policy Xpress também pode verificar a validação em atributos. Isso permite a criação de políticas que podem ser executadas quando um atributo na tela que foi sinalizado como Validar mediante alteração for atualizado.

Essa funcionalidade pode ser usada para a criação de listas suspensas dependentes. Por exemplo, se houver duas listas suspensas na tela, o Policy Xpress será executado quando a primeira opção da lista suspensa for selecionada e, em seguida, determinará os valores para a segunda lista suspensa com base na opção selecionada na primeira. Um número ilimitado de atualizações de listas suspensas e de outras telas podem ser realizadas. É diferente de Dados da caixa de seleção, permitindo que as opções da lista suspensa sejam preenchidas com qualquer lógica, em vez de importar um arquivo XML de opções estáticas.

Outra utilidade é preencher outros atributos com base no valor de um atributo. Por exemplo, quando um administrador tiver selecionado um departamento, o Policy Xpress pode preencher automaticamente outros atributos, tais como um gerente de departamento, um número de departamento e um código de RH do departamento. Isso evita que seja necessário escrever um código personalizado para o manipulador de atributos lógicos.

Para configurar a validação com uma política do Policy Xpress:

1. No console de usuário, modifique uma tela de perfil da tarefa e selecione o campo que deseja monitorar.
2. Acesse as propriedades do campo e selecione Sim na lista suspensa para Validar mediante alteração.
3. No Policy Xpress, crie uma política do tipo UI (na página 489).
4. Na guia Executar mediante eventos, selecione o estado Validar mediante alteração e a tarefa que você modificou na etapa 1.

Caso de uso: verificando nomes ofensivos

Quando um usuário for criado, você pode verificar se o nome de usuário é ofensivo. O processo a seguir descreve como procurar nomes ofensivos usando uma política do Policy Xpress.

1. Certifique-se de que os campos apropriados na tela de perfil Criar usuário da tarefa estão definidos como Validar mediante alteração = Sim.
2. No Policy Xpress, crie uma política do tipo UI.
3. Na guia Executar mediante eventos, selecione o estado Validar mediante alteração e a tarefa Criar usuário.
4. Crie os seguintes elementos de dados para verificar o nome:
   - Obtenha o atributo de nome (Atributos, Atributo de usuário, Obter).
   - Analise todas as letras minúsculas do nome (Geral, Analisador de sequência de caracteres, Para baixo).
   - Verifique o nome em relação a palavras ofensivas em uma tabela de banco de dados (Origens de dados, Dados de consulta SQL).
5. Crie elementos de dados semelhantes, como na etapa 4, para verificar o sobrenome.
6. Crie uma regra de ação, da seguinte maneira:
   - Condição — nome não é igual a "" (isso ocorre se a consulta retorna uma mensagem de que o nome é ofensivo).
   - Ação — mensagem que é exibida (Mensagens, Mensagem na tela), indicando o nome ofensivo.

   Essa regra forçará o usuário a alterar o nome antes do envio da tarefa Criar usuário novamente.
7. Crie uma regra de ação semelhante, como na etapa 6, para o sobrenome.

Eventos

Dependendo do tipo de política selecionada na guia do perfil, você pode definir horários de ativação para estabelecer quando a política será avaliada. Por exemplo, uma política do tipo Evento pode ser definida para avaliação Antes de um evento CreateUserEvent. Uma política do tipo Tarefa pode ser definida para avaliação em Definir a entidade para DisableUserEvent.

Para configurar a hora de ativação, selecione os seguintes campos:

Estado

Especifica o período de tempo ou ação relacionada ao evento que ativa a política. Por exemplo, uma política pode ser definida para ser executada Antes que um evento ocorra.

Nome do evento

Especifica o evento que ativará a política, como um CreateUserEvent.

Uma política pode ter mais de uma hora de ativação. Toda vez que uma determinada hora de ativação (um estado e um evento) ocorre no sistema, o Policy Xpress pesquisa todas as políticas com essa hora de ativação e avalia cada política com base na ordem.

Observação: se uma política corresponder a uma hora de ativação que ocorre no sistema, não significa que a política será executada automaticamente. Os critérios de regras avaliados mais tarde durante o processo determinam se a política foi concluída.

Elementos de dados

Elementos de dados são usados para a criação de dados da política. Uma regra pode conter vários elementos de dados que representam as informações usadas pela política.

O Policy Xpress usa plugins flexíveis para coletar as informações de elementos de dados. Cada plugin pode executar uma tarefa pequena e dedicada. Entretanto, vários plugins podem ser usados em conjunto para criar políticas mais complexas. Um exemplo de um plugin de elemento de dados é um elemento de atributo de usuário. O objetivo do elemento é reunir informações sobre um determinado atributo que faz parte do perfil do usuário.

Elementos de dados são calculados quando são chamados, o que significa que uma regra está usando o elemento de dados, ou outro elemento que precisa de cálculo está usando o elemento de dados como um parâmetro.
Por exemplo, um elemento de dados de consulta SQL pode recuperar um valor de uma tabela, mas precisa do departamento do usuário para criar a consulta. Nesse caso, o elemento de dados de departamento deve ser executado antes do elemento de dados de consulta SQL e, em seguida, o valor pode ser usado como parâmetro (na página 495).

Os campos a seguir definem um elemento de dados:

Nome

Define um nome amigável que descreve o elemento de dados. Alguns elementos de dados são complexos (como aqueles para obter variáveis ou recuperar informações do banco de dados). Certifique-se de selecionar um nome significativo para simplificar o gerenciamento de elemento de dados.

Categoria

Fornece um agrupamento de elementos de dados. Esse campo classifica os elementos de dados e facilita a seleção.

Tipo

Especifica o tipo de elemento de dados, cada um com seu próprio uso dedicado. Esse campo se baseia na categoria selecionada.

Função

Define variações possíveis dos mesmos dados. A maioria dos elementos de dados só oferece suporte à função Obter.

Por exemplo, o elemento de dados de atributo de usuário tem as seguintes funções:

- Obter — retornará os valores do atributo.
- Com vários valores — retornará verdadeiro se o valor tiver vários valores.
- Lógico — retornará verdadeiro se o valor for lógico.

Descrição da função

Fornece uma descrição pré-preenchida da função. Cada função selecionada fornece uma descrição diferente para ajudar a compreender melhor o seu uso e quais são os valores esperados.

Parâmetros

Define os parâmetros passados para o elemento de dados. Elementos de dados são dinâmicos e podem fazer coisas diferentes com base nos parâmetros. Um elemento de dados de atributo de usuário retorna resultados diferentes de acordo com o atributo selecionado. A opção de subtipo também define o número de parâmetros, seus nomes e os valores opcionais, quando disponível.

É possível adicionar outros parâmetros, se necessário. O exemplo de consulta SQL aceita dois parâmetros necessários: a origem de dados e a própria consulta. A consulta pode usar o "?", que será substituído por valores (como uma instrução preparada). A adição de parâmetros permite que você defina esses valores.

Observação: ao visualizar elementos de dados no Policy Xpress, há uma coluna chamada Em uso. Uma marca de seleção nessa coluna indica que o elemento de dados é usado por uma regra, um parâmetro de ação ou como um parâmetro para outros elementos de dados.

Usar valores dinâmicos em elementos de dados ou de ações

Valores dinâmicos são o resultado de elementos de dados calculados, e seus valores são decididos apenas em tempo de execução. Em seguida, esses valores podem ser usados como parâmetros de outros elementos de dados (que são calculados subsequentemente, com base na prioridade).

Para usar um valor dinâmico como um parâmetro para um elemento de dados:

1. Na guia Dados da política, localize o parâmetro para definir um valor dinâmico.
2. No campo de texto vazio, digite qualquer texto normal ou selecione o valor dinâmico na lista suspensa.
3. Clique em OK.

Variáveis

O Policy Xpress tem variáveis que são definidas com as ações e salvas como elementos de dados (categoria Variáveis). As variáveis são compartilhadas por todas as políticas que são executadas ao mesmo tempo, portanto, uma variável que já foi definida pode ser usada por outras políticas de prioridade mais baixa.

Por exemplo, uma variável pode conter um valor calculado uma vez por uma política e, em seguida, compartilhado com outras políticas que não precisam recalcular o valor. A política inicial define um valor para a variável, e as políticas executadas mais tarde leem esse valor usando um elemento de dados que tenha o nome da variável como um parâmetro.

Uma variável também pode ser um gatilho para outras políticas. Nesse caso, as políticas são executadas apenas se a política antes delas tiver sido executada.

Regras de entrada

As regras de entrada definem as condições em que uma política deve ser executada. Essas condições usam os valores coletados pelos elementos de dados da política.

Pode haver várias regras de entrada em uma política, e uma regra de entrada pode ter várias condições. Pelo menos uma regra de entrada deve ser correspondente, o que significa que *todas* as condições dessa regra de entrada devem ser atendidas para que uma política prossiga para as regras de ação.

Os campos a seguir definem uma regra de entrada:

Nome

Fornece um nome amigável para a regra de entrada.

Descrição

Define o significado da regra de entrada.

Condições

Especifica os critérios de correspondência.

Observação: as condições em uma regra de entrada sempre possuem um operador AND entre elas.

Mais informações:

Condições (na página 496)

Condições

Uma condição é usada em regras de entrada e de ação, e consiste nos seguintes componentes:

- Dados da política
- Operador
- Valor

Por exemplo, você deseja criar uma condição que verifica se um departamento do usuário foi alterado. Primeiro, defina um elemento de dados de departamento alterado, em seguida, na condição, selecione o elemento de dados de departamento alterado, defina o operador como Igual a e defina o valor como Verdadeiro.

Mais informações:

Regras de entrada (na página 495)
Regras de ação (na página 496)

Regras de ação

As regras de ação são semelhantes às regras de entrada quanto à estrutura, mas são diferentes em termos de funcionalidade. As regras de ação definem quando a ação deve ser executada. Por exemplo, se desejar que uma política execute uma ação quando o departamento de um usuário for alterado para Vendas, crie uma regra de ação que define quando Departamento = Vendas.

Além disso, em vez de precisar haver correspondência a uma regra de entrada, é possível haver correspondência a várias regras de ação. A regra de ação com a prioridade mais alta (sendo 0 a mais alta) é a *única* usada.

As regras de ação também contêm uma ou mais ações, e as ações são divididas em Ações de adição e Ações de remoção.

Os campos a seguir definem uma regra de ação:

Nome

Fornece um nome amigável para a regra de ação. Esse nome deve ser exclusivo.

Descrição

Define o significado da regra de ação.

Condições

Especifica os critérios de correspondência.

Prioridade

Define qual regra de ação é executada, caso existam várias regras de ação correspondentes. Esse campo é útil para definir ações padrão. Por exemplo, se você possui várias regras, cada uma delas para um nome de departamento, é possível definir uma padrão adicionando uma regra sem condições, mas com uma prioridade mais baixa (como 10, se de todas as outras for 5). Se nenhuma das regras de departamento for correspondente, a padrão será usada.

Ações de adição

Define uma lista de ações executadas quando a regra for correspondente. Por exemplo, você pode definir uma regra que informa se o departamento do usuário corresponde àquele configurado na condição e adiciona um determinado grupo do Active Directory. As regras de ação se comportam de um modo diferente, com base na configuração Executar uma vez. Se a política estiver definida para ser executada uma vez, as ações associadas são executadas na primeira vez em que a regra for correspondente. As ações não são executadas novamente para cada correspondência de regra. No exemplo acima, o grupo do Active Directory é adicionado ao usuário apenas uma vez. Se Executar uma vez não estiver definido, as ações são executadas novamente, contanto que a regra seja correspondente. Esse campo é importante para a aplicação de valores.

Ações de remoção

Define uma lista de ações a serem executadas quando a regra não for mais correspondente. Por exemplo, o exemplo anterior adicionou um grupo do Active Directory ao usuário, com base no departamento. Se o departamento for alterado, a ação de remoção remove o grupo do Active Directory.

Mais informações:

Condições (na página 496)

Ações

Ações executam a lógica de negócios após a tomada de decisões. Uma ação funciona de forma semelhante aos elementos de dados, exceto no final. Quando é executada, executa uma tarefa, em vez de retornar um valor.

Observação: as ações são executadas na ordem em que são exibidas no console de usuário.

Os campos a seguir definem uma ação:

Nome da ação

Define a finalidade da ação.

Categoria

Fornece um agrupamento de ações. Esse campo classifica as ações e facilita a seleção.

Tipo e Função

Define o tipo e a função da ação executada.

Observação: para obter mais informações sobre Tipo e Função, consulte Dados.

Descrição da função

Fornece uma descrição pré-preenchida da função. Cada função selecionada fornece uma descrição diferente para ajudar a compreender melhor o seu uso e quais são os valores esperados.

Parâmetros

Define os parâmetros passados para a ação.

Controle de fluxo

Por padrão, as políticas são classificadas por prioridade e, em seguida, avaliadas uma por uma. Embora esse fluxo quase sempre se aplique, você pode alterá-lo, se necessário.

Essa funcionalidade de alteração de fluxo é representada por uma ação que pode ser anexada a qualquer regra de ação. As funções de alteração de fluxo estão localizadas na categoria Sistema da ação.

Importante: tenha cuidado ao alterar os fluxos de processo. O uso dessas ações pode resultar em um loop infinito. Por exemplo, se você definir Refazer a política atual em uma regra de ação sem condições, a regra sempre será verdadeira, e a política será sempre reiniciada e nunca acabará.

As quatro funções de alteração de fluxo a seguir podem ser usadas:

Interromper o processamento

Faz com que todas as políticas depois da política atual sejam ignoradas, e faz com que o Policy Xpress seja encerrado.
Observação: apenas o Policy Xpress é encerrado. Para forçar também a interrupção do CA Identity Manager, é possível usar o plugin de ação do tipo Exceção.

Reiniciar todas as políticas

Interrompe o processamento do restante das políticas e retorna ao início da lista. Essa opção é útil nos casos em que a ação de uma política faz com que outra política anterior que não foi executada atenda aos critérios de entrada. Desse modo, essa política é reavaliada.

Refazer a política atual

Faz com que uma política seja executada novamente. Essa opção é útil para iteração. Por exemplo, para criar um nome de usuário exclusivo, uma política deve ser executada repetidamente até encontrar um nome exclusivo.

Ir para uma política específica

Essa ação requer a seleção de uma política existente. Se essa política estiver em execução ao mesmo tempo que a política atual (pode ser antes ou depois), o Policy Xpress irá para a política selecionada. Se a nova política tiver prioridade mais baixa, todas as políticas entre a política atual e a política selecionada serão ignoradas. Se a nova política tiver prioridade mais alta, o processo retorna.

Observação: como a ação pode fazer com que o Policy Xpress ignore determinadas políticas, use esse tipo de ação com cuidado.

Definir objetos associados a contas

Ao criar uma ação de adição para definir um objeto que está associado a uma conta, como Integrante de, um formato de relacionamento específico é usado para representar o objeto. Os dois tipos de formato a seguir podem representar o objeto no CA Identity Manager:

- Para representar relacionamentos simples entre o objeto e a conta, por exemplo, grupos do Active Directory:
  `NativeGroup=Administrators,Container=Builtin,EndPoint=LocalAD,Namespace=ActiveDirectory,Domain=im,Server=Server`
- Para representar relacionamentos de ligação entre o objeto e a conta, por exemplo, funções SAP:
  `{"validFromDate":"2009\/12\/01","roleName":"SAPRole=SAP_AUDITOR_ADMIN,EndPoint=sap endpoint,Namespace=SAP R3,Domain=im,Server=Server","validToDate":"2009\/12\/31"}`

  Um relacionamento de ligação difere de um relacionamento simples porque a associação entre o objeto e a conta possui dados adicionais. No exemplo anterior, os parâmetros validFromDate e validToDate contêm apenas dados relacionados à associação entre a conta e a função SAP. Os dados validFromDate e validToDate não existem na conta ou no objeto de função.

Para entender o formato do relacionamento, crie um elemento de dados que obtém o valor do objeto. O valor retornado é o formato usado na ação de adição para definir esse objeto.

Exemplo: grupos do Active Directory

1. Crie uma política do Policy Xpress com as seguintes configurações:
   - Tipo de política: Evento
   - Eventos: Após - Modificar usuário
2. Em Regra de ação, configure a seguinte ação de adição:
   - Categoria: Atributos
   - Tipo: Definir os dados da conta
   - Função: Definir
   - Tipo de terminal: Active Directory
   - Terminal: *nome_do_terminal*
   - Nome da conta: *conta*
   - Atributo: Integrante de (groupMembership)
   - Valor:
     NativeGroup=Administrators,Container=Builtin,Endpoint=*endpoint_name*,Namespace=ActiveDirectory,Domain=im,Server=Server

Avançado

O Policy Xpress permite muitas variações de configuração e também interage com componentes externos. Devido a essa flexibilidade, podem ocorrer erros que não são necessariamente bugs, como uma origem de dados configurada incorretamente, um valor ausente retornado por um elemento de dados dinâmico, ou um terminal que não está respondendo.

Normalmente, quando ocorrer um erro, o sistema interromperá o cálculo de políticas para a etapa atual. No entanto, você pode alterar a resposta de erro padrão, com base na categoria do erro. Por exemplo, se tiver uma política que não é crítica, você pode definir que o processamento continue no caso de um erro.

A guia Avançado permite que as respostas de erro padrão sejam alteradas, se necessário.

Observação: recomendamos que essas respostas de erro fiquem em seus padrões, mas para casos de uso avançado, essas configurações podem ser alteradas por política. Por exemplo, se tiver uma política que não é crítica, você pode definir que o processamento continue mesmo que a política falhe.

As seguintes categorias de erro podem ser configuradas na guia:

- Validação — causado ao fornecer informações incorretas para um plugin. Esse tipo de erro é informado antes da tentativa de execução da ação.
- Ambiente — causado por problemas no ambiente, como um servidor de banco de dados com falha para o plugin do SQL.
- Permitido — um erro não crítico. O comportamento padrão para esse tipo de erro é continuar o processamento da solicitação, como no caso de falha ao enviar um email.

Para cada um dos erros anteriores, as seguintes opções podem ser definidas:

- Evento com falha — interrompe a ação atual. Esse é o padrão para a maioria dos tipos de erro.
- Política com falha — interrompe a política atual e todas as ações associadas a ela. O restante das políticas continuam.
- Ignorar — registra qualquer falha, mas não interrompe as ações ou políticas.

Capítulo 16: Aplicativo móvel do CA Identity Manager

O aplicativo móvel do CA Identity Manager permite que você aproveite a infraestrutura do CA Identity Manager existente para que os usuários possam concluir as tarefas a seguir em um dispositivo móvel, como um smartphone ou um tablet:

- Redefinir uma senha esquecida
- Alterar uma senha
- Responder às solicitações de aprovação aceitando ou rejeitando-as. Use o Console do usuário para reservar ou liberar uma solicitação.
- Exibir informações de usuários

  Este recurso permite que os usuários visualizem informações sobre outros usuários na organização. Por exemplo, os aprovadores de itens de trabalho podem exibir informações básicas sobre um gerenciador de usuários, como o nome e endereço, antes de tomar uma decisão de aprovação. Caso sejam necessárias mais informações, o aprovador pode clicar em um link para exibir todo o perfil.

