



NetIQ Directory and Resource Administrator Guia do usuário

Junho de 2021

Informações legais

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

© Copyright 2007–2021 Micro Focus ou uma de suas afiliadas.

As únicas garantias para produtos e serviços da Micro Focus e suas afiliadas e licenciadas (“Micro Focus”) são apresentadas nas declarações de garantia expressas que acompanham tais produtos e serviços. Nada contido aqui deve ser interpretado como constituindo uma garantia adicional. A Micro Focus não será responsável por erros técnicos nem editoriais, tampouco por omissões aqui existentes. As informações aqui contidas estão sujeitas a mudanças sem aviso prévio.

Índice

Sobre este guia	7
1 Introdução	9
O que é o Directory and Resource Administrator	9
Compreendendo os componentes do Directory and Resource Administrator	10
Servidor de administração DRA	10
Gerenciamento de Recursos e de Contas	11
Console da Web	11
Componentes do Gerador de Relatórios	11
Mecanismo de workflow	12
Arquitetura do produto	13
2 Trabalhando com interfaces do usuário	15
Console da Web	15
Iniciando o Console da Web	15
Configurando o Console da Web	16
Personalizando o Console da Web	20
Gerenciando objetos no Console da Web	22
Gerando Relatórios de Histórico de Mudanças	22
Usando o Workflow Automation	23
Gerenciamento de Recursos e de Contas	24
Conectando-se a um servidor de Administração ou domínio gerenciado	25
Modificando o título do console	26
Personalizando colunas da lista	26
Gerenciando objetos no Gerenciamento de Recursos e de Contas	27
Executando consultas avançadas gravadas	27
Restaurando as configurações do console	28
Restrições de caracteres especiais	28
Usando caracteres curinga	29
Vendo seus poderes e suas funções designadas	30
Vendo o número da versão do produto e os hotfixes instalados	30
Vendo sua licença atual	31
Recuperando uma senha do BitLocker	31
DRA Reporting	32
Compreendendo o DRA Reporting	34
Como o DRA usa arquivos de registro do usuário	34
Compreendendo datas e horários	35
Tarefas do DRA Reporting	35
3 Pesquisando objetos	39
Pesquisa	39
Usando caracteres curinga	40
Pesquisa em vários campos	40
Adicionando e classificando colunas	41
Exportando os resultados da pesquisa	41

Pesquisa Avançada	42
Consultas de Pesquisa Avançada	42
Gerenciando consultas avançadas	43
Exportando os resultados da pesquisa avançada	44
4 Gerenciando Objetos do Active Directory	45
Gerenciando contas do usuário	45
Contas do usuário em domínios confiáveis	46
Tarefas de gerenciamento de contas do usuário	46
Transformando contas do usuário	49
Gerenciando grupos	52
Tarefas de gerenciamento de grupos	52
Gerenciando designações de grupo temporárias no Console de Delegação e Configuração	55
Gerenciando designações de grupo temporárias no Console da Web	56
Gerenciando grupos de distribuição dinâmica	58
Gerenciando grupos dinâmicos	60
Exemplo de cenário	60
Preparação de cenários	61
Tarefas do grupo dinâmico	61
Gerenciando contatos	64
Gerenciando Contas de Serviço Gerenciadas do Grupo	65
5 Gerenciando Objetos do Azure	67
Gerenciando contas do usuário do Azure	67
Gerenciando Grupos do Azure	68
Gerenciando Contatos do Azure	70
6 Gerenciando caixas de correio do Exchange e pastas públicas	71
Tarefas de gerenciamento para caixas de correio do usuário	71
Tarefas de gerenciamento para caixas de correio do Office 365	74
Tarefas de Gerenciamento para as Caixas de Correio de Recursos	75
Tarefas de gerenciamento para caixas de correio compartilhadas	77
Tarefas de gerenciamento para caixas de correio vinculadas	78
Tarefas de gerenciamento para pastas públicas	79
7 Gerenciando recursos	81
Gerenciamento de UOs (Unidades Organizacionais)	81
Gerenciando computadores	82
Gerenciando serviços	84
Gerenciando impressoras e serviços de impressão	85
Tarefas de gerenciamento de impressoras	85
Tarefas de gerenciamento de serviços de impressão	86
Tarefas de gerenciamento de impressoras publicadas	87
Tarefas de gerenciamento de serviços de impressão para impressoras publicadas	88
Gerenciando compartilhamentos	89
Gerenciando usuários conectados	89
Gerenciando dispositivos	90
Gerenciando registros de eventos	90

Tipos de registro de eventos.....	91
Tarefas de gerenciamento de registros de eventos	91
Gerenciando arquivos abertos.....	92

8 Gerenciando a Lixeira

93

Sobre este guia

O *Guia do Usuário* fornece informações conceituais sobre o produto DRA (NetIQ Directory and Resource Administrator). Este livro define a terminologia e vários conceitos relacionados.

Público-alvo

Este guia inclui informações para quem precisa compreender os conceitos de administração e implementar um modelo de administração seguro e distribuído.

Documentação adicional

Este guia faz parte do conjunto de documentação do Directory and Resource Administrator. Para acessar a versão mais recente deste guia e outros recursos de documentação do DRA, visite o [site da Documentação do NetIQ DRA \(https://www.netiq.com/documentation/directory-and-resource-administrator/index.html\)](https://www.netiq.com/documentation/directory-and-resource-administrator/index.html).

Informações dos Contatos

Aguardamos seus comentários e suas sugestões sobre este manual e sobre o restante da documentação que acompanha este produto. Use o link [comentar neste tópico](#) na parte inferior de cada página da documentação online ou envie um e-mail para Documentation-Feedback@microfocus.com.

Para problemas específicos do produto, entre em contato com o Atendimento ao Cliente da Micro Focus em <https://www.microfocus.com/support-and-services/>.

1 Introdução

Antes de começar a gerenciar objetos do Active Directory usando o DRA (NetIQ Directory and Resource Administrator), você deve compreender os princípios básicos do que o DRA fará pela sua empresa e a função dos componentes do DRA na arquitetura do produto.

O que é o Directory and Resource Administrator

O NetIQ Directory and Resource Administrator fornece administração de identidade privilegiada segura e eficiente do Microsoft Active Directory (AD). O DRA realiza a delegação granular de “privilégios mínimos”, de modo que administradores e usuários recebam apenas as permissões necessárias para concluir suas responsabilidades específicas. O DRA também impõe a adesão obrigatória à política, fornece auditoria e gerador de relatórios de atividades detalhadas e simplifica a conclusão de tarefas repetitivas com automação de processos de TI. Cada um desses recursos contribui para proteger os ambientes do AD e do Exchange de seus clientes contra o risco de escalonamento de privilégios, erros, atividade mal-intencionada e não conformidade com normas, ao mesmo tempo reduzindo o fardo do administrador ao oferecer recursos de autoatendimento a usuários, gerentes de negócios e pessoal de Suporte técnico.

O DRA também amplia os eficientes recursos do Microsoft Exchange para fornecer gerenciamento contínuo de objetos do Exchange. Por meio de uma interface do usuário única e em comum, o DRA oferece administração baseada em política para o gerenciamento de caixas de correio, pastas públicas e listas de distribuição em todo o ambiente do Microsoft Exchange.

O DRA fornece as soluções de que você precisa para controlar e gerenciar seus ambientes do Active Directory, do Microsoft Windows, do Microsoft Exchange e do Azure Active Directory.

- ♦ **Suporte para Azure Active Directory e Active Directory local, Exchange e Skype for Business:**

Fornecer gerenciamento administrativo para Azure e Active Directory local, Exchange Server local, Skype for Business local, Exchange Online e Skype for Business Online.

- ♦ **Controles granulares de acesso de privilégio administrativo e do usuário:** A tecnologia patenteada ActiveView (Tela Ativa) delega apenas os privilégios necessários para cumprir responsabilidades específicas e proteger contra escalonamento de privilégios.

- ♦ **Console da Web personalizável:** A abordagem intuitiva permite que pessoal não técnico realize tarefas administrativas de modo rápido e fácil por meio de recursos e acesso limitados (e atribuídos).

- ♦ **Auditoria e gerador de relatórios de atividades detalhados:** Fornece um registro de auditoria de todas as atividades realizadas com o produto. Armazena dados de longo prazo com segurança e demonstra para auditores (por exemplo, PCI DSS, FISMA, HIPAA e NERC CIP) que há processos ativos para controlar o acesso ao AD.

- ♦ **Automação de Processos de TI:** Automatiza workflows para uma variedade de tarefas, como provisionamento e desaprovisionamento, ações de usuário e de caixa de correio, imposição do uso obrigatório de políticas e tarefas de autoatendimento controladas; aumenta as eficiências dos negócios e reduz os esforços administrativos dos tipos manual e repetitivo.

- ♦ **Integridade operacional:** Impede mudanças mal-intencionadas ou incorretas que afetem o desempenho e a disponibilidade de sistemas e serviços, fornecendo controle de acesso granular para administradores e gerenciando o acesso a sistemas e recursos.
- ♦ **Imposição do uso obrigatório do processo:** Mantém a integridade dos processos de gerenciamento de mudança de senha que ajudam você a aumentar a produtividade, reduzir erros, poupar tempo e aumentar a eficiência administrativa.
- ♦ **Integração com o Change Guardian:** Aprimora a auditoria para eventos gerados no Active Directory fora do DRA e a automação de workflow.

Compreendendo os componentes do Directory and Resource Administrator

Os componentes do DRA usados consistentemente para gerenciar o acesso privilegiado incluem servidores principais e secundários, consoles de administrador, componentes de relatórios e o Mecanismo de Workflow para automatizar processos de workflow.

A tabela a seguir identifica as interfaces do usuário típicas e os servidores de administração usados em cada tipo de usuário do DRA:

Tipo de Usuário do DRA	Interfaces do usuário	Servidor de Administração
Administrador do DRA (A pessoa que fará a manutenção das configurações do produto)	Delegation and Configuration Console (Console de Delegação e Configuração)	Servidor principal
Administrador Avançado	DRA Reporting PowerShell CLI Provedor de ADSI do DRA	Qualquer servidor do DRA
Administrador ocasional do suporte técnico	Nó Account and Resource Management (Gerenciamento de Recursos e de Contas) no Console de Delegação e Configuração Console da Web	Qualquer servidor do DRA

Servidor de administração DRA

O Servidor de administração DRA armazena dados de configuração (de política, ambientais e de acesso delegado), executa tarefas do operador e de sistema e audita a atividade do sistema como um todo. Suportando diversos clientes em nível de API e de console, o servidor é projetado para fornecer alta disponibilidade tanto para isolamento geográfico quanto para redundância por meio

de um modelo de expansão de MMS (Multi-Master Set - Conjunto com vários masters). Neste modelo, cada ambiente do DRA exigirá um servidor de Administração principal que será sincronizado com alguns Servidores de administração DRA secundários adicionais.

Recomendamos fortemente que você não instale servidores de Administração em controladores de domínio do Active Directory. Para cada domínio gerenciado pelo DRA, verifique se há pelo menos um controlador de domínio no mesmo site que o servidor de Administração. Por padrão, o servidor de Administração acessa o controlador de domínio mais próximo para todas as operações de leitura e gravação; ao realizar tarefas específicas a um site, como redefinições de senha, você pode especificar um determinado controlador de domínio para processar a operação. Como uma melhor prática, considere a possibilidade de dedicar um servidor de Administração secundário para cargas de trabalho automatizadas, gerador de relatórios e processamento de lote.

Gerenciamento de Recursos e de Contas

O Gerenciamento de Recursos e de Contas é um nó no Console de Delegação e Configuração para que administradores assistentes do DRA possam ver e gerenciar objetos delegados de serviços e domínios conectados.

Console da Web

O Console da Web é uma interface do usuário com base na Web que fornece acesso rápido e fácil para que administradores assistentes do DRA possam ver e gerenciar objetos delegados de serviços e domínios conectados.

Os administradores podem personalizar a aparência e o uso do console da Web para incluir marcas de empresas e propriedades de objeto personalizadas, além de configurar a integração com servidores do Change Guardian para habilitar a auditoria de mudanças que ocorre fora do DRA.

O Administrador do DRA também pode criar e modificar formulários de workflow automatizados para executar tarefas automatizadas de rotina quando acionados.

O Histórico de Mudanças Unificado é outro recurso do console da Web que permite a integração com os servidores de Histórico de Mudanças para auditoria das mudanças feitas a objetos do AD fora do DRA. As opções de relatório do histórico de mudanças incluem o seguinte:

- ♦ Mudanças feitas a...
- ♦ Mudanças feitas por...
- ♦ Caixa de correio criada por...
- ♦ Usuário, grupo e endereço de e-mail do contato criados por...
- ♦ Usuário, grupo e endereço de e-mail do contato apagados por...
- ♦ Atributo virtual criado por...
- ♦ Objetos movidos por...

Componentes do Gerador de Relatórios

O DRA Reporting fornece modelos incorporados personalizáveis para gerenciamento do DRA e mais informações sobre sistemas e domínios gerenciados do DRA:

- ♦ Relatórios de recursos para objetos do AD

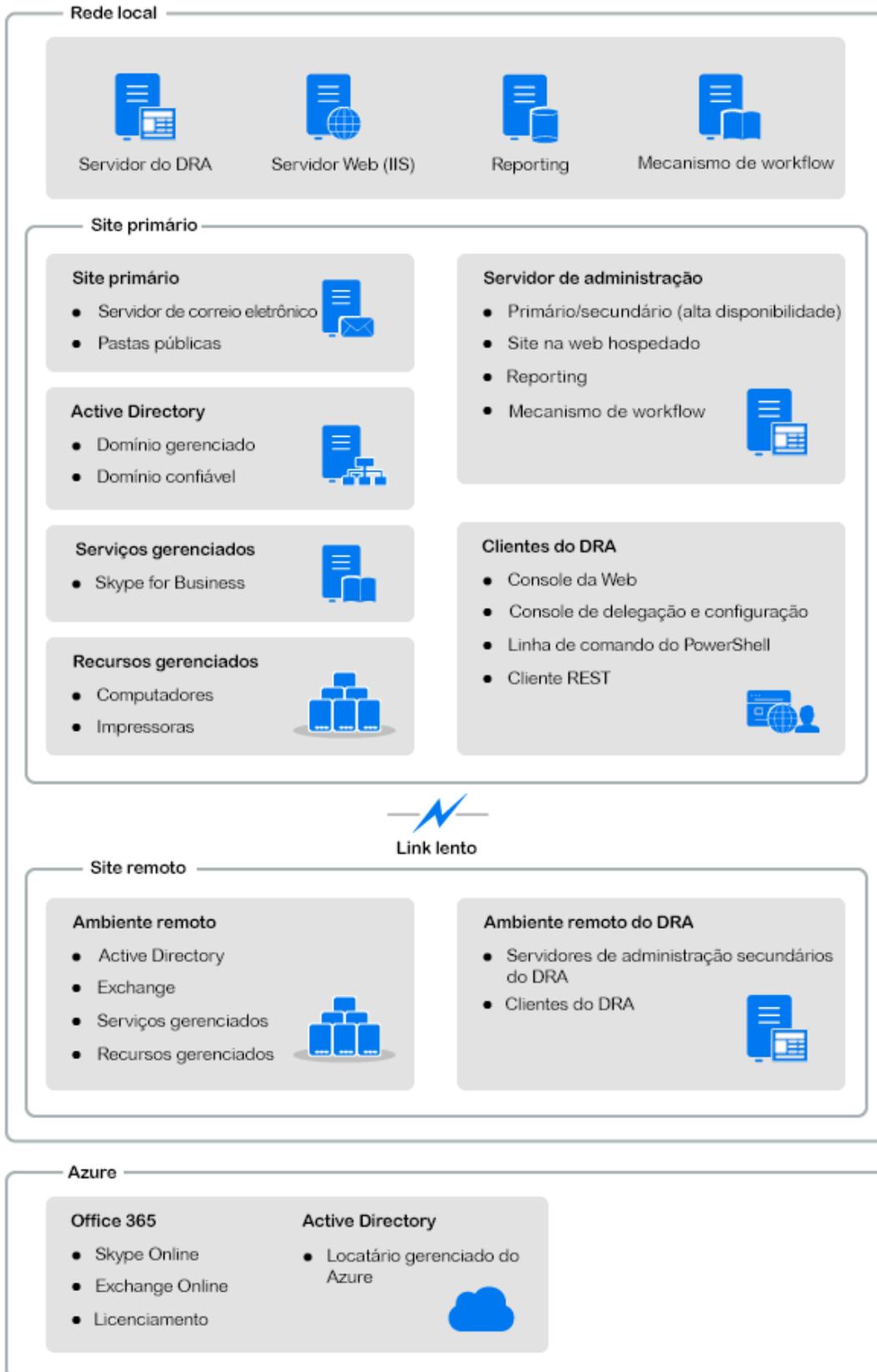
- ♦ Relatórios de dados de objetos do AD
- ♦ Relatórios de resumo do AD
- ♦ Relatórios de configuração do DRA
- ♦ Relatórios de configuração do Exchange
- ♦ Relatórios do Exchange Online do Office 365
- ♦ Relatórios de tendências de atividades detalhadas (por mês, domínio e pico)
- ♦ Relatórios de atividade do DRA resumidos

Relatórios do DRA podem ser agendados e publicados por meio do SQL Server Reporting Services para uma distribuição adequada para os acionistas.

Mecanismo de workflow

O DRA integra-se ao Mecanismo de Workflow para automatizar tarefas de workflow por meio do Console da Web, no qual administradores assistentes podem configurar o Servidor de Workflow, executar formulários de automação de workflow personalizados e então ver o status desses workflows. Para obter mais informações sobre o Mecanismo de Workflow, consulte a documentação do Workflow Automation no [site da Documentação do NetIQ DRA](#).

Arquitetura do produto



2 Trabalhando com interfaces do usuário

As interfaces do usuário do DRA atendem a diversas necessidades de administração. Estas interfaces incluem:

Console da Web

Permite executar tarefas comuns de administração de contas e recursos por meio de uma interface baseada na Web. Você pode acessar o Console da Web de qualquer computador executando o Internet Explorer, o Chrome ou o Firefox.

PowerShell

O módulo do PowerShell permite a clientes não DRA solicitar operações do DRA usando cmdlets do PowerShell.

Console do NetIQ Reporting Center

Permite visualizar e implantar relatórios de gerenciamento para que você possa auditar sua segurança corporativa e controlar atividades de administração. Os relatórios de gerenciamento incluem relatórios de atividades, de configuração e de resumo. Muitos desses relatórios podem ser visualizados em uma representação gráfica.

Console da Web

O Console da Web é uma interface do usuário baseada na Web que fornece acesso rápido e fácil a muitas tarefas de conta do usuário, grupo, computador, recurso e caixa de correio do Microsoft Exchange. Você pode personalizar as propriedades de objeto para aumentar a eficiência das tarefas de rotina. Você também pode gerenciar propriedades gerais de sua própria conta do usuário, como o endereço da rua ou o número do telefone celular.

O Console da Web exibirá uma determinada tarefa somente se você tiver o poder de executá-la.

- ♦ [“Iniciando o Console da Web” na página 15](#)
- ♦ [“Configurando o Console da Web” na página 16](#)
- ♦ [“Personalizando o Console da Web” na página 20](#)
- ♦ [“Gerenciando objetos no Console da Web” na página 22](#)
- ♦ [“Gerando Relatórios de Histórico de Mudanças” na página 22](#)
- ♦ [“Usando o Workflow Automation” na página 23](#)

Iniciando o Console da Web

Você pode iniciar o Console da Web de qualquer computador executando um destes browsers suportados:

- ♦ Google Chrome

- ♦ Mozilla Firefox
- ♦ Microsoft Edge

Para iniciar o Console da Web, especifique o URL apropriado no campo de endereço do browser da Web. Por exemplo, se você instalou o componente da Web no computador do HOUserver, digite `https://HOUserver.entDomain.com/draclient` no campo de endereço do seu browser da Web.

Observação: Para exibir a conta mais atual e as informações do Microsoft Exchange no Console da Web, defina seu browser da Web para verificar versões mais recentes das páginas armazenadas em cache a cada visita.

Conexão ao Servidor DRA

Você pode usar uma das quatro opções para efetuar login no Console da Web. O comportamento de cada opção, ao efetuar login, está descrito na tabela a seguir:

Tela de login - Opções	Descrições da opção de conexão
Usar descoberta automática	Encontra um servidor DRA automaticamente; nenhuma opção de configuração está disponível
Conectar ao servidor DRA padrão	São usados os detalhes do servidor e da porta pré-configurados. Observação: Esta opção será exibida somente quando você tiver configurado o servidor DRA padrão no Console da Web. Além disso, se você especificar que o cliente deve sempre se conectar ao servidor DRA padrão, poderá ver apenas a opção Conectar ao servidor DRA padrão na tela de login.
Conectar a um servidor DRA específico	O usuário configura o servidor e a porta
Conectar a um servidor DRA que gerencia um domínio específico	O usuário fornece um domínio gerenciado e escolhe uma opção de conexão: <ul style="list-style-type: none"> ♦ Usar descoberta automática (no domínio fornecido) ♦ Servidor principal para esse domínio ♦ Pesquisar um servidor DRA (no domínio fornecido)

Configurando o Console da Web

Se tiver poderes de Administração do DRA, você poderá definir as configurações do Advanced Authentication, da marca e da sessão do cliente, além de todas as conexões de servidor necessárias para o Console da Web. Para acessar qualquer uma dessas configurações, efetue login no Console da Web e navegue até **Administração > Configuração**.

Observação: A guia **Administração** no cabeçalho principal não será exibida se você não tiver as capacidades administrativas necessárias.

- ♦ [“Advanced Authentication” na página 17](#)
- ♦ [“Marca do Console da Web” na página 17](#)
- ♦ [“Configurações da Sessão do Cliente” na página 19](#)
- ♦ [“Conexão ao servidor” na página 19](#)

Advanced Authentication

O serviço Advanced Authentication permite que você vá além de um simples nome de usuário e uma senha e use uma maneira mais segura de proteger informações confidenciais usando a autenticação multifator. A autenticação multifator é um método de controle de acesso ao computador que requer mais de um método de autenticação de categorias separadas de credenciais para verificar a identidade de um usuário.

Depois que o Administrador do DRA configurar cadeias e eventos, se você tiver os poderes necessários, poderá efetuar login no Console da Web e habilitar o Advanced Authentication. Depois que a autenticação for habilitada, todos os usuários precisarão se autenticar por meio do Advanced Authentication antes de receber acesso ao Console da Web.

Para habilitar o Advanced Authentication, selecione **Advanced Authentication** na guia Configuração, clique **Habilitar Advanced Authentication** e configure o formulário de acordo com as instruções fornecidas para cada campo.

Para obter mais informações sobre o Advanced Authentication, consulte [“Authentication”](#) (Autenticação) no *DRA Administrator Guide* (Guia do Administrador do DRA).

Marca do Console da Web

Você pode personalizar a tela de login e o cabeçalho do Console da Web do DRA da seguinte forma:

- ♦ **Cabeçalho Principal:** É a barra de navegação de alto nível na parte superior do Console da Web depois de efetuar login.
 - ♦ *Imagem da logo ou texto alternativo:* Exibido no extremo esquerdo da barra de cabeçalho principal. Você pode exibir uma imagem da logo ou um texto alternativo, mas não ambos.
 - ♦ *Cor do cabeçalho principal:* Sobrepõe todo o cabeçalho com esta cor, exceto a área de imagem da logo.
- ♦ **Tela de login temática:** A aparência da página de login ao acessar o URL do Console da Web no seu browser. O tema do DRA é configurado e habilitado por padrão.
 - ♦ *Imagem da logo ou texto alternativo:* É exibido acima do título do produto e dos campos de credenciais. Você pode exibir uma imagem da logo ou um texto alternativo, mas não ambos.

- ♦ *Título do aplicativo*: É exibido entre os campos de credencial e a imagem da logo.
- ♦ *Pertencente ao modo de notificação*: É uma caixa de mensagem que sobrepõe e obscurece a página de login até que o usuário clique **OK**. É normalmente usada para informar ao usuário que o acesso ao console implica consentimento para seguir uma política de segurança da empresa. Uma vez habilitado, todos os usuários que acessarem o Console da Web receberão o prompt.

Configurar o cabeçalho principal

Para configurar o cabeçalho principal:

- 1 Efetue login no Console da Web e navegue até **Administração > Configuração > Marca**.
- 2 Siga um destes procedimentos. Se você adicionar texto e um arquivo de imagem, apenas a imagem será exibida.
 - ♦ Atualize a imagem da logo:
 1. Adicione o nome do arquivo de imagem gravado, incluindo a extensão do arquivo no campo Imagem da Logo do bloco **Cabeçalho Principal**.
 2. Grave a imagem da logo no diretório de “assets” no servidor Web. Por exemplo:
 C:\inetpub\wwwroot\DRAClient\assets
 O tamanho ideal da imagem é de 56x56 pixels.
 - ♦ Digite ou sobregrave o texto existente no campo Texto Alternativo à Imagem da Logo do bloco **Cabeçalho Principal**, conforme necessário.
- 3 Clique em **Gravar** na parte inferior da página para concluir as mudanças na configuração.

Configurar a tela de login

O procedimento abaixo fornece informações para modificar todas as três opções configuráveis, a logo da empresa, o título do aplicativo e o pertencente ao modo de notificação. Você pode modificar uma, duas ou todas as três opções.

