NetIQ Directory and Resource Administrator

Guia do Administrador

Junho de 2021

Aviso legal

Índice

Sobre este guia

O *Guia do Administrador* fornece informações conceituais sobre o produto NetIQ Directory and Resource Administrator (DRA). Este livro define a terminologia e vários conceitos relacionados. Ele também fornece orientação passo a passo para muitas tarefas operacionais e de configuração.

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 a versão mais recente deste guia e outros recursos de documentação do DRA, visite o site na Web da Documentação do DRA (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/.

Introdução

Antes de instalar e configurar todos os componentes do NetIQ Directory and Resource Administrator (DRA), você deve compreender os princípios básicos do que o DRA fará por sua empresa e a função dos componentes do DRA na arquitetura do produto.

1 O que é o Directory and Resource Administrator

O NetIQ Directory and Resource Administrator (DRA) 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 políticas 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 Microsoft Active Directory, do Windows, do Exchange e do Azure Active Directory.

- **Suporte para Azure e Active Directory local, Exchange e Skype for Business:** Fornece 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 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 aprovisionamento e desaproviosamento, 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.

2 Compreendendo os componentes do Directory and Resource Administrator

Os componentes do DRA que você usará de modo consistente para gerenciar o acesso privilegiado incluem os servidores principal e secundário, os consoles do administrador, os componentes do gerador de relatórios e o Workflow Automation Engine 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	Configuração de DRA Reporting Center (NRC) PowerShell *(opcional)* CLI *(opcional)* Provedor ADSI do DRA *(opcional)*	Qualquer servidor do DRA
Administrador ocasional do suporte técnico	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 auditora 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.

Console de Delegação e Configuração

O Console de Delegação e Configuração é uma interface do usuário instalável que fornece acesso de administradores do sistema a funções de administração e configuração do DRA.

- **Delegation Management (Gerenciamento de Delegação):** Permite que você especifique e atribua de modo granular acesso a recursos e tarefas gerenciados a administradores assistentes.
- **Gerenciamento de Política e de Automação:** Permite a você definir e assegurar o uso obrigatório de políticas para garantir a conformidade com os padrões e as convenções do ambiente.
- **Configuration Management (Gerenciamento de Configurações):** Permite a você atualizar as opções e configurações do sistema do DRA, adicionar personalizações e configurar serviços gerenciados (Active Directory, Exchange, Azure Active Directory etc.).
- **Account and Resource Management: (Gerenciamento de Recursos e de Contas):** Permite que administradores assistentes do DRA vejam e gerenciem objetos delegados de serviços e domínios conectados do Console de Delegação e Configuração.

Console da Web

O console da Web é uma interface do usuário baseada na web que fornece acesso rápido e fácil para Administradores Assistentes verem e gerenciarem objetos delegados de serviços e domínios conectados. Os administradores podem personalizar a aparência e o uso do console da Web para incluir marcas corporativas personalizadas e propriedades personalizadas de objetos.

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:

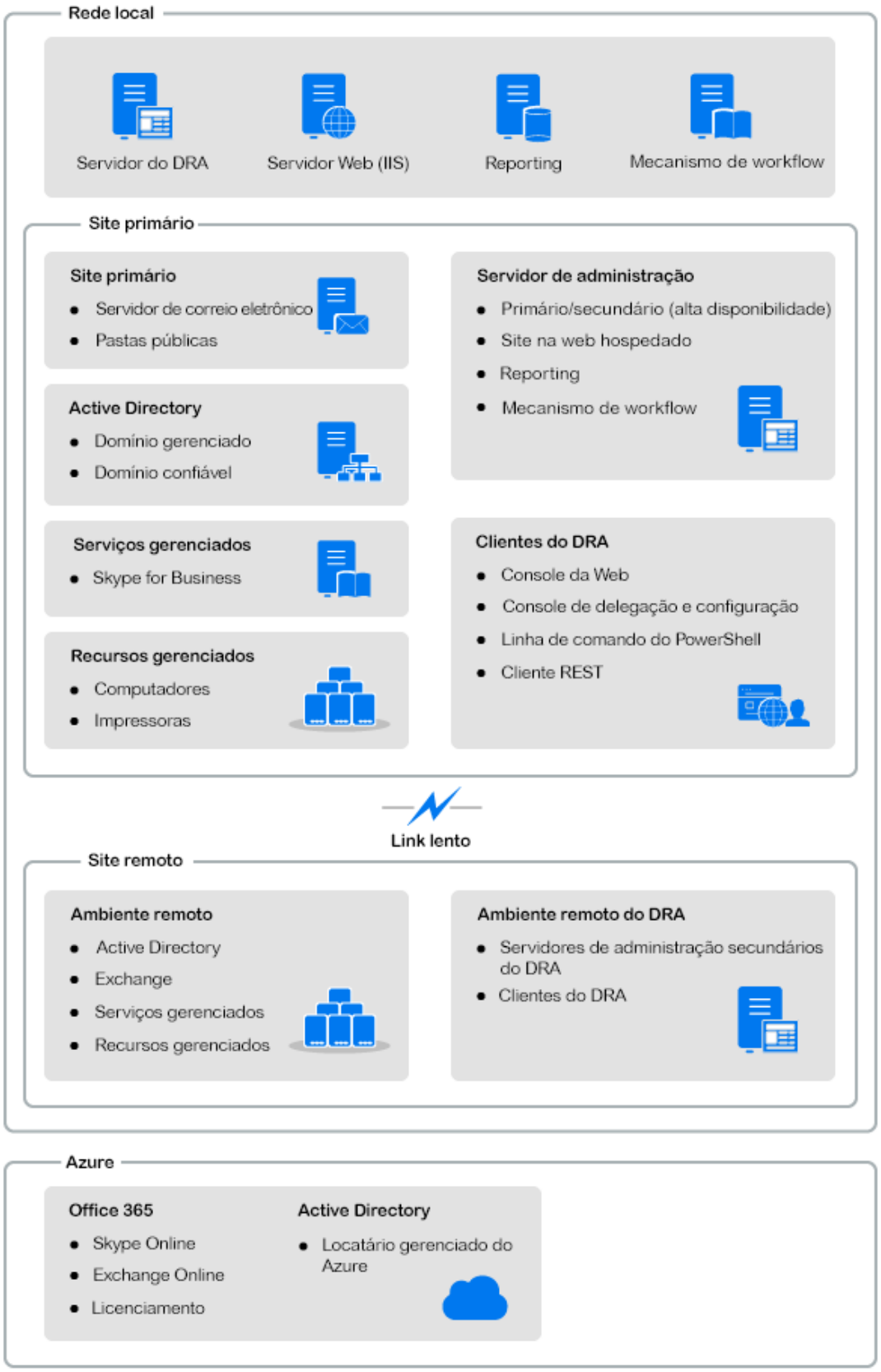
- Relatórios de recursos para objetos do Active Directory
- Relatórios de dados de objeto do Active Directory
- Relatórios de resumo do Active Directory
- Relatórios de configuração do DRA
- Relatórios de configuração do Exchange
- Relatórios do Exchange Online do Office 365
- Relatórios de tendências 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.

Workflow Automation Engine

O DRA integra-se ao Workflow Automation Engine 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 Workflow Automation Engine, consulte o site da Documentação do DRA.

Arquitetura do produto



II Instalação e upgrade do produto

Este capítulo detalha o hardware, o software e os requisitos de conta recomendados exigidos pelo Directory and Resource Administrator. Ele então guia você pelo processo de instalação com uma lista de verificação para cada componente da instalação.

3 Planejando sua implantação

Conforme você planeja a implantação do Directory and Resource Administrator, use esta seção para avaliar seu ambiente de hardware e de software para compatibilidade e para anotar as portas e os protocolos necessários que você precisará configurar para a implantação.

Recomendações de recurso testadas

Esta seção fornece informações de dimensionamento para nossa recomendação de recurso básico. Os resultados podem variar de acordo com o hardware disponível, o ambiente específico e o tipo específico de dados processados, entre outros fatores. É provável que existam configurações de hardware maiores e mais potentes, capazes de lidar com uma carga mais pesada. Se você tiver perguntas, consulte os Serviços de Consultoria da NetIQ.