Esta seção contém os seguintes tópicos:

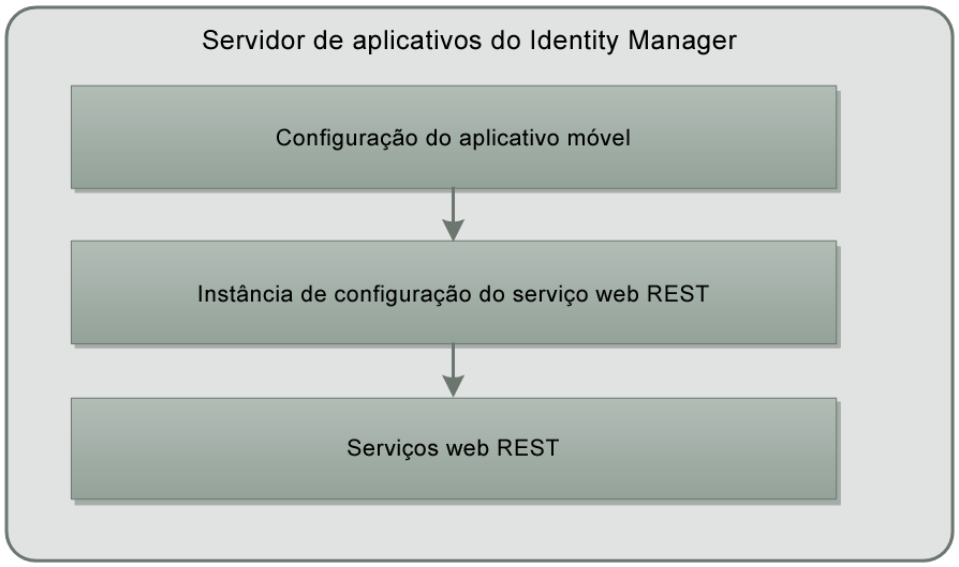
A arquitetura do aplicativo móvel do CA Identity Manager

A arquitetura do aplicativo móvel do CA Identity Manager foi projetada para fornecer um conjunto de recursos do CA Identity Manager para vários dispositivos móveis, como smartphones e Tablets. Os recursos selecionados para o aplicativo móvel baseiam-se nas necessidades essenciais de negócios e naquelas cuja interação com o usuário é adequada para dispositivos menores.

A arquitetura está centralizada no uso de um componente de configuração específico para o aplicativo e em serviços web RESTful que revelam os recursos do servidor do CA Identity Manager. O servidor do CA Identity Manager oferece suporte à capacidade de gerenciar a configuração do aplicativo móvel de um determinado ambiente e à configuração dos serviços web do REST usados pelo aplicativo.

Observação: os serviços web do REST são específicos do aplicativo móvel do CA Identity Manager e não se destinam a ser API públicas, ao contrário do TEWS (Task Execution Web Services - Serviços Web de Execução de Tarefas) com base em SOAP.

Os serviços web do REST podem oferecer suporte a várias configurações por ambiente do CA Identity Manager (IME), onde cada configuração normalmente é associada a um determinado cliente REST, como o aplicativo móvel. A arquitetura de alto nível e o relacionamento entre a configuração do aplicativo móvel e a configuração do serviço web são mostrados abaixo.



A configuração dos serviços web REST requer um conjunto específico de opções selecionadas para que o aplicativo móvel funcione. Uma configuração do serviço web deve ser definida por meio da tarefa de configuração do serviço web antes de criar a configuração do aplicativo móvel, também disponível por meio de uma tarefa administrativa.

Detalhes da configuração do serviço web do aplicativo móvel

Uma configuração do serviço web REST consiste nos seguintes elementos:

- Um perfil que define um nome de configuração exclusivo, um identificador e um sinalizador ativado
- Uma configuração de segurança que define o uso de SSL, de criptografia de carga e de uma chave de criptografia.
- O conjunto de tipos de objeto gerenciado e as operações e os atributos suportados para cada tipo por meio do REST.
- Operações de autoatendimento suportadas, como redefinir senha, e o conjunto de atributos de autoatendimento de usuários permitidos.
- A política de integrantes para a qual os usuários estão autorizados a chamar as operações REST configuradas.

A tabela abaixo mostra os detalhes da configuração do serviço web e a configuração necessária para o aplicativo móvel.

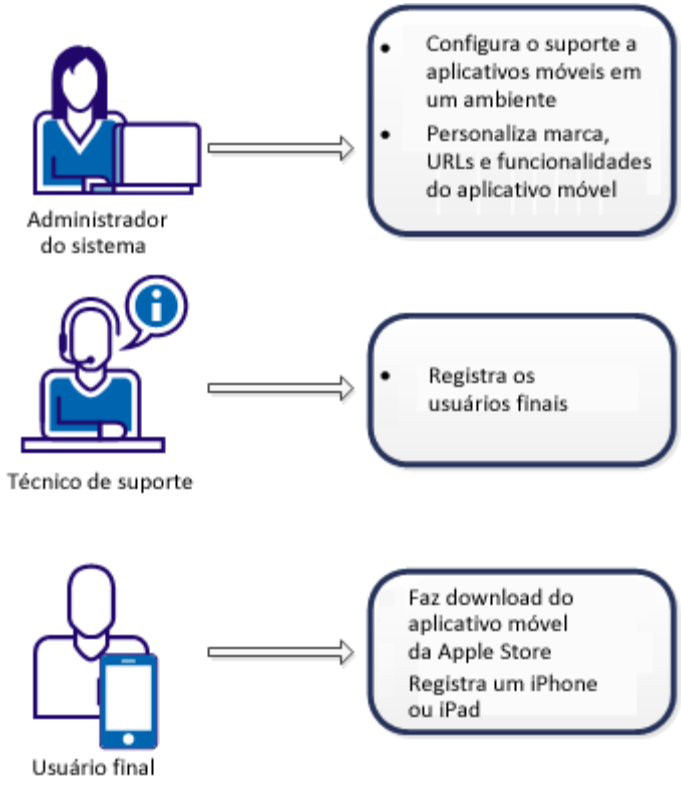
Seção de configuração	Item	Descrição	Configuração do aplicativo móvel
Perfil	nome	O nome da configuração.	Opção de implantação
	identificador	O identificador exclusivo que um determinado cliente deve definir no cabeçalho http "Configuration-Id" em cada solicitação do servidor do CA Identity Manager.	Opção de implantação. O serviço de configuração do aplicativo móvel retorna o identificador que deve ser usado em todas as solicitações REST subsequentes.
	Ativado	Ativa/desativa a configuração	Verdadeiro
Segurança	Requer comunicação segura	https obrigatório ou não	Opção de implantação. Valor baixado pelo serviço de configuração do aplicativo móvel.

	Ativar criptografia	Usado para criptografar a carga para não SSL. Requer biblioteca de criptografia do lado do cliente, conhecimento da chave de criptografia e suporte explícito à criptografia/descriptografia do lado do cliente	Não usado. Deixar desmarcado.
	Segredo de configuração	O segredo compartilhado necessário como parte do cliente REST para o modelo de confiança do servidor.	Deve ser especificado. As implantações devem gerar o segredo ao definir a instância de configuração.
Tipos de objeto	Tipo de objeto	Os tipos de objetos que são expostos como recursos REST.	O tipo de objeto de usuário
	Métodos e atributos	Os métodos de recurso (CRUD) suportados para um tipo de objeto selecionado e o conjunto de atributos permitidos para esses métodos.	O tipo de objeto de usuário com acesso de exibição para os seguintes atributos, conforme representado no esquema de usuário específico da implantação: ■ Telefone comercial ■ Departamento ■ Email ■ Nome ■ Sobrenome ■ Gerente ■ Escritório ■ Cargo
Autoadministração	Regra de integrante	Uma regra que indica quais usuários podem executar a autoadministração.	Deve corresponder à regra de integrante na configuração do aplicativo móvel. O conjunto de atributos para modificação deve estar em branco.

	Ativar redefinição de senha	Permite que os usuários redefinam as próprias senhas	Ativar
	Atributos	O conjunto de atributos que o usuário pode gerenciar por si só	Esvaziar lista
Integrantes	Integrantes	Define regras para as quais os usuários estão autorizados a chamar as operações REST definidas para esta configuração	Uma regra de integrante que corresponde ao conjunto de usuários do aplicativo móvel

Como o processo de implementação funciona

Há três tipos de usuário envolvidos na configuração de aplicativos móveis. O gráfico a seguir ilustra esses tipos de usuário e as tarefas que executam.



Para permitir que um usuário final use o aplicativo móvel com o CA Identity Manager, ocorrem as seguintes atividades:

1. Um administrador de sistema configura o suporte para o aplicativo móvel em um ambiente.

   A configuração envolve as seguintes atividades:

   - Configura a ativação e redefinição dos atributos de código
   - Adição de tarefas, políticas Policy Xpress e um modelo de email para registro de usuários móveis
   - Criação de uma definição dos serviços web
   - Modificação do email de registro.

   O administrador de sistema também configura as identificações visuais, os URLs e as funcionalidades que os usuários móveis podem acessar.

2. Um administrador, como um técnico do Suporte técnico, registra os usuários finais aplicáveis no Console de usuário.

   O processo de registro aciona um código de ativação para cada usuário final e envia automaticamente um email com o código e as instruções de registro ao usuário final.

3. O usuário final faz download do aplicativo móvel na Apple Store e registra um dispositivo, como um smartphone ou um tablet, usando as instruções e o código que recebeu no email.

   O usuário final pode então usar o aplicativo móvel para acessar as funcionalidades do CA Identity Manager.

   Observação: se a opção A senha precisa ser alterada for selecionada durante a criação do usuário, os usuários do aplicativo móvel não poderão concluir a ativação.

Como funciona a configuração do aplicativo

O aplicativo móvel recupera a sua configuração das API de configuração do servidor do CA Identity Manager. Quando o aplicativo móvel é instalado pela primeira vez e não tem nenhuma configuração baixada, ele solicita ao usuário o nome de usuário e a senha, e usa essas credenciais para fazer download da configuração definida usando o link fornecido no email de registro do usuário.

Após o download da configuração inicial, cada vez que o aplicativo é iniciado ele compara a sua versão de configuração com a versão mais recente disponível no servidor do CA Identity Manager. A API de verificação da versão de configuração é usada para detectar se uma versão mais recente está disponível.

Como funciona o registro do usuário

Cada usuário que deseje acesso ao aplicativo móvel deve solicitar o acesso dentro do CA Identity Manager. Se o acesso for aprovado, o usuário é atualizado com um código de ativação que indica que o acesso foi concedido. A política de integrante de configuração do aplicativo móvel e a política subjacente de integrante de serviços web devem atender a todos os critérios definidos para a solicitação de acesso dos usuários móveis. No mínimo, o valor %ACTCODE% de "Registered" ou um valor maior que "0" precisa ser definido.

Se acesso móvel de um usuário for removido, o servidor do CA Identity Manager redefinirá os atributos de ativação e impedirá o acesso do usuário ao aplicativo móvel.

Como configurar o CA Identity Manager para oferecer suporte ao aplicativo móvel

O aplicativo móvel se comunica com o CA Identity Manager (usando serviços web REST) para gerenciar as senhas e as aprovações. Para ativar essa comunicação, um administrador de sistema conclui as seguintes etapas:

1. Configurar os atributos necessários (na página 510).
2. Importar tarefas administrativas. (na página 513)
3. Criar um serviço web (na página 515).
4. Modificar o email de registro (na página 517).
5. Como opção, configure o suporte do SiteMinder para o Aplicativo móvel.

Configurar os atributos necessários

O repositório de usuários do CA Identity Manager deve incluir os seguintes atributos conhecidos para ativar o registro de usuário e o acesso por meio de aplicativos móveis:

- %ACTCODE% — Identifica o atributo que armazena um número de ativação gerado de forma aleatória. Depois que o usuário tiver sido registrado, o atributo apresentará a palavra Registrado.
- %ACTCODEVAL% — Identifica o atributo que armazena o código de ativação que o cliente define durante o registro. O CA Identity Manager compara esse valor com o valor de %ACTCODE%.
- %CURRENT_AUTH_QUESTIONS% — Identifica o atributo que armazena temporariamente os valores de pergunta de desafio. Esse valor é limpo após o usuário responder corretamente.
- %MOBILE_PIN% — Identifica o atributo que armazena o número de identificação pessoal ou o valor de sequência de caracteres, que fornece a senha alfanumérica compartilhada entre um usuário e um sistema que podem ser usados para autenticar o usuário no sistema.
- %PWRESETCODE% — Identifica o atributo que armazena um código criptografado, que fornece autenticação unilateral durante uma redefinição de senha

Mapeie esses atributos conhecidos para os atributos do repositório de usuários disponíveis no arquivo de configuração de diretório (directory.xml). Se não houver atributos disponíveis, estenda o esquema de repositório de usuários. Para obter mais informações sobre como estender o esquema, consulte a documentação do seu armazenamento de usuários.

Inclua as seguintes classificações de dados nas descrições dos atributos:

<DataClassification name="sensitive"/>

Substitui o valor do código de redefinição com caracteres curinga nas telas das tarefas, nos registros de auditoria e nos logs do sistema.

Importante: Não inclua a classificação dos dados confidenciais na definição de atributos %ACTCODE%. Se você incluir o atributo confidencial, o aplicativo móvel não funcionará corretamente.

<DataClassification name=" AttributeLevelEncrypt "/>

Criptografa e descriptografa o valor do código de redefinição que foi escrito e lido no armazenamento de usuários por meio da chave de criptografia definida.

<DataClassification name=" ignore_on_copy "/>

Faz com que o CA Identity Manager ignore um atributo quando um administrador cria uma cópia de um objeto no Console de usuário.

Observação: consulte no final deste tópico exemplos desses atributos conhecidos.

Siga estas etapas:

1. Efetue logon no Management Console.
2. Selecione Directories e clique no diretório que contém os usuários móveis.
3. Exporte o diretório.
4. Adicione ou modifique uma descrições de atributo para incluir o atributo conhecido %ACTCODE%.

   É possível mapear qualquer atributo disponível para o atributo conhecido %ACTCODE%.
5. Repita a etapa 4 para definir o atributo conhecido %ACTCODEVAL%. Inclua as seguintes classificações de dados:
   ```
   <DataClassification name="sensitive"/>
   <DataClassification name="ignore_on_copy"/>
   <DataClassification name=" AttributeLevelEncrypt"/>
   ```
6. Adicionar uma descrição do conhecido atributo %CURRENT_AUTH_QUESTIONS%. Inclua as classificações de dados a seguir:
   ```
   <DataClassification name="ignore_on_copy"/>
   ```
7. Adicione uma descrição de atributo para o conhecido atributo %MOBILE_PIN%. Inclua as seguintes classificações de dados:
   ```
   <DataClassification name="sensitive"/>
   <DataClassification name="ignore_on_copy"/>
   <DataClassification name=" AttributeLevelEncrypt"/>
   ```
8. Adicione uma descrição ao atributo conhecido %PWRESETCODE%. Inclua as seguintes classificações de dados:
   ```
   <DataClassification name="sensitive"/>
   <DataClassification name="ignore_on_copy"/>
   <DataClassification name=" AttributeLevelEncrypt"/>
   ```
9. Salve o arquivo directory.xml.
10. Carregue o arquivo directory.xml salvo clicando em Update na página Directory Properties no Management Console.

Exemplos

Observação: é possível mapear qualquer atributo disponível para esses atributos conhecidos.

%ACTCODE%

```
<ImsManagedObjectAttr
physicalname="attribute_name"
displayname="your_attribute_display_name"
description="your_attribute_description"
valuetype="String"
required="false"
multivalued="false"
```

```
    wellknown="%ACTCODE%"
    maxlength="0"
    hidden="true"
    system="true">
        <DataClassification name="ignore_on_copy"/>
        <DataClassification name=" AttributeLevelEncrypt"/>
        </ImsManagedObjectAttr>
```

%ACTCODEVAL%

```
    ImsManagedObjectAttr
    physicalname="attribute_name"
    displayname="your_attribute_display_name"
    description="your_attribute_description"
    valuetype="String"
    required="false"
    multivalued="false"
    wellknown="%ACTCODEVAL%"
    maxlength="0"
    hidden="true"
    system="true">
        <DataClassification name="ignore_on_copy"/>
        <DataClassification name=" AttributeLevelEncrypt"/>
        </ImsManagedObjectAttr>
```

%CURRENT_AUTH_QUESTIONS%

```
    <ImsManagedObjectAttr
    physicalname="attribute_name"
    displayname="your_attribute_display_name"
    description="your_attribute_description"
    valuetype="String"
    required="false"
    multivalued="false"
    wellknown="%CURRENT_AUTH_QUESTIONS%"
    maxlength="0"
    hidden="true"
    system="true">
        <DataClassification name="ignore_on_copy"/>
```

%MOBILE_PIN%

```
    <ImsManagedObjectAttr
    physicalname="attribute_name"
    displayname="your_attribute_display_name"
    description="your_attribute_description"
```

```
valuetype="String"
required="false"
multivalued="false"
wellknown="%MOBILE_PIN%"
maxlength="0"
hidden="true"
system="true">
   <DataClassification name="ignore_on_copy"/>
   <DataClassification name=" AttributeLevelEncrypt"/>
   </ImsManagedObjectAttr>
```

%PWRESETCODE%

```
<ImsManagedObjectAttr
physicalname="attribute_name"
displayname="your_attribute_display_name"
description="your_attribute_description"
valuetype="String"
required="false"
multivalued="false"
wellknown="%PWRESETCODE%"
maxlength="0"
hidden="true"
system="true">
   <DataClassification name="ignore_on_copy"/>
   <DataClassification name=" AttributeLevelEncrypt"/>
   </ImsManagedObjectAttr>
```

Importar tarefas administrativas

Para que os usuários móveis possam efetuar logon no CA Identity Manager, os administradores os registram no Console de usuário. O processo de registro gera um código de ativação e envia um email ao usuário móvel.

Para oferecer suporte a essas atividades, importe um arquivo de definição de função que adiciona as seguintes funcionalidades a um ambiente:

- Tarefas de configuração móvel
- Tarefas Registrar usuário para aplicativo móvel e Remover usuário do aplicativo móvel
- As políticas do Policy Xpress que geram códigos de ativação e cancelam o registro do cliente móvel de uma conta de usuário.
- Um modelo de email para enviar o email aos usuários móveis

Siga estas etapas:

1. Efetue logon no Management Console.
2. Selecione Environments e clique no ambiente que oferece suporte ao aplicativo móvel.
3. Selecione Role and Task Settings e clique em Import na próxima tela.
4. Selecione MobileApp-RoleDefinitions e clique em Finish.
5. Reinicie o ambiente.
6. Adicione as seguintes tarefas à função Gerente do sistema:
   - Criar configuração móvel
   - Modificar configuração móvel
   - Exibir configuração móvel
   - Excluir configuração móvel
   - Registrar usuário para aplicativo móvel
   - Remover usuário do aplicativo móvel

   As novas tarefas estão nas categorias Usuário e Sistema.

Criar uma configuração dos serviços web

O aplicativo móvel usa serviços web REST para se comunicar com o CA Identity Manager. Para oferecer suporte a aplicativos móveis, um administrador de sistema cria uma definição de serviço web no Console de usuário.

Observação: as chamadas REST não funcionam se a criptografia da configuração de serviço web estiver ativada.

Siga estas etapas:

1. Efetue logon no Console de usuário como um usuário com privilégios de administrador de sistema.
2. Crie uma definição de serviço web da seguinte forma:
   a. Vá para Sistema, Serviços web, Criar configuração dos serviços web.
   b. Na guia Perfil, preencha os seguintes campos:
      - Nome: *qualquer nome.* Por exemplo: RestMobile
      - Identificador: *identificador exclusivo.* O valor padrão é RestMobile.

        O valor do campo Identificador deve corresponder ao valor de **restid** na configuração do aplicativo móvel.

        Considere alterar o valor do Identificador e o restid para aumentar a segurança.
      - Ativar atributo: marque essa caixa de seleção.

c. Na guia Segurança, execute estas etapas:

- Determine se precisa selecionar a opção "Requer comunicação segura":

Observação: considere criptografar todo o tráfego http do aplicativo móvel. Em geral, há duas maneiras de configurar esse tráfego:

- Usando um servidor proxy: nesse caso de uso, o servidor CA Identity Manager será protegido por um firewall. É possível decidir não proteger a comunicação do servidor proxy para o servidor do CA Identity Manager. No entanto, você deve garantir que a comunicação entre o aplicativo móvel e o servidor proxy seja segura. Para esse caso de uso, NÃO selecione a opção "Requer comunicação segura".