Para mudar o tema padrão na tela de login:

- 1 Grave a logo da sua empresa na pasta “assets” no servidor Web. Por exemplo:
 C:\inetpub\wwwroot\DRAClient\assets
 O tamanho ideal da imagem é de 115x28 pixels.
- 2 Efetue login no Console da Web e navegue até **Administração > Configuração > Marca**.
- 3 Substitua o nome do arquivo no campo Imagem da Logo da Empresa do bloco de **Login** pelo nome do arquivo de imagem gravado, incluindo a extensão do arquivo.
- 4 Modifique o texto no campo **Título do aplicativo**, conforme aplicável.
- 5 Clique em **Mostrar um modal de notificação ao efetuar login** para habilitar essa configuração e digite um título para o prompt de notificação. Digite ou cole o conteúdo da mensagem que você deseja que os usuários vejam no campo **Conteúdo**. Por exemplo:
Você está efetuando login em uma rede segura. Ao efetuar login neste sistema, você concorda em cumprir as políticas de segurança da empresa para acesso à rede.

- 6 Selecione o estilo da mensagem. O estilo muda a flag da imagem que está anexada à caixa de mensagem (mostrada abaixo). Se desejar, você poderá clicar em Visualizar para ver como a mensagem será exibida.



- 7 Clique em **Gravar** na parte inferior da página para concluir as mudanças na configuração.

Configurações da Sessão do Cliente

Nas Configurações da Sessão do Cliente, você pode definir um incremento de tempo para que o Console da Web efetue logout automaticamente após a inatividade ou configurá-lo para nunca efetuar logout automaticamente.

Para configurar o Logout Automático no Console da Web, acesse **Administração > Configuração > Configurações da Sessão do Cliente**. Habilite o recurso de logout automático com o switch de alternância e, se necessário, modifique a configuração para a duração da inatividade, em minutos.

Conexão ao servidor

Ao acessar a página de login do Console da Web no seu browser, existem configurações de **Opções** que você pode definir para determinar como se conectará ao DRA. Essas configurações também podem ser localizadas com a opção **Conexão ao Servidor** no menu de perfil do usuário do Console da Web. A porta de serviço do Servidor DRA tem a configuração padrão de 8775. Você poderá definir um novo padrão para o Servidor DRA no perfil do usuário ou na tela de login Opções quando nenhum padrão estiver habilitado. As definições de conexão da configuração Conexão ao Servidor são mantidas com o perfil do usuário do Windows.

As informações sobre as definições que você pode modificar na configuração **Conexão ao Servidor**, seja do menu Opções na tela de login ou do menu de perfil do usuário após o login, são fornecidas abaixo:

Configurações do servidor DRA	Descrição
Usar descoberta automática	Encontra um servidor DRA automaticamente; nenhuma opção de configuração está disponível
Conectar ao servidor DRA padrão (Exibido somente se o padrão estiver habilitado na configuração de Conexão ao Servidor)	Usa a definição padrão da configuração de Conexão ao Servidor (quando habilitada); nenhuma opção de configuração está disponível
Conectar a um servidor DRA específico	O usuário configura o servidor e a porta

Se desejar, você poderá configurar um local, um servidor e um domínio padrão para o Servidor do DRA por meio da configuração da **Conexão ao Servidor** no Console da Web.

Para habilitar as configurações padrão, efetue login no Console da Web e navegue até **Administração > Configuração > Conexão ao Servidor DRA**. Habilite as configurações de conexão que deseja usar e clique em **Gravar**.

Conexão ao Servidor DRA

A configuração da Conexão ao Servidor DRA inclui definir um local do servidor padrão, modificar a porta (se necessário) e um tempo de espera de conexão, em segundos. Você também pode desabilitar a configuração com o switch de alternância.

Ao fornecer a localização do Servidor DRA, use o formato mostrado no exemplo abaixo:

```
NomeDoServidor.NomeDoDomínio.com
```

Personalizando o Console da Web

Você pode personalizar as propriedades de objeto no Console da Web. Quando implementadas corretamente, as personalizações de propriedade ajudarão a automatizar tarefas com o gerenciamento de objetos.

Personalizando Páginas de Propriedades

Se você tiver as capacidades de Administração do DRA, poderá personalizar os formulários de propriedade do objeto usados na sua função de gerenciamento do Active Directory por tipo de objeto. Isso inclui criar e personalizar novas páginas de objetos baseadas em tipos de objetos que são incorporados ao DRA. Você também pode modificar propriedades para os tipos de objetos incorporados.

Os objetos de propriedade são claramente definidos na lista Páginas de Propriedade no Console da Web para que você possa identificar facilmente quais páginas de objeto estão incorporadas, quais páginas incorporadas são personalizadas e quais páginas não estão incorporadas e foram criadas por um administrador.

Personalizando uma página de propriedades do objeto

Você pode personalizar formulários de propriedade do objeto adicionando ou removendo páginas, modificando páginas e campos existentes e criando sub-rotinas personalizadas para atributos de propriedade. As sub-rotinas personalizadas em um campo são executadas sempre que o valor desse campo é modificado. O tempo também pode ser configurado a fim de que o administrador possa especificar se as sub-rotinas devem ser executadas imediatamente (a cada pressionamento de tecla), quando o campo perde o foco ou após um atraso de tempo especificado.

A lista de objetos em Páginas de Propriedades fornece tipos de operação para cada tipo de objeto, Criar Objeto e Editar Propriedades. Essas são as principais operações executadas pelos administradores assistentes no Console da Web. Eles realizam essas operações navegando até **Gerenciamento > Pesquisa** ou **Pesquisa Avançada**. Aqui eles podem criar objetos do menu suspenso Criar ou editar objetos existentes selecionados na tabela de resultados da pesquisa por meio do ícone Propriedades.

Para personalizar uma página de propriedades do objeto no Console da Web:

- 1 Efetue login no Console da Web com privilégios de Administração do DRA.
- 2 Navegue até **Administração > Personalização > Páginas de Propriedade**.
- 3 Selecione um objeto e um tipo de operação (Criar Objeto ou Editar Objeto) na lista Páginas de Propriedades.
- 4 Clique no ícone **Propriedades** .
- 5 Personalize o formulário de propriedade do objeto seguindo um ou mais dos procedimentos a seguir e aplicando as mudanças:
 - ♦ Adicionar uma nova página de propriedades: **+ Adicionar Página**
 - ♦ Reordenar e apagar páginas de propriedades
 - ♦ Selecionar uma página de propriedades e personalizar a página:
 - ♦ Reordenar campos de configuração na página: **↑ ↓**
 - ♦ Editar campos ou subcampos: 
 - ♦ Adicione um ou mais campos: **+** ou **Inserir um novo Campo**
 - ♦ Remover um ou mais campos: **x**
 - ♦ Criar sub-rotinas personalizadas para propriedades usando scripts, caixas de mensagens ou consultas (LDAP, DRA ou REST)

Para obter mais informações sobre como usar sub-rotinas personalizadas, consulte [“Adding Custom Handlers”](#) (Adicionando sub-rotinas personalizadas) no *DRA Administrator Guide* (Guia de Administrador do DRA).

Criando uma nova página de propriedades do objeto

Para criar uma nova página de propriedades do objeto:

- 1 Efetue login no Console da Web com capacidades de Administração do DRA e navegue até **Administração > Personalização > Páginas de Propriedade** e clique em **+ Criar**.
- 2 Crie o formulário inicial de propriedades do objeto definindo nome, ícone, tipo de objeto e configuração de operação.
Após clicar em **OK**, ações de Criar são adicionadas ao menu suspenso Criar, enquanto as ações de Propriedade são exibidas no formulário de objeto quando o usuário seleciona e edita um objeto na lista de pesquisa.
- 3 Personalize o novo formulário conforme necessário. Consulte [Personalizando uma página de propriedades do objeto](#).

Gerenciando objetos no Console da Web

Gerencie objetos no Console da Web navegando para o cabeçalho de Gerenciamento. Ali, você pode pesquisar por tipo de objeto para objetos em domínios gerenciados, locatários do Azure, containers e na Lixeira. Dentro de um domínio ou locatário do Azure, você pode gerenciar e realizar ações em objetos do Active Directory e do Azure Active Directory usando o DRA.

Se você selecionar um objeto na lista de resultados de pesquisa, todas as ações aplicáveis que você pode realizar nesse objeto estarão disponíveis na barra de tarefas acima da grade. As opções disponíveis baseiam-se no tipo de objeto selecionado, nos componentes configurados atualmente para DRA e nos privilégios de administrador designados a você.

Para editar as propriedades de um objeto, coloque o cursor do mouse sobre o objeto e clique no ícone de **Propriedades**  que aparece na linha do objeto. Ali, você pode acessar todas as páginas de Propriedades do objeto no painel de navegação esquerdo.

Importante: Se você quiser **proteger um objeto contra apagamento acidental**, mova a barra de rolagem para o fim da página Propriedades – **Geral**, selecione a caixa de seleção para habilitar esse recurso e selecione **Aplicar** para aplicar as mudanças.

Para obter mais informações sobre ações que você pode realizar em objetos, veja os seguintes tópicos:

- ♦ [Gerenciando Objetos do Active Directory](#)
- ♦ [Gerenciando Objetos do Azure](#)
- ♦ [Gerenciando caixas de correio do Exchange e pastas públicas](#)
- ♦ [Gerenciando recursos](#)

Gerando Relatórios de Histórico de Mudanças

Se o Histórico de Mudanças for configurado pelo seu Administrador do DRA e tiver a capacidade de **Generate UI Reports** (Gerar Relatórios de Interface do Usuário), você poderá gerar relatórios de histórico de mudanças e exportar relatórios para objetos gerenciados no DRA. Isso inclui mudanças feitas no DRA e fora do DRA. Você só pode gerar relatórios de histórico de mudanças do Console da Web, que inclui os seguintes tipos de relatórios:

- ♦ Mudanças feitas pelo usuário
- ♦ Mudanças feitas para o usuário
- ♦ Caixas de correio de usuários criadas pelo usuário
- ♦ Caixas de correio de usuários apagadas pelo usuário
- ♦ Endereços de e-mail de contatos e grupos estabelecidos pelo usuário
- ♦ Endereços de e-mail de contatos e grupos apagados pelo usuário
- ♦ Atributos virtuais criados ou desabilitados pelo usuário
- ♦ Objetos movidos pelo usuário

Para gerar relatórios de Histórico de Mudanças Unificado (UCH):

- 1 Inicie o Console da Web.
- 2 Vá até **Gerenciamento > Pesquisar**.
- 3 Defina os critérios de pesquisa usando as opções **Pesquisar por**, **termo de pesquisa** e **Filtros**.
- 4 Clique no botão **Pesquisar** para exibir os resultados da pesquisa.
- 5 Selecione os objetos para os quais você deseja gerar relatórios.
- 6 Clique no ícone **Ver Relatórios de Histórico de Mudanças** .
- No formulário Relatório de Histórico de Mudanças Unificado, você pode editar e gerar os critérios de relatório nas opções **Tipo**, **Objetos de destino** e **Filtros** para incluir a definição dos servidores nos quais as mudanças foram detectadas (DRA e Change Guardian).
- 7 Clique em **Gerar** para buscar dados de auditoria e gerar um relatório do UCH.
- 8 Você pode classificar e exportar o relatório em um formato obrigatório, como CSV e HTML.

Para criar um arquivo CSV do relatório exibido, você pode exportar todas as mudanças geradas ou apenas aquelas exibidas na página atual, executando uma das seguintes opções após a geração do relatório usando as etapas acima:

- ♦ Clique em **Exportar Tudo**  e grave o relatório exportado.
- ♦ Clique em **Exportar a Página Atual**  e grave o relatório exportado.

Se necessário, mude o número de mudanças que são mostradas na página, até 200 itens.

Usando o Workflow Automation

Com o uso do Workflow Automation, é possível automatizar processos de TI iniciando formulários de workflow que são executados junto com o workflow ou quando acionados por um evento associado nomeado, criado no servidor da Automação de Workflow.

Os formulários de workflow, quando criados ou modificados, são gravados no Servidor Web. Quando você efetuar login no Console da Web para este servidor, terá acesso aos formulários com base em poderes delegados e no modo como os formulários são configurados. Geralmente, os formulários estão disponíveis para todos os usuários com credenciais de Servidor Web. A capacidade de enviar o formulário requer poderes adequados.

Iniciando um formulário de workflow: Os workflows são criados no Servidor do Workflow Automation, que deve ser integrado ao DRA por meio do Console da Web. Para gravar um novo formulário, você deve ter a opção **Iniciar Workflow Específico** ou **Acionar Workflow por Evento** configurada nas propriedades do formulário. Mais informações sobre essas opções são fornecidas abaixo:

- ♦ **Iniciar Workflow Específico:** Esta opção lista todos os workflows disponíveis que estão em produção no Servidor de Workflow para o DRA. Para que os workflows sejam preenchidos nessa lista, eles precisam ser criados na pasta `DRA_Workflows` no servidor do Workflow Automation.
- ♦ **Acionar Workflow por Evento:** Essa opção é usada para executar workflows com acionadores predefinidos. Os workflows com acionadores também são criados no servidor do Workflow Automation.

Observação: Somente formulários de workflow configurados com Iniciar Workflow Específico terão um histórico de execução que pode ser consultado no painel de pesquisa principal em **Tarefas > Solicitações**.

Mais informações sobre o Workflow Automation estão incluídas nos seguintes guias no [site de documentação do DRA](#):

- ♦ *DRA Administrator Guide* (Guia de Administrador do DRA)
- ♦ *WFA Administrator Guide* (Guia de Administrador do WFA)
- ♦ *WFA User Guide* (Guia do Usuário do WFA)
- ♦ *WFA Process Authoring Guide* (Guia de Autoria de Processos do WFA)

Gerenciamento de Recursos e de Contas

O nó Account and Resource Management (Gerenciamento de Recursos e de Contas) no Console de Delegação e Configuração fornece acesso à maioria das tarefas do administrador assistente do DRA, abordando as necessidades de gerenciamento corporativo, desde a administração básica até os problemas avançados do Suporte Técnico. Ao utilizar o Gerenciamento de Recursos e de Contas, é possível executar tarefas de gerenciamento de recursos e de contas e gerenciar caixas de correio do Microsoft Exchange.

O Gerenciamento de Recursos e de Contas contém os seguintes nós:

Todos os Meus Objetos Gerenciados

Permite gerenciar objetos, como contas do usuário, grupos, contatos, recursos, grupos dinâmicos, grupos de distribuição dinâmica, caixas de correio de recursos e pastas públicas para cada domínio em que você tem algum poder.

Temporary Group Assignments (Designações de Grupo Temporárias)

Permite gerenciar participações de grupos para usuários que precisam dessas participações somente por um período de tempo específico.

Consultas Avançadas

Permite que você crie, grave, importe, exporte, copie e gerencie consultas de atributos virtuais e de LDAP pessoal e público.

Lixeira

Permite gerenciar contas do usuário, grupos, contatos e recursos apagados em qualquer domínio do Microsoft Windows em que a Lixeira esteja habilitada.

Para acessar o nó Gerenciamento de Recursos e de Contas, clique em **Delegation and Configuration** (Configuração e Delegação) na pasta do programa de Administrador da NetIQ e expanda o nó Delegation and Configuration (Configuração e Delegação) no console.

Quando você inicia o Console de Delegação e Configuração, inicialmente conecta-se ao melhor servidor de Administração disponível no domínio local. O melhor servidor de Administração disponível é o servidor mais próximo, que normalmente é um servidor no site da rede. Ao procurar o melhor servidor de Administração disponível, o DRA fornece uma conexão mais rápida e melhora o desempenho.

Para saber mais sobre como trabalhar no Gerenciamento de Recursos e de Contas, veja os seguintes tópicos:

- ♦ [“Conectando-se a um servidor de Administração ou domínio gerenciado”](#) na página 25
- ♦ [“Modificando o título do console”](#) na página 26
- ♦ [“Personalizando colunas da lista”](#) na página 26
- ♦ [“Gerenciando objetos no Gerenciamento de Recursos e de Contas”](#) na página 27
- ♦ [“Executando consultas avançadas gravadas”](#) na página 27
- ♦ [“Restaurando as configurações do console”](#) na página 28
- ♦ [“Restrições de caracteres especiais”](#) na página 28
- ♦ [“Usando caracteres curinga”](#) na página 29
- ♦ [“Vendo seus poderes e suas funções designadas”](#) na página 30
- ♦ [“Vendo o número da versão do produto e os hotfixes instalados”](#) na página 30
- ♦ [“Vendo sua licença atual”](#) na página 31
- ♦ [“Recuperando uma senha do BitLocker”](#) na página 31

Conectando-se a um servidor de Administração ou domínio gerenciado

Por padrão, o DRA se conecta ao melhor servidor de Administração disponível para um domínio gerenciado ou computador. O melhor servidor de Administração disponível é o servidor mais próximo, que normalmente é um servidor no site da rede. Se o site não incluir um servidor de Administração, o DRA se conectará ao próximo servidor disponível no domínio gerenciado ou na subárvore gerenciada. Você também pode especificar o domínio ou servidor de Administração ao qual deseja se conectar.

Quando você inicia as interfaces do usuário pela primeira vez, o DRA inicialmente se conecta ao domínio da sua conta de logon. Se você estiver conectado a um domínio que não seja gerenciado por um servidor de Administração ou se o DRA não puder se conectar ao servidor de Administração desse domínio, o DRA poderá exibir uma mensagem de erro. Verifique se o servidor de Administração está disponível e tente novamente.

Para se conectar a um servidor de Administração:

- 1 No menu Arquivo, clique em **Conectar ao Servidor**.
- 2 Clique em **Conectar a este servidor DRA**.
- 3 Digite o nome do servidor de Administração usando o seguinte formato: *nomedocomputador*.
- 4 Clique em **OK**.

Para se conectar a um computador ou domínio gerenciado:

- 1 No menu Arquivo, clique em **Conectar ao Servidor**.
- 2 Selecione a opção apropriada e digite o nome do domínio gerenciado ou do computador.
- 3 Por exemplo, para se conectar ao domínio HOULAB, clique em **Conectar a um servidor DRA que gerencia esse domínio** e digite HOULAB.

- 4 Para especificar um servidor de Administração para o domínio gerenciado ou computador, clique em **Advanced** (Avançado) e selecione a opção apropriada.
- 5 Clique em **OK**.

Modificando o título do console

É possível modificar as informações exibidas na barra de título do Console de Delegação e Configuração. Por conveniência e clareza, você pode adicionar o nome de usuário com o qual o console foi iniciado e o servidor de Administração ao qual o console está conectado. Em ambientes complexos nos quais você precisa se conectar a vários servidores de Administração usando credenciais diferentes, esse recurso ajuda a discernir rapidamente qual console você precisa usar.

Para modificar a barra de título do console:

- 1 Inicie o Console de Delegação e Configuração.
- 2 Clique em **Exibição > Opções**.
- 3 Selecione a guia Window Title (Título da Janela).
- 4 Especifique as configurações apropriadas e clique em **OK**.

Personalizando colunas da lista

Você pode selecionar quais propriedades do objeto o DRA exibe nas colunas da lista. Esse recurso flexível permite personalizar a interface do usuário, como listas de resultados de pesquisa, para melhor atender às demandas específicas de administração da sua empresa. Por exemplo, você pode definir colunas para exibir o nome de logon do usuário ou o tipo de grupo, permitindo encontrar e classificar rapidamente os dados necessários.

Para personalizar colunas da lista:

- 1 Selecione o nó adequado. Por exemplo, para escolher quais colunas serão exibidas ao ver os resultados da pesquisa em objetos gerenciados, selecione **Todos os Meus Objetos Gerenciados**.
- 2 No menu Ver, clique em **Choose Columns** (Escolher Colunas).
- 3 Na lista de propriedades disponíveis para este nó, selecione as propriedades do objeto que você deseja mostrar.
- 4 Para mudar a ordem das colunas, selecione uma coluna e clique em **Mover para Cima** ou **Mover para Baixo**.
- 5 Para especificar a largura da coluna, selecione uma coluna e digite o número apropriado de pixels no campo fornecido.
- 6 Clique em **OK**.

Gerenciando objetos no Gerenciamento de Recursos e de Contas

Gerencie objetos no Gerenciamento de Recursos e de Contas selecionando **Todos os Meus Objetos Gerenciados** ou um sub-nó na árvore do diretório. Ali, você pode pesquisar por tipo de objeto para objetos em domínios, containers e OUs.

Se você selecionar um objeto na lista de resultados da pesquisa, todas as ações aplicáveis que você pode realizar nesse objeto estarão disponíveis no menu **Tarefas** na barra de ferramentas ou no menu do botão direito do mouse. As opções disponíveis baseiam-se no tipo de objeto selecionado, nos componentes configurados atualmente para DRA e nos privilégios de administrador designados a você.

Para editar as propriedades de um objeto, selecione o objeto e clique em **Propriedades** no menu **Tarefas**. Ali, você pode acessar todas as páginas de Propriedades do objeto clicando nos links de página no painel de navegação esquerdo.

Importante: Se você desejar **proteger um objeto contra apagamento acidental**, selecione o objeto e abra **Propriedades**, selecione **Geral** no painel de navegação, selecione a caixa de seleção para habilitar esse recurso e selecione **Aplicar** para aplicar as mudanças.

Para obter mais informações sobre ações que você pode realizar em objetos, veja os seguintes tópicos:

- ♦ [Gerenciando Objetos do Active Directory](#)
- ♦ [Gerenciando caixas de correio do Exchange e pastas públicas](#)
- ♦ [Gerenciando recursos](#)

Executando consultas avançadas gravadas

Usando consultas avançadas, você pode pesquisar usuários, contatos, grupos, computadores, impressoras, OUs e qualquer outro objeto suportado pelo DRA. Se você tiver o poder Executar Consultas Avançadas Gravadas, poderá executar consultas avançadas disponíveis na lista **Saved Queries** (Consultas Gravadas) para qualquer contêiner no nó Gerenciamento de Recursos e de Contas. Para obter mais informações sobre seus poderes designados, consulte [Vendo seus poderes e suas funções designadas](#).

Para executar consultas avançadas gravadas:

- 1 Expanda **Account and Resource Management** (Gerenciamento de Recursos e de Contas) > **Todos os Meus Objetos Gerenciados**.
- 2 Selecione o contêiner adequado. Por exemplo, se desejar que o DRA pesquise informações da conta do usuário, selecione **Usuários**.
- 3 Para ver o painel de pesquisa avançada, clique em **Advanced Search** (Pesquisa Avançada).
- 4 No painel de pesquisa avançada, selecione uma consulta de Pesquisa Avançada da lista **Consultas Gravadas**.
- 5 Clique em **Load Query** (Carregar Consulta) e em **Find Now** (Localizar Agora).

Restaurando as configurações do console

O DRA permite redimensionar janelas e mantém os tamanhos das janelas. O DRA também permite manter muitas outras configurações, incluindo o último servidor de Administração ao qual você se conecta, as colunas adicionadas ou removidas dos resultados da lista e as larguras das colunas. Se desejar restaurar essas configurações para a configuração original com a qual você instalou o DRA, a opção Restore Default Settings (Restaurar Configurações Padrão) permitirá que você faça isso.

Para restaurar as configurações de console padrão:

- 1 Clique em **Ver > Opções**.
- 2 Selecione a guia **Saved settings** (Configurações Gravadas).
- 3 Revise as informações fornecidas na janela e clique em **Restore Default Settings** (Restaurar Configurações Padrão).

Restrições de caracteres especiais

Não é possível usar os seguintes caracteres especiais ao nomear contas do usuário, grupos, contatos, OUs, computadores, Telas Ativas, grupos de AA, funções, políticas ou acionadores de automação. Essas restrições de nomenclatura se aplicam ao nome do objeto, bem como o nome da regra que define o objeto.

Nomeando computadores, grupos e contas do usuário

Ao especificar um nome anterior ao Windows 2000, não é possível usar os seguintes caracteres especiais:

Barra invertida	\
Dois-pontos	:
Vírgula	,
Aspas duplas	"
Sinal de igualdade	=
Barra	/
Maior que	>
Colchete esquerdo	[
Menor que	<
Sinal de adição	+
Colchete direito]
Ponto e vírgula	;
Barra vertical	

Importante: Para Gerenciamento de Pastas Públicas, o caractere de barra invertida (\) não é suportado.

Ao nomear contas do usuário, grupos e computadores em domínios do Microsoft Windows, você pode usar qualquer caractere especial.

Nomeando contatos e OUs

Ao nomear contatos e OUs, você pode usar qualquer caractere especial.

Nomeando Telas Ativas, grupos de AAs e funções

Ao nomear Telas Ativas, grupos de AAs e funções, não é possível usar a barra invertida(\).

Nomeando políticas e acionadores de automação

Ao nomear políticas e acionadores de automação, não é possível usar a barra invertida (\).

Caracteres inválidos no Azure

Caracteres inválidos resultarão em falha na sincronização entre o Azure Active Directory e o seu diretório local. Consulte o subtópico [Directory object and attribute preparation](#) (Objeto do diretório e preparação de atributos) no site de suporte do Microsoft Office na web para saber mais sobre esses caracteres inválidos.

Para assegurar que esses caracteres não sejam usados em suas propriedades de caixa de correio online, faça o seguinte:

1. Clique no nó Configuration Management (Gerenciamento de Configurações) no Console de Delegação e Configuração e selecione **Update Administration Server Options** (Opções de Atualização do Servidor de Administração).
2. Clique em **Azure Sync** no menu da guia.
3. Clique em **Assegurar o uso obrigatório de políticas de caixa de correio online para caracteres inválidos e quantidade de caracteres** e em **OK**.

Usando caracteres curinga

O DRA suporta caracteres curinga em muitos campos nos consoles do DRA e nos comandos da CLI. Os curingas permitem definir regras que correspondem a vários objetos a uma condição ou padrão específico, como uma convenção de nomenclatura. Você pode usar curingas em vez de expressões regulares para restringir ou ampliar o escopo da regra. A correspondência de curingas não diferencia maiúsculas de minúsculas. Você também pode usar os caracteres curinga ponto de interrogação (?), asterisco (*) ou sinal numérico (#) como caracteres normais, prefixando uma barra invertida (\) no caractere curinga específico. Por exemplo, para pesquisar por abc*, digite o texto de pesquisa abc*.