Executado em um ambiente com aproximadamente um milhão de objetos do Active Directory:

Componente	CPU	Memória	Armazenamento
Servidor de administração DRA	8 núcleos de CPU de 2,0 GHz	16 GB	120 GB
Console da Web do DRA	2 núcleos de CPU de 2,0 GHz	8 GB	100 GB
DRA Reporting	4 núcleos de CPU de 2,0 GHz	16 GB	100 GB
Servidor de workflow do DRA	4 núcleos de CPU de 2,0 GHz	16 GB	120 GB

Aprovisionamento de recursos de ambiente virtual

O DRA mantém segmentos de memória grandes ativos por períodos prolongados. Ao aprovisionar recursos para um ambiente virtual, as seguintes recomendações devem ser consideradas:

- Alocar o armazenamento como "Thick Provisioned"

- Definir a reserva de memória para Reservar Toda a Memória de Convidado (Toda Bloqueada)
- Verifique se o arquivo de paginação é suficientemente grande para cobrir a realocação da possível memória inchada na camada virtual

Portas e protocolos necessários

As portas e os protocolos para comunicação com o DRA são fornecidos nesta seção.

- As portas configuráveis são indicadas com um asterisco *
- As portas que requerem um certificado são indicadas com dois asteriscos **

Tabelas de componentes:

- "Servidores de administração DRA" na página 24
- "Servidor REST do DRA" na página 26
- "Console da Web (IIS)" na página 26
- "Console de administração e delegação do DRA" na página 27
- "Servidor de workflow" na página 27

Servidores de administração DRA

Protocolo e porta	Direção	Destino	Uso
TCP 135	Bidirecional	Servidores de administração DRA	Mapeador de endpoint, um requisito básico para comunicação com o DRA; habilita servidores de Administração a localizarem uns aos outros em MMS
TCP 445	Bidirecional	Servidores de administração DRA	Replicação de modelo de delegação; replicação de arquivo durante a sincronização de MMS (SMB)
Faixa de portas TCP dinâmicas *	Bidirecional	Controladores de domínio do Microsoft Active Directory	Por padrão, o DRA atribui portas dinamicamente da faixa de portas TCP de 1024 a 65535. No entanto, você pode configurar essa faixa usando serviços de componente. Para obter mais informações, veja *Using Distributed COM with Firewalls* (Usando COM distribuído com firewalls).
TCP 50000 *	Bidirecional	Servidores de administração DRA	Replicação de atributos e comunicação entre o AD LDS e o servidor do DRA. (LDAP)
TCP 50001 *	Bidirecional	Servidores de administração DRA	Replicação de atributo do SSL (AD LDS)

Protocolo e porta	Direção	Destino	Uso
TCP/UDP 389	Saída	Controladores de domínio do Microsoft Active Directory	Gerenciamento de objetos do Active Directory (LDAP)
	Saída	Microsoft Exchange Server	Gerenciamento de caixa de correio (LDAP)
TCP/UDP 53	Saída	Controladores de domínio do Microsoft Active Directory	Resolução de nome
TCP/UDP 88	Saída	Controladores de domínio do Microsoft Active Directory	Permite autenticação do servidor do DRA para os controladores de domínio (Kerberos)
TCP 80	Saída	Microsoft Exchange Server	Necessário para todos os servidores locais do Exchange 2013 e posteriores (HTTP)
	Saída	Microsoft Office 365	Acesso remoto ao PowerShell (HTTP)
TCP 443	Saída	Microsoft Office 365, Change Guardian	Acesso à API (Application Programming Interface) e integração do Change Guardian (HTTPS)
TCP 443, 5986, 5985	Saída	Microsoft PowerShell	Cmdlets nativos do PowerShell (HTTPS) e comunicação remota com o PowerShell
TCP 5984	Host local	Servidores de administração DRA	Acesso IIS ao Serviço de Replicação para suportar designações temporárias de grupos
TCP 8092 * **	Saída	Servidor de workflow	Status e acionamento de workflow (HTTPS)
TCP 50101 *	Entrada	Cliente DRA	Clique o botão direito do mouse no relatório de histórico de mudanças para o relatório de auditoria da interface do usuário. Pode ser configurado durante a instalação.
TCP 8989	Host local	Serviço de arquivo de registro	Comunicação com o arquivo de registro (não precisa ser aberto por meio do firewall)
TCP 50102	Bidirecional	Serviço básico do DRA	Serviço de arquivo de registro
TCP 50103	Host local	Serviço de cache do DRA	Comunicação do serviço de cache no servidor do DRA (não precisa ser aberto por meio do firewall)
TCP 1433	Saída	Microsoft SQL Server	Coleta de dados do gerador de relatórios
UDP 1434	Saída	Microsoft SQL Server	O serviço de browser do SQL Server usa essa porta para identificar a porta para a instância nomeada.
TCP 8443	Bidirecional	Servidor do Change Guardian	Histórico de mudanças unificado

Protocolo e porta	Direção	Destino	Uso
TCP 8898	Bidirecional	Servidores de administração DRA	Comunicação do Serviço de Replicação do DRA entre servidores do DRA para designações temporárias de grupos
TCP 636	Saída	Controladores de domínio do Microsoft Active Directory	Gerenciamento de objetos do Active Directory (LDAP SSL).

Servidor REST do DRA

Protocolo e porta	Direção	Destino	Uso
TCP 8755 * **	Entrada	Servidor IIS, cmdlets do PowerShell do DRA	Executar atividades de workflow baseadas em REST do DRA (ActivityBroker)
TCP 135	Saída	Controladores de domínio do Microsoft Active Directory	Descoberta automática usando o Ponto de Conexão do Serviço (SCP)
TCP 443	Saída	Controladores de domínio do Microsoft AD	Descoberta automática usando o Ponto de Conexão do Serviço (SCP)

Console da Web (IIS)

Protocolo e porta	Direção	Destino	Uso
TCP 8755 * **	Saída	Serviço REST do DRA	Para comunicação entre o Console da Web do DRA e o PowerShell do DRA
TCP 443	Entrada	Browser do cliente	Abrindo um site na web do DRA
TCP 443 **	Saída	Servidor de Advanced Authentication	Advanced Authentication

Console de administração e delegação do DRA

Protocolo e porta	Direção	Destino	Uso
TCP 135	Saída	Controladores de domínio do Microsoft Active Directory	Descoberta automática usando SCP
Faixa de portas TCP dinâmicas *	Saída	Servidores de administração DRA	Atividades de workflow do adaptador do DRA. Por padrão, o DCOM atribui portas dinamicamente da faixa de portas TCP de 1024 a 65535. No entanto, você pode configurar essa faixa usando serviços de componente. Para obter mais informações, veja *Usando COM distribuído com firewalls* (DCOM)
TCP 50102	Saída	Serviço básico do DRA	Geração de relatórios do histórico de mudanças

Servidor de workflow

Protocolo e porta	Direção	Destino	Uso
TCP 8755	Saída	Servidores de administração DRA	Executar atividades de workflow baseadas em REST do DRA (ActivityBroker)
Faixa de portas TCP dinâmicas *	Saída	Servidores de administração DRA	Atividades de workflow do adaptador do DRA. Por padrão, o DCOM atribui portas dinamicamente da faixa de portas TCP de 1024 a 65535. No entanto, você pode configurar essa faixa usando serviços de componente. Para obter mais informações, veja *Usando COM distribuído com firewalls* (DCOM)
TCP 1433	Saída	Microsoft SQL Server	Armazenamento de dados de workflow
TCP 8091	Entrada	Operations Console (Console de operações) e Configuration Console (Console de configuração)	API (Application Programming Interface) de BSL do workflow (TCP)
TCP 8092 **	Entrada	Servidores de administração DRA	API (Application Programming Interface) de BSL do workflow (HTTP) e (HTTPS)
TCP 2219	Host local	Provedor de Namespace	Usado pelo Provedor de Namespace para executar adaptadores

Protocolo e porta	Direção	Destino	Uso
TCP 9900	Host local	Correlation Engine	Usado pelo Correlation Engine para comunicar-se com o Workflow Automation Engine e o Provedor de Namespace
TCP 10117	Host local	Provedor de namespace do Resource Management (gerenciamento de recursos)	Usado pelo Provedor de namespace do gerenciamento de recursos

Plataformas suportadas

Para obter as informações mais recentes sobre as plataformas de software suportadas, consulte a página do produto Directory and Resource Administrator.