Observação: se não estiver integrando o CA Identity Manager e o SiteMinder, selecione a opção "Requer comunicação segura" para que a comunicação SSL permaneça para as chamadas de serviços web.

- Diretamente para o servidor CA Identity Manager: Nesse caso de uso, o cliente móvel se comunica diretamente para o servidor CA Identity Manager; essa comunicação HTTP deve ser criptografada. Para impor esse requisito, selecione a opção "Requer comunicação segura".
- Verifique se a opção Ativar criptografia não está selecionada.

Observação: se a criptografia estiver ativada, os detalhes do usuário não serão exibidos no aplicativo móvel.

d. Na guia Tipos de objeto, vá para USER, selecione USER e clique no botão Editar.

e. Selecione somente Permitir acesso de exibição.

Remova outras permissões de acesso desmarcando as opções Permitir acesso de modificação, Permitir acesso de criação e Permitir acesso de exclusão.

f. Na guia Autoadministração, execute as seguintes etapas:

- Selecione o botão Adicionar abaixo da Regra de integrante para criar uma função de integrante e especificar “todos”.

  Observação: é possível criar somente uma regra de integrante.

- Ative Redefinição de senha para oferecer suporte ao recurso Alterar senha no aplicativo móvel.

g. Na guia Integrante, crie uma regra de integrante com os seguintes critérios:

- Código de ativação = Registrado ou
- Código de Ativação > 0

h. Envie e salve o serviço web.

Modificar o email de registro

Edite o email de registro padrão para incluir o URL do objeto de configuração móvel.

Siga estas etapas:

1. No Console de usuário, selecione Sistema, Email, Modificar email.
2. Procure e selecione o Usuário registrado para o email do aplicativo móvel.
3. Na guia Content, clique no botão Toggle HTML Source.
4. Especifique o URL do objeto de configuração móvel na entrada href para mobileregservidm como segue:

   <a href="mobileregservidm://{'Attribute:%ACTCODE%'}&https://FQN/iam/im/ws/Alias/mobile/ConfigName">

   FQN

   Especifique o nome ou o endereço IP do servidor CA Identity Manager.

   Alias

   Especifique o nome do ambiente.

   ConfigName

   Especifique o nome do objeto de configuração.
5. Clique em Enviar.

Como configurar o suporte do SiteMinder para o aplicativo móvel

Os serviços web usados pelo aplicativo móvel oferecem suporte à autenticação nativa usando as credenciais de nome de usuário/senha passadas pelo aplicativo móvel por meio do cabeçalho de AUTORIZAÇÃO HTTP ou da autenticação do SiteMinder. A configuração dos serviços web, conforme anteriormente discutida, define a política de autorização para cada um dos recursos REST e solicitações de método.

URL de serviço web REST do IM

Os serviços REST do IM dependem do seguinte URL base:

`http[s]://[FQN]/iam/im/ws/[Alias]`

- FQN - O nome totalmente qualificado e a porta do ponto de acesso do servidor do CA Identity Manager
- Alias - O alias público do ambiente do CA Identity Manager ao qual se conectar.

URL de configuração do aplicativo móvel

A configuração do aplicativo móvel contém um URL específico que permite a recuperação de informações de configuração de inicialização necessárias para o download da configuração do aplicativo móvel. O URL de configuração é como segue:

`http[s]://[FQN]/ iam/im/ws/[Alias]/mobile/[ConfigName]`

ConfigName – O nome da configuração do aplicativo móvel para o ambiente do CA Identity Manager para um determinado conjunto de usuários do aplicativo móvel. O nome da configuração é disponibilizado para o aplicativo por meio de um link para o URL de configuração no email de registro enviado mediante aprovação da solicitação de um usuário por acesso ao aplicativo móvel.

API do REST não autenticada

API de configuração

As seguintes API de configuração não exigem autenticação.

`http[s]://[FQN]/ iam/im/ws/[Alias]/mobile/[ConfigName]/image`
`http[s]://[FQN]/iam/im/ws/[Alias]/mobile/[ConfigName]/ver`

Redefinir API da senha

`https://[FQN]/iam/im/ws/[Alias]/myself/resetpasswordWithResetCodeAndToken`

Observação: a API resetPasswordWithResetCodeAndToken contém os tokens de segurança transmitidos nos cabeçalhos http a partir do aplicativo móvel. O servidor do CA Identity Manager verifica a presença e a validade desses tokens.

Ao integrarem-se com o SiteMinder para proteger o acesso ao CA Identity Manager, esses URL podem ser definidos com um realm que não está protegido ou que está protegido com um esquema de autenticação anônima.

API do REST autenticada

Os URL a seguir são usados pelo aplicativo móvel e exigem a autenticação e o uso das políticas de configuração do serviço web para autorização.

Configuração

`http[s]://[FQN]/iam/im/ws/[Alias]/mobile/[ConfigName]/conf`

Usuário de autoatendimento

`http[s]://[FQN]/iam/im/ws/[Alias]/myself`

Lista de tarefas

`http[s]://[FQN]/iam/im/ws/[Alias]/worklist`

Usuário

`http[s]://[FQN]/iam/im/ws/[Alias]/mo/User`

Configurar um aplicativo móvel

Os administradores do sistema configuram o aplicativo móvel do CA Identity Manager no console de usuário.

Um ambiente pode incluir várias configurações de aplicativos móveis. Criar configurações diferentes permite oferecer suporte a diferentes marcas ou funcionalidades para diferentes tipos de usuários móveis. Por exemplo, é possível criar uma configuração para alterações de senhas do funcionário e outra configuração para os gerentes aprovarem os itens de trabalho.

Os administradores podem configurar as seguintes propriedades para o aplicativo móvel:

- Branding

  Especifique o logotipo da empresa no aplicativo móvel.

- Funcionalidade

  Ative as seguintes opções:

  - Suporte à senha esquecida
  - Suporte à alteração de senha
  - Fila de aprovação de fluxo de trabalho
  - Link Show manager

- Informações de suporte
- Mapeamento de atributos

  Mapeie atributos no repositório de usuários para atributos expostos no aplicativo móvel.

Siga estas etapas:

1. Efetue logon no Console de usuário como um usuário que pode usar as tarefas de configuração móvel.
2. Clique em Tarefas, Sistema, Configuração móvel, Criar configuração móvel.
3. Aceite a opção padrão, Criar um objeto do tipo Configuração móvel.
4. Na guia Geral, preencha os campos obrigatórios. É possível especificar uma imagem para os aplicativos móveis.

   URL base

   Verifique o URL base do ambiente atual. O URL base é preenchido automaticamente ao se criar uma configuração móvel.

   O CA Identity Manager usa o URL base para recuperar o nome do servidor, a porta e o protocolo que o aplicativo móvel usa para construir o URL para chamadas REST.

   Configuração

   Procure uma configuração ou digite um nome de configuração exclusivo.

   Versão

   Aumente o número da versão sempre que modificar e salvar uma configuração.

   O aplicativo móvel usa o número de versão para determinar quando fazer download de uma nova versão da configuração. Quando o aplicativo móvel é iniciado, ele compara o número da versão do servidor com a versão da configuração carregada. Se uma nova versão estiver disponível, o aplicativo móvel atualizará a configuração.

   Observação: não incremente o número de versão quando você, inicialmente, modificar o arquivo.

   Imagem da marca

   Especifique o URL completo de uma imagem PNG, com um tamanho recomendado de 222 por 222 pixels. A imagem aparece na tela inicial, na tela de gerenciamento de senhas e na parte superior da tela no aplicativo móvel.

5. Na guia Recursos, selecione os recursos para o aplicativo móvel.

   Comportamento de redefinição de senha

   Selecione o método a ser usado para o comportamento, que é determinado quando configura os atributos necessários:

   - Padrão
   - Desafio de PIN
   - Desafio de pergunta e resposta

   Observação: se selecionar a opção Desafio de pergunta e resposta, será necessário ir para Tarefas, Administrador do ambiente e selecionar "Configuração de perguntas e respostas". Lembre-se de marcar a caixa Ativar, inserir o número de perguntas de autenticação (1 a 5) e, em seguida, clicar em Enviar. Será necessário clicar no botão Enviar para que as configurações entrem em vigor, mesmo se não fizer nenhuma alteração nas configurações padrão.

6. Na guia Suporte, especifique informações de suporte para usuários móveis.

7. Na guia Mapeamento de atributo, mapeie os atributos do aplicativo móvel para atributos no armazenamento de usuários do CA Identity Manager. É possível mapear os atributos para atributos físicos ou atributos conhecidos.

8. Na guia Propriedades adicionais, especifique os pares de valores da propriedade adicional para oferecer suporte a novas funcionalidades ou campos no aplicativo móvel.

   Use o seguinte formato:

   Key1=value1

   Key2=value2

   Key3=value3

   Observação: a CA Technologies fornecerá instruções quando os administradores precisarem adicionar propriedades adicionais. Nesta release, não será necessário especificar nenhuma propriedade adicional.

9. Na guia Integrantes, especifique as regras que determinam o conjunto de usuários que veem essa configuração em seus aplicativos móveis.

10. Clique em Enviar.

Configurando propriedades adicionais

Depois de configurar o aplicativo móvel, é possível, opcionalmente, especificar pares de chave-valor de propriedades adicionais para oferecerem suporte a novas funcionalidades no aplicativo móvel. Isso é feito usando a guia Propriedades adicionais.

Use o seguinte formato:

- demoMode="Ativar/desativar"
- maxPinRetries=<qualquer valor numérico positivo>
- multiAccount="Ativar/desativar"
- managerTraversal="Ativar/desativar"
- startupWithBrandLogo="verdadeiro/falso"

Observação: a CA Technologies fornecerá instruções quando os administradores precisarem adicionar propriedades adicionais.

No entanto, esses três recursos são ativados por padrão com configurações móveis:

- DemoMode: permite exibir uma versão de demonstração do aplicativo móvel. Essa opção está disponível na seção Configurações do aplicativo móvel.
- maxPinRetries: permite que o administrador configure o número de tentativas de entrada de PIN com falha ou incorretas dos usuários móveis. O número padrão de tentativas com falha é 5.
- MultiAccount: permite adicionar várias contas, especificamente adicionando vários usuários móveis registrados com seus códigos de ativação.
- ManagerTraversal: exibe os detalhes do gerente do aprovador e do solicitante nos detalhes do item de trabalho.
- startupWithBrandLogo: permite que o usuário especifique um logotipo de conta personalizado (a imagem da marca da conta) para ser exibido em vez do logotipo padrão da CA. Se esse par de chave-valor estiver definido como verdadeiro, mas, por alguma razão, o campo do logotipo da marca tiver um URL inválido ou estiver vazio, a tela de início permanecerá em branco durante a inicialização. O logotipo da CA sempre é exibido quando o aplicativo é iniciado pela primeira vez após a instalação. Esta propriedade adicional é parte dos dados de uma conta, e nenhuma dado de conta está disponível na primeira inicialização.
  Observação: essas alterações serão refletidas em uma inicialização subsequente somente após a comunicação bem-sucedida com o servidor do CA Identity Manager.

É necessário adicionar o seguinte par de chave-valor na guia Propriedades adicionais na configuração móvel do CA Identity Manager para ativar esses recursos no cliente móvel.

- Para ativar ou desativar o recurso do modo de demonstração

Defina DemoMode como igual a Ativar ou Desativar

- demoMode="Ativar/desativar"

- Para ativar ou desativar o recurso maxPinRetries

  Defina maxPinRetries como igual a qualquer valor numérico positivo

  - maxPinRetries=<igual a qualquer valor numérico positivo> Observe que o número padrão de tentativas com falha é 5.

- Para ativar ou desativar o recurso de várias contas

  Defina MultiAccount como igual a Ativar ou Desativar

  - multiAccount="Ativar/desativar"

- Para ativar ou desativar o recurso de travessia do gerenciador

  Defina ManagerTraversal como igual a Ativar ou Desativar

  - managerTraversal="Ativar/desativar"

- Para ativar ou desativar o recurso startupWithBrandLogo

  Defina startupWithBrandLogo como verdadeiro ou falso

  - startupWithBrandLogo="verdadeiro/falso"

Siga estas etapas:

1. Efetue logon no console de usuário do CA Identity Manager como administrador (superusuário).
2. Clique em Tarefas, Sistema, Configuração móvel, Criar configuração móvel.
3. Na guia Propriedades adicionais, especifique os pares de chave-valor da propriedade adicional para oferecer suporte a novas funcionalidades no aplicativo móvel.
   - demoMode="Ativar/desativar"
   - maxPinRetries=<qualquer valor numérico positivo> O número padrão de tentativas com falha é 5.
   - multiAccount="Ativar/desativar"
   - managerTraversal="Ativar/desativar"
   - startupWithBrandLogo="verdadeiro/falso"

Fazer download do aplicativo móvel

Quando o aplicativo móvel está configurado, os usuários finais podem fazer download dele na Apple Store. Para localizar o aplicativo móvel na Apple Store, procure por CA Identity Manager.

O usuário final pode, em seguida, registrar seu dispositivo, como um smartphone ou um tablet, usando as instruções e o código recebidos por email.

Solucionando problemas de aplicativo móvel

Permitir que o Suporte solicite um arquivo de log

Se um usuário tiver um problema com o aplicativo móvel, os engenheiros do Suporte podem solicitar um arquivo de log para ajudar na solução.

O usuário móvel ativa a depuração por meio do respectivo iPhone ou iPad. Depois que a depuração estiver ativada, o usuário móvel poderá usar o aplicativo móvel para enviar o log a um endereço de email de Suporte.

Para permitir que o aplicativo móvel gere um log, o usuário móvel precisa concluir as etapas abaixo.

1. No telefone ou iPad, vá para Configurações, Identity Manager, Depurar.
2. Toque em Ativado.
3. Reinicie o aplicativo e execute as ações que deseja que apareçam no log.
4. Na guia Configurações do aplicativo móvel do CA Identity Manager, clique em Enviar logo por email.

   O aplicativo móvel cria um email com o arquivo de log anexado. O email pode ser enviado para o endereço de email configurado para o Suporte no Console de usuário.

A QnA como "Comportamento de redefinição de senha" falha ao usar a definição padrão da Configuração de perguntas e respostas no administrador do ambiente de tarefas do Identity Manager.

Sintoma

Após selecionar a QnA como "Comportamento de redefinição de senha" com as definições padrão da Configuração de perguntas e respostas, a senha de redefinição falha com a seguinte mensagem de erro:

"ERROR [im.webservices.QuestionAndAnswerResource] (http-/0.0.0.0:8443-1) Failed to process get user credential questions. Message:java.lang.NullPointerException in the server log file"

Solução:

Execute as etapas a seguir para que a redefinição de senha funcione com a QnA como Comportamento de redefinição de senha:

Siga estas etapas:

1. Efetue logon no CA Identity Manager como SuperAdmin.

2. Vá para Tarefas, Administrador do ambiente e, em seguida, selecione Configuração de perguntas e respostas.
3. Clique no botão Submit.

   Observação: mesmo os valores padrão da opção Ativar e de Número de perguntas de autenticação se aplicam somente após a execução dessa etapa.

Capítulo 17: Relatórios de atividades de usuários da CA

Esta seção contém os seguintes tópicos:

Funcionalidade do CA UAR

Quando o CA User Activity Reporting (CA UAR) é integrado ao CA Identity Manager, você recebe a seguinte funcionalidade:

- O Agente do CA UAR coleta informações de auditoria do CA Identity Manager e as converte no CA Common Event Grammar (CEG).
- O Console de usuário pode recuperar relatórios e consultas do CA UAR com as informações de contexto do CA Identity Manager usadas para filtrar as informações retornadas.
- O CA Identity Manager é fornecido com uma série de relatórios padrão e a infraestrutura para adicionar relatórios e consultas do CA UAR a uma tarefa nova ou existente.

Observação: antigamente, o CA UAR era chamado de CA Enterprise Log Manager. Em alguns casos, no Console de usuário, o nome CA Enterprise Log Manager ainda é usado.

Componentes do CA UAR

Quando o CA Identity Manager é integrado ao CA UAR, os seguintes componentes são adicionados à arquitetura do CA Identity Manager:

- A guia do Visualizador do CA Elm permite incorporar objetos do CA UAR em qualquer tarefa nova ou existente.

  Observação: é necessária uma conexão com o servidor do CA UAR.
- Definições de função que podem ser importadas.

Limitações de integração

Veja a seguir as limitações conhecidas da integração com o CA UAR:

- A recuperação de listas de consultas e relatórios no tempo de execução para configuração de tarefa pode ser lenta.
- As APIs do CA UAR reconhecem apenas fusos horários denominados pelo Java padrão.
- A operação EQUAL diferencia letras maiúsculas de minúsculas quando usada em um filtro composto.
- Somente uma conexão com um servidor do CA UAR é suportada por vez.

Como integrar o CA UAR com o CA Identity Manager

Para que seja possível exibir e gerenciar relatórios e consultas do CA UAR, um administrador deve concluir as seguintes etapas:

1. Instalar o Agente do CA UAR.
2. Criar um conector.
3. Ativar a auditoria no CA Identity Manager.
4. Configurar o Servidor do CA UAR.

Pré-requisitos de instalação do Agente do CA Enterprise Log Manager

Execute as etapas a seguir antes de instalar o Agente do CA UAR:

- Verifique se a máquina do Servidor do CA UAR pode ser acessada da máquina que está executando o CA Identity Manager ou hospedando o banco de dados de auditoria do CA Identity Manager.
- Verifique se máquina do agente pode ser acessada da máquina do servidor.
- Configure a origem de dados (na página 529) na máquina do agente.
- Verifique se a versão do Adobe Flash Player é 9.0.28 ou superior. É possível fazer download do player em:

  http://www.adobe.com/go/getflash
- Faça download de binários do agente (na página 530).
- Obtenha uma chave de autenticação de agente (na página 530).
- Torne o nome/IP do servidor facilmente acessível.
- Torne as informações da conta facilmente acessíveis, mas não coloque a segurança em risco. O agente usa essa conta quando é executado como um serviço (Windows).
- Se o conector existir, exporte as informações padrão do conector e deixe-as facilmente disponíveis.
- Verifique se a máquina possui 4 GB de RAM.

Configurar a Origem de dados na máquina do agente

Siga este procedimento para configurar a Origem de dados na máquina do agente.

Para configurar a Origem de dados

1. Navegue até Painel de controle, Ferramentas administrativas, Origens de dados (ODBC)
2. Na guia DSN do sistema, adicione o seguinte:

   imsauditevent12 data source (ODBC) pointing to the auditing database.
3. Clique em Aplicar/OK.

   A Origem de dados está configurada.

Fazer download de binários do agente

Siga este procedimento para fazer download dos binários do agente.

Siga estas etapas:

1. Efetue logon no Servidor do CA UAR com o seguinte URL:

   https://<host>:5250/spin/calm/CALMSpindle.csp

2. Navegue para Administração, Log Collection, Agent Explorer, Download Agent Binaries, *versão do SO*.

3. Salve no arquivo.

Obter uma chave de autenticação de agente

Use este procedimento para obter a chave de autenticação de agente.

Siga estas etapas:

1. No Servidor do CA UAR, navegue até Administração, Log Collection, Agent Explorer, Agent Authentication Key.

2. Torne a chave facilmente acessível, mas não coloque a segurança em risco.

Instalar o agente do CA UAR

O agente do CA UAR é responsável por coletar eventos e distribuir essas informações ao Servidor do CA UAR. Instale o agente na máquina do terminal ou em um servidor de banco de dados do CA Identity Manager para ativar o log.

Observação: o Agente do CA UAR é suportado nos sistemas operacionais Windows e Linux.