O DRA suporta os caracteres curinga a seguir. Não é possível usar caracteres curinga em nomes.

Item de correspondência	Caractere	Definição
Qualquer caractere	Ponto de interrogação ?	Corresponde a exatamente um caractere
Qualquer dígito	Sinal numérico #	Corresponde a um dígito
Qualquer caractere, 0 ou mais correspondências	Asterisco *	Faz a correspondência com nenhum ou mais caracteres

A tabela a seguir fornece exemplos de especificações de caracteres curinga e com o que elas correspondem ou não.

Exemplo	Correspondências	Não Corresponde
Den???	Denton e Dennis	Denison
El ????o	El Campo e El Indio	El Paso
Houston, TX #####	Houston, TX 77024	Houston, TX USOFA

O DRA não suporta especificações de curingas que contêm operações lógicas.

Vendo seus poderes e suas funções designadas

As funções e os poderes definem como você gerencia os objetos. Uma função é um conjunto de poderes que fornece as permissões necessárias para executar uma tarefa de administração específica, como criar uma conta do usuário ou mover diretórios compartilhados.

O Administrador do DRA designa funções, adiciona você a grupos específicos do AA e o associa a Telas Ativas (conjuntos de objetos de domínio que você pode gerenciar). Você pode ver essas designações por meio do Console de Delegação e Configuração. Você não precisa de nenhum poder auxiliar para ver as funções e poderes atribuídos a você.

Para ver seus poderes e funções atribuídos:

- 1 No menu File (Arquivo), clique em **DRA Properties** (Propriedades do DRA).
- 2 Clique em **Poderes**.
- 3 Selecione a tela adequada. Por exemplo, clique em **Tela Simples** para ver uma tabela das participações de grupos do AA, funções e poderes atribuídos e Telas Ativas associadas.
- 4 Expanda o item apropriado. Por exemplo, na coluna **Tem Poder**, expanda **Roles and Powers** (Funções e Poderes) para ver funções individuais e poderes atribuídos a você.
- 5 Clique em **OK**.

Vendo o número da versão do produto e os hotfixes instalados

Você pode ver o número da versão do produto e os hotfixes instalados na janela (Propriedades do DRA). Essa janela fornece números de versão e listas de hotfixes instalados para o servidor de Administração e o computador cliente do DRA.

Para ver o número da versão do produto e os hotfixes instalados:

- 1 No File (Arquivo), clique em **DRA Properties** (Propriedades do DRA).
- 2 Clique em **Geral**.
- 3 Veja as informações de que precisa.
- 4 Clique em **OK**.

Vendo sua licença atual

O DRA requer um arquivo de chave de licença. Você pode ver a licença do seu produto de qualquer computador do servidor de Administração. Você não precisa de nenhum poder auxiliar para ver a licença do produto.

Para ver sua licença:

- 1 No menu File (Arquivo), clique em **DRA Properties**.
- 2 Clique em **Licença**.
- 3 Revise as propriedades da licença e clique em **OK**.

Recuperando uma senha do BitLocker

O Microsoft BitLocker armazena suas senhas de recuperação no Active Directory. Com os poderes adequados, você pode usar o recurso Recuperação de BitLocker do DRA para localizar e recuperar senhas perdidas do BitLocker para usuários finais.

Importante: Antes de usar o recurso Senha de Recuperação do BitLocker, verifique se o computador está atribuído a um domínio e se o BitLocker está ativado.

Vendo e copiando uma Senha de Recuperação do BitLocker

Se a senha do BitLocker de um computador for perdida, ela poderá ser redefinida usando a chave de Senha de Recuperação das propriedades do computador no Active Directory. Copie a chave de senha e forneça-a ao usuário final.

Para ver e copiar a senha de recuperação:

- 1 Inicie o Console de Delegação e Configuração e navegue até **Account and Resource Management** (Gerenciamento de Recursos e de Contas) > **Todos os Meus Objetos Gerenciados**.
- 2 Selecione o domínio e execute uma pesquisa para listar todos os computadores no domínio.
- 3 Na lista de computadores, clique com o botão direito do mouse no computador necessário e selecione **Propriedades** > **Senha de Recuperação do BitLocker**.
- 4 Clique com o botão direito do mouse na senha de recuperação do BitLocker e copie e cole o texto da senha em um arquivo texto.

Encontrando uma senha de recuperação

Se o nome de um computador foi mudado, a senha de recuperação deve ser pesquisada no domínio usando os oito primeiros caracteres do ID de senha.

Para encontrar uma senha de recuperação usando um ID de senha:

- 1 Inicie o Console de Delegação e Configuração e navegue até **Account and Resource Management** (Gerenciamento de Recursos e de Contas) > **Todos os Meus Objetos Gerenciados**.
- 2 Clique o botão direito do mouse em **Domínio Gerenciado** e clique em **Encontrar Senha de Recuperação do BitLocker**.

Para encontrar os oito primeiros caracteres da senha de recuperação, consulte [Vendo e copiando uma Senha de Recuperação do BitLocker](#).

- 3 Na página **Encontrar Senha de Recuperação do BitLocker**, cole os caracteres copiados no campo de pesquisa e clique em **Pesquisar**.

DRA Reporting

O DRA Reporting fornece relatórios integrados prontos para uso que permitem rastrear rapidamente contas duplicadas, logons da última conta, detalhes da caixa de correio do Microsoft Exchange e muito mais. O gerador de relatórios também fornece detalhes em tempo real das mudanças feitas em seu ambiente, incluindo valores antes e depois das propriedades alteradas. Você pode exportar, imprimir, ver relatórios ou publicá-los no SQL Server Reporting Services.

O DRA fornece dois métodos de geração de relatórios que permitem coletar e revisar definições de recursos, grupos e contas do usuário em seu domínio: **Relatórios de Detalhes da Atividade** e **Relatórios de Gerenciamento do DRA**. Relatórios de Detalhes da Atividade, exibidos no Console de Delegação e Configuração, fornecem informações de mudança em tempo real para objetos no seu domínio. Por exemplo, você pode ver uma lista de mudanças feitas em um objeto ou por um objeto durante um período de tempo especificado usando os relatórios de detalhes da atividade.

A figura a seguir mostra um exemplo de relatório de Detalhes da Atividade:

Operation Status	UTC Date a...	Assistant Admi...	Operation Name	Action	Object Type
Success	10/16/2009 1:...	DRDOM910\Ad...	GroupMemberAdd	MemberAdd	Group
Success	10/16/2009 1:...	DRDOM910\Ad...	GroupMemberAdd	MemberAdd	Group
Success	10/16/2009 1:...	DRDOM910\Ad...	UserSetInfo	SetInfo	User
Success	10/16/2009 1:...	DRDOM910\Ad...	UserSetInfo	SetInfo	User
Success	10/16/2009 1:...	DRDOM910\Ad...	UserSetInfo	SetInfo	User
Success	10/16/2009 1:...	DRDOM910\Ad...	UserSetInfo	SetInfo	User
Success	10/16/2009 1:...	DRDOM910\Ad...	UserSetInfo	SetInfo	User
Success	10/16/2009 1:...	DRDOM910\Ad...	UserSetInfo	SetInfo	User
Success	10/16/2009 1:...	DRDOM910\Ad...	OUMoveHere	MoveHere	User
Success	10/16/2009 1:...	DRDOM910\Ad...	UserSetInfo	SetInfo	User

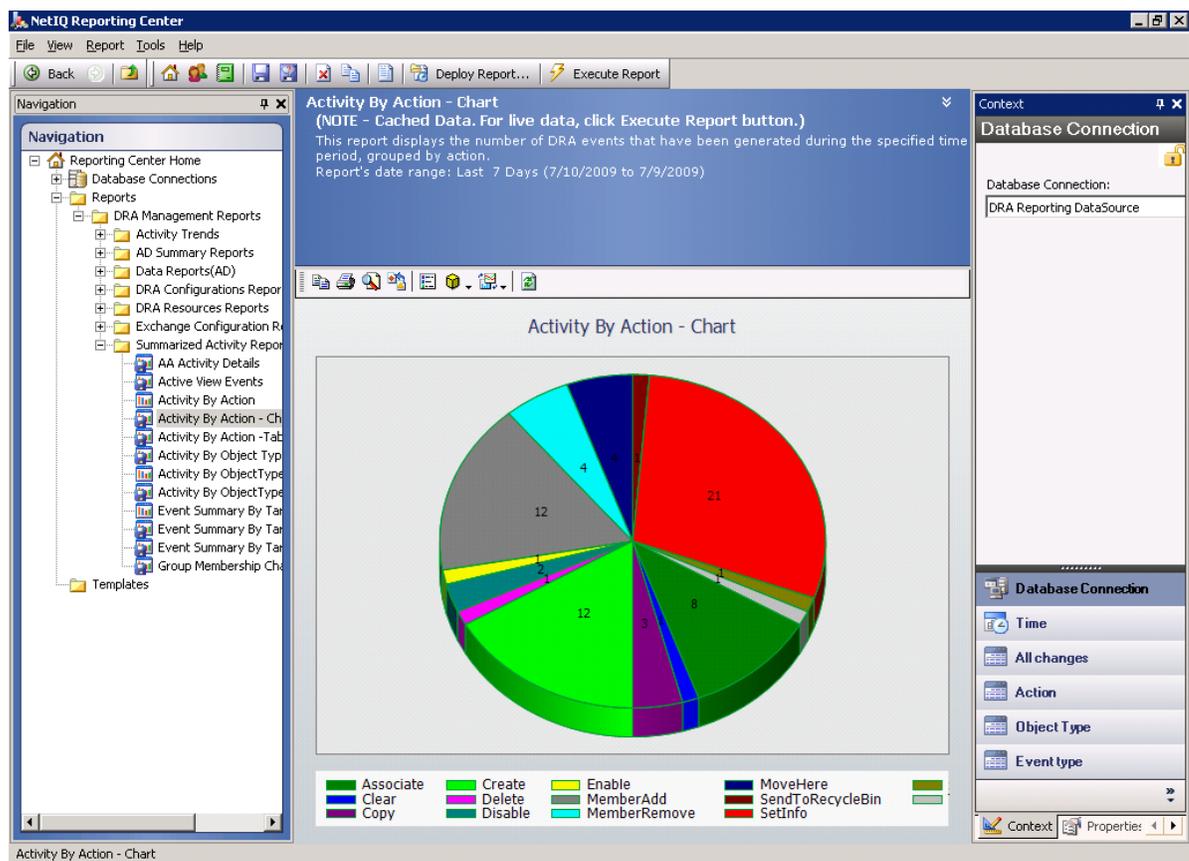
Os **Relatórios de Gerenciamento do DRA** opcionais, visualizados por meio do NetIQ Reporting Center (Reporting Center), fornecem informações de atividades, configuração e resumo sobre eventos em seus domínios gerenciados. Alguns relatórios de Gerenciamento estão disponíveis como representações gráficas dos dados. Esses relatórios integrados também podem ser personalizados para fornecer exatamente as informações de que você precisa.

Por exemplo, você pode ver um gráfico mostrando o número de eventos em cada domínio gerenciado durante um período de tempo especificado usando relatórios de Gerenciamento. O relatório também permite ver detalhes sobre o modelo de segurança do DRA, como as definições de grupo do AA e do Tela Ativa.

Você deve instalar e configurar os relatórios de Gerenciamento opcionais antes de poder vê-los. Para obter mais informações sobre como instalar componentes de relatório, consulte o *Guia de Instalação*. Para obter mais informações sobre o DRA Reporting, consulte [“DRA Reporting” na página 32](#).

Inicie o Console do Reporting Center no grupo de programas NetIQ > Reporting Center.

A figura a seguir mostra a interface do Reporting Center com os relatórios do Gerenciamento do DRA selecionados.



Para saber mais sobre o DRA Reporting, veja os seguintes tópicos:

- ♦ [“Compreendendo o DRA Reporting” na página 34](#)
- ♦ [“Como o DRA usa arquivos de registro do usuário” na página 34](#)
- ♦ [“Compreendendo datas e horários” na página 35](#)
- ♦ [“Tarefas do DRA Reporting” na página 35](#)

Compreendendo o DRA Reporting

O DRA Reporting fornece dois métodos de geração de relatórios que permitem que você veja as mudanças mais recentes em seu ambiente e colete e revise as definições de contas, grupos e recursos de usuários em seu domínio.

Relatórios de Detalhes da Atividade

Acessados por meio do nó Gerenciamento de Recursos e de Contas do Console de Delegação e Configuração, esses relatórios fornecem informações de mudança em tempo real para objetos no seu domínio.

Relatórios de gerenciamento do DRA

Acessados por meio do NetIQ Reporting Center (Reporting Center), esses relatórios fornecem informações sobre atividades, configurações e resumos sobre eventos em seus domínios gerenciados. Alguns relatórios estão disponíveis como representações gráficas dos dados.

Por exemplo, você pode ver uma lista de mudanças feitas em um objeto ou por um objeto durante um período de tempo especificado usando os relatórios de detalhes da atividade. Você também pode ver um gráfico mostrando o número de eventos em cada domínio gerenciado durante um período de tempo especificado usando relatórios de Gerenciamento. O relatório também permite ver detalhes sobre o modelo de segurança do DRA, como as definições de grupo do AA e da Tela Ativa.

O DRA desabilita funções e relatórios que sua licença não suporta. Você também deve ter os poderes adequados para executar e ver relatórios. Portanto, você pode não ter acesso a alguns relatórios.

Os relatórios de Gerenciamento do DRA podem ser instalados e configurados como um recurso opcional e vistos no Reporting Center. Quando você habilita e configura a coleta de dados, o DRA coleta informações sobre eventos auditados e os exporta para um banco de dados do SQL Server em uma programação que você define. Quando você se conecta a esse banco de dados no Reporting Center, tem acesso a mais de 60 relatórios integrados:

- ♦ Relatórios de atividades que mostram quem fez o quê e quando
- ♦ Relatórios de configuração que mostram o estado do AD ou do DRA em um determinado momento
- ♦ Relatórios de resumo que mostram o volume de atividades

Para obter mais informações sobre como configurar a coleta de dados para relatórios de Gerenciamento, consulte o *Guia do Administrador*.

Como o DRA usa arquivos de registro do usuário

Para revisar e relatar as ações do administrador assistente, o DRA registra todas as operações do usuário no arquivo de registro no computador do servidor de Administração. As operações do usuário incluem todas as tentativas de mudar definições, como atualizar contas do usuário, apagar grupos ou redefinir as Telas Ativas. O DRA também registra operações internas específicas, como

inicialização do servidor de Administração e informações relacionadas ao servidor. Além de registrar esses eventos de auditoria, o DRA registra os valores de antes e depois do evento, para que você possa ver exatamente o que mudou.

O DRA usa uma pasta, **NetIQLogArchiveData**, chamada de **arquivo de registro**, para armazenar com segurança dados de registro arquivados. O DRA arquiva os registros ao longo do tempo e apaga os dados mais antigos para liberar espaço para dados mais recentes por meio de um processo chamado **grooming**.

O DRA usa os eventos de auditoria armazenados nos arquivos de registro para exibir relatórios de detalhes de atividades, como mostrar quais mudanças foram feitas em um objeto durante um período especificado. Você também pode configurar o DRA para exportar informações desses arquivos de registro para um banco de dados do SQL Server que o NetIQ Reporting Center usa para exibir relatórios de Gerenciamento.

O DRA sempre grava eventos de auditoria no arquivo de registro. Você também pode habilitar ou desabilitar a gravação de eventos do DRA nos registros de eventos do Windows.

Para obter mais informações sobre a auditoria do DRA, consulte o *Guia do Administrador*.

Compreendendo datas e horários

O DRA usa o **Estilo de data abreviada** e **Estilo de hora** especificados no aplicativo Configurações Regionais no Painel de Controle para exibição do relatório. Os relatórios do DRA mostram a data e a hora UTC, além da data e da hora local dos eventos. Os relatórios do DRA suportam os seguintes formatos de data:

- ◆ m/d/aa
- ◆ m-d-aa
- ◆ m/d/aaaa
- ◆ m-d-aaaa
- ◆ mm/dd/aa
- ◆ mm-dd-aa
- ◆ mm/dd/aaaa
- ◆ mm-dd-yyyy
- ◆ dd/mm/aa
- ◆ dd-mm-aa
- ◆ dd/mm/aaaa
- ◆ dd-mm-aaaa

Tarefas do DRA Reporting

Para gerar relatórios de Gerenciamento do DRA, instale o Reporting Center e habilite a coleta de dados no DRA. Para obter mais informações sobre como habilitar a coleta de dados, consulte o *Guia do Administrador*. Para gerar relatórios de Detalhes da atividade, clique o botão direito do mouse sobre qualquer objeto e clique em **Reporting** (Gerador de relatórios) para ver suas escolhas de relatórios sobre esse objeto. As seções a seguir guiam você pelas várias tarefas do Reporting (Gerador de relatórios).

Vendo relatórios de detalhes da atividade

Os relatórios de detalhes da atividade exibem informações sobre mudanças em seu ambiente. Você pode ver ou imprimir um relatório, bem como gravar um relatório no formato Excel, CSV ou TXT. Para ver ou imprimir relatórios, você deve estar associado à função Administração do Gerador de relatórios.

Ao ver relatórios, insira critérios para especificar o período de tempo sobre o qual você deseja exibir informações. Você também pode optar por visualizar um relatório limitado a mudanças feitas em servidores DRA específicos e pode limitar o número de linhas a serem incluídas no relatório. Se o tamanho do relatório exceder um dos seguintes limites, o DRA exibirá uma mensagem informando que o relatório não está concluído:

- ♦ O tamanho excede 500 MB
- ♦ O tempo necessário para consultar todos os servidores do DRA excede 5 minutos
- ♦ O número de linhas a serem exibidas excede 1.000

Você tem a opção de ver o relatório que contém apenas as informações recuperadas antes de atingir um desses limites ou pode mudar os critérios do relatório para ver um relatório que atenda a esses limites.

Para ver um relatório:

- 1 No painel esquerdo, expanda **Todos os Meus Objetos Gerenciados**.
- 2 Para especificar o objeto para o qual você deseja ver um relatório, conclua as etapas a seguir:
 - 2a **Se você souber o local do objeto**, selecione o domínio e a OU que contém esse objeto.
 - 2b No painel de pesquisa, especifique os atributos do objeto e clique em **Find Now** (Localizar Agora).
- 3 No painel de lista, clique o botão direito do mouse no objeto e clique em **Reporting** (Gerador de relatórios).
- 4 Selecione o tipo de relatório, como **Mudanças feitas no objectName** ou **Mudanças feitas por objectName**. Os relatórios disponíveis variam dependendo do tipo de objeto selecionado.
- 5 Selecione as datas de início e término para especificar as mudanças que você deseja ver.
- 6 **Se desejar mudar o número de linhas a serem exibidas**, digite um número acima do valor padrão de 250.

Observação: O número de linhas exibidas aplica-se a cada servidor de Administração em seu ambiente. Se você incluir 3 servidores de Administração no relatório e usar o valor padrão de 250 linhas para exibir, até 750 linhas poderão ser exibidas no relatório.

- 7 **Se desejar incluir apenas servidores de Administração específicos no relatório**, selecione **Restrict query to these DRA servers** (Restringir consulta a esses servidores do DRA) e digite o nome do servidor ou os nomes que você deseja incluir no relatório. Separe vários nomes de servidores com vírgulas.
- 8 Clique em **OK**.

Observação: O DRA pode levar até 5 segundos para exibir as alterações recentes nos relatórios. Portanto, aguarde pelo menos 5 segundos após fazer uma mudança antes de tentar ver um relatório que contenha a mudança.

Exportando relatórios de detalhes da atividade

Você pode exportar relatórios de Detalhes da atividade nos seguintes formatos: XLS, CSV e TXT. O formato padrão é o formato do Microsoft Excel.

Para exportar relatórios de detalhes da atividade:

- 1 Na janela do relatório, no menu Arquivo, clique em **Visualizar e Exportar**.
- 2 Na janela de Visualização, no menu Arquivo, clique em **Exportar Documento > Arquivo Excel**.
- 3 Selecione as opções de exportação e clique em **OK**.
- 4 Na janela Gravar como, digite um nome para o arquivo e clique em **Gravar**.

Imprimindo relatórios de detalhes da atividade

Para imprimir relatórios, você deve estar associado à função de Administração do Gerador de relatórios. Você pode ver ou imprimir relatórios de detalhes da atividade, além de gravar um relatório em vários formatos.

Para imprimir relatórios de detalhes da atividade:

- 1 Na janela do relatório, no menu Arquivo, clique em **Visualizar e Exportar**.
- 2 Na janela de Visualização, no menu Arquivo, clique em **Imprimir**.

Vendo relatórios de gerenciamento

Você deve instalar o DRA Reporting e configurar os coletores de dados do DRA para poder ver relatórios de Gerenciamento no Reporting Center. Para obter mais informações sobre como instalar o DRA Reporting e configurar os DRA Collectors, consulte o *Guia do Administrador*.

Quando você faz logon no Reporting Center, o Serviço da Web usa o IIS para validar as credenciais da conta de acordo com a forma como você configurou o Serviço da Web durante a instalação.

Para ver relatórios de Gerenciamento:

- 1 Efetue login no computador que está executando o console do Reporting Center.
- 2 Inicie o **Console do Reporting Center** no grupo de programas NetIQ > Reporting Center.
- 3 Forneça as informações necessárias na caixa de diálogo Logon e clique em **Efetuar logon**.
- 4 No painel de Navegação, expanda **Relatórios > Relatórios de Gerenciamento do DRA**.
- 5 Expanda as categorias do relatório até encontrar um relatório que você deseja ver.
- 6 Clique no nome do relatório no painel de Navegação e o relatório será carregado no painel de Resultados do centro, exibindo dados em cache.
- 7 **Se desejar ver o relatório usando os dados mais recentes**, clique em **Executar Relatório** no Painel de Resultados.

Você pode mudar as configurações de contexto padrão para exibir diferentes resultados do relatório. Para obter mais informações sobre as configurações de contexto no Reporting Center, consulte o *Guia do Administrador*.

Personalizando relatórios de gerenciamento

Mais de 60 relatórios de Gerenciamento são enviados com o DRA. O Reporting Center oferece a flexibilidade de personalizar e implantar esses relatórios de várias formas. Para obter mais informações sobre como personalizar e implantar relatórios de Gerenciamento no Reporting Center, consulte o *Guia do Administrador*.

Para personalizar um relatório de Gerenciamento:

- 1 Veja um relatório semelhante a um relatório que você deseja criar. Para obter mais informações, consulte [Vendo relatórios de gerenciamento](#).
- 2 Personalize o relatório mudando as propriedades do relatório e as configurações de contexto para exibir as informações desejadas.
- 3 Clique em **Executar Relatório**.
- 4 No menu Relatório, clique em **Gravar Relatório Como** e especifique um título e um local de relatório para gravar o novo relatório.
- 5 Clique em **Gravar**.

Para obter mais informações sobre como trabalhar com relatórios de Gerenciamento no Reporting Center, consulte o *Guia do Administrador*.

3 Pesquisando objetos

Este capítulo contém informações conceituais e de procedimento sobre as funcionalidades de Pesquisa e Pesquisa LDAP.

- ♦ “Pesquisa” na página 39
- ♦ “Pesquisa Avançada” na página 42

Pesquisa

O DRA permite que você pesquise objetos em locatários do Azure, do Microsoft Exchange e de domínios locais do Active Directory. Pesquise usuários, grupos e contatos em seus locatários do Azure, objetos como usuários, grupos, contatos, computadores, impressoras, OUs e gMSA (contas de serviço gerenciado do grupo) em seus domínios do Active Directory e objetos como caixas de correio de sala, caixas de correio de equipamentos, caixas de correio compartilhadas e grupos de distribuição dinâmica no Exchange. Use os filtros de pesquisa para fazer pesquisas mais eficientes e eficazes. O DRA trunca automaticamente quaisquer espaços à esquerda ou à direita da sua entrada de pesquisa e retorna os resultados da pesquisa.

Para acessar o recurso de pesquisa no Console da Web, navegue até **Gerenciamento > Pesquisa**. Para executar uma pesquisa, selecione um ou mais filtros, selecione uma opção de Pesquisar por, digite um termo de pesquisa e clique em **Pesquisar**.

Por exemplo, a pesquisa executada abaixo retornou todos os usuários no domínio ou container selecionado cujo sobrenome era “Beck” ou cujo sobrenome terminava com essas quatro letras.

Pesquisar por	Termo de pesquisa digitado	Filtro selecionado 
♦ Nome	beck	Usuário
♦ termina com		

Observação: Para obter um retorno preciso dos objetos pesquisados ao usar filtros, quaisquer mudanças feitas na paginação devem ser feitas antes da aplicação dos filtros e da execução da pesquisa. Mudar a configuração de **itens por página** na parte inferior do Console da Web quando filtros de tipo de objeto são aplicados não é uma ação suportada.

Para acessar o recurso de pesquisa no Console de Delegação e Configuração, navegue até Account and Resource Management (Gerenciamento de Recursos e de Contas) e clique em **Accounts and Resources** (Contas e Recursos) no painel de exibição.

- ♦ “Usando caracteres curinga” na página 40
- ♦ “Pesquisa em vários campos” na página 40
- ♦ “Adicionando e classificando colunas” na página 41
- ♦ “Exportando os resultados da pesquisa” na página 41

Usando caracteres curinga

O DRA suporta caracteres curinga como o ponto de interrogação (?), o asterisco (*) ou a cerquilha (#) para maximizar seus resultados de pesquisa. A correspondência de curingas não diferencia maiúsculas de minúsculas.