Sistema Gerenciado	Pré-requisitos
Azure Active Directory	Para habilitar a administração do Azure, você deve instalar os seguintes módulos do PowerShell: ◆ Azure Active Directory V2 (AzureAD) versão 2.0.2.4 ou posterior ◆ AzureRM.Profile versão 5.8.2 ou posterior ◆ PowerShell do Exchange Online V2 1.0.1 ou posterior O PowerShell 5.1 ou o módulo mais recente é necessário para instalar os novos módulos do Azure PowerShell.
Active Directory	◆ Microsoft Server 2012 R2 ◆ Microsoft Server 2016 ◆ Microsoft Windows Server 2019
Microsoft Exchange	◆ Microsoft Exchange 2013 ◆ Microsoft Exchange 2016 ◆ Microsoft Exchange 2019
Microsoft Office 365	◆ Microsoft Exchange Online
Skype for Business	◆ Microsoft Skype for Business 2015
Histórico de mudanças	◆ Change Guardian 5.1 ou posterior
Bancos de Dados	◆ Microsoft SQL Server 2016
Browsers da Web	◆ Google Chrome ◆ Mozilla Firefox ◆ Microsoft Edge

Sistema Gerenciado	Pré-requisitos
Workflow Automation	◆ Microsoft Server 2012 R2 ◆ Microsoft Server 2016 ◆ Microsoft Server 2019

Requisitos do Servidor de Administração e do Console da Web do DRA

Os componentes do DRA têm os seguintes requisitos de contas e software:

- “Requisitos de software” na página 29
- “Domínio do servidor” na página 31
- “Requisitos da conta” na página 31
- “Contas de acesso do DRA com privilégios mínimos” na página 33

Requisitos de software

Componente	Pré-requisitos
Destino de Instalação	**Sistema operacional do Servidor de Administração da NetIQ:**
Sistema Operacional	◆ Microsoft Windows Server 2012 R2, 2016, 2019 **Observação:** O servidor também deve ser um membro de um domínio local suportado do Microsoft Active Directory.
	Interfaces do DRA:
	◆ Microsoft Windows Server 2012 R2, 2016, 2019
Instalador	◆ Microsoft .NET Framework 4.8 e superior

Componente	Pré-requisitos
Servidor de Administração	**Directory and Resource Administrator:** ◆ Microsoft .NET Framework 4.8 e superior ◆ Pacotes Redistribuíveis (x64 e x86) do Microsoft Visual C++ 2015-2019 ◆ Enfileiramento de Mensagens da Microsoft ◆ Funções do Microsoft Active Directory Lightweight Directory Services ◆ Serviço de Registro Remoto iniciado ◆ Módulo de regravação de URL dos Serviços de Informações da Internet da Microsoft ◆ Roteamento de solicitações de aplicativo dos Serviços de Informações da Internet da Microsoft **Observação:** O NetIQ DRA REST Service é instalado com o Servidor de Administração. **Administração do Microsoft Office 365/Exchange Online:** ◆ Módulo do Microsoft Azure Active Directory para o Windows PowerShell ◆ Módulo de PowerShell do Windows ◆ Módulo do PowerShell do Exchange Online V2 ◆ Habilite o WinRM para autenticação básica no lado do cliente para tarefas do Exchange Online. Para obter mais informações, veja Plataformas suportadas.
Interface do Usuário	**Interfaces do DRA:** ◆ Microsoft .NET Framework 4.8 ◆ Pacotes Redistribuíveis (x64 e x86) do Microsoft Visual C++ 2015-2019
Extensões do PowerShell	◆ Microsoft .NET Framework 4.8 ◆ PowerShell 5.1 ou posterior
Console da Web do DRA	**Servidor Web:** ◆ Microsoft .NET Framework 4.x > Serviços WCF > Ativação HTTP ◆ Microsoft Internet Information Server 8.0, 8.5, 10 ◆ Módulo de regravação de URL dos Serviços de Informações da Internet da Microsoft ◆ Roteamento de solicitações de aplicativo dos Serviços de Informações da Internet da Microsoft

Domínio do servidor

Componente	Sistemas operacionais
Servidor do DRA	◆ Microsoft Windows Server 2019 ◆ Microsoft Windows Server 2016 ◆ Microsoft Windows Server 2012 R2

Requisitos da conta

Conta	Descrição	Permissões
Grupo AD LDS	A conta do serviço DRA precisa ser adicionada a este grupo para acesso ao AD LDS	◆ Grupo de segurança local do domínio

Conta	Descrição	Permissões

Conta de serviço do DRA	As permissões necessárias para executar o Serviço de Administração da NetIQ	◆ Para permissões para “Usuários de COM Distribuído”
		◆ Membro do Grupo de Admin do AD LDS
		◆ Grupo de operadores de conta
		◆ Grupos de arquivos de registro (OnePointOp ConfgAdms e OnePointOp)
		◆ Uma das seguintes opções, encontradas na guia Conta > **Opções de conta**, deverá ser selecionada para o usuário da conta do serviço DRA se a instalação do DRA em um servidor for feita usando a metodologia STIG:
		  ◆ Criptografia Kerberos AES de 128 bits
		  ◆ Criptografia Kerberos AES de 256 bits
		Observação
		◆ Para obter mais informações sobre como configurar contas de acesso a domínio com privilégios mínimos, veja: Contas de acesso do DRA com privilégios mínimos.
		◆ Para obter mais informações sobre como configurar uma Conta de Serviço Gerenciado do grupo para o DRA, veja: “Configuring DRA Services for a Group Managed Service Account” (Configurando Serviços do DRA para uma conta de Serviço Gerenciado do Grupo) no *DRA Administrator Guide* (Guia do Administrador do DRA).

Administrador do DRA	Conta do usuário ou grupo provisionado na função incorporada de administrador do DRA	◆ Grupo de segurança local do domínio ou conta do usuário do domínio ◆ Membro do domínio gerenciado ou um domínio confiável ◆ Se você especificar uma conta de um domínio confiável, verifique se o computador do servidor de Administração pode autenticá-la.

Conta	Descrição	Permissões
Contas de Admin Assistente do DRA	Contas às quais serão delegados poderes via DRA	◆ Adicione todas as contas de Admin Assistente do DRA ao grupo “Usuários de COM Distribuído” de modo que elas possam se conectar ao Servidor do DRA por meio de clientes remotos. Isso é necessário somente quando você está usando o thick client ou o Console de Delegação e Configuração. **Observação:** O DRA pode ser configurado para gerenciar isso para você durante a instalação.

Contas de acesso do DRA com privilégios mínimos

Abaixo estão as permissões e privilégios necessários para as contas especificadas e os comandos de configuração que você precisa executar.