Siga estas etapas:

1. No servidor de banco de dados, execute a instalação ca-elmagent-<version>.exe e especifique as seguintes informações:

   - Nome ou endereço IP do servidor
   - Código de autenticação
   - Informações de conta do servidor do agente (usadas para executar o agente como um serviço/demon)

2. Especifique o arquivo de lista de conectores padrão, se disponível.

3. Efetue logon no Servidor do CA UAR com o seguinte URL:

   https://*host* :5250/spin/calm/CALMSpindle.csp

4. Navegue até Administração, Log Collection, Agent Explorer, Default Agent Group.

5. Selecione a máquina do agente e inicie a exibição Status and Command.

Importando definições de função

Antes de configurar a conexão do Enterprise Log Manager no Console de usuário, é preciso importar as Definições de função do CA Enterprise.

Para importar as definições de função:

1. Efetue logon no Management Console com o URL a seguir.

   `http://host:porta/iam/immanage`

2. Navegue até Environment, Role and Task Settings, clique no botão Import e selecione Enterprise Log Manager - Enterprise Log Manager Role Definitions.xml.
3. Clique em Save and Close.
4. Na guia Sistema, no Console de usuário, clique em Configurar a conexão do Enterprise Log Manager, preenche as informações obrigatórias e clique em Enviar.

Criar um novo conector

Siga este procedimento para criar um conector.

Siga estas etapas:

1. Efetue logon no Servidor do CA UAR no seguinte URL:

   `https://host:5250/spin/calm/CALMSpindle.csp`

2. Navegue até Administração, Log Collection, Agent Explorer, Default Agent Group.
3. Selecione a máquina do agente.
4. Alterne para Exibição de conectores.
5. Clique no botão Criar um novo conector e insira as seguintes informações:

   Detalhes do conector

   Selecione o Tipo de integração CAIdentityManager e altere o nome do conector, se desejado.

   Configuração do conector

   Sequência de conexão

   - Driver={SQL Server} ; Server=<Auditing DB Server> ; Database=<Auditing DB>
   - Driver={Microsoft ODBC for Oracle} ; Dbq=<Auditing DB TNSname>

   Nome de usuário: ***usuário do DB de auditoria***

   Senha: ***senha do usuário do DB de auditoria***

6. Aplique as seguintes alterações de configuração de conexão ao Conector do CA Identity Manager para uso com o 12.6.5.

   - SourceName: o nome da Origem de dados na máquina do agente - imsauditevent12
   - AnchorSQL: selecione max(id) em imsauditevent12
   - AnchorField: IMS_EVENTID
   - EventSQL:

     ```
     select imsauditevent12,id as IMS_EVENtid ,imsauditevent12,audit_time as
     IMS_AUDITTIME ,imsauditevent12,envname as ENVNAME
     ,imsauditevent12,admin_name as ADMINUNIQUENAME ,imsauditevent12,admin_dn
     as ADMINID ,imsauditevent12,tasksession_oid as TRANSACTIONID
     ,imsauditevent12,event_description as EVENTINFO
     ,imsauditevent12,event_state as EVENTSTATE
     ,imsauditevent12,tasksession_oid as TASKOID
     ,imsauditтasksession12,task_name as TASKNAME
     ,imsauditeventobject12,object_type as OBJECTTYPE ,
     imsauditeventobject12,object_name as
     ```

```
OBJECTUNIQUENAME ,imsauditobjectattributes12,attribute_name as ATTRNAME
,imsauditobjectattributes12,attribute_oldvalue as ATTROLDVALUE
,imsauditobjectattributes12,attribute_newvalue as ATTRNEWVALUE
,imsauditobjectattributes12,attribute_newvalue as ATTRVALUE from
imsauditTasksession12, imsauditevent12, imsauditeventobject12,
imsauditobjectattributes12 where imsauditevent12,id >? and
imsauditevent12,tasksession_id = imsauditTasksession12,id and
imsauditevent12,tasksession_oid = imsauditTasksession12,tasksession_oid
and
imsauditeventobject12,parent_event_id = imsauditevent12,id and
imsauditobjectattributes12,parent_object_id = imsauditeventobject12,id
ORDER BY
imsauditevent12,id ASC;
```

7. Salve e feche.

Para verificar se o conector está funcionando

1. Navegue até Administração, Log Collection, Agent Explorer, Default Agent Group.
2. Selecione a máquina do agente.
3. Alterne para Connectors View e clique no botão Launch Status and Command View.

   O status deve ser Em execução.

Ativar a auditoria no CA Identity Manager

Para ativar a auditoria no CA Identity Manager

1. Abrir o console de gerenciamento

   `http://host:porta//iam/immanage`

2. Navegue para Environments, <Environment>, Advanced Setting, Auditing.
3. Exporte as configurações existentes e salve o arquivo.
4. Modifique o arquivo salvo como se segue e salve as modificações:
   - <Audit enabled="true" auditlevel="BOTH" datasource="java:/auditDbDataSource"
   - Adicione o perfil de auditoria das políticas de senha no último perfil de auditoria já definido:

     <AuditProfile objecttype="FWPASSWORDPOLICY" auditlevel="BOTHCHANGED"/>
5. Importe o arquivo de volta no Management Console e escolha dentre as opções a seguir para acionar a agregação de informações de auditoria:
   - Tarefas executadas no objeto gerenciado do Usuário
   - Tarefas executadas no objeto gerenciado do Grupo
   - Tarefas executadas no objeto gerenciado de Políticas de senha
6. Efetue logon no Servidor do CA UAR com o seguinte URL:

   https://*host*:5250/spin/calm/CALMSpindle.csp
7. Para praticar em relatórios existentes, navegue para Queries and Reports, Queries, CA Identity Manager

   Observação: o Servidor do CA UAR já deve estar configurado.
8. Dependendo das tarefas que foram executadas, abra os relatórios padrão a seguir para verificar se os eventos estão aparecendo:
   - A tarefa Todos os eventos do sistema por usuário chama 'CA Identity Manager - Todos os eventos do sistema' filtrados por ID do usuário
   - A tarefa Gerenciamento de conta por host chama 'Gerenciamento de conta por host' no estado em que se encontra
   - A tarefa Criações de conta por conta chama 'Criações de conta por conta' no estado em que encontra
   - A tarefa Exclusões de conta por conta chama 'Exclusões de conta por conta' no estado em que encontra
   - A tarefa Bloqueios de conta por conta chama 'Bloqueios de conta por conta' no estado em que encontra

- A tarefa Atividade do processo de certificação pelo host chama 'CA Identity Manager - Atividade de processo por host' no estado em que se encontra
- A tarefa Atividade de alteração da política de senha chama 'CA Identity Manager - Atividade de alteração de política' no estado em que se encontra

Configurar o Servidor do CA UAR

Para poder configurar o Servidor do CA UAR para gerenciamento, verifique os seguintes requisitos:

- Você deve ter credenciais do EiamAdmin.
- É necessário ter o Adobe Flash Play versão 9.0.28 ou superior.

Depois que o servidor do CA UAR estiver configurado, as seguintes funções estão disponíveis:

- Um único servidor do CA UAR ou hierarquia federada pode consumir vários ambientes que geram eventos de auditoria.
- A autorização de dados para sistemas remotos pode ser implementada por meio do Filtro de acesso a dados do CA UAR.

Siga estas etapas:

1. Efetue logon na página de registro do produto do servidor do CA UAR com as credenciais de Administrador usando o seguinte URL:

   `https://host:porta/spin/calmapi/products.csp`

2. Registre um ambiente do CA Identity Manager clicando no botão Registrar e fornecendo o nome do certificado e a senha.

   Observação: cada ambiente deve ter pares de registro (nome/senha do certificado) separados.

3. Navegue até Administração, User and Access Management, New Data Access Filters e forneça um nome para o filtro.
4. Passe para a próxima etapa.
5. Deixe Selected Identities em All Identities e passe para a próxima etapa.
6. Crie um filtro de acesso clicando em New Event Filter.

   Configure o Data Access Filter restringindo o certificado que é criado para o nome do ambiente ou da máquina somente para logs que são coletados do CA Identity Manager. Você também pode restringir o certificado para acessar informações do terminal nativo somente para terminais gerenciados.

7. Salve e feche.
8. Abra Access Policies clicando em Open Access Policies.
9. Selecione Obligation Policies e clique na única política disponível.
10. Remova a opção All Identities e adicione o nome do certificado.
11. Salve a política.
12. Efetue logon no Console de usuário do CA Identity Manager e configure a conexão do Enterprise Log Manager.

Configurar a conexão do Enterprise Log Manager

Use esta tela para gerenciar tarefas de conexão do CA UAR recentemente adicionadas.

Essa janela contém os seguintes campos:

Nome da conexão

Especifica o nome exclusivo para o único objeto gerenciado de conexão do CA UAR.

Esse campo é somente leitura.

Nome do host (obrigatório)

Especifica o nome do host de servidor ou o endereço IP do CA UAR.

Nº da porta (obrigatório)

Especifica a porta de conexão do servidor do CA UAR.

Padrão: 52520

Certificado SSL assinado por autoridade de certificação

Quando marcada, essa opção especifica uma verificação rígida de certificado SSL durante a conexão com um servidor do CA UAR.

Se você tiver um certificado SSL autoassinado, como o instalado com o CA UAR, por padrão, desmarque essa caixa de seleção. O caminho confiável para a autoridade de certificação raiz não existe.

Nome do certificado (obrigatório)

Especifica o nome do certificado do CA UAR a ser usado na autenticação.

Senha do certificado (obrigatório)

Especifica a senha do CA UAR.

Atributo

Não suportado. A versão é recuperada em uma tentativa de salvar informações de conexão como um teste.

Excluir a conexão do Enterprise Log Manager

Selecione uma conexão na lista e clique em Excluir. A tarefa de conexão do CA Enterprise Log Manager é excluída.

Integrar relatórios ou consultas adicionais do CA UAR com o CA Identity Manager

É possível integrar relatórios ou consultas adicionais com o CA Identity Manager usando a guia Visualizador do Enterprise Log Manager. Esses novos relatórios ou consultas podem ser combinados com tarefas existentes (incluindo assistentes) e novas. Os dados federados do CA UAR também podem ser incluídos se necessário. Usando a guia Visualizador do Enterprise Log Manager, você pode aplicar filtros nas informações recuperadas. Esses filtros podem usar:

- Valores constantes
- Atributos de objeto gerenciado
  - Por exemplo, physical - ::MyPhysicalAttribute::

    logical - ::|MyLogicalAttribute|::
- Qualquer campo, conforme descrito pelo Common Event Grammar (CEG)
  - dest_username
  - dest_objectname
  - dest_uid
  - source_username
  - source_objectname
  - source_uid

Configurar a guia Visualizador do Enterprise Log Manager

Configure o visualizador do CA Enterprise Log Manager para incluir um ou mais dos seguintes campos:

Nome

Um nome atribuído para a guia.

Qualificador

Um identificador para a guia que seja exclusivo dentro da tarefa. Ele deve começar com uma letra ou um sublinhado e conter letras, números ou sublinhados. O qualificador é usado principalmente para definir valores de dados por meio de documentos XML ou parâmetros HTTP.

Ocultar guia

Impede que a guia fique visível na tarefa. Esta opção é útil para os aplicativos que precisam ocultar a guia, mas ainda ter acesso aos atributos na guia.

Consulta do Enterprise Log Manager

Especifica que as consultas do CA UAR serão exibidas.

Observação: é possível especificar uma consulta do CA Enterprise Log Manager ou o Relatório do CA Enterprise Log Manager, mas não ambos.

Relatório do Enterprise Log Manager

Especifica que os relatórios do CA UAR serão exibidos.

ID do Enterprise Log Manager

Especifica a ID da consulta ou do relatório.

Incluir dados agrupados

Inclui ou exclui dados federados nos resultados. Por padrão, esse campo não está selecionado.

Mostrar aviso

Especifica apenas as consultas de prompt do CA UAR. Por padrão, esse campo não está selecionado.

Filtro

Especifica condições avançadas com base no SQL que são usadas para estreitar os resultados retornados pelos relatórios e consultas do CA UAR. Os valores dinâmicos e constante podem ser incluídos. O código a seguir é um exemplo de expressão:

```
((source_uid EQUAL ::logical.attribute.X:: ) AND (source_username EQUAL
::logical.attribute.Y:: ))
```

As operações suportadas incluem:

- é igual a (EQUAL)

- diferente (NEQ)
- menor (LESS)
- maior (GREATER)
- menor que ou igual a (LEQ)
- maior que ou igual a (GREATEQ)
- parecido (LIKE)
- não parecido (NOTLIKE)
- no conjunto (INSET)
- fora do conjunto (NOTINSET)

Conjunções de suporte incluem:

- E
- OU

Os parênteses são obrigatórios. Se o valor no lado esquerdo da expressão da condição não tiver o marcador "::" em ambas as partes, o valor é considerado uma constante e o valor é enviado para o CA UAR como está.

Tabela parâmetro/valor

Especifica os campos e valores, por questões de definição de escopo.

Somente consultas ou relatórios correspondentes a tags e lógica de definição de escopo de tags são selecionados.

Parâmetro

Especifica os valores para os parâmetros Início, Término e Limite. Os seguintes parâmetros são suportados:

- Granularidade de tempo (apenas para tendências)
- Hora de início
- Hora de término
- O primeiro evento de grupo é datado após (apenas para consultas agrupadas)
- O último evento agrupado é datado após (apenas para consultas agrupadas)
- O último evento agrupado é datado antes (apenas para consultas agrupadas)
- O número mínimo de eventos no agrupamento (apenas para consultas agrupadas)
- O número máximo de eventos no agrupamento (apenas para consultas agrupadas)

Capítulo 18: Funções de acesso

As funções de acesso fornecem uma maneira adicional de fornecer direitos no CA Identity Manager ou outro aplicativo. Por exemplo, você pode usar as funções de acesso para realizar as seguintes tarefas:

- Fornecer acesso indireto a um atributo de usuário.
- Criar expressões complexas.
- Definir um atributo em um perfil de usuário, que é usado por outro aplicativo para determinar os direitos.

As funções de acesso são semelhantes a políticas de identidade, pois aplicam um conjunto de mudanças nos negócios a um usuário ou grupo de usuários. No entanto, quando você usa uma função de acesso para aplicar mudanças nos negócios, é possível ver para quais usuários as alterações serão aplicadas, exibindo os integrantes da função de acesso.

Na maioria dos casos, as funções de acesso não estão associadas a tarefas.

Observação: quando o CA Identity Manager se integra com o CA SiteMinder, as funções de acesso também podem fornecer acesso aos aplicativos protegidos pelo CA SiteMinder. Nesse caso, as funções de acesso incluem tarefas de acesso. Para obter mais informações, consulte o capítulo sobre a integração com o SiteMinder no *Guia de Configuração*.

Esta seção contém os seguintes tópicos:

Como as funções de acesso gerenciam os direitos

Você pode usar as funções de acesso para gerenciar direitos por meio da especificação de ações de mudança que ocorrem quando um usuário é adicionado ou removido como integrante ou administrador de uma função.

Para usar as funções de acesso, execute as seguintes etapas:

1. Um administrador cria uma função de acesso.
2. Na guia Integrantes, o administrador especifica ações de adição ou remoção, as quais determinam as ações que o CA Identity Manager executa quando a função de acesso é atribuída a um usuário.
3. O administrador especifica as políticas de administrador e proprietário, conforme necessário e, em seguida, envia a tarefa para criar a função de acesso.
4. Os administradores de funções de acesso atribuem a função de acesso aos usuários.
5. O CA Identity Manager conclui as ações de adição especificadas na função.

Exemplo: modificação indireta de atributo do perfil

Você pode usar as funções de acesso para alterar indiretamente um atributo em um perfil de usuário. Por exemplo, uma empresa pode não querer permitir que qualquer usuário altere diretamente o cargo de outro usuário. Essa empresa pode criar uma função de acesso que altera um cargo quando um administrador atribui a função a um usuário.

Para alterar indiretamente um atributo, é preciso definir as ações de alteração para a função de acesso. Quando um administrador atribui a função, a ação de alteração pode fazer uma ou mais alterações em um atributo no perfil do usuário.

Para usar uma função de acesso para modificar indiretamente um atributo, faça o seguinte:

1. Crie uma função de acesso.
2. Na guia Integrantes, marque a caixa de seleção Os administradores podem adicionar e remover integrantes desta função e clique no ícone em forma de seta.

   O CA Identity Manager exibe os campos adicionais Ação de adição e Ação de remoção.
3. No campo Ação de adição ou Ação de remoção, selecione uma ação na caixa de listagem.

   O CA Identity Manager exibe os campos adicionais com base na opção selecionada.
4. Configure Ação de adição ou Ação de remoção, conforme necessário.

5. Selecione a guia Administrador para especificar os administradores que podem adicionar integrantes à função de acesso que você estiver criando.
6. Selecione a guia Proprietários para especificar os administradores que podem modificar a definição da função de acesso.
7. Clique em Enviar para concluir a criação da função de acesso.
8. Atribua a função de acesso aos usuários, conforme necessário.

Criar uma função de acesso

A criação de uma função de acesso envolve estas etapas:

- Iniciar a criação da função de acesso (na página 543)
- Definir o perfil de uma função de acesso (na página 544)
- Definir políticas de integrante para uma função de acesso (na página 544)
- Definir políticas administrativas para uma função de acesso (na página 545)
- Definir regras de proprietário para uma função de acesso (na página 545)

Iniciar a criação da função de acesso

Siga estas etapas:

1. Efetue logon em uma conta do CA Identity Manager com uma função que inclui uma tarefa para a criação de funções de acesso.
2. Clique em Funções de acesso, Criar função de acesso.

   Escolha a opção de criar uma cópia de uma função ou a função. Se selecionar a opção Copiar, pesquise a função.
3. Prossiga para a próxima seção, Definir o perfil de uma função de acesso.

Definir o perfil de uma função de acesso

Siga estas etapas:

1. Insira um nome e uma descrição e preencha os atributos personalizados definidos para a função.

   Observação: é possível especificar atributos personalizados na guia Perfil que especificam informações adicionais sobre as funções de acesso. Você pode usar essas informações adicionais para facilitar as pesquisas de funções em ambientes que incluem um número significativo de funções.

2. Selecione Ativado se estiver pronto para tornar a função disponível para uso assim que criá-la.

3. Prossiga para a próxima seção, Definir políticas de integrante para uma função de acesso (na página 544).

Definir políticas de integrante para uma função de acesso

Na guia Integrantes:

1. Selecione Adicionar para definir as políticas de integrante.

2. (Opcional) Na página Política de integrante, você tem a opção de definir uma regra de integrante para quem poderá usar essa função.

   Isso atribui automaticamente a função aos usuários que corresponderem ao critério da política de integrante.

3. Verifique se a Política de integrante é exibida na guia Integrantes.

   Para editar uma política, clique no símbolo de seta à esquerda. Para removê-la, clique no ícone do sinal de menos.

4. Na guia Integrantes, marque a caixa de seleção Os administradores podem adicionar e remover integrantes desta função.

   Ao ativar esse recurso, você pode definir Adicionar ação e Remover ação. Essas ações definem o que acontece quando um usuário é adicionado ou removido como um integrante da função.

5. Prossiga para a próxima seção, Definir políticas administrativas para uma função de acesso (na página 545).

Definir políticas administrativas para uma função de acesso

Na guia Administradores:

1. Se desejar tornar a opção Gerenciar administradores disponível, marque a caixa de seleção Os administradores podem adicionar e remover administradores desta função.

   Ao ativar esse recurso, defina as ações para quando um usuário é adicionado ou removido como um administrador da função.

2. Na guia Administradores, adicione as políticas administrativas que incluem regras administrativas e de escopo, bem como os privilégios de administrador. Cada política exige pelo menos um privilégio (Gerenciar integrantes ou Gerenciar administradores).