A tabela a seguir fornece exemplos de especificações de caracteres curinga e com o que elas correspondem ou não.

Caractere	Item de correspondência
Ponto de interrogação ?	Qualquer caractere ou dígito
Cerquilha #	Qualquer dígito
Asterisco *	Qualquer número de caracteres ou dígitos

Pesquisa em vários campos

A opção de Correspondência de Vários Campos permite que você pesquise correspondências para vários atributos com apenas uma pesquisa. Quando você pesquisa usando a Correspondência de Vários Campos, sua string de pesquisa é comparada a vários atributos, como nome, nome de exibição e sobrenome, e, se a string de pesquisa corresponde a qualquer um desses atributos, o objeto é retornado nos resultados da pesquisa.

A opção Correspondência de Vários Campos suporta exclusivamente o critério de pesquisa "**começa com**".

Por exemplo, se você tiver dois usuários, um cujo *nome de exibição* é "Martin Smith" e outro cujo nome principal é `martha.jones@acme.com`, e você realizar uma pesquisa usando a string "Mart", ambos os usuários serão retornados nos resultados da pesquisa.

A tabela abaixo lista os atributos que são pesquisados para cada tipo de objeto:

Tipo de Objeto	Atributos Pesquisados
Contato do Azure	displayName, givenName, mail, mailNickname, surname
Grupo do Azure	displayName, mail
Usuário do Azure	displayName, employeeId, givenName, mail, surname, userPrincipalName
Computador	displayName, name, sAMAccountName
Contato	displayName, employeeId, givenName, mail, mailNickname, name, surname
Grupo de Distribuição Dinâmica	displayName, mail, mailNickname, name
Grupo	displayName, mail, mailNickname, name, sAMAccountName
Conta de Serviço Gerenciado do Grupo	displayName, name, sAMAccountName

Tipo de Objeto	Atributos Pesquisados
Unidade Organizacional	nome
Lixeira	name, sAMAccountName
Usuário	displayName, employeeId, givenName, mail, mailNickname, name, sAMAccountName, surname

Observação: O recurso de correspondência múltipla não é suportado em pesquisas do Seletor de Objetos no Console de Delegação e Configuração ao adicionar delegados ou permissões para os objetos do Exchange listados abaixo:

- ♦ caixa de correio do usuário
- ♦ usuário habilitado para correio
- ♦ grupo habilitado para correio
- ♦ contato habilitado para correio
- ♦ grupo de distribuição dinâmica
- ♦ caixa de correio compartilhada
- ♦ caixa de correio de recursos

Adicionando e classificando colunas

Você pode classificar os objetos de resultado de pesquisa por qualquer um dos atributos a seguir quando clica no cabeçalho da coluna de um atributo:

- ♦ Álias
- ♦ Nome de exibição
- ♦ E-mail
- ♦ EmployeeID
- ♦ Nome
- ♦ Sobrenome
- ♦ Local
- ♦ Nome
- ♦ Nome anterior ao Windows 2000
- ♦ Nome Principal do Usuário

Para adicionar ou remover colunas de atributo, clique no ícone de coluna.

Exportando os resultados da pesquisa

O DRA permite que os administradores assistentes exportem os resultados da **Pesquisa** do Console da Web para um arquivo CSV. Para exportar os resultados da **Pesquisa** do Console da Web, acesse **Gerenciamento > Pesquisa** e clique no ícone **Fazer Download**.

Observação: Apenas as colunas selecionadas são exportadas. Se você quiser dados adicionais, não exibidos no momento, adicione essas colunas primeiro e, em seguida, exporte os resultados da Pesquisa.

Pesquisa Avançada

O DRA permite que você realize consultas LDAP e de atributo virtual em seus domínios do Active Directory por meio da página de Pesquisa Avançada. Você pode pesquisar usando uma consulta existente, modificar uma consulta existente, criar uma consulta e gravar consultas novas e modificadas para uso futuro como consultas públicas ou particulares. Use os filtros de pesquisa para pesquisas mais eficientes e eficazes.

Para acessar o recurso de consultas de Pesquisa Avançada no Console da Web, navegue até [Gerenciamento > Pesquisa Avançada](#).

Para acessar consultas de Pesquisa Avançada no Console de Delegação e Configuração, selecione o domínio, o locatário do Azure ou o subnó em Account and Resource Management (Gerenciamento de Recursos e de Contas) e clique em [Pesquisa Avançada](#) na barra de ferramentas.

Consultas de Pesquisa Avançada

O DRA suporta consultas LDAP e de atributo virtual para pesquisar objetos do DRA e do Active Directory. Atributos virtuais podem ser associados a tipos de objetos do Active Directory como usuários, grupos, grupos de distribuição dinâmica, contatos, computadores e OUs. Com uma consulta de atributo virtual, você pode filtrar os resultados retornados da consulta LDAP para retornar apenas aqueles resultados que correspondem à consulta de atributo virtual. As strings de consulta de atributo virtual devem começar com `(objectCategory=<tipo do objeto>)`. Para realizar uma consulta de atributo virtual, você deve especificar strings tanto para as consultas LDAP quanto para as de atributo virtual.

Exemplos de consulta LDAP:

- ♦ Para pesquisar “todos os objetos computador” no DRA:

Consulta LDAP: `(objectCategory=computer)`

- ♦ Para pesquisar objetos usuário com a descrição “Vendas Leste\Oeste” no DRA:

Consulta LDAP: `(&(objectCategory=user)(description=East\5CWest Sales))`

- ♦ Para pesquisar “todos os objetos computador” no DRA:

Consulta LDAP: `(objectCategory=computer)`

Importante: O caractere de barra invertida deve ser usado como prefixo em filtros LDAP. Substituir `\5C`.

- ♦ Para “listar todos os objetos usuário” no DRA:

Consulta LDAP:

```
(&(objectCategory=person)(objectClass=user)(userAccountControl:1.2.840.113556.1.4.803:=2))
```

A string 1.2.840.113556.1.4.803 especifica LDAP_MATCHING_RULE_BIT_AND. Isso especifica um operador de lógica binária AND de um atributo de flag (um inteiro), como userAccountControl, groupType ou systemFlags, bem como uma máscara de bits (como 2, 32 ou 65536). A cláusula será True se o operador de lógica binária AND do valor de atributo e a máscara de bits forem não zero, indicando que o bit está definido.

Exemplos de consulta de atributo virtual:

- ♦ Para encontrar todos os usuários cujo nome da empresa é ABC:

Consulta: (&(objectCategory=User)(CompanyName=ABC))

O objeto DRA é "User" e o atributo virtual é "CompanyName" (associado a user).

- ♦ Para encontrar todos os usuários com o nome de empresa ABC no domínio Storage:

Consulta: (&(objectCategory=User)(CompanyName=ABC)(Domain=Storage))

O objeto DRA é "User" e os atributos virtuais são "CompanyName" e "Domínio" (associados a user)

- ♦ Para encontrar todos os grupos com o nome do produto DRA ou todos os usuários com o nome da empresa ABC:

Consulta:

```
( | (&(objectCategory=Group)(ProductGroupName=DRA)) (&(objectCategory=User)(CompanyName=ABC)) )
```

Os objetos DRA são "User" e "Group" e os atributos virtuais são CompanyName (associado a user) e ProductGroupName (associado a group).

- ♦ Para encontrar todos os grupos cujo nome de produto é DRA ou todos os usuários com o nome de empresa ABC no domínio Storage:

Consulta:

```
( | (&(objectCategory=Group)(ProductGroupName=DRA)) (&(objectCategory=User)(CompanyName=ABC)(Domain=Storage)) )
```

Os objetos DRA são "User" e "Group" e os atributos virtuais são CompanyName (associado a user), ProductGroupName (associado a group) e Domain (associado a user).

Gerenciando consultas avançadas

O DRA usa LDAP para suportar o recurso de Pesquisa Avançada. Ao utilizar consultas avançadas, é possível pesquisar usuários, contatos, grupos, computadores, OUs e qualquer outro objeto suportado pelo DRA. Se você tiver poderes para Executar Consultas Avançadas Gravadas, execute as consultas avançadas disponíveis nas listas [Minhas Pesquisas](#) e [Pesquisas Públicas](#) para qualquer container.

Além de executar uma pesquisa com uma consulta avançada gravada e visualizar os detalhes dela, você também poderá fazer o seguinte com consultas avançadas da página Pesquisa Avançada, se tiver as permissões aplicáveis:

Criar uma consulta

Crie uma consulta avançada no servidor de Administração principal ou no servidor de Administração secundário fornecendo a string de consulta (LDAP e, se aplicável, atributo virtual) para a nova consulta avançada. Após executar a pesquisa, expanda o menu suspenso **Pesquisa** para gravar a consulta na lista Minhas Pesquisas ou na lista Pesquisas Públicas.

Modificar uma consulta

Selecione uma consulta avançada existente em Minhas Pesquisas ou em Pesquisas Públicas e use a opção **Modificar** para mudar qualquer um dos critérios de pesquisa. Depois que você executar a pesquisa com os critérios de pesquisa atualizados, se quiser, poderá expandir o menu suspenso **Pesquisa** e selecionar **Gravar** para gravar as mudanças nessa consulta.

Copiar uma consulta

Selecione uma consulta avançada existente em Minhas Pesquisas ou em Pesquisas Públicas e execute a pesquisa. Após executar a pesquisa, expanda o menu suspenso **Pesquisa** e selecione **Gravar Como** para gravar a consulta com um nome diferente.

Personalizar os resultados da consulta

O DRA fornece um conjunto padrão de colunas na lista de resultados da pesquisa. Para personalizar os resultados da pesquisa de uma consulta gravada ou não gravada, clique no ícone  de **Adicionar/Remover Colunas** no lado direito da página para mudar o modo como os resultados da pesquisa são exibidos.

Apagar uma consulta

Você pode apagar qualquer consulta avançada que esteja na lista **Minhas Pesquisas**. Com as permissões aplicáveis, você também pode apagar consultas avançadas na lista **Pesquisas Públicas**. Para apagar uma consulta avançada gravada, selecione-a na lista aplicável e clique em **Apagar** no menu suspenso Pesquisa.

Limpar uma consulta

No Console da Web, é possível limpar os campos de formulário de uma consulta gravada ou não gravada para fazer mudanças de um formulário limpo. Para limpar os campos em uma consulta, selecione **Limpar** no menu suspenso Pesquisa.

Exportando os resultados da pesquisa avançada

O DRA permite que os administradores assistentes exportem os resultados da **Pesquisa Avançada** do Console da Web para um arquivo CSV. Para exportar os resultados da **Pesquisa Avançada** do Console da Web, acesse **Gerenciamento > Pesquisa Avançada** e clique no ícone **Fazer Download**.

Observação: Apenas as colunas selecionadas são exportadas. Se você quiser dados adicionais, não exibidos no momento, adicione essas colunas primeiro e, em seguida, exporte os resultados da **Pesquisa Avançada**.

4 Gerenciando Objetos do Active Directory

Este capítulo contém informações conceituais e de procedimentos para o gerenciamento de contas do usuário, grupos, grupos dinâmicos, grupos de distribuição dinâmica e contatos tanto no nó Gerenciamento de Recursos e de Contas do Console de Delegação e Configuração quanto no Console da Web. As informações para contas do usuário são mais abrangentes para fornecer um exemplo de como gerenciar objetos em geral em ambos os aplicativos cliente.

- ♦ [“Gerenciando contas do usuário” na página 45](#)
- ♦ [“Gerenciando grupos” na página 52](#)
- ♦ [“Gerenciando grupos de distribuição dinâmica” na página 58](#)
- ♦ [“Gerenciando grupos dinâmicos” na página 60](#)
- ♦ [“Gerenciando contatos” na página 64](#)
- ♦ [“Gerenciando Contas de Serviço Gerenciadas do Grupo” na página 65](#)

Gerenciando contas do usuário

O Microsoft Windows depende do tipo de conta do usuário para determinar as permissões de acesso para a conta do usuário associada. Uma conta do usuário pode ser global ou local. O DRA também suporta objetos InetOrgPerson, mas reconhece objetos InetOrgPerson como usuários normais.

Conta do usuário global

Uma conta do usuário que pode ser usada em qualquer domínio que confie no domínio em que a conta do usuário foi criada. Você pode conceder permissões específicas para uma conta do usuário. Você também pode tornar uma conta do usuário um membro de um grupo e atribuir permissões a esse grupo. Agrupar contas do usuário ajuda a simplificar o processo de gerenciamento de permissões de rede para muitas contas do usuário.

Conta do usuário local

Uma conta do usuário local é igual a qualquer conta que você usa para efetuar login em um sistema operacional Windows. Ela permite-lhe acessar os recursos do sistema em seu próprio espaço de usuário.

Para saber mais sobre como gerenciar contas do usuário, veja os seguintes tópicos:

- ♦ [“Contas do usuário em domínios confiáveis” na página 46](#)
- ♦ [“Tarefas de gerenciamento de contas do usuário” na página 46](#)
- ♦ [“Transformando contas do usuário” na página 49](#)

Contas do usuário em domínios confiáveis

O Microsoft Windows armazena as definições de grupos e contas do usuário no diretório do domínio gerenciado. Portanto, um servidor de Administração não pode modificar as informações de diretório de um domínio confiável, a menos que esse domínio também seja gerenciado pelo DRA.

Por exemplo, no Gerenciamento de Recursos e de Contas, talvez você veja contas e grupos de usuários que não podem ser modificados. Esses grupos e contas do usuário são definidos em domínios confiáveis por um dos domínios gerenciados. No entanto, você pode adicionar contas e grupos de um domínio confiável a outros grupos no domínio gerenciado.

Tarefas de gerenciamento de contas do usuário

Esta seção orienta você na administração de contas do usuário no nó Gerenciamento de Recursos e de Contas do Console de Delegação e Configuração e no Console da Web. Com os poderes adequados, você pode executar várias tarefas de gerenciamento de contas do usuário, como criar e apagar contas. Se você selecionar várias contas do usuário, poderá executar tarefas selecionadas em uma operação, como apagar, mover ou adicionar usuários a um grupo. Para obter mais informações sobre seus poderes designados, consulte [Vendo seus poderes e suas funções designadas](#).

Tarefas de conta do usuário em no Gerenciamento de Recursos e de Contas

Você pode executar todas as tarefas aplicáveis abaixo do menu **Tarefas** ou no menu do botão direito do mouse. Geralmente, você seleciona o nó **Todos os Meus Objetos Gerenciados** e executa a operação **Find Now** (Localizar Agora) para localizar e selecionar o objeto usuário desejado. O menu Tarefas indica quais tarefas você pode executar quando seleciona uma ou várias contas do usuário. Mais opções estarão disponíveis para um único usuário.

No caso de criar um novo usuário, você deve selecionar o domínio ou a OU em que deseja criar o usuário. Por exemplo:

1. Selecione o container **Usuários** em um domínio em Todos os Meus Objetos Gerenciados.
2. Selecione **Novo > Usuário** no menu Tarefas.
3. Conclua as etapas do Assistente Criar Usuário.

Gerenciar sua própria conta

Você pode gerenciar sua própria conta modificando propriedades gerais, como seu número de telefone. Antes de gerenciar sua conta, verifique se você tem o poder adequado.

Copiar uma conta do usuário para outra Tela Ativa

Você pode copiar uma conta do usuário para outra Tela Ativa. Essa ação é chamada de transferência de uma conta do usuário. Para copiar uma conta do usuário para outra Tela Ativa, você precisa do poder Copiar Usuário para Outra Tela Ativa nas Telas Ativas de origem e de destino. Transferir uma conta do usuário para outra Tela Ativa não remove a conta do usuário da Tela Ativa de origem.

Observação: Só é possível copiar uma conta do usuário para outra Tela Ativa do Console de Delegação e Configuração por meio do nó Gerenciamento de Recursos e de Contas.

Renomear uma conta do usuário

Você pode renomear contas do usuário no domínio gerenciado ou na subárvore gerenciada. Mudar o nome de logon do usuário também muda o nome da caixa de correio associada à conta do usuário.

Tarefas da conta do usuário no Console da Web

Você pode executar a maioria das tarefas abaixo na guia **Gerenciamento** > **Pesquisar** no Console da Web. Execute uma operação de pesquisa para localizar e selecionar o objeto usuário necessário. Depois de selecionar um ou mais objetos na lista, a barra de tarefas fica ativa com opções da barra de ferramentas e opções de menu suspenso para **Contas** e **Exchange**. Passe o mouse sobre um ícone da barra de ferramentas ou clique em um menu suspenso para exibir as funções ou as opções.

Criar uma conta do usuário

Você pode criar contas do usuário no domínio gerenciado ou na subárvore gerenciada. Você também pode modificar propriedades, criar uma caixa de correio, habilitar e-mail e especificar participações de grupo para a nova conta.

Observação

- ♦ Sua empresa pode ter uma convenção de nomenclatura aplicada por meio de uma política que determina o nome que você pode designar à nova conta do usuário.
 - ♦ Por padrão, o DRA coloca a nova conta do usuário na OU de Usuários do domínio gerenciado.
 - ♦ Não é possível criar objetos InetOrgPerson no DRA.
-

Clonar uma conta do usuário

Quando você clona uma conta do usuário, todos os grupos dos quais o usuário é membro são adicionados automaticamente à nova conta do usuário, economizando tempo na configuração da nova conta. Você pode adicionar ou remover grupos da nova conta, habilitar e-mails e fazer qualquer outra configuração de propriedade como faria com qualquer nova conta.

Observação: Quando você clona um objeto InetOrgPerson, uma conta do usuário é criada.

Modificar propriedades da conta do usuário

Você pode gerenciar as propriedades de contas do usuário no domínio gerenciado ou na subárvore gerenciada. Os seus poderes determinam quais propriedades você pode modificar para uma conta do usuário. Se você instalou o Exchange e habilitou o suporte do Microsoft Exchange, poderá modificar as propriedades de caixa de correio associadas enquanto gerencia as contas do usuário.

Observação: Se as políticas do diretório pessoal estiverem habilitadas, o DRA modificará automaticamente o diretório pessoal de uma conta do usuário quando você gerencia essa conta. Por exemplo, quando você muda o local do diretório pessoal, o DRA tenta criar o diretório pessoal especificado e mover o conteúdo do diretório pessoal para o novo local. O DRA também aplica as ACLs atribuídas do diretório anterior ao novo diretório.

Observação: O DRA permite que você exporte os resultados de **Membro De** como um arquivo CSV. Para exportar os resultados de **Membro De** do Console da Web, acesse **Gerenciamento > Pesquisa** e clique em **Propriedades**. Navegue até a guia **Membro De** e clique no ícone **Fazer Download**. As mudanças não gravadas não são exportadas. Grave quaisquer mudanças recentes para que elas estejam disponíveis no arquivo exportado.

Habilitar uma conta do usuário

Você pode habilitar uma conta do usuário no domínio gerenciado ou na subárvore gerenciada. Se você estiver gerenciando uma conta do Microsoft Windows, poderá especificar o controlador de domínio no qual o DRA aplica essa mudança.

Quando você aplica essa mudança a um controlador de domínio específico, o DRA também aplica essa mudança ao controlador de domínio padrão desse domínio gerenciado. Para verificar qual controlador de domínio padrão o DRA está usando, veja as propriedades do domínio.

Desabilitar uma conta do usuário

Você pode desabilitar uma conta do usuário no domínio gerenciado. Se você estiver gerenciando uma conta do Microsoft Windows, poderá especificar o controlador de domínio no qual o DRA aplica essa mudança.

Quando você aplica essa mudança a um controlador de domínio específico, o DRA também aplica essa mudança ao controlador de domínio padrão desse domínio gerenciado. Para verificar qual controlador de domínio padrão o DRA está usando, veja as propriedades do domínio.

Desbloquear uma conta do usuário

Você pode desbloquear uma conta do usuário no domínio gerenciado ou na subárvore gerenciada.

Como o DRA recupera o status da conta do usuário do cache de contas, a interface do usuário pode indicar que a conta selecionada está desbloqueada quando na verdade está bloqueada. O DRA permite desbloquear uma conta do usuário, mesmo que o status da conta indique que ela está desbloqueada no momento. Você também pode especificar um controlador de domínio ao desbloquear uma conta do usuário usando o console do DRA sem precisar redefinir a senha da conta do usuário.

Redefinir uma senha da conta do usuário

Você pode redefinir a senha de uma conta no domínio gerenciado ou na subárvore gerenciada. Os seus poderes determinam os campos que você pode mudar para essa conta do usuário.

Quando você redefine a senha de uma conta do usuário, o DRA desbloqueia automaticamente a conta. Você pode selecionar se o DRA gera uma nova senha para a conta do usuário. Você também pode modificar várias opções relacionadas à senha para a conta. Se você estiver gerenciando uma conta do Microsoft Windows, poderá especificar o controlador de domínio no qual o DRA aplica essas mudanças

Observação: Quando você aplica essa mudança a um controlador de domínio específico, o DRA também aplica essa mudança ao controlador de domínio padrão desse domínio gerenciado. Para verificar qual controlador de domínio padrão o DRA está usando, veja as propriedades do domínio.

Mover uma conta do usuário para outro contêiner

Você pode mover uma conta do usuário para outro contêiner, como uma OU, no domínio gerenciado ou na subárvore gerenciada.

Apagar uma conta do usuário

Você pode apagar uma conta do usuário no domínio gerenciado ou na subárvore gerenciada. Se a Lixeira estiver desabilitada para esse domínio, apagar uma conta do usuário a removerá permanentemente do Active Directory. Se a Lixeira estiver habilitada para esse domínio, apagar uma conta do usuário moverá a conta do usuário para a Lixeira.

Aviso: Quando você cria uma conta do usuário, o Microsoft Windows designa um Identificador de Segurança (SID) a essa conta. O SID não é gerado do nome da conta. O Microsoft Windows usa SIDs para registrar privilégios em listas de controle de acesso (ACLs) para cada recurso. Se você apagar uma conta do usuário, não poderá retornar recursos de acesso para essa conta criando uma nova conta do usuário com o mesmo nome.

Especificar participações do grupo para contas do usuário

Você pode adicionar ou remover contas do usuário de um grupo específico no domínio gerenciado ou na subárvore gerenciada. Você também pode ver ou modificar propriedades de grupos existentes aos quais essa conta pertence.

Transformando contas do usuário

O DRA oferece a capacidade de transformar de forma rápida e eficiente as contas do usuário. Quando o indivíduo associado a uma conta do usuário faz a transição para novas responsabilidades de trabalho, você pode usar os recursos de transformação do DRA. Aproveitando os modelos de função de trabalho, você pode adicionar, remover ou atualizar rapidamente as participações de grupo associadas a uma conta. Independentemente de um indivíduo ser promovido, mudar de departamento ou deixar a empresa, a capacidade de transformar uma conta do usuário economizará tempo, dinheiro e suposições.

Compreendendo o processo de transformação

Você pode usar os recursos de conta do usuário de transformação para atender a qualquer uma das seguintes necessidades:

- ♦ Remover participações do grupo de uma conta do usuário
- ♦ Adicionar participações do grupo a uma conta do usuário
- ♦ Mudar propriedades de usuários
- ♦ Remover participações de grupos específicos ao adicionar outras participações de grupo a uma conta do usuário

Considere o seguinte processo antes de tentar transformar uma conta do usuário:

- 1 Decida se você precisa adicionar, remover ou adicionar e remover participações de grupos.
- 2 Revise seus modelos atuais subtrativos e aditivos para garantir que você tenha os modelos de conta do usuário necessários.

3 Se necessário, crie as contas do modelo necessárias.

4 Conclua o assistente de Transformar Usuário.

À medida que o DRA transforma um usuário, as participações do grupo designadas pelo modelo subtrativo são removidas da conta do usuário, enquanto as participações designadas pelo modelo aditivo são atribuídas à conta do usuário. O DRA deixa todas as participações fora dos modelos subtrativos ou aditivos intactas. Por exemplo, um indivíduo em seu departamento de vendas externo é transferido das vendas dos EUA para vendas na Europa. Em sua organização, você tem grupos de distribuição e grupos de segurança exclusivos para essas equipes de vendas e um número que é compartilhado entre todas as equipes de vendas. A equipe de vendas dos EUA tem os grupos de distribuição Lista de Distribuição de Hotspots dos EUA e Lista de Distribuição de Gerenciamento de Vendas dos EUA, enquanto a equipe de vendas europeia tem os grupos de distribuição Hotspots da Europa e Gerenciamento de Vendas da Europa. Ambas as equipes são membros do grupo Segurança de vendas global, mas também têm grupos de segurança específicos do local.

Ao seu modelo subtrativo, chamado US Sales Template, seriam designadas as seguintes participações de grupo:

- ♦ Lista de Distribuição de Hotspots dos EUA
- ♦ Lista de Distribuição de Gerenciamento de Vendas dos EUA
- ♦ Segurança de vendas global
- ♦ US Sec

Ao seu modelo aditivo, chamado Euro Sales Template, seriam designadas as seguintes participações de grupo:

- ♦ Euro Hotspots DL
- ♦ Lista de Distribuição de Gerenciamento de Vendas da Europa
- ♦ Segurança de vendas global
- ♦ Euro Sec

Durante o processo de transformação, a conta do usuário do vendedor transferida é primeiramente removida de todas as participações de grupo designadas pelo US Sales Template e, depois, adicionada a todas as participações de grupo designadas pelo Euro Sales Template. Se esse indivíduo também for um membro do grupo de distribuição de Jogadores de Pôquer, essa participação de grupo permanecerá inalterada.