Conta de acesso a domínio: Ao utilizar o Editor ADSI, conceda à conta de Acesso ao Domínio as seguintes Permissões do Active Directory no nível de domínio superior para os seguintes tipos de objeto descendentes:

- Controle TOTAL sobre objetos builtInDomain
- Controle TOTAL sobre objetos Computador
- Controle TOTAL sobre objetos Ponto de Conexão
- Controle TOTAL sobre objetos de Contato
- Controle TOTAL sobre objetos de Container
- Controle TOTAL sobre objetos Grupo
- Controle TOTAL sobre objetos InetOrgPerson
- Controle TOTAL sobre objetos MsExchDynamicDistributionList
- Controle TOTAL sobre objetos MsExchSystemObjectsContainer
- Controle TOTAL sobre objetos msDS-GroupManagedServiceAccount
- Controle TOTAL sobre objetos Unidade Organizacional
- Controle TOTAL sobre objetos Impressora
- Controle TOTAL sobre objetos publicFolder
- Controle TOTAL sobre objetos Pasta Compartilhada
- Controle TOTAL sobre objetos Usuário

Conceda à conta de Acesso ao Domínio as seguintes permissões do Active Directory no nível de domínio superior para este objeto e todos os objetos descendentes:

- Permitir a criação de objetos Computador
- Permitir a criação de objetos Contato
- Permitir a criação de objetos Container

- Permitir a criação de objetos Grupo
- Permitir a criação de objetos MsExchDynamicDistributionList
- Permitir a criação de objetos msDS-GroupManagedServiceAccount
- Permitir a criação de objetos Unidade Organizacional
- Permitir a criação de objetos publicFolders
- Permitir a criação de objetos Pasta Compartilhada
- Permitir a criação de objetos Usuário
- Permitir o apagamento de objetos Computador
- Permitir o apagamento de objetos Contato
- Permitir o apagamento de Container
- Permitir o apagamento de objetos Grupo
- Permitir o apagamento de objetos InetOrgPerson
- Permitir o apagamento de objetos MsExchDynamicDistributionList
- Permitir o apagamento de objetos msDS-GroupManagedServiceAccount
- Permitir o apagamento de objetos Unidade Organizacional
- Permitir o apagamento de objetos publicFolders
- Permitir o apagamento de objetos Pasta Compartilhada
- Permitir o apagamento de objetos Usuário

Observação

- Por padrão, alguns objetos container Incorporados do Active Directory não herdam permissões do nível superior do domínio. Por esse motivo, tais objetos exigirão que a herança esteja habilitada ou que permissões explícitas sejam definidas.
- Caso você use a conta de menor privilégio como a conta de acesso, verifique se a conta recebeu a permissão “Redefinir Senha” para si mesma no Active Directory para que a redefinição de senha seja bem-sucedida no DRA.

Conta de Acesso ao Exchange: Para gerenciar objetos locais do Microsoft Exchange, designe a função de Gerenciamento Organizacional à Conta de Acesso ao Exchange e a Conta de Acesso ao Exchange ao grupo de Operadores de Conta.

Conta de Acesso ao Skype: Verifique se essa conta é um usuário habilitado para o Skype e que é um membro de pelo menos uma das seguintes opções:

- Função CSAdministrator
- Ambas as funções CSUserAdministrator e CSArchiving

Conta de Acesso à Pasta Pública: Atribua as permissões do Active Directory a seguir à conta de acesso à pasta pública:

- Gerenciamento de Pasta Pública
- Pastas Públicas Habilitadas para E-mail

Conta de Acesso de Locatário do Azure: Designe as permissões do Azure Active Directory a seguir à Conta de Acesso de Locatário do Azure:

- Grupos de Distribuição
- Destinatários de Correio
- Criação de Destinatário de Correio
- Criação e Participação em Grupo de Segurança
- (Opcional) Administrador do Skype for Business

  Se você quiser gerenciar o Skype for Business Online, designe poderes de administrador do Skype for Business à conta de acesso de locatário do Azure.
- Administrador de Usuários

Permissões de Conta de Serviço de Administração da NetIQ:

- Administradores Locais
- Conceda à conta de anulação de menor privilégio “Permissão Total” para pastas de compartilhamento ou pastas DFS em que Diretórios pessoais são provisionados.
- **Gerenciamento de Recursos**: Para gerenciar recursos publicados em um domínio gerenciado do Active Directory, é necessário conceder permissões de administração local desses recursos à conta de Acesso do Domínio.

Após a instalação do DRA: Você deve executar os seguintes comandos antes de gerenciar os domínios necessários:

- Para delegar a permissão para o “Container de Objetos Apagados” da pasta Instalação do DRA (observação: o comando deve ser executado por um administrador do domínio):

  `DraDelObjsUtil.exe /domain:<nome_do_domínio_netbios> /delegate:<nome_da_conta>`
- Para delegar permissão para a “OU NetIQReceyleBin” da pasta de Instalação do DRA:

  `DraRecycleBinUtil.exe /domain:<nome_do_domínio_netbios> /delegate:<nome_da_conta>`

Acesso remoto ao SAM: Designe os Controladores de Domínio ou servidores membros gerenciados pelo DRA para habilitar as contas listadas na configuração de GPO abaixo, de modo que elas possam fazer consultas remotas ao banco de dados do SAM (Security Account Manager – Gerenciador de Contas de Segurança). A configuração precisa incluir a conta do serviço DRA.

Acesso à rede: Restringir os clientes com permissão de fazer chamadas remotas ao SAM

Para acessar essa configuração, faça o seguinte:

1. Abra o console de Gerenciamento de Políticas de Grupo no controlador de domínio.
2. Expanda **Domínios** > **[controlador de domínio]** > **Objetos Política de Grupo** na árvore de nós.
3. Clique o botão direito do mouse em **Política de Controladores de Domínio Padrão** e selecione **Editar** para abrir o editor de GPO para essa política.
4. Expanda **Configuração do Computador** > **Políticas** > **Configurações do Windows** > **Configurações de Segurança** > **Políticas Locais** na árvore de nós do editor de GPO.
5. Clique duas vezes em **Acesso à rede: Restringir os clientes com permissão de fazer chamadas remotas ao SAM** no painel de políticas e selecione **Definir esta configuração de política**.

6 Clique em **Editar Segurança** e habilite **Permitir** para o Acesso Remoto. Adicione uma conta do serviço DRA se ela ainda não estiver incluída como um usuário ou como parte do grupo de administradores.

7 Aplique as mudanças. Isso adicionará o descritor de segurança, `O:BAG:BAD:(A;;RC;;;BA)`, às configurações da política.

Para obter mais informações, consulte o artigo 7023292 da Base de Conhecimento.

Requisitos do gerador de relatórios

Os requisitos para o DRA Reporting incluem os seguintes:

Requisitos de software

Componente	Pré-requisitos
Destino de Instalação	**Sistema Operacional:** ◆ Microsoft Windows Server 2012 R2, 2016, 2019

Componente	Pré-requisitos
NetIQ Reporting Center (v3.3)	**Banco de dados:** ◆ Microsoft SQL Server 2016 ◆ Microsoft SQL Server Reporting Services ◆ O administrador de domínio que gerencia tarefas do Agente SQL requer permissões de segurança para o Microsoft SQL Server Integration Services, ou alguns relatórios NRC podem não ser processados. **Servidor Web:** ◆ Microsoft Internet Information Server 8.0, 8.5, 10 ◆ Componentes do Microsoft IIS: ◆ ASP .NET 4.0 **Microsoft .NET Framework 3.5:** ◆ Requerido para executar o instalador do NRC ◆ Também requerido no Servidor Principal do DRA para a configuração do DRA Reporting Services **Observação:** Ao instalar o NetIQ Reporting Center (NRC) em um computador com SQL Server, o .NET Framework 3.5 pode exigir uma instalação manual antes de instalar o NRC. **Protocolo de Segurança de Comunicação:** ◆ O SQL Server deve suportar o TLS 1.2. Para obter mais informações, consulte TLS 1.2 support for Microsoft SQL Server (Suporte para TLS 1.2 para Microsoft SQL Server). ◆ O SQL Server deve ter um driver com suporte ao TLS atualizado instalado no servidor DRA. O driver sugerido é o Microsoft® SQL Server® 2012 Native Client – QFE mais recente ◆ A mesma versão de protocolo TLS deve ser suportada no sistema operacional tanto do SQL Server quanto do Servidor de Administração do DRA. Por exemplo, apenas o TLS 1.2 foi habilitado.
DRA Reporting	**Banco de dados:** ◆ Microsoft SQL Server Integration Services ◆ Microsoft SQL Server Agent

Requisitos para licenciamento

Sua licença determina os produtos e recursos que você pode usar. O DRA requer que uma chave de licença esteja instalada com o Servidor de Administração.