   Você pode adicionar várias políticas administrativas com regras e privilégios diferentes para administradores que atendam à regra.

3. Para editar uma política, clique no símbolo de seta à esquerda. Para removê-la, clique no ícone do sinal de menos.

4. Prossiga para a próxima seção, Definir regras de proprietário para uma função de acesso (na página 545).

Definir regras de proprietário para uma função de acesso

Na guia Proprietários:

1. Defina as regras de proprietário, que determinam os usuários que podem modificar a função.

2. Clique em Enviar.

   Uma mensagem é exibida, indicando que a tarefa foi enviada. Um atraso momentâneo pode ocorrer antes que um usuário possa usar a função.

Capítulo 19: Tarefas do sistema

Esta seção contém os seguintes tópicos:

Tarefas do sistema padrão

O CA Identity Manager inclui as seguintes tarefas que ajudam os administradores a gerenciar o ambiente do CA Identity Manager:

- Tarefas de Exibir minhas tarefas enviadas

  Permite que administradores exibam o status das tarefas no ambiente. Também remove tarefas obsoletas das telas de Exibir minhas tarefas enviadas.

- Tarefas do carregador de itens em massa

  Faz upload de arquivos do alimentador que são usados para manipular um grande número de objetos gerenciados simultaneamente.

- Tarefa em massa

  Executa uma tarefa em um objeto, como Usuário, com base nos atributos do objeto, como departamento, cidade, data de rescisão e assim por diante. É possível executar essa tarefa periodicamente, como todo sábado.

  Também é possível usar essa tarefa para fazer alterações em massa em usuários.

- Tarefas de Dados da caixa de seleção

  Permite que os administradores façam upload de arquivos que são usados para preencher as opções nos campos, como caixas de seleção, em tarefas administrativas.

- Tarefas de Manipulador de atributos lógicos

  Permite que os administradores gerenciem os atributos lógicos, que são usados para exibir atributos de repositório de usuários (chamados de atributos físicos) em um formato de fácil utilização nas telas de tarefas.

- Tarefas de Gerenciamento de conexão JDBC

  Configura os detalhes da conexão do servidor de banco de dados no CA Identity Manager.

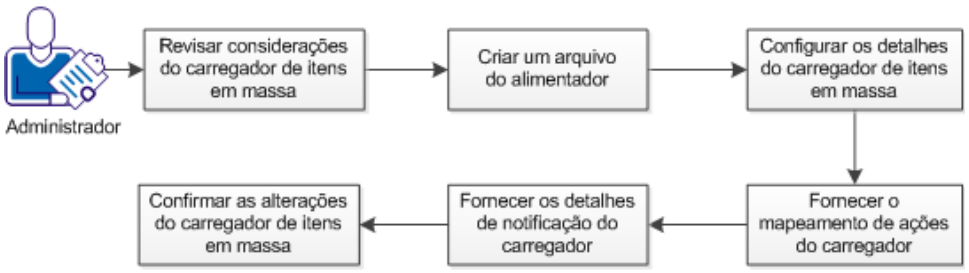
- Tarefas de email

  Gerencia as políticas de notificação por email.

Como adicionar usuários com um arquivo do alimentador

Você pode usar a guia Carregador de itens em massa para fazer upload de arquivos do alimentador que são usados para manipular um grande número de objetos gerenciados simultaneamente. Por exemplo, você pode criar 1.000 usuários no sistema manualmente, ou usar o carregador de itens em massa. A tarefa do Carregador de itens em massa também pode ser mapeada para um processo de fluxo de trabalho.

O cliente de carregamento em massa é um utilitário de linha de comando que existe para o processamento em lote. É recomendável usar o cliente de carregamento em massa se o ambiente estiver em um agrupamento (para fins de balanceamento de carga). O cliente de carregamento em massa pode ser encontrado na mídia de componentes de provisionamento.



Siga estas etapas:

1. Revise as considerações do carregador de itens em massa (na página 549).
2. Crie um arquivo do alimentador CSV ou XLS (na página 552) e faça upload dele.
3. Configure Detalhes dos registros do carregador (na página 553).

   Essa guia permite especificar os campos de ação e do identificador no arquivo do alimentador.
4. Forneça o Mapeamento de ações do carregador (na página 554).

   Essa guia permite que você selecione o objeto principal e especifique qual tarefa executar para a ação em um objeto.
5. Forneça Detalhes da notificação do carregador (na página 555).

   Essa guia permite que você selecione os usuários para certificar as alterações de tarefa do carregador de itens em massa.
6. Confirme e modifique o progresso das alterações de tarefa do carregador de itens em massa (na página 555).

Considerações sobre o carregador de itens em massa

Você pode usar a guia Carregador de itens em massa para fazer upload de arquivos do alimentador que são usados para manipular um grande número de objetos gerenciados simultaneamente. Considere as seguintes questões ao usar o carregador de itens em massa:

- Considere programar carregamentos em massa grandes fora do horário de pico, como durante a noite. Carregamentos em massa grandes podem afetar o desempenho. Em alguns casos, um carregamento em massa que inclui diversas subtarefas pode impedir que as tarefas enviadas pelo usuário sejam concluídas até que o carregamento em massa seja concluído.
- Se o servidor cair durante uma tarefa de longa duração, como o carregamento de muitos objetos, reinicie a tarefa em Exibir tarefas enviadas. Quando a tarefa for reiniciada, começará a partir do último registro bem-sucedido.
- Se estiver usando o LDAP como um repositório de usuários com Solaris, o carregador de itens em massa pode travar durante uma importação. Para solucionar esse problema, consulte o tópico Especificar as configurações de conexão LDAP no *Guia de Configuração* e aplique as configurações descritas.

- Se você usar o carregador de itens em massa para importar uma grande quantidade de usuários, é possível que haja exceções de falta de memória. Para resolver esse problema, ajuste os seguintes parâmetros de tamanho de heap da memória:
  - -Xmx
  - -XX:maxPermSize

    Observação: para obter mais informações sobre como reajustar os parâmetros de memória, consulte a documentação do servidor de aplicativos.
- O uso do carregador de itens em massa para manipular vários objetos gerenciados, como a criação de muitos usuários, pode afetar o desempenho. Para aprimorar o desempenho, considere as seguintes recomendações:
  - Divida um arquivo CSV grande em vários arquivos pequenos ao usar o console de usuário para carregamentos em massa. Por exemplo, fazer dez carregamentos em massa de 10.000 usuários é mais rápido do que fazer um carregamento em massa de 100.000 usuários.

    Observação: um arquivo CSV com mais de 10 mil entradas pode causar problemas no sistema.
  - Limite o número de tarefas do usuário que estiver fazendo o carregamento em massa. Por exemplo, o desempenho aumenta quando o administrador que inicia o carregamento em massa possui apenas algumas tarefas. Quando o administrador tem muitas tarefas, o CA Identity Manager precisa fazer verificações de permissão mais amplas, o que pode afetar o desempenho.
  - Limite o número de políticas do Policy Xpress associadas às alterações em massa, que envolvem o provisionamento. Além disso, considere a criação de políticas do Policy Xpress simples, que não afetam o desempenho tanto quanto as políticas complexas durante uma operação de carregamento em massa.
  - Verifique se você possui recursos do sistema suficientes.

Limitar a validação de dados para melhorar o desempenho do carregamento de itens em massa

Uma tarefa administrativa normalmente inclui várias guias. Por padrão, as operações em massa validam os dados em cada guia em uma tarefa.

A validação pode afetar o desempenho das operações em massa. Para melhorar o desempenho, é possível desativar a validação de dados das guias de tarefas, se a validação não for necessária.

Siga estas etapas:

1. Efetue logon no Console de usuário como um usuário que pode modificar tarefas administrativas.
2. Selecione Tarefas, Funções e tarefas, Tarefas administrativas, Modificar tarefa administrativa.

3. Procure e selecione a tarefa que se aplica à operação em massa.
4. Selecione Guias e, em seguida, selecione a guia que você deseja modificar.
5. Selecione Não validar na operação em massa e, em seguida, clique em OK.
6. Repita as etapas 4 e 5 para cada guia que não necessite de validação de dados.
7. Clique em Enviar.

   A validação de dados é desativada para as guias que você modificou.

Limitar a lógica de negócios personalizada

Incluir a lógica de negócios personalizada, tal como manipuladores de tarefas lógicas de negócios e ouvintes de eventos, em tarefas que são usadas em operações em massa, pode afetar o desempenho.

Para melhorar o desempenho, desative a lógica de negócios personalizada nas operações de carregamento em massa.

Siga estas etapas:

1. Abra o console de gerenciamento.
2. Selecione o ambiente aplicável que inclui o ouvinte de evento ou manipulador de tarefas lógicas de negócios.
3. Selecione Configurações avançadas, Manipuladores de tarefas lógicas de negócios (se aplicável).
4. Defina o valor da propriedade UseInBulkOperation como falso e, em seguida, clique em Salvar.
5. Repita a etapa 4 para os ouvintes de eventos.
6. Depois de concluídas as modificações dos manipuladores de tarefas lógicas de negócios e dos ouvintes de eventos, reinicie o ambiente.

Criar um arquivo do alimentador

Um arquivo do carregador de itens em massa é usado para automatizar ações repetidas realizadas em um grande número de objetos gerenciados. Ao fazer upload de um arquivo do alimentador, o sistema analisa e lê esse arquivo.

O arquivo do alimentador deve ter uma extensão CSV ou XLS e as seguintes propriedades:

- O arquivo deve conter uma linha de cabeçalho que especifica atributos físicos, atributos lógicos ou nomes de atributos conhecidos de um objeto gerenciado.
- A linha de cabeçalho deve incluir uma coluna que indica a ação a ser executada nos registros.
- Um registro é nomeado para cada linha no arquivo do alimentador. Os registros contêm os valores para cada um dos atributos especificados pela linha de cabeçalho. As opções a seguir são valores aceitáveis para um atributo:
  - Valor — o atributo será definido com o valor especificado.
  - Value;Value;Value;... — o atributo será definido com o atributo com vários valores que você especificar.
  - ' ' (em branco) — o atributo não será alterado.
  - NULO — o atributo será excluído. A sequência de exclusão é definida como NULO por padrão, mas pode ser editada na tela Pesquisa de upload de arquivo do carregador de itens em massa.

Observação: para usar um hash (#) no arquivo do alimentador, coloque a marca # entre aspas, por exemplo, user#1 deve ser especificado como "user#1".

Importante: o arquivo do alimentador deve ser salvo com a codificação UTF-8.

Amostra de arquivo do alimentador para criação de usuários

Este exemplo de arquivo do alimentador cria usuários com determinados atributos necessários.

```
action,%USER_ID%,%FIRST_NAME%,%LAST_NAME%,%FULL_NAME%,%PASSWORD%,%EMAIL%
create,JD,John,Doe,John Doe,mypassword,Johndoe@a.com
create,BD,Baby,Doe,Baby Doe,mypassword2,Babydoe@a.com
```

No código anterior, o arquivo do alimentador tem as seguintes propriedades:

Cabeçalho

A primeira linha do código é a linha de cabeçalho. A linha de cabeçalho tem atributos físicos ou conhecidos para o usuário do objeto gerenciado.

Ação

A coluna de ação identifica a tarefa a ser executada para cada registro. Por exemplo, o arquivo acima especifica que uma ação de criação deve ser executada no Nome John.

Amostra de arquivo do alimentador para ativação de usuários

Este exemplo de arquivo do alimentador altera o valor do atributo lógico |enabled|. Você pode especificar o atributo lógico no cabeçalho e o valor (neste caso, verdadeiro ou falso) em cada entrada de usuário no arquivo.

```
action,%USER_ID%,|enable|

MODIFY,user1,false

MODIFY,user2,true
```

Guia Detalhes dos registros do carregador

A guia Detalhes dos registros do carregador exibe uma curta visualização dos registros disponíveis no arquivo do alimentador. A tabela de visualização exibe no máximo cinco registros. A tabela de visualização ajuda os usuários a identificar se estão carregando o arquivo correto. Além disso, essa guia permite identificar a ação que deseja executar nos objetos gerenciados especificados no arquivo do alimentador. É necessário preencher os campos a seguir:

Qual campo representa a ação a ser executada no objeto?

Identifica os campos do arquivo do alimentador que indicam a ação que você deseja executar nos objetos gerenciados. Por exemplo, você pode usar um arquivo do alimentador com um campo de ação que aceite os valores de Criar, Modificar e Excluir. Você deve mapear cada uma dessas ações para uma tarefa administrativa no Mapeamento de ações do carregador (na página 554).

Qual campo será usado para identificar o objeto de maneira exclusiva?

Identifica o campo do arquivo do alimentador que pode identificar o objeto principal de maneira exclusiva.

Observação: se o arquivo do alimentador tiver uma linha de cabeçalho inválida, os registros do arquivo do alimentador não serão exibidos na guia Detalhes dos registros do carregador. Selecione outro arquivo do alimentador no caso de linhas de cabeçalho inválidas. Se o arquivo do alimentador contiver alguns registros inválidos, o status detalhado do upload estará em Exibir tarefas enviadas, na guia Sistema.

Guia Mapeamento de ações do carregador

A guia Mapeamento de ações do carregador permite que você selecione um objeto principal no qual as ações especificadas no arquivo do alimentador serão executadas. Você também deve mapear as ações do arquivo do alimentador a tarefas administrativas para o objeto principal selecionado.

Qual é o objeto principal?

Identifica o objeto principal a ser manipulado pelo CA Identity Manager usando o arquivo do alimentador. Você pode selecionar qualquer um dos seguintes objetos principais:

- Usuário
- Grupos
- Organização

Selecionar uma tarefa para executar para a ação

Identifica as tarefas administrativas a serem realizadas para cada ação especificada pelo arquivo do alimentador, como as tarefas de exclusão ou modificação.

Observação: você deve mapear todas as ações no arquivo do alimentador para uma tarefa administrativa. Além disso, as tarefas administrativas exibidas nesse campo dependem do objeto principal selecionado. Por exemplo, se você selecionar Usuário como objeto principal, somente as tarefas administrativas relacionadas a Usuário serão exibidas.

Selecionar uma tarefa para objeto não existente para a ação

Identifica as tarefas administrativas alternativas a serem executadas para uma ação especificada no arquivo do alimentador caso o objeto gerenciado ainda não exista no CA Identity Manager, como a tarefa de criação.

Guia Detalhes da notificação do carregador

Importante: por padrão, essa guia não está incluída no assistente do carregador de itens em massa. Você deve adicioná-la manualmente, modificando a tarefa do carregador de itens em massa e adicionando a guia Detalhes da notificação do carregador. Além disso, essa guia exige que você ative o fluxo de trabalho no ambiente.

A guia Detalhes da notificação do carregador permite selecionar os gerenciadores de certificações para a tarefa do carregador de itens em massa. Quando uma tarefa do carregador de itens em massa é concluída, o CA Identity Manager cria uma Notificação do carregador de itens em massa para todos os gerenciadores de certificações configurados para a tarefa. Esta notificação é exibida na guia Principal em Notificações do carregador de itens em massa. Clicar na notificação exibe detalhes sobre as tarefas iniciadas pela operação de carregamento em massa. Em seguida, os gerenciadores de certificações podem revisar e confirmar as alterações detalhadas nas notificações.

Observação: para oferecer uma lista de gerenciadores de certificações, use qualquer resolvedor participante disponível na lista suspensa. Para obter mais informações sobre resolvedores participantes, consulte a seção Fluxo de trabalho deste guia.

Confirmar alterações de tarefa do carregador de itens em massa

A opção Notificações do carregador de itens em massa contém detalhes sobre todas as alterações que a tarefa do carregador de itens em massa iniciou. Os gerenciadores de certificações podem revisar e confirmar as alterações iniciadas por uma tarefa do carregador de itens em massa.

Para revisar e confirmar as alterações de tarefa do carregador de itens em massa:

1. Efetue logon no console de usuário como um usuário que está listado como um gerenciador de certificações de uma tarefa do carregador de itens em massa.
2. Vá para Principal, Exibir minhas notificações do carregador de itens em massa.

3. Selecione a Notificação do carregador de itens em massa que deseja revisar.

   A tela Gerenciar notificações do carregador de itens em massa é exibida e mostra uma tabela listando todas as alterações de tarefa do carregador de itens em massa que foram iniciadas.

   Nessa tela, é possível fazer o seguinte:

   - Para revisar os detalhes de uma tarefa específica de um objeto de criação ou modificação, clique no hiperlink na coluna Descrição.
   - Se houver violações de conformidade ou se desejar remover uma função que foi adicionada a um usuário, é possível editar o usuário diretamente na tela de notificação, clicando no ícone Editar ao lado da ID do usuário.
   - Para revisar as funções adicionadas a um usuário, clique no hiperlink na coluna Atribuições da função solicitada associada à ID do usuário.

4. Uma vez que tiver revisado todas as alterações em um objeto específico, marque a caixa de seleção Confirmar para esse objeto.
5. Quando terminar de confirmar as alterações, clique em Confirmar para remover todas as notificações de alteração selecionadas da lista.

   Observação: é possível selecionar Confirmar tudo para confirmar todas as alterações em uma notificação do carregador de itens em massa. Isso exclui a Notificação do carregador de itens em massa da guia Principal. Além disso, é possível marcar a caixa de seleção na parte superior da coluna Confirmar para selecionar todas as notificações de alteração na tela naquele momento e confirmar as alterações de acordo com a tela.

   Quando todas as alterações do usuário associadas a uma tarefa do carregador de itens em massa tiverem sido confirmadas, Notificação do carregador de itens em massa desaparecerá da guia Principal.

Configurar notificações por email para tarefas do carregador de itens em massa

Em alguns ambientes, as notificações por email de operação em massa são configuradas por padrão. Para verificar se as notificações por email de operação em massa estão configuradas em seu sistema, vá para Sistema, Email, Exibir email e pesquise o termo "em massa".

Se nenhuma notificação por email estiver configurada em seu ambiente, configure o email que será enviado quando uma operação em massa for concluída.

Siga estas etapas:

1. Vá para Sistema, Email, Criar email no console de usuário.
2. Preencha os campos necessários na guia Perfil.

3. Na guia Quando enviar, execute as seguintes etapas:
   a. Selecione Conclusão da tarefa no primeiro campo.
   b. Selecione o carregador de itens em massa no segundo campo.
4. Preencha as guias Destinatários e Conteúdo e, em seguida, clique em Enviar.

   As notificações por email estão configuradas para tarefas do carregador de itens em massa.

Programar uma tarefa do carregador de itens em massa

A tarefa do carregador de itens em massa pode ser programada no sistema. Para programar a tarefa do carregador de itens em massa, adicione uma guia Agendador (na página 61) à tarefa.

Modificar o arquivo do analisador para o carregador de itens em massa

Para modificar o analisador usado para analisar os arquivos do alimentador, configure a respectiva tarefa administrativa.

Para modificar a tarefa administrativa do carregador de itens em massa:

1. Vá para Funções e Tarefas, Tarefas administrativas, Gerenciar tarefa administrativa.
2. Pesquise a tarefa do carregador de itens em massa.
3. Selecione a tarefa do carregador de itens em massa e clique em Selecionar.
4. Selecione a guia Pesquisar para a tarefa do carregador de itens em massa.
5. Clique em Procurar para localizar as telas de pesquisa.

   A lista de telas de pesquisa disponíveis é exibida.
6. Selecione uma tela de pesquisa e clique em Editar.

   Os detalhes da tela de pesquisa são exibidos.

7. (Opcional) Edite o Nome totalmente qualificado do analisador.

   O Nome totalmente qualificado do analisador deve corresponder ao nome do arquivo do analisador.

   Observação: para obter mais informações sobre como criar um analisador CSV personalizado, consulte o Javadoc da classe FeederParser. Se você usar o JBoss como seu servidor de aplicativos e criar um analisador personalizado, o arquivo do analisador personalizado deve estar no diretório iam_im.ear/user_console_war/WEB-INF/classes.