As seguintes capacidades permitem que um administrador assistente modifique ainda mais uma conta do usuário durante o processo de transformação:

- ♦ Modificar propriedades do endereço ao transformar uma conta do usuário
- ♦ Modificar descrição ao transformar uma conta do usuário
- ♦ Modificar o Office ao transformar uma conta do usuário
- ♦ Modificar propriedades do telefone ao transformar uma conta do usuário

Você também pode restringir a capacidade de adicionar ou remover participações em grupos, concedendo a um administrador assistente apenas uma das seguintes capacidades:

- ♦ Adicionar um usuário a grupos encontrados em um modelo
- ♦ Remover um usuário de grupos encontrados em um modelo

Você pode usar qualquer uma dessas opções limitadoras baseadas em poderes para criar uma camada de segurança em sua organização. Ao conceder a certos indivíduos o poder de remover somente os grupos encontrados em um modelo, você pode criar contas do usuário provisórias. Essas contas provisórias podem, então, ser revisadas antes que um administrador assistente diferente use uma conta de gabarito adicionável para conceder as novas participações em grupos.

Criando modelos de transformação do usuário

A transformação de contas do usuário está diretamente vinculada às funções e às escalas de trabalho de sua organização. Crie um modelo para cada função ou trabalho em sua empresa. O DRA não faz distinção entre um modelo de conta do usuário usado como subtrativo versus aditivo. Crie um modelo de conta do usuário para cada função em sua organização. Durante a transformação, você seleciona o modelo como subtrativo ou aditivo. A seleção de um modelo como subtrativo não impede que o mesmo modelo seja usado como aditivo em uma transformação futura.

Para criar um modelo de transformação de usuário, você deve ter os poderes para criar uma conta do usuário e designar essa conta aos grupos apropriados. Esses poderes podem ser obtidos através da associação de sua conta com as funções Criar e Apagar Contas do Usuário e Administração de Grupos nas Telas Ativas apropriadas ou através da designação de poderes individuais.

Transformando contas do usuário

Transformar uma conta do usuário permite adicionar, remover ou adicionar e remover participações de grupos de contas do usuário. Use este workflow para ajudá-lo quando indivíduos passarem de uma responsabilidade de trabalho para outra na sua organização. Você deve ter a função Transformar um Usuário ou uma função que contenha os poderes adequados para transformar contas do usuário. Esta função só pode ser executada do Console de Delegação e Configuração por meio do nó Gerenciamento de Recursos e de Contas.

Para transformar uma conta do usuário:

- 1 No painel esquerdo, expanda **Todos os Meus Objetos Gerenciados**.
- 2 Para especificar a conta do usuário que você deseja gerenciar, execute uma operação **Find Now**(Localizar Agora) para localizar e, então, selecione o objeto usuário.
- 3 Clique em **Tarefas > Transformar**.
- 4 Revise a janela de Boas-Vindas e clique em **Next** (Próximo).
- 5 Na janela Selecionar Modelo de Usuário, use **Browse** (Procurar) para selecionar o usuário do modelo subtrativo apropriado.
- 6 Se desejar revisar as propriedades do modelo de conta do usuário subtrativo, clique em **Ver**.
- 7 Use **Browse** (Procurar) para selecionar o usuário do modelo aditivo apropriado.
- 8 Se desejar revisar as propriedades do modelo de conta do usuário aditivo, clique em **Ver**.
- 9 Se você tiver os poderes adequados, pode verificar **Mudar outras propriedades do usuário** e selecionar propriedades para modificar. Clique em **Next** (Próximo) para navegar pelas propriedades disponíveis.
- 10 Clique em **Próximo**.
- 11 Revise a janela Summary (Resumo) e clique em **Finish** (Terminar).

Gerenciando grupos

Como administrador assistente, você pode usar o DRA para gerenciar grupos e modificar propriedades de grupos. Os grupos permitem que você conceda permissões específicas a um conjunto definido de contas do usuário. Os grupos permitem controlar quais dados e recursos uma conta do usuário pode acessar em qualquer domínio.

Você pode gerenciar grupos de qualquer tipo e escopo. Por exemplo, você pode aninhar grupos, permitindo que um grupo possa herdar permissões de outro grupo. Você também pode controlar efetivamente as participações de grupos nos domínios, adicionando grupos de domínios confiáveis a outros grupos no domínio gerenciado e gerenciando designações de grupo temporárias.

Para saber mais sobre como gerenciar grupos, veja os seguintes tópicos:

- ♦ [“Tarefas de gerenciamento de grupos” na página 52](#)
- ♦ [“Gerenciando designações de grupo temporárias no Console de Delegação e Configuração” na página 55](#)
- ♦ [“Gerenciando designações de grupo temporárias no Console da Web” na página 56](#)

Tarefas de gerenciamento de grupos

Esta seção guia você pela administração de grupos no Console de Delegação e Configuração por meio do nó Gerenciamento de Recursos e de Contas. Com os poderes adequados, você pode executar várias tarefas de gerenciamento de grupo, como modificar participações no grupo. Se você selecionar vários grupos, poderá executar tarefas selecionadas em uma operação, como apagar, mover ou adicionar membros a um grupo. O menu Tarefas indica quais tarefas você pode executar quando seleciona um ou vários grupos.

Adicionar contas a grupos

Você pode adicionar contas do usuário, contatos e computadores a um grupo gerenciado.

Observação: Esta tarefa adiciona várias contas a um grupo selecionado. Você pode adicionar uma única conta a um grupo selecionando a conta apropriada e clicando em Adicionar aos grupos no menu Tarefas.

Se adicionar uma conta a outro grupo aumenta seus poderes para a conta, o DRA não permite que você adicione a conta.

Adicionar grupos a outros grupos

Você pode aninhar grupos adicionando um grupo a outro grupo gerenciado. Quando um grupo é aninhado em outro grupo, o grupo filho pode herdar as permissões do grupo pai

Observação: Se adicionar um grupo a outro grupo aumenta seus poderes para o grupo de origem, o DRA não permite que você adicione o grupo.

Modificar propriedades de grupos

Você pode modificar propriedades para grupos locais e globais. Os seus poderes determinam quais propriedades você pode modificar para um grupo no domínio gerenciado ou na subárvore gerenciada. Se você instalou o Exchange e habilitou o suporte do Microsoft Exchange, poderá modificar as propriedades da lista de distribuição ao gerenciar grupos.

Criar um grupo

Você pode criar um grupo no domínio gerenciado ou na subárvore gerenciada. Você também pode modificar propriedades, como membros do grupo, para o novo grupo.

Observação

- ♦ Sua empresa pode ter uma convenção de nomenclatura aplicada por meio de uma política que determina o nome que você pode designar ao novo grupo.
 - ♦ Por padrão, o DRA coloca o novo grupo na OU de Usuários do domínio gerenciado.
-

Especificar membros do grupo

Você pode adicionar ou remover contas do usuário, contatos, computadores ou outros grupos do grupo gerenciado. O DRA permite remover apenas entidades de segurança estrangeiras. Você também pode ver ou modificar propriedades de membros de grupos existentes, exceto para entidades de segurança estrangeiras.

Quando você remove membros de um grupo, o DRA não apaga os objetos. Quando você adiciona membros a um grupo, deve ter o poder de modificar os objetos que deseja adicionar.

Observação

- ♦ Não é possível adicionar contas ou grupos de usuários a nenhum grupo especial do Windows (Administradores, Operadores de Contas, Operadores de Backup ou Operadores de Servidor), a menos que você seja um administrador do Windows ou um membro desse grupo especial específico.
 - ♦ O DRA permite que você exporte os resultados dos **Membros** como um arquivo CSV. Para exportar os resultados dos **Membros** do Console da Web, acesse **Gerenciamento > Pesquisa** e clique em **Propriedades**. Navegue até a guia **Membros** e clique no ícone **Fazer Download**. As mudanças não gravadas não são exportadas. Grave quaisquer mudanças recentes para que elas estejam disponíveis no arquivo exportado.
-

Especificar participação do grupo para grupos

Você pode adicionar ou remover um grupo de outros grupos no domínio gerenciado ou na subárvore gerenciada. Você também pode ver ou modificar propriedades de grupos existentes aos quais esse grupo pertence.

Observação: O DRA permite que você exporte os resultados de **Membro De** como um arquivo CSV. Para exportar os resultados de **Membro De** do Console da Web, acesse **Gerenciamento > Pesquisa** e clique em **Propriedades**. Navegue até a guia **Membro De** e clique no ícone **Fazer Download**. As mudanças não gravadas não são exportadas. Grave quaisquer mudanças recentes para que elas estejam disponíveis no arquivo exportado.

Configurar permissões de segurança da participação do grupo

Você pode definir permissões de segurança do Active Directory para participações de grupos. Essas permissões especificam quem pode ver (ler) e modificar (gravar) participações de grupos usando o Microsoft Outlook. Essas configurações permitem que você proteja com mais eficácia listas de distribuição e grupos de segurança em seu ambiente. Você não pode modificar permissões de segurança herdadas.

Observação: Quando você gerencia a segurança da participação do grupo, as permissões desabilitadas podem indicar permissões herdadas.

Configurar propriedade do grupo

Você pode definir a propriedade de qualquer grupo de distribuição ou segurança do Microsoft Windows. Você pode conceder a permissão de propriedade de grupo a uma conta do usuário, um grupo ou um contato. A concessão de propriedade de grupo permite que a conta do usuário, o grupo ou o contato especificado modifique a participação desse grupo.

Observação: O DRA desabilita a caixa de seleção **O gerente pode atualizar a lista de associados** quando a participação do grupo estiver oculta no servidor do Microsoft Exchange. Para habilitar esta caixa de seleção, clique em **Expor Participação do Grupo** na guia Exchange da janela Group Properties (Propriedades do Grupo).

Clonar um grupo

Você pode clonar grupos locais e globais em domínios gerenciados. A clonagem de grupos cria novos grupos do mesmo tipo e atributos que o grupo original. O DRA também tenta adicionar todos os membros do grupo original ao novo grupo.

Ao clonar um grupo, você pode criar rapidamente grupos com base em outros grupos com propriedades semelhantes. Quando você clona um grupo, o DRA preenche o Assistente de Clonagem de Grupo com valores do grupo selecionado. Você também pode modificar propriedades para o novo grupo.

Observação

- ◆ Sua empresa pode ter uma convenção de nomenclatura aplicada por meio de uma política que determina o nome que você pode designar ao novo grupo.
 - ◆ Por padrão, o DRA coloca o novo grupo na OU de Usuários do domínio gerenciado.
-

Apagar um grupo

Você pode apagar grupos locais e globais no domínio gerenciado ou na subárvore gerenciada. Se a Lixeira estiver desabilitada para esse domínio, apagar um grupo o removerá permanentemente do Active Directory. Se a Lixeira estiver habilitada para esse domínio, apagar um grupo o moverá para a Lixeira e as propriedades do grupo serão desabilitadas.

Para obter mais informações sobre a Lixeira, consulte [Gerenciando a Lixeira](#).

Aviso: Quando você cria um grupo, o Microsoft Windows atribui um Identificador de Segurança (SID) a esse grupo. O SID não é gerado do nome do grupo. O Microsoft Windows usa SIDs para registrar privilégios em listas de controle de acesso (ACLs) para cada recurso. Se você apagar um grupo, não poderá retornar recursos de acesso para esse grupo criando um novo grupo com o mesmo nome.

Mover um grupo para outro contêiner

Você pode mover um grupo para outro contêiner, como uma OU, no domínio gerenciado ou na subárvore gerenciada.

Expor participações de grupos em listas de distribuição

Você pode expor as participações do grupo em listas de distribuição para grupos no domínio gerenciado ou na subárvore gerenciada.

Ocultar participações de grupos de listas de distribuição

Você pode ocultar as participações do grupo em listas de distribuição para grupos no domínio gerenciado ou na subárvore gerenciada.

Gerenciando designações de grupo temporárias no Console de Delegação e Configuração

Designações de grupo temporárias permitem que você gerencie participações em grupos para usuários que somente precisam participar do grupo por um período de tempo específico. Esta seção guia você pela administração de designações de grupo temporárias no Console de Delegação e Configuração em **Account and Resource Management** (Gerenciamento de Recursos e de Contas). Com os poderes adequados, execute tarefas como criar designações de grupo temporárias ou remover designações de grupo temporárias expiradas.

Administradores assistentes podem ver apenas designações temporárias de grupo para grupos cujo administrador assistente tem capacidade de modificar participações (adicionar ou remover membros).

Você não poderá mudar o grupo associado nem modificar a lista de usuários enquanto a designação de grupo temporária estiver no estado Ativo. Se você quiser modificar esses itens, deverá cancelar a designação de grupo temporária.

Gerenciar propriedades de designação de grupo temporária

Você pode gerenciar propriedades para designações de grupo temporárias ou designações de grupo temporárias expiradas gravadas.

Se você quiser reprogramar uma designação de grupo temporária, mude a programação nas **Propriedades** da designação e grave suas mudanças.

Criar uma designação de grupo temporária

Você pode criar uma designação de grupo temporária nos servidores de Administração principal e secundário.

Por padrão, quando uma designação de grupo temporária expira, ela é apagada após sete dias, a menos que você tenha selecionado a opção **Mantenha esta designação temporária de grupo para uso futuro**. Para mudar esse período de retenção, clique com o botão direito do mouse no nó **Designação de Grupo Temporária** em Todos os Meus Objetos Gerenciados, selecione **Propriedades** e modifique o número de dias de retenção das designações de grupo temporárias.

Gerenciar contas do usuário em uma designação de grupo temporária

É possível adicionar ou remover contas do usuário de designações de grupo temporárias nos servidores de Administração principal e secundário.

Observação: Você só pode gerenciar contas do usuário para designações de grupo temporárias que ainda não estão ativas.

Apagar uma designação de grupo temporária

Você pode apagar qualquer designação de grupo temporária nos servidores de Administração principal e secundário.

Gerenciando designações de grupo temporárias no Console da Web

Designações de grupo temporárias permitem que você gerencie participações em grupos para usuários que precisam participar do grupo por um período de tempo específico. Se o Azure Active Directory for configurado pelo Administrador do DRA, você poderá criar designações temporárias de grupo para grupos do Azure e adicionar usuários do Azure e usuários sincronizados a uma participação no grupo do Azure. No Console da Web, crie e gerencie designações tanto do servidor do DRA principal quanto do secundário. No entanto, as ações que você pode executar para designações existentes variam dependendo do estado atual da designação.

Administradores assistentes podem ver designações de grupo temporárias apenas para grupos nos quais eles têm poderes para modificar pelas respectivas designações de Tela Ativa, como adicionar ou remover membros do grupo.

Para gerenciar designações de grupo temporárias no Console da Web, navegue até **Tarefas > Designações de Grupo Temporárias**.

É possível executar as seguintes ações:

Criar uma designação temporária de grupo

Você pode criar designações temporárias de grupo usando grupos nos quais você tem poderes para modificar e especificar o controlador de domínio. O grupo de destino pode ser um grupo de um locatário gerenciado pelo Azure ou um grupo de um domínio do Active Directory. Quando a designação temporária de grupo expira, o DRA apaga-a automaticamente após sete dias, a menos que você selecione a opção para manter a designação temporária de grupo para uso futuro.

Observação: Se a designação temporária de grupo configurada com a participação no grupo do Azure for modificada fora do DRA, a designação temporária de grupo se tornará inválida.

Para criar uma nova designação temporária de grupo:

1. Navegue até **Tarefas > Designações Temporárias de Grupos** e clique em **Criar**.
2. Clique em **Selecionar** e encontre o grupo executando uma Pesquisa no container aplicável.
3. Se você precisar adicionar membros ao grupo, clique em **Adicionar**, que fica em **Membros**, na página Criar Designação Temporária de Grupo, depois localize e use a opção **Adicionar** **+** na lista de resultados para adicionar membros ao grupo.
4. Configure a Programação.
5. Nomeie o TGA em Informações Gerais e clique em **Criar**.

Pesquisar designações existentes

Quando você pesquisa TGAs (designações de grupo temporárias) existentes, elas são listadas nos resultados com base no status da designação, que pode incluir os seguintes estados:

- ♦ **Pendente:** A TGA está programada para iniciar no futuro. Você pode cancelar, apagar e reprogramar.

- ♦ **Ativa:** A TGA iniciou e adicionou membros aplicáveis ao grupo. Você pode cancelar e apagar.
- ♦ **Ativa com erro:** A TGA foi iniciada, mas não conseguiu adicionar todos os membros aplicáveis ao grupo. Você pode cancelar e apagar.
- ♦ **Concluído:** A TGA expirou e removeu todos os membros aplicáveis do grupo. Você pode apagar e reprogramar.
- ♦ **Concluído com Erro:** A TGA expirou, mas não conseguiu remover todos os membros aplicáveis do grupo. Você pode apagar e reprogramar.
- ♦ **Cancelado:** A TGA foi cancelada por um usuário e removeu todos os membros aplicáveis do grupo. Você pode apagar e reprogramar.
- ♦ **Cancelado com Erro:** A TGA foi cancelada por um usuário, mas não conseguiu remover todos os membros aplicáveis do grupo. Você pode apagar e reprogramar.
- ♦ **Erro:** A TGA não conseguiu adicionar ou remover todos os membros. Você pode apagar e reprogramar.

Você pode filtrar os resultados com base nesses estados e em outros critérios, incluindo o nome da designação, o grupo de destino, o tempo de duração e o administrador que criou a designação.

Ver ou modificar propriedades de designação de grupo temporária

Você pode ver ou modificar qualquer uma das designações de grupo temporárias que foram definidas quando a designação de grupo temporária foi criada. Após realizar uma pesquisa por designações de grupo temporárias, selecione uma designação para ver ou modificar as propriedades dela.

Se você quiser reprogramar uma designação de grupo temporária, mude a programação nas **Propriedades** da designação e grave suas mudanças. Se a designação estiver no estado Ativo, você poderá mudar apenas a data de término.

Importante: Você não poderá mudar o grupo associado nem modificar a lista de usuários enquanto a designação de grupo temporária estiver no estado Ativo. Se você quiser modificar esses itens, deverá primeiro cancelar a designação.

Cancelar uma designação de grupo temporária

Você pode cancelar uma designação de grupo temporária somente quando ela está em um dos seguintes estados:

- ♦ Ativo
- ♦ Ativo com Erro
- ♦ Pendente

Apagar uma designação de grupo temporária

Você pode selecionar várias designações de grupo temporárias e apagá-las. Se as designações de grupo temporárias estiverem no estado Ativo, Ativo com Erro ou Pendente, a opção **Cancelar** também estará habilitada.

Gerenciando grupos de distribuição dinâmica

Um grupo de distribuição dinâmica é um objeto de grupo do Active Directory habilitado para e-mail que você pode criar para agilizar o envio em massa de mensagens de e-mail e outras informações.

A lista de associados de um grupo de distribuição dinâmica é calculada cada vez que uma mensagem é enviada ao grupo, com base nos filtros e condições que você define. Isso difere de um grupo de distribuição regular, que contém um conjunto definido de membros. Quando uma mensagem de e-mail é enviada para um grupo de distribuição dinâmica, ela é entregue a todos os destinatários da organização que correspondem aos critérios definidos para esse grupo.

O DRA suporta os seguintes recursos:

- ♦ Auditoria e gerador de relatórios da interface do usuário
- ♦ Suporte a enumeração para grupos de distribuição dinâmica
- ♦ Relatório do NetIQ Reporting Center (NRC) para grupos de distribuição dinâmica
- ♦ Suporte à operação do acionador para grupos de distribuição dinâmica
- ♦ Suporte à extensão da interface do usuário para grupos de distribuição dinâmica do Exchange

Tarefas do grupo de distribuição dinâmica:

Criar um grupo de distribuição dinâmica

Você pode criar um grupo de distribuição dinâmica no domínio gerenciado ou na subárvore gerenciada. Você também pode modificar propriedades, como membros do grupo, para o novo grupo de distribuição dinâmica.

Observação

- ♦ Sua empresa pode ter uma convenção de nomenclatura aplicada por meio de uma política que determina o nome que você pode designar ao novo grupo de distribuição dinâmica.
- ♦ Por padrão, o DRA coloca o novo grupo de distribuição dinâmica na OU de Usuários do domínio gerenciado.

Para criar um grupo de distribuição dinâmica no Console de Delegação e Configuração:

1. Selecione o container no qual criar um grupo de Todos os Meus Objetos Gerenciados no nó Gerenciamento de Recursos e de Contas.
2. Selecione **Novo > Grupo de Distribuição Dinâmica** no menu Tarefas.
3. Conclua as etapas do assistente.

Para criar um grupo de distribuição dinâmica no Console da Web:

1. Selecione o cabeçalho principal **Gerenciamento** e selecione o container no qual criar um grupo de Todos os Meus Objetos Gerenciados no nó Gerenciamento de Recursos e de Contas.
2. Selecione **Grupo de Distribuição Dinâmica** no menu suspenso Criar.
3. Digite as informações necessárias no formulário e clique em **Criar**.

Clonar um grupo de distribuição dinâmica

Você pode clonar grupos de distribuição dinâmica locais e globais em domínios gerenciados. A clonagem de grupos de distribuição dinâmica cria novos grupos de distribuição dinâmica do mesmo tipo e atributos que o grupo de distribuição dinâmica original.

Ao clonar um grupo de distribuição dinâmica, você pode criar rapidamente grupos de distribuição dinâmica com base em outros grupos de distribuição dinâmica com propriedades semelhantes. Quando você clona um grupo de distribuição dinâmica, o DRA preenche o Assistente de Clonagem de Grupos de Distribuição Dinâmica com valores do grupo de distribuição dinâmica selecionado. Você também pode modificar propriedades para o novo grupo de distribuição dinâmica.

Mover um grupo de distribuição dinâmica para outro contêiner

Você pode mover um grupo de distribuição dinâmica para outro contêiner, como uma OU, no domínio gerenciado ou na subárvore gerenciada.

Apagar um grupo de distribuição dinâmica

Você pode apagar grupos de distribuição dinâmica locais e globais no domínio gerenciado ou na subárvore gerenciada. Se a Lixeira estiver desabilitada para esse domínio, apagar um grupo de distribuição dinâmica o removerá permanentemente do Active Directory. Se a Lixeira estiver habilitada para esse domínio, apagar um grupo de distribuição dinâmica o moverá para a Lixeira e as propriedades do grupo de distribuição dinâmica serão desabilitadas.

Para obter mais informações sobre a Lixeira, consulte [Gerenciando a Lixeira](#).

Aviso: Quando você cria um grupo de distribuição dinâmica, o Microsoft Windows atribui um Identificador de Segurança (SID) a esse grupo de distribuição dinâmica. O SID não é gerado do nome do grupo de distribuição dinâmica. O Microsoft Windows usa SIDs para registrar privilégios em listas de controle de acesso (ACLs) para cada recurso. Se você apagar um grupo de distribuição dinâmica, não poderá retornar recursos de acesso para esse grupo de distribuição dinâmica criando um novo grupo de distribuição dinâmica com o mesmo nome.

Modificar propriedades de grupos de distribuição dinâmica

Você pode modificar propriedades para grupos de distribuição dinâmica locais e globais. Os seus poderes determinam quais propriedades você pode modificar para um grupo no domínio gerenciado ou na subárvore gerenciada.

Especificar um filtro

A associação de uma lista de distribuição dinâmica é determinada por seu filtro, que você pode definir.

Especificar condições

As condições definem os critérios que um objeto deve atender para ser um membro do grupo de distribuição dinâmica.

Gerenciando grupos dinâmicos

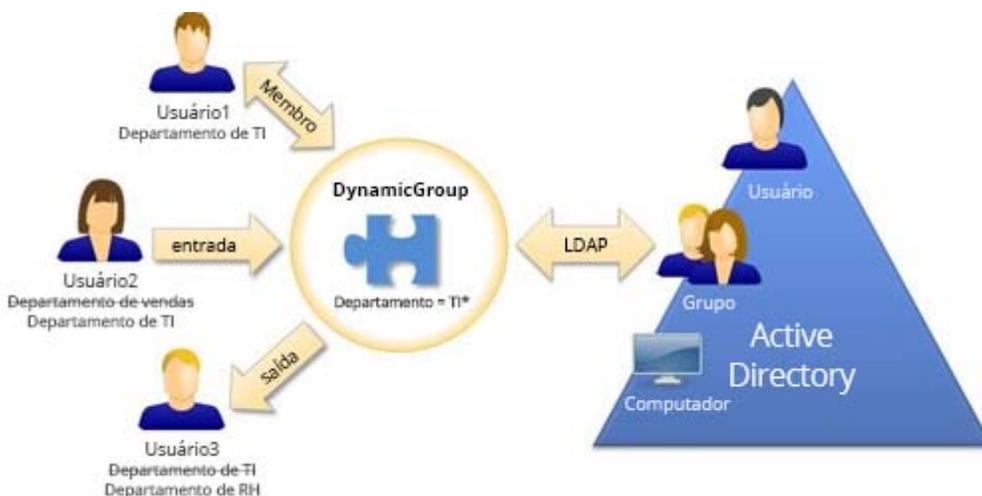
Um grupo dinâmico é aquele cuja associação é alterada com base em um conjunto definido de critérios. No DRA, crie grupos dinâmicos sem necessidade de ter um ambiente do Exchange. Os filtros de participação usados para gerenciar grupos dinâmicos no Active Directory são exclusivos para o DRA.

O Administrador do DRA configura a programação de atualização de domínio para grupos dinâmicos no Console de Delegação e Configuração. Novos membros são adicionados dinamicamente ao grupo quando uma ou mais propriedades de usuário que correspondem aos critérios de Filtro de Membros do grupo são atualizadas e, em seguida, ocorre uma atualização. Da mesma forma, um membro pode ser removido dinamicamente do grupo quando as propriedades correspondentes são mudadas ou removidas do usuário.

Exemplo de cenário

O gráfico abaixo descreve um uso típico para um grupo dinâmico do Active Directory. Há três grupos dinâmicos no gráfico. Cada grupo tem um conjunto de critérios que determina quem pode ser adicionado ao grupo e quem não pode. Cada grupo controla o acesso a um conjunto específico de arquivos, pastas e aplicativos.