Após instalar o servidor de Administração, use o Utilitário de Verificação de Saúde para instalar sua licença comprada. Uma chave de licença de avaliação (TrialLicense.lic) também está incluída no pacote de instalação que permite o gerenciamento de um número ilimitado de contas de usuário e caixas de correio por 30 dias.

Consulte o Contrato de Licença por Usuário Final (EULA) para obter informações adicionais sobre definição e restrições de licenças.

4 Instalação do produto

Este capítulo guia você pela instalação do Directory and Resource Administrator. Para obter mais informações sobre como planejar sua instalação ou upgrade, veja Planejando sua implantação.

Instalar o Servidor de administração DRA

Você pode instalar o Servidor de administração DRA como um nó primário e como um nó secundário em seu ambiente. Os requisitos para o servidor de administração principal e para o secundário são os mesmos; no entanto, toda implantação do DRA precisa incluir um servidor de administração principal.

O pacote do servidor do DRA tem os seguintes recursos:

- **Servidor de Administração:** Armazena dados de configuração (ambientais, de acesso delegado e de política), executa tarefas de operador e de automação e audita atividades em todo o sistema. Ele conta com estes recursos:
  - **Kit de Recursos de Arquivo de Registro:** Permite que você veja informações de auditoria.
  - **SDK do DRA:** Fornece os scripts de exemplo do ADSI e ajuda você a criar seus próprios scripts.
  - **Designações Temporárias de Grupos:** Fornece os componentes para habilitar a sincronização de Designações Temporárias de Grupos.
- **Interfaces do Usuário:** A interface do cliente da Web que é usada principalmente pelos administradores assistentes, mas também inclui opções de personalização.
  - **Provedor ADSI:** Permite que você crie seus próprios scripts de política.
  - **Interface de linha de comando:** Permite que você realize operações de DRA.
  - **Delegação e Configuração:** Permite que os administradores do sistema acessem as funções de administração e de configuração do DRA. Além disso, permite especificar e designar aos administradores assistentes, de modo granular, acesso a recursos e tarefas gerenciados.
  - **Extensões do PowerShell:** Fornece um módulo do PowerShell que permite a clientes não DRA solicitar operações do DRA usando cmdlets do PowerShell.
  - **Console da Web:** A interface do cliente da Web que é usada principalmente pelos administradores assistentes, mas também inclui opções de personalização.

Para obter informações sobre como instalar clientes de linha de comando e consoles do DRA específicos em vários computadores, consulte Install the DRA Clients (Instalar os Clientes do DRA).

Lista de Verificação de Instalação Interativa:

Etapa	Mais informações
Efetuar logon no servidor de destino	Efetue logon no servidor de destino do Microsoft Windows para a instalação com uma conta que tem privilégios administrativos locais.
Copie e execute o Kit de Instalação do Admin	Execute o kit de instalação do DRA (NetIQAdminInstallationKit.msi) para extrair a mídia de instalação do DRA para o sistema de arquivos local. **Observação:** O kit de instalação instalará o .NET Framework no servidor de destino, se necessário.
Instalar o DRA	Clique em **Install DRA** (Instalar o DRA) e em **Next** (Próximo) para ver as opções de instalação. **Observação:** Para executar a instalação posteriormente, navegue até o local em que a mídia de instalação foi extraída (veja o Kit de Instalação) e execute `Setup.exe`.
Instalação Padrão	Escolha os componentes a serem instalados e aceite o local de instalação padrão, `C:\Program Files (x86)\NetIQ\DRA` ou especifique um local alternativo para a instalação. Opções de componente: **Servidor de Administração** ◆ Kit de Recursos de Arquivo de Registro (Opcional) ◆ SDK do DRA ◆ Designações Temporárias de Grupos **Interfaces do Usuário** ◆ Provedor ADSI (Opcional) ◆ Interface de linha de comando (opcional) ◆ Delegação e Configuração ◆ Extensões do PowerShell ◆ Console da Web
Verificar pré-requisitos	A caixa de diálogo **Prerequisites List** (Lista de Pré-requisitos) exibirá a lista de softwares necessários com base nos componentes selecionados para a instalação. O instalador guiará você pela instalação de quaisquer pré-requisitos ausentes que sejam necessários para a instalação ser concluída com êxito.
Aceitar o contrato de licença EULA	Aceite os termos do Contrato de Licença por Usuário Final.
Especificar localização do registro	Especifique um local para o DRA armazenar todos os arquivos de registro. **Observação:** Os registros do Console de Delegação e Configuração e os registros do ADSI são armazenados na pasta do perfil do usuário.

Etapa	Mais informações
Selecione o modo de operação do servidor	Selecione **Primary Administration Server** (Servidor de Administração Principal) para instalar o Servidor de Administração do DRA em um conjunto com multimaster (haverá apenas um principal em uma implantação) ou **Secondary Administration Server** (Servidor de Administração Secundário) para ingressar um novo Servidor de Administração do DRA em um conjunto multimaster existente. Para obter informações sobre o conjunto multimaster, veja “Configuring the Multi-Master Set” (Configurando o conjunto multimaster) no *DRA Administrator Guide* (Guia do Administrador do DRA).
Especifique as contas de instalação e as credenciais	◆ Conta de serviço do DRA ◆ Grupo AD LDS ◆ Administrador do DRA Conta Para obter mais informações, veja: Requisitos do Servidor de Administração e do Console da Web do DRA.
Configurar permissões DCOM	Habilite o DRA para configurar o acesso “COM Distribuído” para usuários autenticados.
Configurar portas	Para obter mais informações sobre as portas padrão, veja Portas e protocolos necessários.
Especificar local de armazenamento	Especifique a localização do arquivo local a ser usada pelo DRA para armazenamento de dados de auditoria e de cache.
Especificar a localização do banco de dados de replicação do DRA	◆ Especifique a localização do arquivo do banco de dados de replicação do DRA e a porta do serviço de replicação. ◆ Especifique o certificado SSL que você deseja usar para comunicações seguras com o banco de dados por IIS e especifique a porta de replicação do IIS.
Especificar o certificado SSL do serviço REST	Selecione o certificado SSL que você usará para o serviço REST e especifique a porta do serviço REST.
Especifique o certificado SSL do Console da Web	Especifique o certificado SSL que você usará para a vinculação HTTPS.
Verificar a configuração de instalação	Você pode verificar a configuração na página de resumo da instalação antes de clicar em **Instalar** para prosseguir com a instalação.
Verificação pós-instalação	Após a instalação ser concluída, o Verificador de Saúde será executado para verificar a instalação e atualizar a licença do produto. Para obter mais informações, consulte “Health Check Utility” (Utilitário de Verificação de Saúde) no *DRA Administrator Guide* (Guia do Administrador do DRA).

Instalar clientes do DRA

Você pode instalar clientes de linha de comando e consoles do DRA específicos executando o DRAInstaller.msi com o pacote .mst correspondente no destino de instalação:

NetIQDRACLI.mst	Instala a interface de linha de comando
NetIQDRAADSI.mst	Instala o provedor de ADSI do DRA
NetIQDRAClients.mst	Instala todas as interfaces do usuário do DRA

Para implantar clientes do DRA específicos para múltiplos computadores em toda a sua empresa, configure um objeto de política de grupo para instalar o pacote .MST específico.

1. Inicie os usuários e computadores do Active Directory e crie um objeto de política de grupo.
2. Adicione o pacote DRAInstaller.msi a este objeto de política de grupo.
3. Verifique se esse objeto de política de grupo tem uma das seguintes propriedades:
   - Cada conta do usuário no grupo tem permissões de Power User para o computador apropriado.
   - Habilite a configuração de política Sempre Instalar com Privilégios Elevados.
4. Adicione o arquivo .mst da interface do usuário a esse objeto política de grupo.
5. Distribua sua política de grupo.