8. Clique em OK.

Suporte ao serviço web para o carregador de itens em massa

O carregador de itens em massa possui uma API de serviço web que pode ser chamada usando a interface do serviço web de execução de tarefa (TEWS) do CA Identity Manager. O TEWS permite que aplicativos cliente enviem tarefas remotas ao CA Identity Manager para execução. Essa interface implementa os padrões abertos WSDL e SOAP para fornecer acesso remoto ao CA Identity Manager.

O CA Identity Manager inclui exemplos de cliente Java que demonstram a chamada do carregador de itens em massa como um serviço web. Os exemplos de Java estão localizados no seguinte arquivo de origem:

ferramentas_administrativas\samples\WebService\Axis\optional\ObjectsFeeder.java

As amostras de dados e a documentação para chamar o carregador de itens em massa como um serviço web estão localizadas no seguinte diretório:

ferramentas_administrativas\samples\Feeder\

Observação: para obter mais informações, consulte o *Guia de Programação do Java*.

Gerenciamento de conexão JDBC

As informações de relatórios do CA Identity Manager podem ser provenientes de várias origens, e cada relatório deve ser associado a uma origem de dados específica, de acordo com as informações que deseja ver no relatório.

Para estabelecer diferentes origens de dados para a geração de relatórios (como um banco de dados de auditoria ou um banco de dados de persistência de tarefas), crie um objeto gerenciado de conexão no CA Identity Manager. Depois de criar a conexão, você pode associar um relatório com um determinado objeto gerenciado de conexão, modificando a tarefa de geração de relatório e configurando o Objeto de conexão para o relatório na guia de pesquisa da tarefa de geração de relatório.

Criar conexão JDBC

Execute as etapas a seguir para fornecer os detalhes da conexão no CA Identity Manager.

Para criar uma conexão JDBC:

1. Clique em Sistema, Gerenciamento de conexão JDBC, Criar conexão JDBC.
2. Crie um objeto de conexão ou escolha um objeto de conexão com base em uma origem de dados específica do JNDI.
3. Preencha todos os campos necessários e clique em Enviar.

   Uma conexão JDBC é criada.

Manipuladores de atributos lógicos

Os atributos lógicos do CA Identity Manager permitem exibir atributos de repositório de usuários (chamados de atributos físicos) em um formato de fácil utilização nas telas de tarefas. Os administradores do CA Identity Manager usam as telas de tarefas para executar funções no CA Identity Manager. Os atributos lógicos não existem em um repositório de usuários. Em geral, eles representam um ou mais atributos físicos para simplificar a apresentação. Por exemplo, a data do atributo lógico pode representar o dia, mês e ano dos atributos físicos.

Os atributos lógicos são processados por manipuladores de atributos lógicos, que são objetos Java escritos utilizando a API de atributos lógicos. (Consulte o *Guia de Programação do Java*). Por exemplo, quando uma tela de tarefa é exibida, um manipulador de atributos lógicos pode converter dados do atributo físico do repositório de usuários em dados de atributos lógicos, que são exibidos na tela de tarefa. Você pode usar atributos lógicos predefinidos e manipuladores de atributos lógicos do CA Identity Manager ou criar outros usando a API de atributos lógicos.

Observação: para obter mais informações sobre os atributos lógicos, consulte o *Guia de Programação do Java*.

No console de usuário, a categoria Ambiente contém tarefas de gerenciamento de manipuladores de atributos lógicos. A lista inclui os manipuladores predefinidos fornecidos com o CA Identity Manager e quaisquer manipuladores personalizados definidos em seu local.

Na categoria de tarefa Ambiente, você pode fazer o seguinte:

- Criar um novo manipulador de atributos lógicos com o CA Identity Manager
- Copiar um manipulador

- Excluir um manipulador
- Modificar a configuração de um manipulador existente

Observação: para alterar a ordem de execução dos manipuladores de atributos lógicos, use o Management Console.

Criar manipulador de atributos lógicos

Para criar um manipulador de atributos lógicos:

1. Vá para Sistema, Atributos lógicos, Criar manipulador de atributos lógicos.
2. Na tela Criar manipulador de atributos lógicos, selecione Criar manipulador de atributos lógicos padrão e clique em OK.
3. Na tela Criar manipulador de atributos lógicos, defina as configurações para o manipulador de atributos lógicos.

   Para obter uma descrição de cada campo, clique no link Ajuda nesta tela.
4. Clique em Enviar.

   O manipulador é adicionado à lista de manipuladores na tela Manipulador de atributos lógicos.

Observação: não é necessário reiniciar o servidor de aplicativos depois de configurar manipuladores de atributos lógicos usando o console de usuário.

Copiar um manipulador de atributos lógicos

Para copiar um manipulador de atributos lógicos:

1. Vá para Sistema, Atributos lógicos, Criar manipulador de atributos lógicos.
2. Na tela Criar manipulador de atributos lógicos, selecione Criar cópia de uma definição do manipulador de atributos lógicos e clique em Pesquisar.
3. Selecione um manipulador de atributos lógicos (por exemplo, ConfirmPasswordHandler) e clique em OK.
4. Na tela Criar manipulador de atributos lógicos, defina as configurações para o manipulador de atributos lógicos.

   Para obter uma descrição de cada campo, clique no link Ajuda nesta tela.
5. Clique em Enviar.

   O manipulador é adicionado à lista de manipuladores na tela Manipulador de atributos lógicos.

Observação: não é necessário reiniciar o servidor de aplicativos depois de configurar manipuladores de atributos lógicos usando o console de usuário.

Criar um manipulador de atributos lógicos ForgottenPasswordHandler

O manipulador de atributos lógicos ForgottenPasswordHandler usa atributos lógicos separados para o seguinte:

- configuração
- perguntas e respostas de tempo de execução

Para criar um manipulador de atributos lógicos ForgottenPasswordHandler:

1. Vá para Sistema, Atributos lógicos, Criar manipulador de atributos lógicos.
2. Na tela Criar manipulador de atributos lógicos, selecione Criar manipulador de atributos lógicos padrão e clique em Pesquisar.
3. Selecione ForgottenPasswordHandler e clique em OK.
4. Na tela Criar manipulador de atributos lógicos: ForgottenPasswordHandler, defina as configurações para o manipulador de atributos lógicos.

   Para obter uma descrição de cada campo, clique no link Ajuda nesta tela.
5. Clique em Enviar.

   O manipulador é adicionado à lista de manipuladores na tela Manipulador de atributos lógicos.

Observação: não é necessário reiniciar o servidor de aplicativos depois de configurar manipuladores de atributos lógicos usando o console de usuário.

Excluir um manipulador de atributos lógicos

Para excluir um manipulador de atributos lógicos:

1. Vá para Sistema, Atributos lógicos, Criar manipulador de atributos lógicos.
2. Na tela Excluir manipulador de atributos lógicos, selecione a caixa de seleção à esquerda de cada atributo lógico a excluir.
3. Clique em Selecionar.

   O CA Identity Manager exibirá uma mensagem de confirmação.
4. Clique em Sim para confirmar a exclusão.

Modificar um manipulador de atributos lógicos

Para modificar um manipulador de atributos lógicos:

1. Vá para Sistema, Atributos lógicos, Criar manipulador de atributos lógicos.
2. Na tela Modificar manipulador de atributos lógicos, selecione o manipulador que deseja modificar e clique em Selecionar.
3. Selecione um manipulador de atributos lógicos (por exemplo, ConfirmPasswordHandler) e clique em OK.
4. Na tela Modificar manipulador de atributos lógicos, defina as configurações para o manipulador de atributos lógicos.

   Para obter uma descrição de cada campo, clique no link Ajuda nesta tela.
5. Clique em Enviar.

Observação: não é necessário reiniciar o servidor de aplicativos depois de configurar manipuladores de atributos lógicos usando o console de usuário.

Exibir um manipulador de atributos lógicos

Para exibir um manipulador de atributos lógicos:

1. Vá para Sistema, Atributos lógicos, Criar manipulador de atributos lógicos.
2. Na tela Exibir manipulador de atributos lógicos, selecione o manipulador que deseja exibir e clique em Selecionar.
3. Exiba as propriedades do manipulador de atributos lógicos e clique em Fechar.

Dados da caixa de seleção

Você pode preencher as opções que estão disponíveis nos seguintes campos:

- Seleção múltipla de caixa de seleção
- Lista suspensa
- Caixa suspensa
- Seleção múltipla
- Seletor de opções
- Combinação do seletor de opções

- Botão de opção de seleção única
- Seleção única

Essas opções são armazenadas em arquivos XML de Dados da caixa de seleção. Por exemplo, você pode usar os arquivos XML de Dados da caixa de seleção para preencher as opções de uma caixa suspensa de Cidade ou Estado em uma guia Perfil para a tarefa Criar usuário.

Você também pode usar o arquivo XML de dados da caixa de seleção para configurar uma dependência entre dois campos em uma tarefa administrativa. Por exemplo, as opções disponíveis no campo Cidade podem depender de uma opção que o usuário seleciona no campo Estado.

Observação: para obter mais informações sobre os dados da caixa de seleção, consulte o *Guia de Design do Console de Usuário*.

Tela de tarefas Configurar atributos de correlação

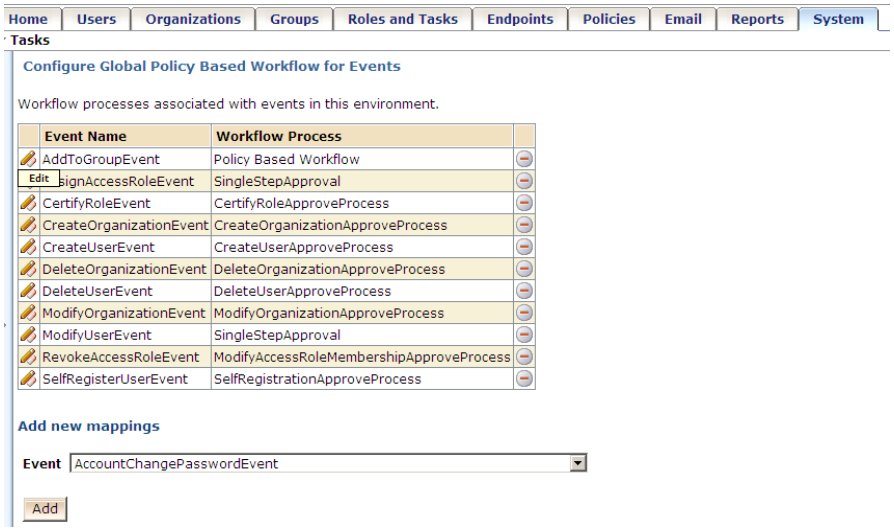
Esse tópico aplica-se apenas ao CA CloudMinder.

Use a tela de tarefas Configurar atributos de correlação para configurar regras de correlação para o ambiente.

O CA Identity Manager lê os parâmetros de configuração da memória e periodicamente sincroniza a versão da memória com a versão do banco de dados do DSA comum. Como os atributos de correlação são específicos para os inquilinos, o servidor de provisionamento lê os atributos de correlação do DSA do inquilino correspondente durante uma operação de Explorar e correlacionar. As regras de correlação atualizadas entram em vigor imediatamente, sem precisar esperar pela hora de atualização dos parâmetros.

Tela de tarefa Configurar política global para o fluxo de trabalho com base em eventos

A tarefa de Configurar política global para o fluxo de trabalho com base em eventos permite que um administrador configure um fluxo de trabalho com base em política ou que não se baseia em nenhuma política para todos os eventos no ambiente atual. Clicar na tarefa exibe o mapeamento do evento padrão para definições de processo do fluxo de trabalho. Cada mapeamento do evento pode ser modificado ou excluído, e novos mapeamentos de eventos podem ser adicionados para eventos que não foram configurados.



Os campos nessa tela são os seguintes:

Processos de fluxo de trabalho associados aos eventos neste ambiente.

Especifica os processos de fluxo de trabalho associados a políticas de aprovação.

Adicionar novos mapeamentos

Especifica uma política de aprovação para mapear para um processo de fluxo de trabalho.

Botão Adicionar

Adiciona o novo mapeamento.

Adicionar ou modificar um mapeamento abre a tela Mapeamento de fluxo de trabalho, em que você pode selecionar os mapeamentos de processo e as políticas de aprovação. O comportamento é o mesmo que o da configuração do fluxo de trabalho em nível de evento. Clicar no botão Adicionar na página Mapeamento de fluxo de trabalho exibe uma outra página, na qual é possível configurar uma política de aprovação.

Mais informações

Como configurar o fluxo de trabalho com base em políticas para eventos (na página 324)
Como configurar uma política de aprovação (na página 327)

Status da tarefa no CA Identity Manager

Talvez os administradores queiram acompanhar o status das tarefas do CA Identity Manager após o envio para processamento. O CA Identity Manager fornece os seguintes métodos para exibir o status da tarefa:

- **Guia Exibir tarefas enviadas**

  Esta guia permite procurar e exibir as tarefas do CA Identity Manager que foram enviadas para processamento.

  Os administradores podem exibir os detalhes da tarefa em uma visualização de alto nível ou em níveis adicionais de detalhes.

  A guia Exibir tarefas enviadas está incluída em duas tarefas padrão:

  - Exibir minhas tarefas enviadas

    Permite que os administradores pesquisem e exibam informações sobre as tarefas que eles enviaram para processamento.

  - Exibir tarefas enviadas

    Permite que os administradores pesquisem e exibam informações sobre as tarefas que outros administradores enviaram para processamento.

- **Guia Histórico do usuário**

  Esta guia, que pode ser adicionada às tarefas do usuário, como Exibir e Modificar usuário, permite que os administradores exibam as seguintes informações para um usuário selecionado:

  - Tarefas executadas no usuário
  - Tarefas executadas pelo usuário
  - Aprovações de fluxo de trabalho pelo usuário

- **Relatórios**

  Os relatórios do CA Identity Manager permitem ver o estado atual de um ambiente do CA Identity Manager. Você pode usar essas informações para assegurar a conformidade com as políticas de negócios internas ou com os regulamentos externos.

  Geração de relatórios (na página 399) apresenta mais informações sobre como configurar e usar os relatórios.

- **Logs**

  Exibem informações sobre todos os componentes em uma instalação do CA Identity Manager e fornecem detalhes sobre todas as operações do CA Identity Manager.

  Consulte o *Guia de Configuração* para obter mais informações sobre os logs do CA Identity Manager.

Como o CA Identity Manager determina o status da tarefa

Uma *tarefa* é uma função administrativa que um usuário pode executar no CA Identity Manager. As tarefas incluem os *eventos*, que são ações que o CA Identity Manager executa para concluir a tarefa. Uma tarefa pode incluir vários eventos. Por exemplo, a tarefa Criar usuário pode incluir eventos que criam o perfil do usuário, adicionam o usuário a um grupo e atribuem funções.

As tarefas e eventos do CA Identity Manager podem ser associados a um processo de fluxo de trabalho, que determina como o CA Identity Manager executa as ações necessárias e outras lógicas de negócios personalizadas. Tarefas também podem ser associadas a outras tarefas, chamadas de tarefas aninhadas. Nesse caso, o CA Identity Manager processa as tarefas aninhadas com a tarefa original.

O status de uma tarefa depende do status de seus eventos, processos de fluxo de trabalho, tarefas aninhadas e lógicas de negócios personalizadas associadas.

Exibir tarefas enviadas

O CA Identity Manager inclui um recurso Exibir tarefas enviadas que fornece informações sobre as tarefas em um ambiente do CA Identity Manager. Você pode usar esse recurso para pesquisar e exibir detalhes de alto nível sobre as ações que o CA Identity Manager executa. As telas de detalhes fornecem informações adicionais sobre cada tarefa e evento.

Dependendo do status da tarefa, é possível usar Exibir tarefas enviadas para cancelar ou reenviar uma tarefa.

Exibir tarefas enviadas permite controlar o processamento de uma tarefa do início ao fim. Por exemplo, se uma tarefa do CA Identity Manager incluir a atribuição de uma função de provisionamento e essa atribuição acionar a criação de contas em outros sistemas, a guia Exibir tarefas enviadas exibirá todos os detalhes da tarefa original e os detalhes da criação de contas.

Exibir tarefas enviadas inclui detalhes sobre as operações realizadas no sistema. Essas operações podem ser resultado de um evento do CA Identity Manager, como EnableUserEvent. As notificações enviadas pelo sistema são agrupadas nesse evento. Exibir tarefas enviadas exibe uma mensagem indicando que as notificações estão Em andamento até que a notificação End Detail seja enviada. Em seguida, a mensagem é alterada para Concluído.

Por padrão, o CA Identity Manager inclui a guia Exibir tarefas enviadas em duas tarefas:

- Exibir tarefas enviadas
- Exibir minhas tarefas enviadas

Pesquisar tarefas enviadas

Execute as etapas a seguir para pesquisar as tarefas enviadas.

Para pesquisar tarefas enviadas

1. Clique em Sistema, Exibir tarefas enviadas.

   A página Exibir tarefas enviadas é exibida.

2. Especifique os critérios de pesquisa, digite o número de linhas a serem exibidas e clique em Pesquisar.

   As tarefas que atenderem seus critérios de pesquisa são exibidas.

   Observação: para obter mais informações sobre como especificar atributos nos critérios de pesquisa, consulte Atributos de pesquisa para exibição de tarefas enviadas (na página 568).

Atributos de pesquisa para exibição de tarefas enviadas

Para analisar as tarefas que foram enviadas para processamento, é possível usar o recurso de pesquisa em Exibir tarefas enviadas. É possível pesquisar as tarefas com base nos seguintes critérios:

Iniciado por

Identifica o nome do usuário que iniciou uma tarefa conforme os critérios da pesquisa. As pesquisas tem como base o nome de usuário. Para certificar-se de ter inserido um nome de usuário válido, use o botão Validar.

Tarefas de aprovação executadas por

Identifica o nome do aprovador da tarefa conforme os critérios da pesquisa. As pesquisas tem como base o nome de usuário. Para certificar-se de ter inserido um nome de usuário válido, use o botão Validar.

Observação: caso tenha selecionado o critério Tarefas de aprovação realizadas por para filtrar as tarefas, o critério Mostrar tarefas de aprovação também é ativado por padrão.

Nome da tarefa

Identifica o nome da tarefa conforme os critérios da pesquisa. É possível refinar a pesquisa especificando condições como igual a, contém, começa com ou termina com o valor do campo Onde o nome da tarefa. Por exemplo, é possível especificar o critério de pesquisa "nome da tarefa igual a Criar usuário" selecionando a condição igual e inserindo Criar usuário no campo de texto.

Status da tarefa

Identifica o status da tarefa conforme os critérios da pesquisa. É possível selecionar o status da tarefa, ativando a opção Onde o status da tarefa é igual a e selecionando a condição. É possível refinar ainda mais a pesquisa com base nas seguintes condições:

- Concluído
- Em andamento
- Com falha
- Recusado
- Parcialmente concluído
- Cancelado
- Programado

Observação: consulte Descrição do status da tarefa (na página 570) para obter mais informações.

Prioridade da tarefa

Identifica a prioridade da tarefa conforme os critérios da pesquisa. É possível selecionar a prioridade da tarefa, ativando a opção Onde a prioridade da tarefa é igual a e selecionando a condição. É possível refinar ainda mais a pesquisa com base nas seguintes condições:

Baixa

Especifica que é possível pesquisar tarefas com prioridade baixa.

Média

Especifica que é possível pesquisar tarefas com prioridade média.

Alta

Especifica que é possível pesquisar tarefas com prioridade alta.

Realizado em

Identifica as tarefas realizadas na instância selecionada do objeto. Se você não selecionar uma instância do objeto, serão exibidas as tarefas executadas em todas as instâncias do objeto.