Dica: Você pode criar uma *lista de membros estáticos* que contenha membros permanentes do grupo dinâmico; você também pode criar uma *lista de membros excluídos* que negue a participação desses usuários no grupo dinâmico.



O Usuário2 se juntou recentemente ao departamento de TI. Quando o grupo dinâmico do departamento de TI for atualizado, ele será adicionado ao grupo. Quando o grupo dinâmico do departamento de vendas for atualizado, o Usuário2 será removido da sua lista de membros.

O Usuário3, que saiu do departamento de TI para o departamento de RH, será removido do grupo dinâmico do departamento de TI e adicionado ao grupo dinâmico do departamento de RH.

Preparação de cenários

As informações abaixo fornecem um exemplo das ações que você tomaria no Console da Web para habilitar o cenário acima. Você pode tornar dinâmico um grupo existente ou criar um novo grupo dinâmico. Por uma questão de simplicidade, não adicionaremos nenhum membro estático nem excluído e tornaremos dinâmicos três grupos existentes: Grupo de RH, Grupo de TI e Grupo de Vendas.

Configurando o grupo dinâmico:

- 1 Para cada grupo fornecido acima, realize uma operação de Pesquisa com o filtro Grupo habilitado para localizar o grupo.
- 2 Abra **Propriedades** para o grupo e acesse a página **Filtro de Membro Dinâmico**.
- 3 Clique no controle deslizante **Tornar o grupo dinâmico** para habilitar o recurso.
- 4 Clique em **Modificar** e digitar ou cole os critérios do Filtro de Membro no campo de consulta LDAP. Neste caso, buscamos critérios na propriedade **Usuário > Departamento**. Os exemplos abaixo mostram os critérios LDAP que usaremos para cada grupo no [exemplo de cenário](#):
 - ♦ Grupo de RH: `(&(objectClass=user)(objectCategory=person)(department=HR*))`
 - ♦ Grupo de TI: `(&(objectClass=user)(objectCategory=person)(department=IT*))`
 - ♦ Grupo de Vendas: `(&(objectClass=user)(objectCategory=person)(department=Sales*))`
- 5 Clique em **Aplicar** para gravar as mudanças.

Ações tomadas para mudar dinamicamente a afiliação do grupo dos usuários nas propriedades do usuário selecionado:

- ♦ Usuário2: Mudou a propriedade **Organização > Departamento** de “Vendas” para “TI”.
- ♦ Usuário3: Mudou a propriedade **Organização > Departamento** de “TI” para “RH”.

As mudanças dinâmicas ocorrem durante a Atualização do Grupo Dinâmico programada ou quando são atualizadas manualmente pelo Administrador do DRA.

Tarefas do grupo dinâmico

As tarefas do grupo dinâmico que você pode executar no Console da Web são descritas abaixo.

Criar um grupo dinâmico

Você pode criar um grupo dinâmico no domínio gerenciado ou na subárvore gerenciada. Você também pode modificar propriedades, como membros do grupo, para o novo grupo dinâmico. Para criar um novo grupo dinâmico, navegue até **Criar > Grupo Dinâmico** no cabeçalho principal de Gerenciamento.

Observação: Sua empresa pode ter uma convenção de nomenclatura imposta por meio de uma política que determina o nome que você pode designar ao novo grupo dinâmico.

Criar um filtro

O grupo dinâmico usa o **Filtro de Membro Dinâmico** para adicionar ou remover usuários de sua lista de associados toda vez que o grupo é atualizado. Para obter exemplos de como fazer consultas LDAP e de Atributo virtual para o filtro, você pode consultar os exemplos mostrados em “Consultas de Pesquisa Avançada”. Embora o filtro funcione como critério para participação no grupo e não uma pesquisa, os exemplos de consulta ainda são aplicáveis:

- ♦ [Exemplos de consulta LDAP](#)
- ♦ [Exemplos de consulta de atributo virtual](#)

Gerenciar a lista de membros estáticos

Os usuários colocados em uma lista de membros estáticos de um grupo dinâmico tornam-se membros permanentes do grupo até que você os remova manualmente. Você pode modificar essa lista na página de propriedades Filtro de Membros Dinâmico em um usuário selecionado.

Quando você remove membros de um grupo dinâmico, o DRA não apaga os objetos. Quando você adicionar membros a um grupo dinâmico, deve ter o poder de modificar os objetos que deseja adicionar.

Gerenciar a lista de membros excluídos

Os usuários colocados na lista de membros apagados de um grupo dinâmico não poderão ingressar no grupo até que você os remova manualmente dessa lista. Você pode modificar essa lista na página de propriedades Filtro de Membros Dinâmico em um usuário selecionado.

Atualizar a lista de membros

Você pode atualizar os membros em um grupo dinâmico por uma ação **Atualizar membros**.

Clonar um grupo dinâmico

Você pode clonar grupos dinâmicos locais e globais em domínios gerenciados. A clonagem de grupos dinâmicos cria novos grupos dinâmicos do mesmo tipo e atributos que o grupo dinâmico original.

Ao clonar um grupo dinâmico, você pode criar rapidamente grupos dinâmicos com base em outros grupos dinâmicos com propriedades semelhantes. Quando você clona um grupo dinâmico, o DRA preenche o Assistente de Clonagem de Grupos Dinâmicos com valores do grupo dinâmico selecionado. Você também pode modificar propriedades para o novo grupo dinâmico.

Para clonar um grupo dinâmico, selecione o grupo no painel de resultados da Pesquisa e clique em **Clonar**  na barra de ferramentas.

Mover um grupo dinâmico para outro contêiner

Mover um grupo dinâmico para outro contêiner, como uma OU, no domínio gerenciado ou na subárvore gerenciada.

Para mover um grupo dinâmico, selecione o grupo no painel de resultados da Pesquisa e clique em **Mover Objetos**  na barra de ferramentas.

Apagar um grupo dinâmico

Você pode apagar grupos dinâmicos locais e globais no domínio gerenciado ou na subárvore gerenciada. Se a Lixeira estiver desabilitada para esse domínio, apagar um grupo dinâmico o removerá permanentemente do Active Directory. Se a Lixeira estiver habilitada para esse

domínio, apagar um grupo dinâmico o moverá para a Lixeira e as propriedades do grupo dinâmico serão desabilitadas. Para obter mais informações sobre a Lixeira, consulte [Gerenciando a Lixeira](#).

Para apagar um grupo dinâmico, selecione o grupo no painel de resultados da Pesquisa e clique em **Apagar**  na barra de ferramentas.

Aviso: Quando você cria um grupo dinâmico, o Microsoft Windows atribui um Identificador de Segurança (SID) a esse grupo dinâmico. O SID não é gerado do nome do grupo dinâmico. O Microsoft Windows usa SIDs para registrar privilégios em listas de controle de acesso (ACLs) para cada recurso. Se você apagar um grupo dinâmico, não poderá retornar recursos de acesso para esse grupo dinâmico criando um novo grupo dinâmico com o mesmo nome.

Modificar propriedades de grupos dinâmicos

Você pode modificar propriedades para grupos dinâmicos locais e globais. Os seus poderes determinam quais propriedades você pode modificar para um grupo no domínio gerenciado ou na subárvore gerenciada.

Observação: O DRA permite que você exporte os resultados de **Membros** e **Membro De** como um arquivo CSV. Para exportar os resultados de **Membros** ou **Membro De** do Console da Web, acesse **Gerenciamento > Pesquisa** e clique em **Propriedades**. Navegue até a guia **Membros** ou **Membro De** e clique no ícone **Fazer Download**. As mudanças não gravadas não são exportadas. Grave quaisquer mudanças recentes para que elas estejam disponíveis no arquivo exportado.

Para modificar as propriedades de um grupo dinâmico, selecione o grupo no painel de resultados da Pesquisa e clique em **Propriedades**  na barra de ferramentas.

Adicione grupos dinâmicos a outros grupos dinâmicos

Você pode aninhar grupos dinâmicos adicionando um grupo dinâmico a outro grupo dinâmico gerenciado. Quando um grupo dinâmico é aninhado em outro grupo dinâmico, o grupo dinâmico filho pode herdar as permissões do grupo dinâmico pai.

Para adicionar um grupo dinâmico a outro grupo dinâmico, selecione o grupo no painel de resultados da Pesquisa e clique em **Adicionar aos Grupos**  na barra de ferramentas.

Observação: Se adicionar um grupo dinâmico a outro grupo dinâmico aumenta seus poderes para o grupo dinâmico de origem, o DRA não permitirá que você adicione o grupo dinâmico.

Configurar permissões de segurança da participação do grupo

Você pode definir permissões de segurança do Active Directory para membros de grupos dinâmicos. Essas permissões especificam quem pode ver (ler) e modificar (gravar) participações de grupos dinâmicos usando o Microsoft Outlook. Essas configurações permitem que você proteja com mais eficácia listas de distribuição e grupos dinâmicos de segurança em seu ambiente. Você não pode modificar permissões de segurança herdadas.

Você pode atualizar essas configurações na página de propriedades **Segurança da Participação** em um grupo dinâmico selecionado.

Observação: Quando você gerencia a segurança da participação do grupo dinâmico, as permissões desabilitadas podem indicar permissões herdadas.

Configurar propriedade do grupo dinâmico

Você pode conceder a permissão de propriedade de grupo dinâmico a uma conta do usuário, um grupo ou um contato. A concessão de propriedade de grupo dinâmico permite que a conta do usuário, o grupo ou o contato especificado modifique a participação desse grupo dinâmico.

Você pode atualizar essas configurações na página de propriedades **Gerenciado por** em um grupo dinâmico selecionado.

Expor participações de grupos dinâmicos em listas de distribuição

Você pode expor as participações do grupo dinâmico em listas de distribuição para grupos no domínio gerenciado ou na subárvore gerenciada.

Você pode acessar esta opção no menu suspenso **Exchange** na barra de ferramentas para um grupo dinâmico selecionado.

Ocultar participações de grupos dinâmicos de listas de distribuição

Você pode ocultar as participações do grupo dinâmico em listas de distribuição para grupos no domínio gerenciado ou na subárvore gerenciada.

Você pode acessar esta opção no menu suspenso **Exchange** na barra de ferramentas para um grupo dinâmico selecionado.

Observação: A opção **Ocultar Participações de Grupo** está desabilitada nas listas de distribuição do Microsoft Exchange 2007.

Gerenciando contatos

O DRA permite gerenciar muitos objetos de rede, incluindo contatos e os endereços de e-mail associados. Os contatos estão disponíveis apenas no modo misto ou em domínios nativos do Microsoft Windows. Contatos não têm um Identificador de Segurança (SID), como contas do usuário e grupos. Use os contatos para adicionar membros a listas de distribuição ou grupos sem conceder acesso aos serviços de rede.

Você pode adicionar contatos a grupos de segurança ou de distribuição em domínios mistos e nativos. Como os grupos de segurança podem ser usados como listas de distribuição no Microsoft Windows, convém adicionar contatos a esses grupos. Ter um contato em um grupo de segurança global não impede que o grupo seja convertido em um grupo de segurança universal quando você migra para um domínio do Microsoft Windows em modo nativo.

Você pode executar a maioria das tarefas abaixo na guia **Gerenciamento > Pesquisar** no Console da Web. Execute uma operação de pesquisa para localizar e selecionar o contato necessário. Depois de selecionar um ou mais contatos na lista, a barra de tarefas fica ativa com opções da barra de ferramentas e opções de menu suspenso para **Exchange**. Passe o mouse sobre um ícone da barra de ferramentas ou clique em um menu suspenso para exibir as funções ou as opções.

Modificar propriedades do contato

Você pode modificar propriedades do contato. Os seus poderes determinam quais propriedades você pode modificar para um contato no domínio gerenciado. Se você instalou o Exchange e habilitou o suporte do Exchange, poderá modificar as propriedades do endereço de e-mail ao gerenciar os contatos.

Observação: O DRA permite que você exporte os resultados de **Membro De** como um arquivo CSV. Para exportar os resultados de **Membro De** do Console da Web, acesse **Gerenciamento > Pesquisa** e clique em **Propriedades**. Navegue até a guia **Membro De** e clique no ícone **Fazer Download**. As mudanças não gravadas não são exportadas. Grave quaisquer mudanças recentes para que elas estejam disponíveis no arquivo exportado.

Criar um contato

Você pode gerenciar contatos no domínio gerenciado ou na subárvore gerenciada. Você também pode modificar propriedades, habilitar e-mail e especificar endereços de e-mail e especificar participações de grupo para o novo contato.

Para criar um novo contato, navegue até **Gerenciamento > Pesquisar** e selecione **Contato** no menu suspenso Criar.

Clonar um contato

Ao clonar um contato, você pode criar rapidamente contatos com base em outros contatos com propriedades semelhantes. Quando você clona um contato, o DRA preenche o Assistente de Clonagem de Contatos com valores do contato selecionado. Você também pode modificar propriedades, habilitar e-mail e especificar endereços de e-mail e especificar participações de grupo para o novo contato.

Gerenciar participações de grupos para contatos

Você pode adicionar ou remover contatos de um grupo específico no domínio gerenciado ou na subárvore gerenciada. Você também pode ver ou modificar propriedades de grupos existentes aos quais esse contato pertence.

Mover um contato para outra OU

Você pode mover um contato para outro contêiner, como uma OU, no domínio gerenciado ou na subárvore gerenciada.

Apagar um contato

Você pode apagar um contato do domínio gerenciado ou da subárvore gerenciada. Se a Lixeira estiver desabilitada para esse domínio, apagar um contato o removerá permanentemente do Active Directory. Se a Lixeira estiver habilitada para esse domínio, apagar um contato o moverá para a Lixeira.

Para obter mais informações sobre a Lixeira, consulte [Gerenciando a Lixeira](#).

Gerenciando Contas de Serviço Gerenciadas do Grupo

Uma gMSA (conta de serviço gerenciada do grupo) é uma conta de domínio gerenciada que você pode designar a serviços em recursos de computador. Você não precisa atualizar manualmente a senha dessas contas no Active Directory, pois as senhas dessas contas são gerenciadas automaticamente pelo Windows Server.

Você pode criar e gerenciar uma gMSA do Console da Web do DRA. Uma conta de serviço gerenciada do grupo pode ser usada com vários computadores para executar serviços. Computadores que usam uma gMSA solicitam a senha atual do Active Directory para iniciar os serviços.

Com as capacidades apropriadas, você pode executar várias tarefas relacionadas a Contas de Serviço Gerenciadas do grupo. Execute uma operação de pesquisa para localizar e selecionar o objeto da gMSA necessário. Depois de selecionar um ou mais objetos na lista, a barra de tarefas fica ativa com opções para apagar objetos, adicionar objetos a grupos, remover objetos de grupos, mover objetos de um container para outro e modificar propriedades da gMSA. Você também pode fazer download dos resultados da pesquisa como um arquivo CSV. Clique nas opções para exibir as respectivas funções.

Crie uma gMSA

Ao criar uma gMSA, você deve especificar o host no qual a conta é usada e os objetos de computador que podem usar a conta. Objetos Computador definidos na política de participação podem usar o gMSA para executar serviços. Alternativamente, você pode especificar um grupo de segurança que contém uma lista de objetos Computador.

Para criar uma nova gMSA, navegue até **Gerenciamento > Pesquisar** e selecione **Conta de Serviço Gerenciado do Grupo** no menu suspenso Criar.

Modificar propriedades da gMSA

Você pode modificar as propriedades da gMSA. As suas capacidades determinam quais propriedades de uma gMSA você pode modificar no domínio gerenciado.

Habilitar a gMSA

Habilitar uma gMSA permite que você use a gMSA como credenciais de login para um serviço de computador. Você pode habilitar ou desabilitar uma gMSA da guia Contas.

Gerenciar participações em grupos para a gMSA

Você pode adicionar ou remover contas de serviço gerenciadas do grupo de um grupo específico no domínio gerenciado ou na subárvore gerenciada.

Mover uma gMSA para outro container

Uma gMSA é criada por padrão no container Conta de Serviço Gerenciada no Active Directory. Você pode mover uma conta de serviço gerenciada do grupo do container padrão para outro container, como um OU, no domínio gerenciado ou na subárvore gerenciada.

Apagar uma gMSA

Você pode apagar permanentemente uma conta de serviço gerenciado do grupo do domínio gerenciado ou da subárvore gerenciada.

5 Gerenciando Objetos do Azure

Este capítulo contém informações conceituais e de procedimento para gerenciar contas do usuário do Azure, contatos do Azure e grupos do Azure no Console da Web. Com os poderes adequados, realize diversas tarefas de gerenciamento de grupos do Azure, de contatos do Azure e de usuários do Azure, como criar e apagar objetos conta do usuário do Azure.

Você pode executar a maior parte das tarefas para objetos grupo do Azure, contatos do Azure e usuário do Azure por meio da guia **Gerenciamento > Pesquisa** no Console da Web para pesquisar objetos em um dos seguintes nós:

- ♦ Todos os Meus Objetos Gerenciados
- ♦ Todos os Meus Locatários Gerenciados
- ♦ Um sub-nó de Todos os Meus Locatários Gerenciados

Os tópicos incluem os seguintes:

- ♦ [“Gerenciando contas do usuário do Azure” na página 67](#)
- ♦ [“Gerenciando Grupos do Azure” na página 68](#)
- ♦ [“Gerenciando Contatos do Azure” na página 70](#)

Gerenciando contas do usuário do Azure

Como um administrador assistente, use o DRA para gerenciar contas do usuário do Azure e modificar propriedades de conta do usuário do Azure quando o Azure Active Directory tiver sido configurado pelo Administrador do DRA.

Execute uma operação de pesquisa para localizar e selecionar o objeto usuário do Azure necessário. Após selecionar um ou mais objetos na lista, a barra de tarefas ficará ativa, com opções como apagar, permitir, bloquear, redefinir senha e modificar propriedades. Você também pode fazer download dos resultados da pesquisa como um arquivo CSV. Clique nas opções para exibir as respectivas funções.

Criar uma conta do usuário do Azure

Você pode criar contas do usuário do Azure no Azure Active Directory. Você também pode habilitar e-mails e especificar participações em grupos para a nova conta.

Modificar propriedades da conta do usuário do Azure

Você pode gerenciar as propriedades de contas do usuário do Azure no Azure Active Directory. As capacidades que você tem determinam quais propriedades de uma conta do usuário do Azure você pode modificar. Se a conta do usuário do Azure tiver uma caixa de correio do Office 365 ou se a conta do usuário do Azure for habilitada por correio, você poderá gerenciar propriedades relacionadas à caixa de correio e relacionadas ao e-mail para a conta do usuário do Azure. Você pode gerenciar políticas de caixa de correio, definir restrições e opções de entrega, definir limites de armazenamento, delegar permissões de caixa de correio, colocar litígios em pausa, gerenciar endereços de e-mail e assim por diante.

Observação

- ♦ Você pode atualizar as propriedades de Celular e de Telefones Comerciais apenas para usuários do Azure que não são administradores.
 - ♦ O DRA permite que você exporte os resultados de **Membro De** como um arquivo CSV. Para exportar os resultados de **Membro De** do Console da Web, acesse **Gerenciamento > Pesquisa** e clique em **Propriedades**. Navegue até a guia **Membro De** e clique no ícone **Fazer Download**. As mudanças não gravadas não são exportadas. Grave quaisquer mudanças recentes para que elas estejam disponíveis no arquivo exportado.
-

Permitir entrada de conta do usuário do Azure

Você pode habilitar uma conta do usuário do Azure para efetuar login no Azure Active Directory.

Bloquear entrada de conta do usuário do Azure

Você pode bloquear o login de uma conta do usuário do Azure no Azure Active Directory.

Redefinir uma senha de conta do usuário do Azure

Você pode redefinir a senha para uma conta do usuário do Azure no Azure Active Directory e escolher se o DRA gerará uma nova senha para a conta.

Apagar uma conta do usuário do Azure

Você pode apagar uma conta do usuário do Azure Active Directory, mas ela não poderá ser restaurada do DRA.

Especificar uma participação de grupo do Azure para contas do usuário do Azure

Você pode adicionar ou remover contas do usuário do Azure de um grupo do Azure específico no Azure Active Directory.

Gerenciando Grupos do Azure

Como um administrador assistente, use o DRA para gerenciar grupos do Azure quando o Azure Active Directory tiver sido configurado pelo Administrador do DRA. Os grupos do Azure permitem que você conceda permissões específicas a um conjunto definido de contas do usuário. Os grupos do Azure permitem controlar quais dados e recursos uma conta do usuário poderá acessar em qualquer localitário.

Execute uma operação de pesquisa para localizar e selecionar o objeto grupo do Azure necessário. Depois de selecionar um ou mais objetos na lista, a barra de tarefas fica ativa com opções para apagar objetos, adicionar objetos a grupos, remover objetos de grupos, adicionar grupos a outros grupos, remover grupos de grupos existentes e modificar propriedades do grupo. Clique nas opções para exibir as respectivas funções.

Observação: Membros Suportados: Os membros de grupo do Azure podem ser usuários do Azure, grupos do Azure, contatos do Azure, usuários sincronizados, contatos sincronizados e grupos sincronizados.

Adicionar contas a grupos do Azure

Adicione contas do usuário, contatos e grupos, tanto locais como do Azure a um grupo gerenciado do Azure.

Esta tarefa adiciona várias contas a um grupo selecionado. Você pode adicionar uma conta individual a um grupo selecionando a conta adequada. Se a adição de uma conta a outro grupo aumentar seus poderes para a conta, o DRA não permitirá que você adicione a conta.

Aninhar grupos no Azure

Você pode aninhar grupos adicionando outros grupos (tanto localmente quanto no Azure) a um grupo do Azure gerenciado. Quando um grupo é aninhado em um grupo do Azure, o grupo filho herda as permissões do grupo pai.

Se a adição de um domínio ou de um grupo do Azure a outro grupo do Azure aumentar seus poderes para o grupo de origem, o DRA não permitirá que você adicione o grupo.

Criar um grupo do Azure

Crie um grupo do Azure no Azure Active Directory. Você também pode modificar as propriedades para o novo grupo, como adicionar membros do grupo.

Se nenhum proprietário for especificado, o DRA fornecerá a conta de acesso do locatário do Azure por padrão como o proprietário.

Modificar propriedades do grupo do Azure

As suas capacidades determinam quais propriedades você pode modificar em um grupo no Azure Active Directory. Se a Política do Exchange estiver habilitada, você poderá gerenciar propriedades do Exchange para grupos do Azure habilitados por correio, como o grupo do Office 365, o grupo de segurança habilitado por correio e a lista de distribuição. Dependendo do tipo de grupo, você pode gerenciar endereços de e-mail para o grupo, especificar quem pode enviar e-mails para o grupo, especificar usuários que podem enviar e-mails em nome do grupo, definir opções de aprovação de e-mail e assim por diante.

Observação: O DRA permite que você exporte os resultados de **Membros** e **Membro De** como um arquivo CSV. Navegue até a guia **Membros** ou **Membro De** e clique no ícone **Fazer Download**. As mudanças não gravadas não são exportadas. Grave quaisquer mudanças recentes para que elas estejam disponíveis no arquivo exportado.

Configurar propriedade do grupo do Azure

Defina a propriedade para quaisquer grupos. Conceda permissão de propriedade de grupo a uma conta do usuário ou a um grupo. A concessão da propriedade de grupo permite que a conta do usuário ou o grupo especificados gerencie o grupo, incluindo a participação.

Apagar um grupo do Azure

Você pode apagar grupos do Azure no Azure Active Directory, mas eles não poderão ser restaurados do DRA.

Gerenciando Contatos do Azure

Os contatos do Azure são objetos habilitados por correio que contêm um endereço de e-mail externo. Como um administrador assistente, use o DRA para gerenciar contatos do Azure e modificar propriedades de contatos do Azure quando o Azure Active Directory tiver sido configurado pelo Administrador do DRA.

Execute uma operação de pesquisa para localizar e selecionar o objeto contato do Azure necessário. Depois de selecionar um ou mais objetos na lista, a barra de tarefas fica ativa com opções para apagar objetos, adicionar objetos a grupos, remover objetos de grupos e modificar propriedades de contatos. Você também pode fazer download dos resultados da pesquisa como um arquivo CSV. Clique nas opções para exibir as respectivas funções.

Criar um contato do Azure

Você pode criar um contato do Azure no locatário gerenciado e especificar informações de contato e endereços de e-mail para o novo contato do Azure.

Modificar propriedades do contato do Azure

Você pode modificar propriedades do contato do Azure. As suas capacidades determinam quais propriedades de um contato do Azure você pode modificar no domínio gerenciado. Se a Política do Exchange estiver habilitada, você poderá gerenciar propriedades relacionadas a e-mail, como definir restrições de entrega de mensagens, especificar quem pode enviar mensagens em nome desse contato do Azure, especificar se o contato do Azure está visível na lista de endereços e assim por diante.

Habilitar a moderação de mensagens

Você pode definir opções para moderar mensagens enviadas para um contato do Azure. Quando você habilitar a moderação, as mensagens enviadas ao contato do Azure serão aprovadas por um mediador que você definirá, antes que sejam entregues. Você também pode especificar usuários e grupos que estão isentos do processo de aprovação.

Gerenciar participações em grupos para contatos do Azure

Você pode adicionar ou remover contatos do Azure em grupos de segurança e listas de distribuição habilitados por correio.

Observação: O DRA permite que você exporte os resultados de **Membro De** como um arquivo CSV. Navegue até a guia **Membro De** e clique no ícone **Fazer Download da Participação Gravada**. As mudanças não gravadas não são exportadas. Grave quaisquer mudanças recentes para que elas estejam disponíveis no arquivo exportado.

Apagar um contato do Azure

Você pode apagar contatos do Azure no Azure Active Directory, mas eles não poderão ser restaurados do DRA.