Observação: Para obter mais informações sobre a política de grupo, veja a Ajuda do Microsoft Windows. Para testar e implantar a política de grupo com segurança pela sua empresa, use o *Administrador de Política de Grupo*.

Instalar o Workflow Automation e definir as configurações

Para gerenciar as solicitações do Workflow Automation no DRA, você precisa fazer o seguinte:

- Instale e configure o Workflow Automation e o Adaptador do DRA.

  Para obter informações, consulte o *Workflow Automation Administrator Guide* (Guia do Administrador do Workflow Automation) e a *Workflow Automation Adapter Reference for DRA* (Referência do Adaptador do Workflow Automation para DRA).
- Configure a integração do Workflow Automation com o DRA.

  Para obter informações, consulte “Configuring the Workflow Automation Server” (Configurando o servidor do Workflow Automation) no *DRA Administrator Guide* (Guia do Administrador do DRA).
- Delegue poderes do Workflow Automation no DRA.

  Para obter informações, consulte “Delegating Workflow Automation Server Configuration Powers” (Delegando poderes de configuração do servidor no Workflow Automation) no *DRA Administrator Guide* (Guia do Administrador do DRA).

Os documentos mencionados acima estão disponíveis no site da Documentação do DRA.

Instalar o DRA Reporting

O DRA Reporting requer que você instale o arquivo DRAReportingSetup.exe do Kit de Instalação do DRA da NetIQ.

Etapas	Mais informações
Efetuar logon no servidor de destino	Efetue logon no servidor de destino do Microsoft Windows para a instalação com uma conta que tem privilégios administrativos locais. Verifique se essa conta tem privilégios administrativos de domínio e locais, além de privilégios de administrador do sistema no SQL Server.
Copie e execute o Kit de Instalação do Admin da NetIQ	Copie o kit de instalação do DRA NetIQAdminInstallationKit.msi para o servidor de destino e execute-o clicando duas vezes no arquivo ou chamando-o da linha de comando. O kit de instalação extrairá a mídia de instalação do DRA para o sistema de arquivos local para um local personalizável. Além disso, o kit de instalação instalará o .NET Framework no servidor de destino se isso for necessário para cumprir os requisitos do instalador do produto DRA.
Executar a instalação do DRA Reporting	Navegue até o local em que a mídia de instalação foi extraída e execute DRA`ReportingSetup.exe` para instalar o componente de gerenciamento para integração com o gerador de relatórios do DRA.
Verificar e instalar pré-requisitos da instalação	A caixa de diálogo **Pré-requisitos** exibirá a lista de aplicativos de software necessários com base nos componentes selecionados para a instalação. O instalador guiará você pela instalação de quaisquer pré-requisitos ausentes que sejam necessários para a instalação ser concluída com êxito. Para obter informações sobre o NetIQ Reporting Center, consulte o *Reporting Center Guide* (Guia do Reporting Center) no site na web da documentação.
Aceitar o contrato de licença EULA	Aceite os termos do Contrato de Licença por Usuário Final para concluir a execução da instalação.

5 Upgrade do produto

Este capítulo fornece um processo que ajuda você a fazer upgrade ou migrar um ambiente distribuído nas fases controladas.

Este capítulo presume que seu ambiente contenha vários servidores de administração, com alguns servidores localizados em sites remotos. Essa configuração é chamada de conjunto com vários masters (MMS). Um MMS consiste em um servidor de administração principal e em um ou mais servidores de administração secundários associados. Para obter mais informações sobre como funciona um MMS, veja “Configuring the Multi-Master Set” (Configurando o conjunto multimaster) no *DRA Administrator Guide* (Guia do Administrador do DRA).

Planejando um upgrade do DRA

Execute o `NetIQAdminInstallationKit.msi` para extrair a mídia de instalação do DRA e instale e execute o Utilitário de Verificação de Saúde.

Planeje sua implantação do DRA antes de iniciar o processo de upgrade. Conforme você planejar a implantação, considere as seguintes diretrizes:

- Teste o processo de upgrade em seu ambiente de laboratório antes de enviar o upgrade por push para o ambiente de produção. Os testes permitem que você identifique e resolva quaisquer problemas inesperados sem afetar as responsabilidades de administração diárias.
- Revise Portas e protocolos necessários.
- Determine quantos administradores assistentes dependem de cada MMS. Se a maioria dos administradores assistentes depende de servidores ou de conjuntos de servidores específicos, faça o upgrade desses servidores primeiro fora dos horários de pico.
- Determine quais administradores assistentes precisam do console de Delegação e Configuração. Você pode obter essas informações de uma das seguintes maneiras:
  - Revise quais administradores assistentes estão associados aos grupos de administradores assistentes incorporados.
  - Revise quais administradores assistentes estão associados às Telas Ativas incorporadas.
  - Use o Directory and Resource Administrator Reporting para gerar relatórios de modelo de segurança, como os relatórios Mais Informações sobre Admin Assistente da Tela Ativa e Grupos de Admin Assistentes.

  Notifique a esses administradores assistentes seus planos de fazer upgrade das interfaces de usuário.

- Determine quais administradores assistentes precisam se conectar ao servidor de Administração principal. Esses administradores assistentes deverão fazer upgrade dos respectivos computadores cliente depois que você fizer upgrade do servidor de Administração principal.

  Notifique a esses administradores assistentes seus planos de fazer upgrade dos servidores de Administração e das interfaces do usuário.
- Determine se você precisa implementar quaisquer mudanças de delegação, configuração ou política antes de começar o processo de upgrade. Dependendo do seu ambiente, essa decisão pode ser tomada de modo independente para cada site.
- Coordene os upgrades de seus computadores cliente e servidores de administração para assegurar o mínimo tempo de espera possível. Esteja ciente de que o DRA não suporta a execução de versões anteriores do DRA junto com a versão atual do DRA no mesmo servidor de administração ou computador cliente.

Importante

- Se a sua versão anterior do DRA tiver o console do ARM (Gerenciamento de Recursos e de Contas) instalado, o console do ARM será removido durante o upgrade.
- Quando você fizer upgrade do Servidor do DRA de uma versão 9.x, isso removerá eventuais locatários gerenciados existentes do DRA. Para continuar usando esses locatários ao usar o Azure, você precisa adicioná-los após fazer upgrade. Para obter informações sobre como adicionar locatários, veja “Creating an Azure Application and Adding an Azure Tenant” (Criando um aplicativo do Azure e adicionando um locatário do Azure) no *DRA Administrator Guide* (Guia do Administrador do DRA).
- Já que o Exchange 2010 não é suportado no DRA 10.1, ele será desabilitado ao fazer upgrade do DRA 9.x. Para continuar a realizar operações com o Exchange após o upgrade, desabilite e habilite novamente a opção **Enable Exchange Policy** (Habilitar a Política do Exchange) no Console de Delegação e Configuração. As duas mudanças precisam ser “aplicadas” para que a política seja redefinida.

  Para obter informações sobre essa configuração de política, consulte “Enabling Microsoft Exchange” (Habilitando o Microsoft Exchange) no *DRA Administrator Guide* (Guia do Administrador do DRA).

Tarefas antes do upgrade

Antes de iniciar as instalações de upgrade, siga as etapas de pré-upgrade abaixo para preparar cada conjunto de servidores para upgrade.

Etapas	Mais informações
Fazer backup da instância do AD LDS	Abra o utilitário de verificação de saúde e execute a verificação de **Fazer backup da instância do AD LDS** para criar um backup da sua instância do AD LDS atual.
Fazer um plano de implantação	Faça um plano de implantação para fazer upgrade dos servidores de Administração e interfaces do usuário (computadores cliente de administradores assistentes). Para obter mais informações, veja Planejando um upgrade do DRA.