Observação: esse campo é exibido apenas quando o campo Configuração realizada em estiver preenchido na tela Configurar tarefas enviadas. Use esta tela para configurar a guia Tarefas enviadas. Consulte a ajuda online da tela para obter mais informações.

Intervalo de datas

Identifica o intervalo de datas desejado para pesquisar as tarefas enviadas. É preciso fornecer as datas nos campos De e Até.

Mostrar tarefas não enviadas

Identifica as tarefas no estado Auditado. Identifica as tarefas que já iniciaram outras tarefas ou tarefas que não foram enviadas. Todas essas tarefas serão auditadas e exibidas se essa guia for selecionada.

Mostrar tarefas de aprovação

Identifica as tarefas que precisam ser aprovadas como parte de um fluxo de trabalho.

Pesquisar arquivo morto de tarefas enviadas

Identifica as tarefas enviadas que foram arquivadas.

Mais informações:

Descrição do status da tarefa (na página 570)

Descrição do status da tarefa

As tarefas enviadas existem em um dos estados descritos abaixo. Com base no estado da tarefa, é possível executar ações como cancelar ou reenviar uma tarefa.

Observação: para cancelar ou reenviar uma tarefa, é preciso configurar Exibir tarefas enviadas para exibir os botões de cancelamento e reenvio com base no status das tarefas. Para obter mais informações sobre como cancelar e reenviar tarefas, consulte Personalizar a guia Exibir tarefas enviadas (na página 573).

Em andamento

Exibido mediante uma das seguintes ocorrências:

- O fluxo de trabalho foi iniciado, mas ainda não foi concluído
- As tarefas iniciadas antes das tarefas atuais estão em andamento
- As tarefas aninhadas foram iniciadas, mas ainda não foram concluídas
- O evento principal foi iniciado, mas ainda não foi concluído
- Os eventos secundários foram iniciados, mas ainda não foram concluídos

É possível cancelar uma tarefa neste estado.

Observação: o cancelamento de uma tarefa irá cancelar todas as tarefas incompletas aninhadas, bem como os eventos para a tarefa atual.

Cancelado

Exibido mediante o cancelamento de todas as tarefas ou eventos em andamento.

Recusado

Exibido quando o CA Identity Manager recusa um evento ou tarefa que faça parte de um processo de fluxo de trabalho. É possível reenviar uma tarefa recusada.

Observação: ao reenviar uma tarefa, o CA Identity Manager irá reenviar todos os eventos e tarefas aninhadas com falha ou recusados.

Parcialmente concluído

Exibido mediante o cancelamento de alguns eventos ou tarefas aninhadas. É possível reenviar um evento ou tarefa aninhada parcialmente concluídos.

Concluído

Exibido quando uma tarefa é concluída. Uma tarefa é considerada concluída quando as tarefas e os eventos aninhados da tarefa atual tiverem sido concluídos.

Com falha

Exibido quando uma tarefa, tarefa aninhada ou evento aninhado na tarefa atual são inválidos. Este status é exibido quando a tarefa falha. É possível reenviar uma tarefa com falha.

Programado

Exibido quando a tarefa está programada para execução em uma data posterior. É possível cancelar uma tarefa neste estado.

Auditado

Exibido quando a tarefa atual é auditada.

Exibir detalhes de tarefas

O CA Identity Manager fornece detalhes sobre as tarefas, tais como o status de uma tarefa enviada, as tarefas aninhadas e os eventos associados a ela.

Para exibir os detalhes de uma tarefa enviada

1. Clique no ícone em forma de seta para a direita, ao lado da tarefa selecionada, na guia Exibir tarefas enviadas.

   Os detalhes da tarefa são exibidos.

   Observação: eventos e tarefas aninhadas (se houver) são exibidos na página Detalhes da tarefa. É possível exibir os detalhes da tarefa para cada uma das tarefas e eventos.

2. Clique em Fechar.

   A guia Detalhes da tarefa é fechada e o CA Identity Manager exibe a guia Exibir tarefas enviadas com a lista de tarefas.

Exibir detalhes de eventos

O CA Identity Manager fornece detalhes sobre os eventos, tais como o status de um evento enviado, os atributos do evento e qualquer informação adicional sobre os eventos.

Para exibir os detalhes de um evento enviado

1. Clique no ícone em forma de seta para a direita, ao lado de um evento, na página Exibir os detalhes da tarefa.

   Os detalhes do evento são exibidos.

2. Clique em Fechar.

   A página Detalhes do evento é fechada.

Descrição do status do evento

Os eventos no CA Identity Manager podem estar em um dos estados descritos abaixo. Com base no status do evento, é possível cancelar ou reenviar um evento para execução.

Observação: para permitir que os administradores cancelem ou reenviem um evento, é preciso configurar Exibir tarefas enviadas para exibir os botões de cancelamento e reenvio de eventos. Ao configurar a tarefa, você pode especificar quais administradores podem cancelar e reenviar eventos. Para obter mais informações sobre como cancelar e reenviar eventos, consulte Personalizar a guia Exibir tarefas enviadas (na página 573).

Em andamento

Exibido mediante uma das seguintes ocorrências:

- Fluxo de trabalho ou pré-eventos iniciados, em andamento ou aprovados
- O CA Identity Manager está executando o evento
- O CA Identity Manager executa pós-eventos

É possível cancelar um evento neste estado.

Recusado

Exibido quando o CA Identity Manager recusa um evento que faz parte do fluxo de trabalho. É possível reenviar um evento recusado.

Cancelado

Exibido mediante o cancelamento de algum dos eventos em andamento. É possível reenviar um evento cancelado.

Concluído

Exibido quando um evento é concluído.

Com falha

Exibido quando o CA Identity Manager encontra uma exceção durante a execução de um evento. É possível reenviar um evento cancelado.

Observação: não é possível reenviar um evento secundário até que o evento principal esteja no estado concluído.

Programado

Exibido quando o evento está programado para execução em uma data posterior. É possível cancelar um evento neste estado.

Auditado

Exibido quando o evento atual é auditado.

Personalizar a guia Exibir tarefas enviadas

Você pode personalizar a guia Exibir tarefas enviadas da seguinte maneira:

- Especifique outro nome de tarefa e tag.
- Altere as propriedades de exibição padrão. Quando instalada, os usuários verão uma tela de pesquisa na qual é possível inserir os critérios que determinam as tarefas que aparecem na guia. Você pode configurar a guia para exibir automaticamente as tarefas enviadas em um dia atual, evitando que os usuários precisem digitar critérios de pesquisa.
- Determine se os eventos de auditoria serão exibidos na página Detalhes da tarefa.
- Adicione outra coluna à exibição de tarefa.
- Especifique os critérios para cancelar ou reenviar tarefas e eventos.

Observação: determinados detalhes de tarefas e eventos podem incluir dados, como salários ou senhas, que não devem ser exibidos em texto não criptografado na guia Exibir tarefas enviadas. É possível ocultar esses atributos, especificando parâmetros de classificação de dados ao definir os atributos no arquivo directory.xml. Para obter mais informações sobre o arquivo directory.xml, consulte o *Guia de Configuração*.

Você pode configurar a guia Exibir tarefas enviadas modificando a tarefa administrativa correspondente.

Para configurar a guia Exibir tarefas enviadas:

1. Clique em Funções e tarefas, Tarefa administrativa, Modificar tarefa administrativa.

   A página Selecionar tarefa administrativa é exibida.

2. Selecione Nome ou Categoria no campo de onde Pesquisar tarefas administrativas e, em seguida, digite a sequência de caracteres que deseja pesquisar e clique em Pesquisar.

   O CA Identity Manager exibe as tarefas administrativas que atendem aos critérios de pesquisa.

3. Selecione Exibir tarefas enviadas e clique em Selecionar.

   O CA Identity Manager exibe os detalhes da tarefa administrativa Exibir tarefas enviadas.

4. Clique na guia Guias.

   As guias que são usadas para a guia Exibir tarefas enviadas são exibidas.

5. Clique no ícone em forma de seta para a direita para editar a guia Tarefas enviadas.

   Os detalhes da guia são exibidos.

6. Edite os campos para personalizar a guia Exibir tarefas enviadas, conforme necessário. Consulte Definições de configuração para a guia Tarefas enviadas (na página 574).

Definições de configuração para a guia Exibir tarefas enviadas

Use os campos a seguir para alterar a aparência e a funcionalidade da guia Exibir tarefas enviadas.

Nome

Define o nome da tarefa.

Qualificador

Define um identificador exclusivo para a tarefa. É usada em URLs, serviços web ou arquivos de propriedades. Deve consistir em letras, números ou sublinhados, começando com uma letra ou sublinhado.

Ocultar guia

Identifica que a guia é exibida para os usuários, mas não será executada. Se você selecionar essa opção, o CA Identity Manager exibirá uma mensagem de erro para os usuários.

Mostrar lista de tarefas ao carregar

Exibe as tarefas que foram enviadas para o dia atual.

Observação: se a opção tiver sido ativada, os usuários que clicarem em Exibir tarefas enviadas poderão ver diretamente as tarefas que foram enviadas no mesmo dia.

Mostrar eventos de auditoria

Especifica se eventos de auditoria estão incluídos em tarefas na página Exibir tarefas enviadas.

Permitir coluna personalizada

Indica que você pode acrescentar uma coluna personalizada à tabela de tarefas que pode ser visualizada na guia Exibir tarefas enviadas e na guia Histórico do usuário. Por exemplo, você pode acrescentar uma coluna "ID de usuário" à tabela de tarefas que é exibida na guia Histórico do usuário.

Título da coluna personalizada

Indica o nome de exibição da coluna personalizada.

Atributo da coluna personalizada

Indica o atributo que será usado para preencher a coluna personalizada na tabela de tarefas. Por exemplo, se você estiver procurando tarefas que são realizadas em funcionários de uma organização, pode acrescentar uma coluna que exiba a organização para cada um dos funcionários.

Cancelar tarefas e eventos

Identifica os critérios para cancelamento de tarefas ou eventos. Você pode definir o escopo deste campo selecionando uma das seguintes opções:

O criador da tarefa deve ser o usuário atual

Identifica que você pode cancelar ou reenviar tarefas ou eventos que você criou.

O criador da tarefa deve estar no escopo

Identifica que você pode cancelar ou reenviar as tarefas que foram iniciadas por outros usuários que atenderem às regras de escopo do usuário para a função administrativa que fornece acesso à guia.

Por exemplo, se você recebeu a função Gerenciador de usuários, que inclui Exibir tarefas enviadas, por ter atendido aos critérios em uma regra de associação que inclui o escopo de todos os usuários na organização do funcionário. Você pode cancelar ou reenviar tarefas que foram enviadas por todos os usuários na organização do funcionário.

Sem restrições

Identifica que qualquer usuário poderá cancelar ou reenviar uma tarefa ou evento.

Não permitido

Especifica que uma tarefa ou evento não pode ser cancelado ou reenviado.

Reenviar tarefas e eventos

Identifica os critérios para reenviar uma tarefa ou evento. Você pode definir o escopo deste campo selecionando uma das seguintes opções:

O criador da tarefa deve ser o usuário atual

Identifica que você pode cancelar ou reenviar tarefas ou eventos que você criou.

O criador da tarefa deve estar no escopo

Identifica que você pode cancelar ou reenviar as tarefas que foram iniciadas por outros usuários que atenderem às regras de escopo do usuário para a função administrativa que fornece acesso à guia.

Por exemplo, se você recebeu a função Gerenciador de usuários, que inclui Exibir tarefas enviadas, por ter atendido aos critérios em uma regra de associação que inclui o escopo de todos os usuários na organização do funcionário. Você pode cancelar ou reenviar tarefas que foram enviadas por todos os usuários na organização do funcionário.

Sem restrições

Identifica que qualquer usuário poderá cancelar ou reenviar uma tarefa ou evento.

Não permitido

Especifica que uma tarefa ou evento não pode ser cancelado ou reenviado.

Guia Histórico do usuário

A guia Histórico do usuário permite exibir as tarefas que estão relacionadas a um usuário. Os detalhes da tarefa que são exibidos nessa guia também podem ser visualizados na guia Exibir tarefas enviadas.

Observação: não é possível adicionar essa guia para criar tarefas, como Criar usuário.

Você pode usar essa guia para visualizar um histórico das seguintes tarefas:

- **Tarefas executadas no usuário**

  Exibe todas as tarefas que são executadas no usuário selecionado.

- **Tarefas executadas pelo usuário**

  Exibe todas as tarefas que são executadas pelo usuário selecionado.

- **Aprovações de fluxo de trabalho pelo usuário**

  Exibe todas as tarefas que o usuário aprovou como parte de um fluxo de trabalho.

Observação: o tipo de tarefa que pode ser exibido nessa guia depende da configuração da guia. Personalizar a guia Histórico do usuário (na página 578) fornece mais informações.

Atributos de pesquisa para exibição de histórico do usuário

Para analisar as tarefas que foram enviadas para processamento, é possível usar o recurso de pesquisa em Exibir tarefas enviadas. É possível pesquisar as tarefas com base nos seguintes critérios:

Nome da tarefa

Identifica o nome da tarefa conforme os critérios da pesquisa. É possível refinar a pesquisa especificando condições como igual a, contém, começa com ou termina com o valor do campo Onde o nome da tarefa. Por exemplo, é possível especificar o critério de pesquisa nome da tarefa igual a Criar usuário, selecionando a condição igual e inserindo Criar usuário no campo de texto.

Status da tarefa

Identifica o status da tarefa conforme os critérios da pesquisa. É possível selecionar o status da tarefa, ativando a opção Onde o status da tarefa é igual a e selecionando a condição. É possível refinar ainda mais a pesquisa com base nas seguintes condições:

- Concluído
- Em andamento
- Com falha
- Recusado
- Parcialmente concluído
- Cancelado
- Programado

Observação: consulte Descrição do status da tarefa (na página 570) para obter mais informações.

Prioridade da tarefa

Identifica a prioridade da tarefa conforme os critérios da pesquisa. É possível selecionar a prioridade da tarefa, ativando a opção Onde a prioridade da tarefa é igual a e selecionando a condição. É possível refinar ainda mais a pesquisa com base nas seguintes condições:

Baixa

Especifica que é possível pesquisar tarefas com prioridade baixa.

Média

Especifica que é possível pesquisar tarefas com prioridade média.

Alta

Especifica que é possível pesquisar tarefas com prioridade alta.

Intervalo de datas

Identifica o intervalo de datas desejado para pesquisar as tarefas enviadas. É preciso fornecer as datas nos campos De e Até.

Personalizar a guia Histórico do usuário

Os administradores podem personalizar a guia Histórico do usuário da seguinte maneira:

- Especifique outro nome de tarefa e tag.
- Altere as propriedades de exibição padrão. Por padrão, os usuários podem inserir critérios que determinam quais tarefas são exibidas na guia. Os administradores podem configurar a guia para exibir automaticamente as tarefas de um dia atual, evitando que os usuários precisem digitar critérios de pesquisa.
- Determine se os eventos de auditoria serão exibidos na página Detalhes da tarefa.
- Adicione uma coluna à exibição de tarefa.
- Especifique os critérios para cancelar ou reenviar tarefas e eventos.

Siga estas etapas:

1. Vá para Funções e tarefas, Tarefas administrativas, Gerenciar tarefas administrativas.

   A página Selecionar tarefa administrativa é exibida.

2. Selecione Nome ou Categoria no campo de onde Pesquisar tarefas administrativas e, em seguida, digite a sequência de caracteres que deseja pesquisar e clique em Pesquisar.

   O CA Identity Manager exibe as tarefas administrativas que atendem aos critérios de pesquisa.

3. Selecione a tarefa que inclui a guia Histórico do usuário e clique em Selecionar.

   O CA Identity Manager exibe os detalhes da tarefa para a tarefa administrativa.

4. Clique na guia Guias.

5. Clique no ícone Editar ao lado da guia Histórico do usuário.

   Os detalhes da guia são exibidos.

6. Edite os campos para personalizar a guia Histórico do usuário.

Definições de configuração para a guia Histórico do usuário

Use os campos a seguir para alterar a aparência e a funcionalidade da guia Histórico do usuário.

Nome

Define o nome da tarefa.

Qualificador

Define um identificador exclusivo para a tarefa. É usada em URLs, serviços web ou arquivos de propriedades. Deve consistir em letras, números ou sublinhados, começando com uma letra ou sublinhado.

Ocultar guia

Identifica que a guia é exibida para os usuários, mas não será executada. Se você selecionar essa opção, o CA Identity Manager exibirá uma mensagem de erro para os usuários.

Mostrar lista de tarefas ao carregar

Exibe as tarefas que foram enviadas para o dia atual.

Observação: se a opção tiver sido ativada, os usuários que clicarem em Exibir tarefas enviadas poderão ver diretamente as tarefas que foram enviadas no mesmo dia.

Mostrar eventos de auditoria

Especifica se eventos de auditoria estão incluídos em tarefas na página Exibir tarefas enviadas.

Permitir coluna personalizada

Indica que você pode acrescentar uma coluna personalizada à tabela de tarefas que pode ser visualizada na guia Exibir tarefas enviadas e na guia Histórico do usuário. Por exemplo, você pode acrescentar uma coluna "ID de usuário" à tabela de tarefas que é exibida na guia Histórico do usuário.

Título da coluna personalizada

Indica o nome de exibição da coluna personalizada.

Atributo da coluna personalizada

Indica o atributo que será usado para preencher a coluna personalizada na tabela de tarefas. Por exemplo, se você estiver procurando tarefas que são realizadas em funcionários de uma organização, pode acrescentar uma coluna que exiba a organização para cada um dos funcionários.

Cancelar tarefas e eventos

Identifica os critérios para cancelamento de tarefas ou eventos. Você pode definir o escopo deste campo selecionando uma das seguintes opções:

O criador da tarefa deve ser o usuário atual

Identifica que você pode cancelar ou reenviar tarefas ou eventos que você criou.

O criador da tarefa deve estar no escopo

Identifica que você pode cancelar ou reenviar as tarefas que foram iniciadas por outros usuários que atenderem às regras de escopo do usuário para a função administrativa que fornece acesso à guia.

Por exemplo, se você recebeu a função Gerenciador de usuários, que inclui Exibir tarefas enviadas, por ter atendido aos critérios em uma regra de associação que inclui o escopo de todos os usuários na organização do funcionário. Você pode cancelar ou reenviar tarefas que foram enviadas por todos os usuários na organização do funcionário.

Sem restrições

Identifica que qualquer usuário poderá cancelar ou reenviar uma tarefa ou evento.

Não permitido

Especifica que uma tarefa ou evento não pode ser cancelado ou reenviado.

Reenviar tarefas e eventos

Identifica os critérios para reenviar uma tarefa ou evento. Você pode definir o escopo deste campo selecionando uma das seguintes opções:

O criador da tarefa deve ser o usuário atual

Identifica que você pode cancelar ou reenviar tarefas ou eventos que você criou.

O criador da tarefa deve estar no escopo

Identifica que você pode cancelar ou reenviar as tarefas que foram iniciadas por outros usuários que atenderem às regras de escopo do usuário para a função administrativa que fornece acesso à guia.

Por exemplo, se você recebeu a função Gerenciador de usuários, que inclui Exibir tarefas enviadas, por ter atendido aos critérios em uma regra de associação que inclui o escopo de todos os usuários na organização do funcionário. Você pode cancelar ou reenviar tarefas que foram enviadas por todos os usuários na organização do funcionário.

Sem restrições

Identifica que qualquer usuário poderá cancelar ou reenviar uma tarefa ou evento.

Não permitido

Especifica que uma tarefa ou evento não pode ser cancelado ou reenviado.

Mostrar tarefas

Determina as tarefas que são exibidas na guia Histórico do usuário.

Tarefas executadas no usuário

Exibe todas as tarefas que são executadas no usuário selecionado.