6 Gerenciando caixas de correio do Exchange e pastas públicas

Usando o DRA, você pode gerenciar as caixas de correio do Microsoft Exchange como uma extensão das propriedades da conta do usuário. Essa integração permite simplificar os workflows de administração para que você possa administrar efetivamente as propriedades do Exchange. Você também pode vincular caixas de correio de florestas de conta do usuário e de conta do Exchange e gerenciar caixas de correio de recursos, caixas de correio compartilhadas e pastas públicas.

Gerenciar tarefas de caixa de correio no Console de Delegação e Configuração

Ao usar o nó do ARM, você executa as tarefas de caixa de correio aplicáveis da guia **Tarefas do Exchange** nas propriedades do objeto, que também estão acessíveis em **Tarefas** ou no menu do botão direito do mouse para um objeto selecionado. Geralmente, você seleciona o nó **Todos os Meus Objetos Gerenciados** e executa a operação **Find Now** (Localizar Agora) para localizar e selecionar o objeto desejado.

Gerenciando tarefas de caixa de correio no Console da Web

Ao usar o Console da Web, você executa as tarefas de caixa de correio aplicáveis abaixo por meio da guia **Gerenciamento > Pesquisar**. Geralmente, você executa uma operação de pesquisa para localizar e selecionar o objeto de caixa de correio necessário. Após você selecionar um ou mais objetos na lista, a barra de tarefas ficará ativa. Clique nas opções para exibir as respectivas funções.

Veja os seguintes tópicos:

- ♦ [“Tarefas de gerenciamento para caixas de correio do usuário” na página 71](#)
- ♦ [“Tarefas de gerenciamento para caixas de correio do Office 365” na página 74](#)
- ♦ [“Tarefas de Gerenciamento para as Caixas de Correio de Recursos” na página 75](#)
- ♦ [“Tarefas de gerenciamento para caixas de correio compartilhadas” na página 77](#)
- ♦ [“Tarefas de gerenciamento para caixas de correio vinculadas” na página 78](#)
- ♦ [“Tarefas de gerenciamento para pastas públicas” na página 79](#)

Tarefas de gerenciamento para caixas de correio do usuário

Você pode gerenciar caixas de correio do Microsoft Exchange para contas do usuário no domínio gerenciado ou na subárvore gerenciada. Cada aspecto do gerenciamento de caixas de correio do Microsoft Exchange requer diferentes poderes. Os seus poderes controlam as propriedades da caixa de correio que podem ser modificadas ou se você pode criar, clonar, exibir ou apagar caixas de correio do Microsoft Exchange. Você também pode gerenciar direitos e permissões de caixa de correio associados a uma conta do usuário, permitindo controlar a segurança de seus ambientes do

Microsoft Exchange. Se você não tiver o poder necessário para modificar uma guia ou um campo para a caixa de correio selecionada, o DRA desabilitará as guias e os campos que você não pode modificar.

Além das tarefas definidas abaixo, as contas do usuário podem ter opções habilitadas nas propriedades do objeto pelo Administrador DRA para definir as configurações do Skype e do Skype Online. O Skype pode ser configurado de contas do usuário no Console de Delegação e Configuração e também no Console da Web. O Skype Online só pode ser configurado do Console da Web.

Criar uma caixa de correio

Você pode criar uma caixa de correio do Microsoft Exchange para uma conta do usuário existente. Você também pode modificar propriedades para a nova caixa de correio.

Observação: Quando você cria uma caixa de correio, o Exchange gera as strings de proxy necessárias com base nas configurações de política do Exchange. O Microsoft Exchange também gera strings de proxy padrão. Como resultado, ao exibir as propriedades da caixa de correio recém-criada, você vê os dois tipos de strings de proxy.

Clonar uma conta do usuário

Quando você clona uma conta do usuário, todos os grupos dos quais o usuário é membro são adicionados automaticamente à nova conta do usuário, economizando tempo na configuração da nova conta. Você pode adicionar ou remover grupos da nova conta, habilitar e-mails e fazer qualquer outra configuração de propriedade como faria com qualquer nova conta.

Observação: Quando você clona um objeto `InetOrgPerson`, uma conta do usuário é criada.

Mover uma caixa de correio

Você pode mover uma caixa de correio do Microsoft Exchange para uma conta do usuário para outro armazenamento de caixa de correio ou servidor do Microsoft Exchange.

Modificar propriedades da caixa de correio

Você pode modificar propriedades das caixas de correio do Microsoft Exchange à medida que gerencia as contas do usuário associadas. Seus poderes determinam quais propriedades da caixa de correio você pode modificar.

Observação: Você não pode modificar as propriedades da caixa de correio de contas do usuário gerenciadas em servidores membros.

Configurar permissões de segurança da caixa de correio

Você pode especificar a quais contas do usuário, grupos ou computadores deseja conceder ou negar a capacidade de enviar e receber e-mails usando uma caixa de correio específica do Microsoft Exchange. Essas configurações permitem que você proteja com mais eficácia o ambiente do Exchange. Você não pode modificar permissões de segurança herdadas.

Observação: Quando você gerencia a segurança da caixa de correio, as permissões desabilitadas podem indicar permissões herdadas.

Remover permissões de segurança da caixa de correio

Você pode remover permissões de segurança da caixa de correio de uma conta do usuário, grupo ou computador associado a uma caixa de correio do Microsoft Exchange. A remoção de permissões de segurança da caixa de correio impede que a conta do usuário, grupo ou conta de computador envie e receba e-mails por meio da caixa de correio especificada. Você não pode remover permissões de segurança herdadas.

Configurar direitos de caixa de correio

Você pode conceder ou negar direitos de outras contas do usuário, grupos ou computadores a uma caixa de correio específica do Microsoft Exchange. Essas configurações permitem que você proteja com mais eficácia o ambiente do Exchange. Você não pode modificar direitos de caixa de correio herdados.

Observação: Quando você gerencia direitos de caixa de correio, as permissões desabilitadas podem indicar permissões herdadas.

Remover direitos de caixa de correio

Você pode remover direitos de caixa de correio de contas do usuário, grupos ou computadores associados a uma caixa de correio do Microsoft Exchange específica. A remoção de direitos de caixa de correio impede que a conta do usuário, o grupo ou a conta de computador use a caixa de correio especificada. Você não pode remover direitos de caixa de correio herdados.

Apagar uma caixa de correio

Você pode apagar uma caixa de correio associada a uma conta do usuário no domínio gerenciado ou na subárvore gerenciada. Apagar uma caixa de correio também apaga todas as mensagens da caixa de correio.

Adicionar ou modificar um endereço de e-mail

Você pode especificar endereços de e-mail para caixas de correio associadas a contas do usuário em seu domínio gerenciado ou subárvore gerenciada. Você também pode designar endereços de e-mail a contas do usuário que ainda não tenham caixas de correio. Ao gerenciar caixas de correio do Microsoft Exchange, você pode adicionar apenas os tipos de endereço de e-mail definidos por suas políticas de geração de proxy.

Especificar um endereço de resposta

Você pode definir endereços de resposta para uma caixa de correio associada a uma conta do usuário no domínio gerenciado ou na subárvore gerenciada. Você pode definir vários endereços de resposta para uma caixa de correio. No entanto, você não pode definir mais de um tipo de endereço de e-mail como um endereço de resposta. Por exemplo, você não pode especificar mais de um endereço na Internet como um endereço de resposta.

Apagar um endereço de e-mail

Você pode apagar um endereço de e-mail removendo o endereço da caixa de correio.

Especificar opções de envio

Você pode especificar quais caixas de correio o usuário pode usar para enviar mensagens, definir opções de encaminhamento e especificar limites de destinatários.

Especificar restrições de envio

Ao definir restrições de entrega, você pode limitar o tamanho das mensagens recebidas e enviadas e a aceitação das mensagens recebidas de uma caixa de correio específica.

Especificar limites de armazenamento

Você pode especificar limites de armazenamento, como avisos com base no tamanho de uma caixa de correio. Você também pode especificar tempos de retenção para itens apagados.

Verificar status de movimentação da caixa de correio

Você pode verificar o status das movimentações de caixa de correio e executar ações, como limpar o status, cancelar um movimento e retomar um movimento que tenha sido interrompido.

Tarefas de gerenciamento para caixas de correio do Office 365

Esta seção contém informações para administrar caixas de correio do Microsoft Office 365 no Console de Delegação e Configuração por meio do nó Gerenciamento de Recursos e de Contas e no Console da Web. Com as capacidades adequadas, execute várias tarefas de gerenciamento de contas do usuário, como aplicar pausas no litígio, configurar o encaminhamento de e-mail e assim por diante.

Importante: O DRA gerencia caixas de correio de usuários do Office 365, bem como caixas de correio migradas compartilhadas, de sala e de equipamentos. Para que o DRA gerencie essas caixas de correio, elas devem estar associadas a um usuário local ou a um usuário do Azure gerenciado pelo DRA. As propriedades da caixa de correio estarão disponíveis por meio das páginas de propriedade para esses usuários associados.

Estabelecer uma pausa no litígio

Defina uma pausa no litígio em uma caixa de correio para preservar todo o conteúdo da caixa de correio, incluindo itens apagados e versões originais dos itens modificados. Colocar uma caixa de correio do usuário em pausa no litígio também preserva o conteúdo, se existir, na caixa de correio de arquivo do usuário. A pausa pode durar por um período especificado ou até você remover a pausa no litígio da caixa de correio.

Você deve ter uma licença adequada do Exchange Online para fazer uma pausa no litígio. Você configura o recurso por meio da guia **Litigation Hold** (Pausa no Litígio) nas propriedades do objeto usuário.

Delegar permissões da caixa de correio

Você pode delegar permissões de caixa de correio do Office 365 por meio da guia de Delegação de caixa de correio nas propriedades do objeto usuário. Existem três tipos de permissões que você pode delegar, enviar como, enviar em nome de e acesso total. Os tipos de permissão que podem ser delegados dependem do tipo de objeto receptor.

Ver status da caixa de correio de arquivo

Você pode ver o status da caixa de correio de arquivo para um usuário e as estatísticas da caixa de correio de arquivo, como limite de armazenamento e limite de aviso. Quando a caixa de correio de arquivo excede o limite de aviso de arquivo, o usuário é notificado.

Ver estatísticas de uso da caixa de correio

Você pode ver o valor da cota total da caixa de correio que foi usada.

Configure restrições de entrega de mensagens

Ao definir restrições de entrega, você pode limitar o tamanho das mensagens recebidas e enviadas e aceitar ou rejeitar as mensagens recebidas para um usuário específico.

Especificar opções de envio

Você pode configurar opções de encaminhamento de mensagens e especificar os destinatários máximos para os quais um usuário pode enviar uma mensagem.

Adicionar ou remover um endereço de e-mail

Você pode configurar mais de um endereço de e-mail para uma caixa de correio do usuário e especificar o endereço de e-mail principal. Você também pode designar endereços de e-mail para contas do usuário que ainda não tenham caixas de correio.

Ocultar endereço de e-mail

Você pode especificar se deve ocultar o endereço de e-mail da lista de endereços.

Adicionar MailTip

Você pode adicionar texto informativo que deseja que seja exibido quando um e-mail é enviado ao usuário.

Designar políticas a caixa de correio

Você pode designar uma política de compartilhamento, uma política de retenção de e-mails, uma política de designação de função ou uma política de bloco de endereços à caixa de correio.

Tarefas de Gerenciamento para as Caixas de Correio de Recursos

O recurso de caixa de correio de recursos do Microsoft Exchange permite criar uma caixa de correio que represente um recurso, como uma sala de conferência, para que você possa reservá-la enviando um convite para reunião, como faria com uma pessoa. O DRA contém um conjunto de funções, poderes e políticas que permitem gerenciar suas caixas de correio de recursos com eficiência.

O DRA tem suporte de extensão da interface para caixas de correio de recursos, bem como suporte para gerar relatórios de auditoria ou de interface do usuário. O suporte para scripts ADSI também está integrado ao DRA.

Criar uma caixa de correio de recursos

Você pode criar caixas de correio de recursos no domínio gerenciado ou na subárvore gerenciada.

Mover uma caixa de correio de recursos para outro contêiner

Você pode mover uma caixa de correio de recursos para outro contêiner, como uma OU, no domínio gerenciado ou na subárvore gerenciada.

Mover uma caixa de correio de recursos para outro armazenamento de caixa de correio ou servidor do Exchange

Você pode mover uma caixa de correio de recursos para outro armazenamento de caixa de correio ou servidor do Microsoft Exchange.

Clonar uma caixa de correio de recursos

Ao clonar uma caixa de correio de recursos, você pode criar rapidamente outras caixas de correio de recursos com propriedades semelhantes. Quando você clona uma caixa de correio de recursos, o DRA preenche o Assistente de Clonagem de Caixa de Correio de Recursos com valores do recurso selecionado.

Renomear uma caixa de correio de recursos

Você pode renomear caixas de correio de recursos no domínio gerenciado ou na subárvore gerenciada. Mudar o nome de logon do usuário também muda o nome da caixa de correio associada à conta do usuário.

Adicionar uma caixa de correio de recursos a um grupo

Você pode adicionar caixas de correio de recursos a um grupo específico no domínio gerenciado ou na subárvore gerenciada.

Apagar uma caixa de correio de recursos

Você pode apagar uma caixa de correio de recursos no domínio gerenciado ou na subárvore gerenciada. Apagar uma caixa de correio de recursos também apaga todas as mensagens contidas nela e eventuais objetos usuário desabilitados associados a ela. Se assim desejar, anule o apagamento de objetos usuário desabilitados quando apagar a caixa de correio. Se você apagar um objeto usuário associado a uma caixa de correio de recursos, ela também será apagada.

Restaurar uma caixa de correio de recursos apagada

Você poderá restaurar uma caixa de correio de recursos que foi apagada se a Lixeira desse domínio estiver habilitada.

Modificar propriedades da caixa de correio de recursos

Você pode gerenciar as propriedades das caixas de correio de recursos no domínio gerenciado ou na subárvore gerenciada. Seus poderes determinam quais propriedades você pode modificar.

Observação: O DRA permite que você exporte os resultados de **Membro De** como um arquivo CSV. Para exportar os resultados de **Membro De** do Console da Web, acesse **Gerenciamento > Pesquisa** e clique em **Propriedades**. Navegue até a guia **Membro De** e clique no ícone **Fazer Download**. As mudanças não gravadas não são exportadas. Grave quaisquer mudanças recentes para que elas estejam disponíveis no arquivo exportado.

Tarefas de gerenciamento para caixas de correio compartilhadas

As caixas de correio compartilhadas são úteis para os administradores de Suporte técnico e para a equipe de suporte técnico, pois todas as respostas podem ser configuradas para entrar em uma única caixa de correio que pode ser acessada por vários usuários. A caixa de correio deve estar em um domínio gerenciado por DRA com a Política do Exchange habilitada e você deve ter poderes delegados a você para gerenciar caixas de correio compartilhadas.

Quando você cria uma caixa de correio compartilhada, há dois tipos de permissões que podem ser delegadas aos usuários: Enviar como e Acesso completo. Enviar como fornece permissão para ler e enviar e-mails. Você pode delegar permissões para objetos de usuário e de grupo. Você também pode especificar restrições de entrega, opções de entrega, limites de armazenamento, permissões de pasta e várias outras opções nas propriedades do objeto.

Observação: Você pode realizar tarefas de gerenciamento para caixas de correio compartilhadas apenas por meio do Console da Web.

Criar uma caixa de correio compartilhada

Você pode criar caixas de correio compartilhadas no domínio gerenciado ou na subárvore gerenciada.

Mover uma caixa de correio compartilhada para outro contêiner

Você pode mover uma caixa de correio compartilhada para outro contêiner, como uma OU, no domínio gerenciado ou na subárvore gerenciada.

Mover uma caixa de correio compartilhada para outro armazenamento de caixa de correio

Você pode mover uma caixa de correio compartilhada para outro armazenamento de caixa de correio.

Clonar uma caixa de correio compartilhada

Ao clonar uma caixa de correio compartilhada, você pode criar rapidamente outras caixas de correio compartilhadas com propriedades semelhantes.

Renomear uma caixa de correio compartilhada

Você pode renomear caixas de correio compartilhadas no domínio gerenciado ou na subárvore gerenciada. Mudar o nome de logon do usuário também muda o nome da caixa de correio associada à conta do usuário.

Apagar uma caixa de correio compartilhada

Você pode apagar uma caixa de correio compartilhada no domínio gerenciado ou na subárvore gerenciada. Se a Lixeira estiver desabilitada para esse domínio, apagar uma caixa de correio de recursos a removerá permanentemente do Active Directory. Se a Lixeira estiver habilitada para esse domínio, apagar uma caixa de correio compartilhada a moverá para a Lixeira.

Apagar uma caixa de correio compartilhada também apaga todas as mensagens contidas nela e eventuais objetos usuário desabilitados associados a ela. Se você apagar um objeto usuário associado a uma caixa de correio compartilhada, ela também será apagada.

Restaurar uma caixa de correio compartilhada apagada

Você poderá restaurar uma caixa de correio compartilhada que foi apagada se a Lixeira desse domínio estiver habilitada.

Criar uma caixa de correio do arquivo compartilhada

Você pode criar caixas de correio compartilhadas arquivadas no domínio gerenciado ou na subárvore gerenciada.

Apagar uma caixa de correio do arquivo compartilhada

Você pode apagar caixas de correio compartilhadas arquivadas no domínio gerenciado ou na subárvore gerenciada.

Modificar propriedades da caixa de correio compartilhada

Você pode gerenciar as propriedades das caixas de correio compartilhadas no domínio gerenciado ou na subárvore gerenciada. Seus poderes determinam quais propriedades você pode modificar.

Observação: O DRA permite que você exporte os resultados de **Membro De** como um arquivo CSV. Para exportar os resultados de **Membro De** do Console da Web, acesse **Gerenciamento > Pesquisa** e clique em **Propriedades**. Navegue até a guia **Membro De** e clique no ícone **Fazer Download**. As mudanças não gravadas não são exportadas. Grave quaisquer mudanças recentes para que elas estejam disponíveis no arquivo exportado.

Tarefas de gerenciamento para caixas de correio vinculadas

As caixas de correio vinculadas são úteis para grandes mudanças organizacionais que ocorrem durante fusões, aquisições e divisões de empresas, quando a migração da caixa de correio é comum. Esse recurso permite vincular caixas de correio de diferentes florestas do Exchange para negar a interrupção do e-mail do usuário. As caixas de correio devem estar em um domínio gerenciado por DRA com a Política do Exchange habilitada e você deve ter poderes delegados para gerenciar caixas de correio vinculadas. Quando você cria uma caixa de correio vinculada, uma guia **Caixa de Correio Vinculada** é adicionada às propriedades do objeto usuário.

O gerenciamento de caixas de correio vinculadas é suportado apenas no Console da Web. Você cria uma caixa de correio vinculada na barra de ferramentas de uma conta do usuário selecionada. Essa opção só é habilitada quando o domínio do usuário selecionado tem uma confiança de floresta externa com outros domínios gerenciados no DRA. Apenas as contas do usuário desabilitadas serão listadas ao procurar uma conta para vincular em outro domínio gerenciado pelo DRA.

Criar uma caixa de correio vinculada

Você pode criar uma caixa de correio vinculada de duas contas do usuário selecionadas em diferentes florestas gerenciadas do Exchange.

Apagar uma caixa de correio vinculada

Você pode apagar uma caixa de correio vinculada da barra de ferramentas de um usuário selecionado que tenha uma caixa de correio vinculada.

Modificar propriedades da caixa de correio vinculada

Você pode modificar as propriedades de uma caixa de correio vinculada da guia **Caixa de Correio Vinculada** nas propriedades de um usuário selecionado.

Criar uma caixa de correio de arquivo vinculada

Você pode criar uma caixa de correio de arquivo vinculada de um usuário selecionado que tenha uma caixa de correio vinculada.

Apagar uma caixa de correio de arquivo vinculada

Você pode apagar uma caixa de correio de arquivo vinculada da barra de ferramentas de um usuário selecionado que tenha uma caixa de correio vinculada.

Restaurar uma caixa de correio vinculada apagada

Você poderá restaurar uma caixa de correio vinculada que foi apagada se a Lixeira desse domínio estiver habilitada.

Tarefas de gerenciamento para pastas públicas

Se o Administrador DRA tiver criado florestas de Pastas Públicas na empresa gerenciada pelo DRA e lhe concedido poderes para gerenciar pastas públicas no DRA, você poderá criar pastas públicas, modificar suas propriedades e gerar relatórios de histórico de mudanças. Só é possível criar e modificar pastas públicas no Console da Web. Use a opção de pesquisa para pesquisar pastas públicas. Para obter informações, veja *“Pesquisa” na página 39*.

Você executa tarefas de Pasta Pública da guia **Gerenciamento > Pastas Públicas**.

Criar uma pasta pública

Você pode criar pastas públicas em domínios, subárvores e caixas de correio de Pasta Pública especificados por meio do Console da Web. Você pode usar a caixa de correio padrão para o domínio selecionado ou escolher um.

Habilitar o e-mail para uma pasta pública

Você pode habilitar o e-mail de uma pasta pública usando a opção **Habilitar Correio** na barra de ferramentas da lista. Isso permite que você associe endereços de e-mail à pasta pública e modifique as propriedades da pasta pública.

Desabilitar o e-mail para uma pasta pública

Você pode desabilitar o e-mail de uma pasta pública usando a opção **Desabilitar Correio** na barra de ferramentas da lista.

Modificar propriedades de pastas públicas

Após habilitar o e-mail em uma pasta pública existente, você pode ver as estatísticas da pasta e modificar as propriedades dessa pasta pública. Nessas propriedades, é possível especificar opções de entrega e restrição de usuários, limites de tamanho e avisos de cota, propriedades de e-mail, limites de idade de armazenamento, inclusão de moderadores para aprovação de e-mail e atributos personalizados.

Observação: Você também pode atualizar algumas propriedades para várias pastas públicas quando mais de uma estiver selecionada, como cotas de armazenamento.

Apagar uma pasta pública

Você poderá apagar pastas públicas se elas não tiverem subpastas e a opção de e-mail estiver desativada.

7 Gerenciando recursos

O DRA permite gerenciar recursos, incluindo computadores, impressoras e outros dispositivos, bem como processos associados a esses recursos. Por exemplo, se você precisar iniciar um serviço específico em um computador gerenciado, poderá procurar esse objeto Computador no DRA, acessar seus serviços por meio de propriedades de objeto e reiniciar um serviço específico nesse computador por meio do DRA sem ter necessidade de controle remoto para esse computador.

- ♦ [“Gerenciamento de UOs \(Unidades Organizacionais\)” na página 81](#)
- ♦ [“Gerenciando computadores” na página 82](#)
- ♦ [“Gerenciando serviços” na página 84](#)
- ♦ [“Gerenciando impressoras e serviços de impressão” na página 85](#)
- ♦ [“Gerenciando compartilhamentos” na página 89](#)
- ♦ [“Gerenciando usuários conectados” na página 89](#)
- ♦ [“Gerenciando dispositivos” na página 90](#)
- ♦ [“Gerenciando registros de eventos” na página 90](#)
- ♦ [“Gerenciando arquivos abertos” na página 92](#)

Gerenciamento de UOs (Unidades Organizacionais)

Esta seção guia você pela administração de OUs no Console de Delegação e Configuração por meio do nó Gerenciamento de Recursos e de Contas. Com os poderes adequados, realize várias tarefas de gerenciamento de OUs, como mover uma OU para outro container.

Observação: Você só pode gerenciar OUs por meio do Console de Delegação e Configuração.

Modificando propriedades de UOs

Você pode modificar propriedades de UOs. Os seus poderes determinam quais propriedades você pode modificar para uma OU no domínio gerenciado ou na subárvore gerenciada.

Criando uma OU

Você pode criar uma OU no domínio gerenciado ou na subárvore gerenciada. Você também pode modificar propriedades gerais, como a descrição da OU.

Clonando uma OU

Você pode criar uma nova OU clonando uma existente do domínio gerenciado ou da subárvore gerenciada. Você também pode modificar propriedades gerais para a nova OU, como a descrição da OU. Clonar uma OU não clona os objetos que ela contém.

Abrindo a Árvore do Active Directory em uma Localização de OU

Você pode abrir de modo rápido e fácil a árvore do Active Directory na localização de uma OU específica no domínio gerenciado ou na subárvore gerenciada.

Movendo uma UO para outro container

Você pode mover uma UO para um container diferente no domínio gerenciado. Ao gerenciar uma subárvore de um domínio, você pode mover UOs dentro da hierarquia dessa subárvore.

Observação

- ♦ Se a mudança de uma UO para outro container aumentar seus poderes para a UO movida, o DRA não permitirá que você mova essa UO.
 - ♦ Você também pode mover uma UO arrastando-a para a nova localização.
-

Apagando uma UO

Você pode apagar UOs no domínio gerenciado ou na subárvore gerenciada. Você só pode apagar UOs vazias. Se uma UO contém objetos, você não pode apagá-la. Para apagar uma UO que contém objetos, apague todos os objetos primeiro, depois a UO.

Gerenciando computadores

O DRA permite administrar computadores no domínio gerenciado ou na subárvore gerenciada. Por exemplo, você pode adicionar ou remover contas de computador nos domínios gerenciados, bem como gerenciar os recursos em cada computador. Quando você adiciona um computador a um domínio, o DRA cria uma conta de computador nesse domínio para esse computador. Você pode então conectar o computador nesse domínio e configurar o computador para usar essa conta de computador. Você também pode ver e modificar as propriedades das contas de computador. O DRA também permite encerrar um computador e sincronizar os controladores de domínio em um domínio gerenciado.