Etapas	Mais informações
Dedique um servidor secundário para a execução de uma versão anterior do DRA	*Opcional:* Dedique um servidor de administração secundário à execução de uma versão anterior do DRA ao fazer o upgrade de um site.
Fazer as mudanças necessárias para este MMS	Faça quaisquer mudanças necessárias às definições de delegação, configuração ou política para este MMS. Use o servidor de Administração principal para modificar essas configurações.
Sincronizar o MMS	Sincronize os conjuntos de servidores de modo que cada servidor de Administração contenha as definições de segurança e de configuração mais recentes.
Fazer backup do registro do servidor principal	Faça backup do registro do servidor de Administração principal. Ter um backup das configurações de registro anteriores permite que você recupere com facilidade suas definições de segurança e de configuração anteriores.
Converter gMSAs em contas do usuário do DRA	*Opcional:* Se você estiver usando uma gMSA (Conta de Serviço Gerenciado do grupo) para a conta do Serviço DRA, mude-a para uma conta do usuário do DRA antes de fazer upgrade. Após o upgrade, você precisará mudar a conta, tornando-a novamente uma gMSA.

Observação: Se você precisar restaurar a instância do AD LDS, faça o seguinte:

1. Pare a instância do AD LDS atual em Gerenciamento do computador > Serviços. Isso terá um título diferente: `NetIQDRASecureStoragexxxxx`.
2. Substitua o arquivo **atual** `adamnts.dit` pelo arquivo de **backup** `adamnts.dit` conforme indicado abaixo:
   - Local do arquivo atual: `%ProgramData%/NetIQ/DRA/<DRAInstanceName>/data/`
   - Local do arquivo de backup: `%ProgramData%/NetIQ/ADLDS/`
3. Reinicie a instância do AD LDS.

Tópicos antes do upgrade:

- “Dedicar um servidor de administração local à execução de uma versão anterior do DRA” na página 48
- “Sincronizar seu conjunto de servidores com versão anterior do DRA” na página 49
- “Fazer backup do registro de servidor de administração” na página 49

Dedicar um servidor de administração local à execução de uma versão anterior do DRA

Dedicar um ou mais servidores de administração secundários à execução de uma versão anterior do DRA localmente em um site durante o upgrade pode ajudar a minimizar o tempo de espera e as conexões onerosas a sites remotos. Esta etapa é opcional e permite que os administradores assistentes usem uma versão anterior do DRA durante todo o processo de upgrade até que você esteja satisfeito quanto à conclusão da implantação.

Considere essa opção se você tem um ou mais dos seguintes requisitos de upgrade:

- Você precisa de pouco ou nenhum tempo de espera.
- Você precisa suportar um grande número de administradores assistentes e não é capaz de fazer upgrade de todos os computadores cliente imediatamente.
- Você deseja continuar a suportar o acesso a uma versão anterior do DRA depois do upgrade do servidor de Administração principal.
- Seu ambiente inclui um MMS que abrange diversos sites.

Você pode instalar um novo servidor de Administração secundário ou atribuir um servidor secundário executando uma versão anterior do DRA. Se você planeja fazer upgrade desse servidor, ele deve ser o último servidor a passar por upgrade. Caso contrário, desinstale completamente o DRA desse servidor quando você terminar seu upgrade com êxito.

Configurando um novo servidor secundário

Instalar um novo servidor de Administração secundário em um site local pode ajudar você a evitar conexões onerosas a sites remotos, além de assegurar que seus administradores assistentes possam continuar usando uma versão anterior do DRA sem interrupção. Se o seu ambiente inclui um MMS que abrange vários sites, você deve considerar essa opção. Por exemplo, se o MMS consiste em um servidor de Administração principal no site de Londres e um servidor de Administração secundário no site de Tóquio, considere instalar um servidor secundário no site de Londres e adicioná-lo ao MMS correspondente. Esse servidor adicional permite que administradores assistentes do site de Londres usem uma versão anterior do DRA até que o upgrade esteja concluído.

Usar um servidor secundário existente

Você pode usar um servidor de Administração secundário como o servidor dedicado para uma versão anterior do DRA. Se você não planeja fazer upgrade de um servidor de Administração secundário em um determinado site, deve considerar essa opção. Se você não pode dedicar um servidor secundário existente, considere a possibilidade de instalar um novo servidor de Administração para esse fim. Dedicar um ou mais servidores secundários à execução de uma versão anterior do DRA permite que seus administradores assistentes continuem a usar uma versão anterior do DRA sem interrupção até que o upgrade esteja concluído. Essa opção funciona melhor em ambientes grandes que usam um modelo de administração centralizado.

Sincronizar seu conjunto de servidores com versão anterior do DRA

Antes de você fazer backup do registro da versão anterior do DRA ou de começar o processo de upgrade, sincronize os conjuntos de servidores de modo que cada servidor de Administração contenha as definições mais recentes de segurança e de configuração.

Observação: Verifique se você fez todas as mudanças necessárias às definições de delegação, configuração ou política para este MMS. Use o servidor de Administração principal para modificar essas configurações. Após fazer upgrade do servidor de Administração principal, você não poderá sincronizar definições de delegação, configuração ou política com nenhum servidor de Administração que execute versões anteriores do DRA.

Para sincronizar seu conjunto de servidores existente:

1. Efetue logon no servidor de Administração principal como o Admin Incorporado.
2. Abra o Console de Delegação e Configuração e expanda **Gerenciamento de Configurações**.
3. Clique em **Servidores de Administração**.
4. No painel direito, selecione o servidor de Administração principal apropriado para este conjunto de servidores.
5. Clique em **Propriedades**.
6. Na guia Programação de sincronização, clique em **Atualizar agora**.
7. Verifique se a sincronização é concluída com êxito e se todos os servidores de Administração secundários estão disponíveis.

Fazer backup do registro de servidor de administração

Fazer backup do registro de servidor de administração assegura que você possa retornar às suas configurações anteriores. Por exemplo, se você precisa desinstalar totalmente a versão do DRA atual e usar a versão do DRA anterior, ter um backup das configurações do registro anteriores permite recuperar com facilidade as definições de segurança e configuração anteriores.

No entanto, tenha cuidado ao editar seu registro. Se há um erro em seu registro, o servidor de Administração pode não funcionar como esperado. Se ocorrer um erro durante o processo de upgrade, você poderá usar o backup de suas configurações do registro para restaurar o registro. Para obter mais informações, veja a *Ajuda do Editor do Registro*.

Importante: A versão do servidor do DRA, o nome do OS Windows e a configuração do domínio gerenciado devem ser exatamente os mesmos ao restaurar o registro.

Importante: Antes de fazer upgrade, faça backup do OS Windows da máquina que está hospedando o DRA ou crie uma imagem de instantâneo de máquina virtual dessa máquina.

Para fazer backup do registro do Servidor de Administração:

1. Execute `regedit.exe`.

2 Clique o botão direito do mouse no nó `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Mission Critical Software\OnePoint` e selecione **Exportar**.

3 Especifique o nome e o local do arquivo no qual gravar a chave do registro e clique em **Gravar**.

Fazendo upgrade do Servidor de administração DRA

A lista de verificação a seguir guia você por todo o processo de upgrade. Use esse processo para fazer upgrade de cada conjunto de servidores em seu ambiente. Se você ainda não fez isso, use o Utilitário de Verificação de Saúde para criar um backup de sua instância atual do AD LDS.

Aviso: Não faça upgrade dos seus servidores de Administração secundários até ter feito upgrade do servidor de Administração principal para esse MMS.

Você pode repartir o processo de upgrade em várias fases, fazendo o upgrade de um MMS por vez. Esse processo de upgrade também permite que você inclua temporariamente servidores secundários executando uma versão anterior do DRA e servidores secundários executando a versão atual do DRA no mesmo MMS. O DRA suporta a sincronização entre servidores de Administração executando uma versão anterior do DRA e servidores executando a versão atual do DRA. No entanto, esteja ciente de que o DRA não suporta a execução de uma versão anterior do DRA junto com a versão atual do DRA no mesmo servidor de administração ou computador cliente.

Importante: A instalação do upgrade do DRA realiza as seguintes mudanças quando você faz upgrade do Servidor do DRA de uma versão 9.x para uma versão 10.x do DRA:

- Move as configurações de usuário do servidor do Workflow Automation e do UCH do console da Web para o Console de Delegação e Configuração
- Remove o componente da Web antigo do servidor.
- Remove eventuais locatários gerenciados.