Tarefas executadas pelo usuário

Exibe todas as tarefas que são executadas pelo usuário selecionado.

Aprovações de fluxo de trabalho pelo usuário

Exibe todas as tarefas que o usuário aprovou como parte de um fluxo de trabalho.

A tarefa Exibir a atividade do usuário

A atividade do usuário é um histórico das tarefas que envolvem um usuário específico. Os administradores podem usar a tarefa Exibir a atividade do usuário para acompanhar as seguintes informações do usuário:

- Tarefas executadas no usuário
- Tarefas executadas pelo usuário
- Aprovações de fluxo de trabalho executadas pelo usuário

Para exibir a atividade do usuário

1. Vá para Usuários, Gerenciar usuários, Exibir a atividade do usuário.

   A tela Selecionar usuário é exibida.

2. Procure um usuário e clique em Selecionar.

   A tela Exibir a atividade do usuário é exibida.

Observação: para obter mais informações sobre a atividade do usuário exibida, consulte a Ajuda online do console de usuário.

Limpar tarefas enviadas

Com cada tarefa enviada, o desempenho de tempo de execução de tarefas e eventos fica mais lento, à medida que o banco de dados de persistência de tarefas aumenta. A coleta de lixo dos procedimentos armazenados reduz o potencial de problemas de desempenho e falhas de sistema, pois o espaço de armazenamento do banco de dados de persistência fica cada vez menor. A capacidade de arquivar as tarefas oferece ao administrador a capacidade de exibir as informações atuais de eventos e tarefas, bem como tarefas e eventos que foram excluídos.

No console de usuário, os administradores do CA Identity Manager podem programar tarefas para realizar automaticamente a coleta de lixo e o arquivamento repetidamente.

Guia Recorrência

Use essa guia para programar sua tarefa. Os campos nesta guia são os seguintes:

Executar agora

Executa a tarefa imediatamente.

Programar nova tarefa

Programa uma nova tarefa.

Modificar a tarefa existente

Especifica que você deseja modificar uma tarefa que já existe.

Observação: esse campo aparece apenas se uma tarefa já tiver sido programada para essa tarefa.

Nome da tarefa

Especifica o nome da tarefa que você deseja criar ou modificar.

Fuso horário

Especifica o fuso horário do servidor.

Observação: se o seu fuso horário for diferente do fuso horário do servidor, uma caixa suspensa será exibida para que você possa escolher entre o seu fuso horário ou o do servidor ao programar uma nova tarefa. Não é possível alterar o fuso horário ao modificar uma tarefa existente.

Programação diária

Especifica que a tarefa é executada a cada número determinado de dias.

A cada (número de dias)

Define o número de dias entre as execuções da tarefa.

Programação semanal

Especifica que a tarefa é executada em um ou mais dias e hora específicos durante uma semana.

Dia da semana

Especifica os dias da semana em que a tarefa é executada.

Programação mensal

Especifica um dia da semana ou dia do mês em que a tarefa é executada mensalmente.

Programação anual

Especifica um dia da semana ou dia do mês em que a tarefa é executada anualmente.

Programação avançada

Especifica informações adicionais de programação.

Expressão cron

Para obter informações sobre como preencher esse campo, consulte o seguinte:

http://quartz-scheduler.org/api/2.1.0/org/quartz/CronExpression.html

Hora da execução

Especifica a hora do dia, no formato de 24 horas, em que a tarefa é executada. Por exemplo, 14h15.

Executar uma tarefa agora

Para executar uma tarefa imediatamente, use o assistente Limpar tarefas enviadas.

Siga estas etapas:

1. Vá para Sistema, Limpar tarefas enviadas.

   A etapa Recorrência do assistente é exibida.

2. Selecione Executar agora e Avançar.

   A etapa Limpar tarefas enviadas do assistente é exibida.

3. Insira as informações de duração mínima, arquivamento, tempo limite da auditoria, limite de tempo e limite de tarefas, e clique em Finalizar.

   A tarefa é enviada imediatamente.

Programar uma nova tarefa

Para programar uma nova tarefa, use o assistente Limpar tarefas enviadas.

Siga estas etapas:

1. Vá para Sistema, Limpar tarefas enviadas.

   A etapa Recorrência é exibida.

2. Selecione Programar nova tarefa, digite o nome da tarefa e informações de programação para a tarefa e clique em Avançar.

   A etapa Limpar tarefas enviadas é exibida.

3. Insira as informações de duração mínima, arquivamento, tempo limite da auditoria, limite de tempo e limite de tarefas, e clique em Finalizar.

   A nova tarefa é programada.

Modificar uma tarefa existente

Para modificar uma tarefa existente, use o assistente Limpar tarefas enviadas.

Siga estas etapas:

1. Vá para Sistema, Limpar tarefas enviadas.

   A etapa Recorrência é exibida.

2. Selecione Modificar a tarefa existente e escolha uma tarefa existente, modifique as informações de programação e clique em Avançar.

   A etapa Limpar tarefas enviadas é exibida.

3. Modifique as informações de duração mínima, arquivamento, tempo limite da auditoria, limite de tempo e limite de tarefas, e clique em Finalizar.

   A tarefa existente é modificada.

Excluir uma tarefa recorrente

Para excluir uma tarefa recorrente, siga este procedimento.

Siga estas etapas:

1. Vá para Sistema, Selecione excluir tarefa recorrente.
2. Selecione a tarefa a ser excluída.
3. Clique em Enviar.

Guia Limpar tarefas enviadas

Use essa guia para especificar a duração mínima, o arquivamento, o tempo limite da auditoria, o limite de tempo e o limite de tarefas da tarefa. Clique em Finalizar depois de preencher todos os campos obrigatórios. Os campos nesta guia são os seguintes:

Duração mínima

Especifica a duração mínima das tarefas em um estado final (Concluído, Com falha, Recusado ou Cancelado) para limpeza. Por exemplo, se 1 mês for especificado, qualquer tarefa que tiver atingido um estado final no mês passado será mantida. As tarefas que tiverem atingido o estado final mais de um mês atrás estarão sujeitas à limpeza e arquivamento.

Esse é um campo obrigatório.

Arquivar

Faz backup de tarefas para o banco de dados de arquivamento antes de excluí-las do banco de dados de tempo de execução.

Depois de executar a tarefa, se arquivar estiver selecionado, os dados serão salvos no banco de dados de arquivamento e removidos do banco de dados de persistência da tarefa de tempo de execução. Os dados não são excluídos até que sejam confirmados com êxito no banco de dados de arquivamento.

Tempo limite da auditoria

Especifica o período de espera até que as tarefas em estado de auditoria sejam limpas. As tarefas no estado de auditoria não são consideradas em um estado final até que esse período de espera tenha passado. As tarefas no estado de auditoria não foram enviadas.

Limite de tempo

Limita a limpeza a um período específico.

Limite da tarefa

Limita a limpeza a um número de tarefas específico.

Excluir tarefas recorrentes

Quando uma tarefa não precisa mais ser executada repetidamente, o administrador do CA Identity Manager tem a capacidade de excluí-la. Depois que a tarefa for excluída, a coleta de lixo e o arquivamento não serão executados para essa tarefa.

Todas as tarefas programadas usando o assistente de Limpar tarefas enviadas: Recorrência são listadas nessa página, e o administrador do CA Identity Manager pode escolher quais tarefas deseja excluir.

Observação: as tarefas ainda ficam presentes no banco de dados, apenas a recorrência de programação é excluída.

Configurar a conexão do Enterprise Log Manager

Use esta tela para gerenciar tarefas de conexão do CA User Activity Reporting (CA UAR) recém-adicionadas.

Observação: o CA Enterprise Log Manager foi renomeado. Agora, se chama CA UAR.

Os campos dessa tela são listados abaixo:

Nome da conexão

Especifica o nome exclusivo usado para o único objeto gerenciado de conexão do CA UAR.

Esse é um campo somente leitura.

Descrição

Descreve a conexão do CA UAR.

Nome do host

Especifica o nome do host de servidor ou o endereço IP do CA UAR.

Esse é um campo obrigatório.

Porta nº

Especifica a porta de conexão do servidor do CA UAR.

Padrão: 52520

Esse é um campo obrigatório.

Certificado SSL assinado por autoridade de certificação

Quando marcada, essa opção especifica uma verificação rígida de certificado SSL durante a conexão com um servidor do CA UAR.

Se você tiver um certificado SSL autoassinado, por exemplo, um instalado com o CA UAR por padrão, essa caixa de seleção não deve ser marcada, pois o caminho confiável para a autoridade de certificação raiz não existe.

Nome do certificado

Especifica o nome do certificado do CA UAR a ser usado na autenticação.

Esse é um campo obrigatório.

Senha do certificado

Especifica a senha do CA UAR.

Esse é um campo obrigatório.

Atributo

Não suportado. A versão é recuperada em uma tentativa de salvar informações de conexão como um teste.

Excluir a conexão do Enterprise Log Manager

Selecione uma conexão na lista e clique em Excluir. A conexão do CA UAR é excluída.

Gerenciar chaves secretas

Usar chaves secretas para gerenciar chaves dinâmicas que criptografam ou descriptografam dados. Se houver a suspeita de que um usuário obteve acesso não autorizado a uma chave, é possível alterar a senha do keystore. O keystore é o banco de dados que armazena chaves secretas. Depois de alterar essa senha, o <idmgr> criptografa novamente os valores das chaves.

Cada ambiente tem um conjunto de chaves dinâmicas e uma senha do keystore. Se ambientes compartilharem um diretório de usuários, use as mesmas chaves dinâmicas e senha do keystore para cada ambiente.

As senhas do keystore são criptografadas usando chaves incorporadas no código de criptografia ou os parâmetros que são inseridos durante a instalação do servidor do CA Identity Manager. Em um agrupamento, todos os nós compartilham os valores de chaves dinâmicas e a senha do keystore.

As operações de criptografia usam a chave dinâmica mais recente para o algoritmo e ambiente correspondentes. As operações de descriptografia verificam se uma ID de chave existe nos dados criptografados, de modo que a chave correta seja usada. A seção Formatos de texto criptografado do *Guia de Configuração* fornece mais detalhes.

Siga estas etapas:

1. Digite ou modifique a senha do keystore.
2. Clique em Adicionar uma chave caso precise de outra chave.
3. Selecione um algoritmo.
4. Digite uma senha para a chave.

   Para PBE e RC2, o comprimento máximo da chave é de 128 bytes.

   Para AES, os tamanhos de chave válidos são 16, 24 e 32 bytes.
5. Clique em Submit.
6. Se você tiver modificado a Senha do keystore, clique em Enviar.

   O CA Identity Manager criptografa os valores das chaves novamente.

Capítulo 20: Persistência de tarefas

Esta seção contém os seguintes tópicos:

Arquivamento e coleta de lixo da persistência de tarefa automatizada

Nessa release, um administrador pode programar e modificar tarefas com parâmetros específicos usando a tarefa Limpar tarefas enviadas para limpar e arquivar informações de eventos e tarefas no banco de dados de persistência de tarefas, bem como excluir essas tarefas recorrentes conforme a necessidade.

Na guia Sistema, você pode iniciar o assistente selecionando Limpar tarefas enviadas. O assistente guia você pela configuração e programação de tarefas, bem como pelo processo de arquivar ou não os dados. Você também pode optar por excluir as tarefas recorrentes quando necessário, selecionando Excluir tarefas recorrentes na guia Sistema.

Ao programar as tarefas para limpar e arquivar dados de tarefa, a possibilidade de problemas de desempenho ou interrupções do sistema é enormemente reduzida. Com o recurso de arquivamento, é possível fazer backup de tarefas no banco de dados de arquivamento antes de excluí-las do banco de dados de tempo de execução. Se você precisar voltar e exibir essas tarefas excluídas, marque a caixa de seleção Search the archive em Exibir tarefas enviadas para procurar e exibir uma lista de todas as tarefas que foram excluídas e arquivadas.

Guia Recorrência

Use essa guia para programar sua tarefa. Os campos nesta guia são os seguintes:

Executar agora

Executa a tarefa imediatamente.

Programar nova tarefa

Programa uma nova tarefa.

Modificar a tarefa existente

Especifica que você deseja modificar uma tarefa que já existe.

Observação: esse campo será exibido apenas se um tarefa já tiver sido programada.

Nome da tarefa

Especifica o nome da tarefa que você deseja criar ou modificar.

Fuso horário

Especifica o fuso horário do servidor.

Observação: se o seu fuso horário for diferente do fuso horário do servidor, uma caixa suspensa será exibida para que você possa escolher entre o seu fuso horário ou o do servidor ao programar uma nova tarefa. Não é possível alterar o fuso horário ao modificar uma tarefa existente.

Programação semanal

Especifica que a tarefa é executada dias e horas específicos durante uma semana.

Programação avançada

Especifica informações adicionais de programação.

Dia da semana

Especifica os dias da semana em que a tarefa é executada.

Hora da execução

Especifica a hora do dia, no formato de 24 horas, em que a tarefa é executada. Por exemplo, 14h15.

Expressão cron

Para obter informações sobre como preencher esse campo, consulte:

http://www.opensymphony.com/quartz/api/org/quartz/CronExpression.html

Observação: esse campo aparece quando a opção Programação avançada é selecionada.

Mais informações

Excluir uma tarefa recorrente (na página 585)
Programar uma nova tarefa (na página 584)
Modificar uma tarefa existente (na página 585)
Executar uma tarefa agora (na página 584)

Guia Limpar tarefas enviadas

Use essa guia para especificar a duração mínima, o arquivamento, o tempo limite da auditoria, o limite de tempo e o limite de tarefas da tarefa. Clique em Finalizar depois de preencher todos os campos obrigatórios. Os campos nesta guia são os seguintes:

Duração mínima

Especifica a duração mínima das tarefas em um estado final (Concluído, Com falha, Recusado ou Cancelado) para limpeza. Por exemplo, se 1 mês for especificado, qualquer tarefa que tiver atingido um estado final no mês passado será mantida. As tarefas que tiverem atingido o estado final mais de um mês atrás estarão sujeitas à limpeza e arquivamento.

Esse é um campo obrigatório.

Arquivar

Faz backup de tarefas para o banco de dados de arquivamento antes de excluí-las do banco de dados de tempo de execução.

Depois de executar a tarefa, se arquivar estiver selecionado, os dados serão salvos no banco de dados de arquivamento e removidos do banco de dados de persistência da tarefa de tempo de execução. Os dados não são excluídos até que sejam confirmados com êxito no banco de dados de arquivamento.

Tempo limite da auditoria

Especifica o período de espera até que as tarefas em estado de auditoria sejam limpas. As tarefas no estado de auditoria não são consideradas em um estado final até que esse período de espera tenha passado. As tarefas no estado de auditoria não foram enviadas.

Limite de tempo

Limita a limpeza a um período específico.

Limite da tarefa

Limita a limpeza a um número de tarefas específico.

Executar uma tarefa agora

Para executar uma tarefa imediatamente, use o assistente Limpar tarefas enviadas.

Siga estas etapas:

1. Vá para Sistema, Limpar tarefas enviadas.

   A etapa Recorrência do assistente é exibida.

2. Selecione Executar agora e Avançar.

   A etapa Limpar tarefas enviadas do assistente é exibida.

3. Insira as informações de duração mínima, arquivamento, tempo limite da auditoria, limite de tempo e limite de tarefas, e clique em Finalizar.

   A tarefa é enviada imediatamente.

Programar uma nova tarefa

Para programar uma nova tarefa, use o assistente Limpar tarefas enviadas.

Siga estas etapas:

1. Vá para Sistema, Limpar tarefas enviadas.

   A etapa Recorrência é exibida.

2. Selecione Programar nova tarefa, digite o nome da tarefa e informações de programação para a tarefa e clique em Avançar.

   A etapa Limpar tarefas enviadas é exibida.

3. Insira as informações de duração mínima, arquivamento, tempo limite da auditoria, limite de tempo e limite de tarefas, e clique em Finalizar.

   A nova tarefa é programada.

Modificar uma tarefa existente

Para modificar uma tarefa existente, use o assistente Limpar tarefas enviadas.

Siga estas etapas:

1. Vá para Sistema, Limpar tarefas enviadas.

   A etapa Recorrência é exibida.

2. Selecione Modificar a tarefa existente e escolha uma tarefa existente, modifique as informações de programação e clique em Avançar.

   A etapa Limpar tarefas enviadas é exibida.

3. Modifique as informações de duração mínima, arquivamento, tempo limite da auditoria, limite de tempo e limite de tarefas, e clique em Finalizar.

   A tarefa existente é modificada.

Excluir uma tarefa recorrente

Para excluir uma tarefa recorrente, siga este procedimento.

Siga estas etapas:

1. Vá para Sistema, Selecione excluir tarefa recorrente.
2. Selecione a tarefa a ser excluída.
3. Clique em Enviar.

Como migrar o banco de dados de persistência de tarefas

Nas releases anteriores, a migração era feita 'dinamicamente' e usando o Management Console. Uma ferramenta de migração de linha de comando foi fornecida para remover gargalos de desempenho ao migrar um grande volume de tarefas. Também é possível ajustar a migração para um ambiente específico, estado da tarefa, e as tarefas que foram criadas e executadas durante um intervalo de datas específico. A ferramenta de linha de comando, runmigration, está localizada na seguinte pasta:

```
ferramentas_administrativas/tools/tpmigration
```

Para migrar o banco de dados de persistência de tarefas, faça o seguinte:

1. Atualize o arquivo tpmigration125.properties
2. Defina a variável JAVA_HOME.
3. Execute a ferramenta runmigration.

Atualize o arquivo tpmigration125.properties

Para configurar a migração do banco de dados de persistência de tarefas, você deve atualizar o arquivo tpmigration.properties com o repositório de objetos e as informações de persistência de tarefas, incluindo os valores do repositório. O arquivo tpmigration125.properties está localizado no seguinte local:

<pasta do IAM suite>/tools/tpmigration/com/ca/tp/migratetpto125

Para configurar a migração, preencha as seguintes informações no arquivo de propriedades:

```
############################################################
# The object store is required to obtain the environment details.
############################################################
os.db.hostname=<hostname>
os.db.dbname=<database-name or SID>
os.db.username=<db user name>
os.db.password=<db user's password>
os.db.port=<db port number>
os.db.dbType=<type of the database.  For ex. for SQL server sql2005 and for
oracle 'oracle'>

############################################################
# Task persistence data where the old and new tables are.
############################################################
tp.db.hostname=<hostname>
tp.db.dbname=<database-name or SID>
tp.db.username=<db user name>
tp.db.password=<db user's password>
tp.db.port=<db port number>
tp.db.dbType=<type of the database.  For ex. for SQL server sql2005 and for
oracle 'oracle'>
```

Definir a variável JAVA_HOME

Para que a ferramenta runmigration seja executada corretamente, você deve verificar se a variável de ambiente JAVA_HOME está definida.

Executar a ferramenta runmigration

Para iniciar a migração, use o procedimento a seguir.

Em uma linha de comando

1. Execute a ferramenta runmigration.

   Para Windows:

   ```
   runmigration.bat
   ```

   Para UNIX:

   ```
   runmigration.sh
   ```

2. Digite as seguintes informações:

   - O alias protegido pelo ambiente ('tudo' para todos os ambientes).

     Observação: se você não especificar 'tudo', somente um ambiente poderá ser inserido.

   - O estado da tarefa.
     Observação: se você não especificar 'tudo', somente um estado de tarefa poderá ser inserido.

   - A versão do CA Identity Manager para migrar de (1-8.x, 2-12.0).

   - Deseja especificar um intervalo de datas para as tarefas a serem migradas (s/n).

     Observação: se você escolher 's', você deverá digitar o seguinte:

     - Insira a data de início (dd/mm/aa)
     - Insira a data de término (dd/mm/aa)

   A migração é iniciada.

Depois que a migração for concluída, o status indica quantas tarefas foram migradas.