Observação

- ♦ Você só pode gerenciar computadores por meio do Console de Delegação e Configuração.
 - ♦ Você não pode gerenciar controladores de domínio ocultos. O cache de domínio não inclui controladores de domínio ocultos. Portanto, o DRA não exibe computadores de domínio ocultos em listas ou janelas de propriedades
-

Especificar participação do grupo para computadores

Você pode adicionar ou remover computadores de um grupo específico no domínio gerenciado ou na subárvore gerenciada. Você também pode ver ou modificar propriedades de grupos existentes aos quais esse computador pertence.

Observação: O DRA permite que você exporte os resultados de **Membro De** como um arquivo CSV. Para exportar os resultados de **Membro De** do Console da Web, acesse **Gerenciamento > Pesquisa** e clique em **Propriedades**. Navegue até a guia **Membro De** e clique no ícone **Fazer Download**. As mudanças não gravadas não são exportadas. Grave quaisquer mudanças recentes para que elas estejam disponíveis no arquivo exportado.

Gerenciar propriedades da conta de computador

Você pode gerenciar as propriedades da conta de computador. Os seus poderes determinam quais propriedades você pode modificar para um computador no domínio gerenciado ou na subárvore gerenciada.

Adicionar um computador a um domínio

Você pode adicionar um computador a um domínio gerenciado ou subárvore gerenciada criando uma nova conta de computador.

Remover um computador de um domínio

Você pode remover um computador de um domínio gerenciado ou de uma subárvore gerenciada apagando a conta de computador.

Mover um computador

Você pode mover um computador para outro contêiner, como uma OU, no domínio gerenciado ou na subárvore gerenciada.

Encerrar ou reiniciar um computador

Você pode encerrar e reiniciar um computador imediatamente ou em uma data e hora definidas.

Redefinir a senha da conta de Administrador

Para redefinir a senha da conta de administrador de um computador, você deve ter a senha de Redefinição para o poder de administrador local ou estar associado a uma função que contenha esse poder. Você pode redefinir a senha do administrador para servidores membros em seu domínio gerenciado ou subárvore gerenciada. Você não pode redefinir a senha do administrador para um controlador de domínio.

Reiniciar a conta de computador

Você pode redefinir uma conta de computador para servidores membros em seu domínio gerenciado ou subárvore gerenciada. Você não pode redefinir a conta de computador para um controlador de domínio.

Apagar uma conta de computador

Você pode apagar uma conta de computador do domínio gerenciado ou da subárvore gerenciada. Se você estiver gerenciando um domínio do Microsoft Windows, poderá apagar contas de computador que contenham outros objetos, como um recurso compartilhado. Habilite a opção **Forçar Apagamento** para apagar objetos Computador do Active Directory. Isso também apagará objetos-filho, incluindo impressoras e pastas compartilhadas. Computadores apagados e os respectivos objetos associados são movidos para a Lixeira do DRA. Se a Lixeira estiver desabilitada no momento do apagamento, os objetos serão apagados permanentemente.

Observação: Você não pode apagar contas de computador de servidores membros no domínio gerenciado ou na subárvore gerenciada.

Desabilitar uma conta de computador

Você pode desabilitar uma conta de computador no domínio gerenciado ou na subárvore gerenciada. Desabilitar uma conta de computador impede que os usuários nesse computador efetuem login em qualquer domínio.

Habilitar uma conta de computador

Você pode habilitar uma conta de computador no domínio gerenciado ou na subárvore gerenciada. Habilitar uma conta de computador permite que os usuários nesse computador façam logon em qualquer domínio.

Gerenciando recursos de computador

Para cada conta de computador no domínio gerenciado ou na subárvore gerenciada, você pode gerenciar recursos associados, como serviços, compartilhamentos, dispositivos, impressoras e serviços de impressão.

Gerenciando serviços

Um serviço é um tipo de aplicativo que recebe tratamento especial do sistema operacional Windows. Os serviços podem ser executados mesmo quando nenhum usuário estiver conectado a um computador no momento. Os administradores assistentes com as capacidades apropriadas podem gerenciar serviços que estão sendo executados em computadores no domínio gerenciado ou na subárvore gerenciada.

Gerenciar propriedades de serviços

Você pode gerenciar propriedades para serviços executados em computadores no domínio gerenciado ou na subárvore gerenciada. Você pode gerenciar serviços enquanto gerencia outros recursos para esse computador.

Iniciar um serviço

Você pode iniciar um serviço em qualquer computador no domínio gerenciado ou na subárvore gerenciada.

Iniciar um serviço com parâmetros

Quando você inicia serviços que aceitam parâmetros, pode especificar esses parâmetros na inicialização. Você pode iniciar serviços em computadores no domínio gerenciado ou na subárvore gerenciada.

Observação: Você pode iniciar um serviço com parâmetros apenas por meio do Console de Delegação e Configuração.

Especificar um tipo de inicialização de serviço

Você pode mudar o tipo de inicialização de um serviço, como exigir uma inicialização manual.

Especificar uma conta de logon de serviço

Você pode mudar a conta de logon de serviço para uma conta diferente da conta do sistema atual. Você pode especificar a conta do sistema local, uma conta de usuário específica ou uma GMSA (conta de serviço gerenciada do grupo) como a conta de logon do serviço.

Reiniciar um serviço

Você pode reiniciar um serviço em execução em um computador no domínio gerenciado ou na subárvore gerenciada.

Para reiniciar um serviço, você deve ter capacidades para Parar um Serviço e Iniciar um Serviço ou estar associado a uma função que contenha essas capacidades, como a função Iniciar Serviço e a função Parar Serviço.

Parar um serviço

Você pode parar um serviço em execução em um computador no domínio gerenciado ou na subárvore gerenciada.

Pausar um serviço

Você pode pausar um serviço em execução em um computador específico no domínio gerenciado ou na subárvore gerenciada. Se um serviço pode ser pausado ou não, depende do tipo de serviço. Por exemplo, talvez você não consiga pausar um serviço que tenha serviços dependentes.

Retomar um serviço pausado

Você pode retomar um serviço que foi pausado em um computador no domínio gerenciado ou na subárvore gerenciada.

Gerenciando impressoras e serviços de impressão

Para gerenciar impressoras, você gerencia as filas de impressão que atendem essas impressoras. O DRA permite pausar ou retomar, iniciar, modificar, parar e ver impressoras de recursos e impressoras publicadas. O DRA também permite modificar as propriedades e prioridades dos serviços de impressão. Para adicionar ou apagar uma impressora, use as ferramentas nativas do Windows.

Um servidor de impressão é um computador no qual uma ou mais impressoras lógicas estão instaladas. Uma impressora lógica é definida no computador que tem o driver do dispositivo da impressora. Uma impressora lógica inclui o driver de impressão, a fila de impressão e as portas de uma impressora. O servidor de impressão associa impressoras lógicas a dispositivos de impressora.

Uma impressora conectada é definida nos computadores dos quais os documentos são selecionados para impressão. Uma impressora conectada é uma conexão para um compartilhamento de impressão na rede. Portanto, você pode gerenciar impressoras e serviços de impressão por meio dos computadores associados.

Uma impressora publicada é uma impressora publicada no Active Directory. Uma impressora publicada pode ser uma impressora de rede que não esteja diretamente conectada a um servidor ou pode ser uma impressora hospedada pelo servidor de cluster.

Observação: Você só pode gerenciar impressoras e trabalhos de impressão por meio do Console de Delegação e Configuração.

Para saber mais sobre como gerenciar impressoras e tarefas de impressão, veja os seguintes tópicos:

- ♦ [“Tarefas de gerenciamento de impressoras” na página 85](#)
- ♦ [“Tarefas de gerenciamento de serviços de impressão” na página 86](#)
- ♦ [“Tarefas de gerenciamento de impressoras publicadas” na página 87](#)
- ♦ [“Tarefas de gerenciamento de serviços de impressão para impressoras publicadas” na página 88](#)

Tarefas de gerenciamento de impressoras

Você pode gerenciar impressoras associadas a computadores no domínio gerenciado ou na subárvore gerenciada. O DRA permite que você gerencie impressoras enquanto gerencia outros recursos para esse computador.

Esta seção guia você pela administração de impressoras no Console de Delegação e Configuração por meio do nó Gerenciamento de Recursos e de Contas. Com os poderes adequados, você pode executar várias tarefas de gerenciamento de impressora, como parar uma impressora.

Gerenciar propriedades de impressoras

Você pode gerenciar propriedades para impressoras no domínio gerenciado ou na subárvore gerenciada. O DRA permite que você gerencie impressoras enquanto gerencia outros recursos para esse computador.

Pausar uma impressora

Você pode pausar uma impressora associada a um computador no domínio gerenciado ou na subárvore gerenciada. O DRA permite que você gerencie impressoras enquanto gerencia outros recursos para esse computador.

Retomar uma impressora

Você pode retomar uma impressora associada a um computador no domínio gerenciado ou na subárvore gerenciada. O DRA permite que você gerencie impressoras enquanto gerencia outros recursos para esse computador.

Tarefas de gerenciamento de serviços de impressão

Você pode gerenciar serviços de impressão associados a impressoras no domínio gerenciado ou na subárvore gerenciada. Como os serviços de impressão estão associados a uma impressora, você pode gerenciá-los enquanto gerencia a impressora.

Esta seção guia você pelo gerenciamento de trabalhos de impressão no nó Gerenciamento de Recursos e de Contas do Console de Delegação e Configuração. Com os poderes adequados, você pode executar várias tarefas de gerenciamento de serviços de impressão, como cancelar um serviço de impressão.

Gerenciar propriedades do serviço de impressão

Você pode modificar propriedades do serviço de impressão como parte do workflow do gerenciamento da impressora. Como os serviços de impressão estão associados às impressoras, você pode modificar o serviço de impressão enquanto gerencia a impressora correspondente. As propriedades do serviço de impressão que você pode modificar dependem do tipo de poder que você tem. Para modificar as propriedades do serviço de impressão, você deve poder acessar a impressora e o computador correspondentes.

Pausar um serviço de impressão

Você pode pausar um serviço de impressão em uma impressora em um domínio gerenciado ou uma subárvore gerenciada. Para pausar um serviço de impressão, você deve poder acessar a impressora e o computador correspondentes. Pausar um serviço de impressão não o apaga da fila de impressão.

Retomar um serviço de impressão

Você pode retomar um serviço de impressão que foi interrompido. Para retomar um serviço de impressão, você deve poder acessar a impressora e o computador correspondentes.

Reiniciar um serviço de impressão

Você pode reiniciar um serviço de impressão que foi interrompido. Para reiniciar um serviço de impressão, você deve poder acessar a impressora e o computador correspondentes.

Cancelar um serviço de impressão

Você pode cancelar um serviço de impressão que esteja na fila da impressora. Quando você cancela um serviço de impressão, o DRA apaga permanentemente o serviço de impressão da fila da impressora. Para cancelar um serviço de impressão, você deve poder acessar a impressora e o computador correspondentes.

Tarefas de gerenciamento de impressoras publicadas

Você pode gerenciar impressoras publicadas no domínio gerenciado ou na subárvore gerenciada. Você pode adicionar ou procurar por qualquer impressora publicada no Active Directory ou em impressoras hospedadas pelo servidor de cluster.

Esta seção guia você pela administração de impressoras publicadas no nó Gerenciamento de Recursos e de Contas. Com os poderes adequados, você pode executar várias tarefas de gerenciamento de impressora, como parar uma impressora.

Gerenciar propriedades de impressoras publicadas

Você pode gerenciar propriedades para impressoras publicadas no domínio gerenciado ou na subárvore gerenciada. O DRA permite gerenciar impressoras publicadas enquanto gerencia outros recursos.

Atualizar informações da impressora publicada

Você pode atualizar as informações publicadas da impressora no domínio gerenciado ou na subárvore gerenciada. O DRA permite gerenciar impressoras publicadas enquanto gerencia outros recursos.

Pausar uma impressora publicada

Você pode pausar uma impressora publicada no domínio gerenciado ou na subárvore gerenciada. O DRA permite gerenciar impressoras publicadas enquanto gerencia outros recursos.

Retomar uma impressora publicada

Você pode retomar uma impressora publicada que foi pausada no domínio gerenciado ou na subárvore gerenciada. O DRA permite gerenciar impressoras publicadas enquanto gerencia outros recursos.

Mover uma impressora publicada

Você pode mover uma impressora publicada disponível em um contêiner no domínio gerenciado para outro contêiner no mesmo domínio. O DRA permite gerenciar impressoras publicadas enquanto gerencia outros recursos.

Renomear uma impressora publicada

Você pode renomear uma impressora publicada compartilhada no Active Directory. O DRA permite gerenciar impressoras publicadas enquanto gerencia outros recursos.

Observação: Renomear uma impressora publicada no Active Directory não muda o nome do compartilhamento de impressora de recursos nem propaga a mudança de nome para a impressora de recursos que você deseja gerenciar. Por exemplo, se o nome da impressora de

recursos for Esmeralda e você renomear a impressora para Rubi no Active Directory, outros usuários verão o nome da impressora como Rubi, mas o nome da impressora de recursos continuará sendo Esmeralda.

Tarefas de gerenciamento de serviços de impressão para impressoras publicadas

Você pode gerenciar serviços de impressão associados a impressoras publicadas no domínio gerenciado ou na subárvore gerenciada. Como os serviços de impressão estão associados a uma impressora, você pode gerenciá-los enquanto gerencia a impressora publicada.

Esta seção guia você pela administração de impressoras publicadas no nó Gerenciamento de Recursos e de Contas. Com os poderes adequados, você pode executar várias tarefas de gerenciamento de serviços de impressão, como cancelar um serviço de impressão.

Gerenciar propriedades do serviço de impressão

Você pode modificar propriedades do serviço de impressão como parte do workflow do gerenciamento da impressora publicada. Como os serviços de impressão estão associados às impressoras, você pode modificar o serviço de impressão enquanto gerencia a impressora publicada correspondente. As propriedades do serviço de impressão que você pode modificar dependem do tipo de poder que você tem. Para modificar as propriedades do serviço de impressão, você deve poder acessar a impressora publicada correspondente.

Pausar um serviço de impressão

Você pode pausar um serviço de impressão em uma impressora publicada em um domínio gerenciado ou uma subárvore gerenciada. Para pausar um serviço de impressão, você deve poder acessar a impressora publicada correspondente. Pausar um serviço de impressão não o apaga da fila de impressão.

Retomar um serviço de impressão

Você pode retomar um serviço de impressão que foi interrompido em um domínio gerenciado ou uma subárvore gerenciada. Para retomar um serviço de impressão, você deve poder acessar a impressora publicada correspondente.

Reiniciar um serviço de impressão

Você pode reiniciar um serviço de impressão que foi interrompido em um domínio gerenciado ou uma subárvore gerenciada. Para reiniciar um serviço de impressão, você deve poder acessar a impressora publicada correspondente.

Cancelar um serviço de impressão

Você pode cancelar um serviço de impressão que esteja na fila da impressora em um domínio gerenciado ou uma subárvore gerenciada. Quando você cancela um serviço de impressão, o DRA apaga permanentemente o serviço de impressão da fila da impressora. Para cancelar um serviço de impressão, você deve poder acessar a impressora publicada correspondente.

Gerenciando compartilhamentos

Um compartilhamento é uma maneira de disponibilizar recursos, como arquivos ou impressoras, para outros usuários na rede. Cada compartilhamento tem um nome de compartilhamento que se refere a uma pasta compartilhada no servidor. O DRA gerencia os compartilhamentos somente nos computadores nos domínios gerenciados. Para gerenciar os compartilhamentos com sucesso, a conta de acesso deve ter permissões de administrador, como ser membro do grupo local Administradores, em todos os computadores nos quais você deseja gerenciar recursos. Para atribuir essas permissões, adicione a conta de acesso ao grupo de administradores de domínio nativo no domínio do computador.

Observação: Você só pode gerenciar compartilhamentos por meio do Console de Delegação e Configuração.

Gerenciar propriedades de compartilhamento

Você pode gerenciar propriedades para compartilhamentos no domínio gerenciado ou na subárvore gerenciada. O DRA permite gerenciar compartilhamentos enquanto gerencia outros recursos para esse computador.

Criar um compartilhamento

Você pode criar um compartilhamento para um computador no domínio gerenciado ou na subárvore gerenciada. Você também pode modificar propriedades para esse compartilhamento.

Clonar um compartilhamento

Você pode clonar um compartilhamento para um computador no domínio gerenciado ou na subárvore gerenciada. Ao clonar um compartilhamento, você pode criar rapidamente compartilhamentos com base em outros compartilhamentos com propriedades semelhantes. Essa flexibilidade permite impor configurações consistentes para todos os compartilhamentos que você cria em um determinado domínio.

Quando você clona um compartilhamento, o DRA preenche o Assistente de Clonagem de Compartilhamentos com valores do compartilhamento selecionado. Você também pode modificar propriedades para o novo compartilhamento.

Apagar um compartilhamento

Você pode apagar compartilhamentos de computadores no domínio gerenciado ou na subárvore gerenciada.

Gerenciando usuários conectados

Uma sessão é estabelecida sempre que um usuário se conecta a um recurso específico em um computador remoto. Um usuário conectado é um usuário conectado a um recurso compartilhado na rede.

O DRA gerencia os usuários conectados somente nos computadores nos domínios gerenciados. A conta de acesso deve ter permissões de administrador, como membro do grupo Administradores local, em todos os computadores em que você deseja gerenciar usuários conectados. Para atribuir essas permissões, adicione a conta de acesso ao grupo de administradores de domínio nativo no domínio do computador.

Desconectar um usuário

Você pode desconectar um usuário conectado de um computador no domínio gerenciado ou na subárvore gerenciada. Você deve poder acessar o computador e esta sessão aberta. Desconectar um usuário conectado encerra a sessão aberta.

Atualizar a lista de usuários conectados

Para garantir a visualização das informações mais recentes sobre sessões abertas em um computador, atualize manualmente a lista de usuários conectados. Você deve poder acessar o computador e esta sessão aberta.

Gerenciando dispositivos

Um dispositivo é qualquer equipamento conectado a uma rede, como um computador, uma impressora, um modem ou qualquer outro equipamento periférico.

Embora um dispositivo possa estar instalado em seu computador, o Windows não pode reconhecê-lo até que você instale e configure o driver apropriado. Um driver do dispositivo permite que uma peça específica de hardware se comunique com o sistema operacional.

O DRA permite configurar e gerenciar os dispositivos somente nos computadores nos domínios gerenciados. A conta de acesso deve ter permissões de administrador, como membro do grupo Administradores local, em todos os computadores em que você deseja gerenciar dispositivos. Para atribuir essas permissões, adicione a conta de acesso ao grupo de administradores de domínio nativo no domínio do computador.

Gerenciar propriedades de dispositivo

Você pode modificar as propriedades de um dispositivo em um computador específico. Modificar as propriedades de dispositivo para um dispositivo permite modificar o tipo de inicialização de um dispositivo.

Iniciar um dispositivo

Você pode iniciar um dispositivo em um computador específico no domínio gerenciado ou na subárvore gerenciada.

Parar um dispositivo

Você pode parar um dispositivo em um computador específico no domínio gerenciado ou na subárvore gerenciada.

Gerenciando registros de eventos

Um evento é uma importante ocorrência de sistema ou de aplicativo. O sistema operacional Windows registra informações sobre eventos em arquivos de registro de eventos. Pode haver vários registros de eventos armazenados em cada computador. Use o Windows Event Viewer nativo para exibir registros de eventos. O DRA gerencia os registros de eventos somente nos computadores nos domínios gerenciados.

O DRA registra as operações iniciadas pelo usuário no arquivo de registro, um repositório seguro. Você tem a opção de fazer com que o DRA também registre operações iniciadas pelo usuário no registro de eventos do Windows, além de registrar as informações no arquivo de registro do DRA. Para obter mais informações, consulte [Compreendendo datas e horários](#).

Tipos de registro de eventos

Computadores que executam o Microsoft Windows registram informações adicionais em vários registros. Os registros são descritos resumidamente da seguinte forma:

Tipo de registro	Descrição
ADAM	Registra eventos registrados pelo repositório do ADAM.
Aplicativo	Registra eventos registrados por um aplicativo no computador, como uma inicialização ou falha de serviço. Por exemplo, o DRA armazena eventos no registro do aplicativo.
Serviço de diretório	Registra eventos relacionados aos controladores de domínio que mantêm o banco de dados de segurança.
Serviço de replicação de arquivos	Registra eventos relacionados aos serviços de replicação de arquivos fornecidos pelo sistema operacional.
Segurança	Registra eventos que incluem tentativas de logon, acesso a arquivos e diretórios e mudanças na política de segurança com base nas opções de política de auditoria.
Sistema	Registra eventos registrados pelos componentes do sistema Windows, como a falha de um driver ou serviços iniciando e parando.

Tarefas de gerenciamento de registros de eventos

Quando você instala o DRA, os eventos de auditoria não são registrados no registro de eventos do Windows por padrão. Você pode habilitar esse tipo de registro, modificando uma chave do Registro.

Aviso: Tenha cuidado ao editar seu Registro do Windows. Se houver um erro no seu Registro, seu computador poderá se tornar não funcional. Se ocorrer um erro, você poderá restaurar o Registro para o estado em que ele estava da última vez em que o computador foi iniciado com êxito. Para obter mais informações, consulte a Ajuda do Windows Registry Editor.

Você pode especificar o tamanho máximo de um arquivo de registro de eventos e o que acontece com um registro de eventos quando ele fica cheio. A janela de propriedades exibe também o nome do registro, o caminho e o nome do arquivo de registro, quando ele foi criado, modificado pela última vez e acessado pela última vez. Se você optar por fazer backup do arquivo de registro, o DRA gravará o registro de eventos com um nome de arquivo exclusivo em um local padrão no computador selecionado.

O DRA permite gerenciar registros de eventos enquanto gerencia outros recursos para esse computador. Com as capacidades adequadas, você pode executar várias tarefas, como mudar as propriedades do registro de eventos.

Gerenciar propriedades do registro de eventos

Você pode modificar propriedades do registro de eventos para um computador específico.

Ver entradas do registro de eventos

Você pode ver entradas em um registro de eventos específico para um computador no domínio gerenciado ou na subárvore gerenciada. No Console de Delegação e Configuração, você pode ver o arquivo de registro de eventos no Visualizador de Eventos nativo do Windows.

Limpar o registro de eventos

Você pode limpar entradas em um registro de eventos específico para um computador no domínio gerenciado ou na subárvore gerenciada. Você também pode gravar as entradas do registro de eventos antes de limpar o log.

Gerenciando arquivos abertos

Um arquivo aberto é uma conexão para recursos compartilhados, como arquivos ou pipes. Um pipe é um mecanismo de comunicação entre processos que permite que um processo se comunique com outro processo local ou remoto.

O DRA gerencia arquivos abertos somente em computadores no domínio gerenciado e na subárvore gerenciada. Como os arquivos abertos estão associados a um computador, você pode gerenciá-los enquanto gerencia outros recursos para esse computador. Por exemplo, você pode querer fechar arquivos abertos ao encerrar um sistema ou instalar um novo dispositivo ou serviço. Você também pode monitorar quais arquivos os usuários acessam com mais frequência, ajudando a avaliar melhor a segurança dos arquivos.

Observação: Você só pode gerenciar arquivos abertos por meio do Console de Delegação e Configuração.

Fechar um arquivo

Você pode fechar arquivos abertos de recursos na rede. É uma boa ideia notificar os usuários quando você pretende fechar arquivos abertos. Eles podem precisar de tempo para gravar seus dados. Para fechar um arquivo aberto, você deve poder acessar o computador correspondente.

Atualizar a lista de arquivos abertos

Para garantir a visualização das informações mais recentes sobre sessões abertas em um computador, atualize manualmente a lista de usuários conectados. Para atualizar a lista de arquivos abertos, você deve poder acessar o computador correspondente.

8

Gerenciando a Lixeira

A Lixeira fornece uma rede de segurança, permitindo apagar contas do usuário, grupos, contatos e contas de computador temporariamente. Você pode restaurar esses objetos ao estado original com todos os dados, como SIDs, ACLs e associações de grupo intactos ou apagar permanentemente esses objetos. Essa flexibilidade oferece uma maneira mais segura de gerenciar contas do usuário, grupos, contatos e contas de computador. Use a opção de pesquisa para pesquisar objetos necessários. Para obter informações, veja [Pesquisando objetos](#).

Restaurar um objeto da Lixeira

Você pode restaurar objetos apagados de volta aos contêineres dos quais você os apagou. O DRA restaura esses objetos para seu estado original com todos os dados, como SIDs, ACLs e participações de grupos, intactos. Um objeto pode ser uma conta do usuário, um grupo, um contato, um grupo dinâmico, uma caixa de correio de recursos, um grupo dinâmico de distribuição ou uma conta de computador.

Restaurar todos os objetos

Você pode restaurar todos os objetos da Lixeira de um domínio gerenciado. Você pode restaurar objetos da Lixeira de um domínio específico ou em todos os domínios gerenciados. Para restaurar objetos de uma Lixeira de um domínio específico, a Lixeira deve estar habilitada para esse domínio.

Apagar um objeto da Lixeira

Você pode apagar permanentemente todos os objetos da Lixeira de um domínio gerenciado. Após apagar um objeto da Lixeira, você não poderá restaurar o objeto. Um objeto pode ser uma conta do usuário, um grupo, um contato, um grupo dinâmico, uma caixa de correio de recursos, um grupo dinâmico de distribuição ou uma conta de computador.

Esvaziar a Lixeira

Você pode esvaziar a Lixeira de um domínio gerenciado. Esvaziar a Lixeira apaga permanentemente todos os objetos atualmente nela. Você pode esvaziar a Lixeira de um domínio específico ou em todos os domínios gerenciados. Para esvaziar uma Lixeira de um domínio específico, a Lixeira deve estar habilitada para esse domínio. Após esvaziar a Lixeira, não será possível restaurar os objetos apagados.