  Para obter informações sobre como adicionar locatários, consulte “Configuring Azure Tenants” (Configurando locatários do Azure) no *DRA Administrator Guide* (Guia do Administrador do DRA).
- Se você tiver instalado o Console de Gerenciamento de Recursos e de Contas em uma versão anterior, ele será removido quando você fizer o upgrade para a versão 10.x do DRA.
- Durante um upgrade do MMS, o upgrade do servidor principal ocorre primeiro, seguido dos servidores secundários. Para uma replicação bem-sucedida das designações temporárias de grupos no servidor secundário, execute a **Programação de sincronização de multimaster** ou aguarde pela execução programada dela.
- Já que o Exchange 2010 não é suportado no DRA 10, ele será desabilitado ao fazer upgrade do DRA 9.x. Para continuar a realizar operações com o Exchange após o upgrade, desabilite e habilite novamente a opção **Habilitar a Política do Exchange** no Console de Delegação e Configuração. As duas mudanças precisam ser “aplicadas” para que a política seja redefinida.

  Para obter informações sobre essa configuração de política, consulte “Enabling Microsoft Exchange” (Habilitando o Microsoft Exchange) no *DRA Administrator Guide* (Guia do Administrador do DRA).

Etapas	Mais informações
Executar utilitário de Verificação de Saúde	Instale o utilitário de Verificação de Saúde independente do DRA e execute-o usando uma conta de serviço. Corrija quaisquer problemas.
Fazer um upgrade de teste	Faça um upgrade de teste em seu ambiente de laboratório para identificar possíveis problemas e minimizar o tempo de espera em produção.
Determinar a ordem do upgrade	Determine a ordem em que você deseja fazer upgrade de seus conjuntos de servidores.
Preparar cada MMS para upgrade	Prepare cada MMS para upgrade. Para obter mais informações, veja Tarefas antes do upgrade.
Fazer upgrade do servidor principal	Faça upgrade do servidor de Administração principal no MMS apropriado. Para obter informações, consulte Fazer upgrade do Servidor de Administração Principal.
Instalar um novo servidor secundário	*(Opcional)* Para minimizar o tempo de espera em sites remotos, instale um servidor de Administração secundário local executando a versão mais recente do DRA. Para obter informações, consulte Instalar um servidor de Administração secundário local para a versão atual do DRA.
Implantar interfaces do usuário	Implante as interfaces do usuário para seus administradores assistentes. Para obter informações, consulte Implantar as interfaces do usuário do DRA
Fazer upgrade dos servidores secundários	Faça upgrade dos servidores de Administração secundários no MMS. Para obter informações, consulte Fazer upgrade de servidores de Administração secundários.
Fazer upgrade do DRA Reporting	Faça upgrade do DRA Reporting. Para obter informações, consulte Fazendo upgrade do Reporting.
Executar utilitário de Verificação de Saúde	Execute o utilitário de Verificação de Saúde que foi instalado como parte do upgrade. Corrija quaisquer problemas.
Adicionar locatários do Azure *(depois do upgrade)*	(*Opcional, depois do upgrade)* Se você estava gerenciando locatários do Azure antes do upgrade, eles são removidos durante o upgrade. Você precisará adicionar esses locatários novamente e executar uma atualização completa de cache de contas por meio do Console de Delegação e Configuração. Para obter mais informações, consulte "Configuring Azure Tenants" (Configurando locatários do Azure) no *DRA Administrator Guide* (Guia do Administrador do DRA).
Atualizar a configuração do Console da Web *(após o upgrade)*	*(Condicional, após o upgrade)* Se você tiver qualquer uma das configurações do Console da Web abaixo antes do upgrade, elas precisarão ser atualizadas após a conclusão da instalação do upgrade: ◆ Conexões padrão do servidor habilitadas ◆ Arquivos de configuração modificados Para obter mais informações, veja Atualizando a configuração do Console da Web – Após a instalação.

Tópicos de upgrade do servidor:

Fazer upgrade do Servidor de Administração Principal

Após você ter preparado seu MMS com êxito, faça upgrade do servidor de Administração principal. Não faça upgrade de interfaces do usuário nos computadores cliente até a conclusão do upgrade do servidor de Administração principal. Para obter mais informações, consulte Implantar as interfaces do usuário do DRA.

Observação: Para obter mais instruções e considerações sobre o upgrade, consulte os *Directory and Resource Administrator Release Notes* (Detalhes da versão do Directory and Resource Administrator).

Antes de fazer upgrade, notifique a seus administradores assistentes quando você planeja iniciar esse processo. Se você dedicou um servidor de Administração secundário à execução de uma versão anterior do DRA, identifique também esse servidor para que os administradores assistentes possam continuar usando a versão anterior do DRA durante o upgrade.

Observação: Após fazer upgrade do servidor de Administração principal, você não poderá sincronizar definições de delegação, configuração ou política desse servidor com nenhum servidor de Administração secundário que execute uma versão anterior do DRA.

Instalar um servidor de Administração secundário local para a versão atual do DRA

Instalar um novo servidor de Administração secundário para executar a versão atual do DRA em um site local pode ajudar você a minimizar conexões onerosas a sites remotos, reduzindo simultaneamente o tempo de espera total e permitindo implantação mais rápida das interfaces do usuário. Esta etapa é opcional e permite que os administradores assistentes usem tanto a versão atual quanto uma versão anterior do DRA durante todo o processo de upgrade até que você esteja satisfeito quanto à conclusão da implantação.

Considere essa opção se você tem um ou mais dos seguintes requisitos de upgrade:

- Você precisa de pouco ou nenhum tempo de espera.
- Você precisa suportar um grande número de administradores assistentes e não é capaz de fazer upgrade de todos os computadores cliente imediatamente.
- Você deseja continuar a suportar o acesso a uma versão anterior do DRA depois do upgrade do servidor de Administração principal.
- Seu ambiente inclui um MMS que abrange diversos sites.

Por exemplo, se o MMS consiste em um servidor de Administração principal no site de Londres e um servidor de Administração secundário no site de Tóquio, considere instalar um servidor secundário no site de Tóquio e adicioná-lo ao MMS correspondente. O servidor adicional equilibra melhor a carga de administração diária no site de Tóquio e permite que os administradores assistentes de qualquer site usem tanto a versão anterior quanto a versão atual do DRA até que o upgrade esteja concluído. Além disso, seus administradores assistentes não passam por nenhum tempo de espera porque você pode implantar as interfaces do usuário do DRA imediatamente. Para obter mais informações sobre o upgrade de interfaces do usuário, veja Implantar as interfaces do usuário do DRA.

Implantar as interfaces do usuário do DRA

Normalmente, você deve implantar as interfaces do usuário do DRA atuais após fazer upgrade do servidor de Administração principal e de um servidor de Administração secundário. No entanto, para administradores assistentes que precisam usar o servidor de Administração principal, faça primeiro o upgrade dos respectivos computadores cliente instalando o console de Delegação e Configuração. Para obter mais informações, consulte Planejando um upgrade do DRA.

Se você realiza o processamento de lote com frequência por meio da CLI, do provedor ADSI, do PowerShell ou se gera relatórios com frequência, considere a possibilidade de instalar essas interfaces do usuário em um servidor de Administração secundário para manter um equilíbrio de carga apropriado pelo MMS.

Você pode permitir que seus administradores assistentes instalem as interfaces do usuário do DRA ou pode implantar essas interfaces por meio de política de grupo. Você também pode implantar de modo rápido e fácil o console da Web para vários administradores assistentes.

Observação: Não é possível executar várias versões de componentes do DRA lado a lado no mesmo servidor do DRA. Se você planeja fazer upgrade de seus computadores cliente de administrador assistente gradualmente, considere a possibilidade de implantar o console da Web para assegurar acesso imediato a um servidor de Administração executando a versão atual do DRA.

Fazer upgrade de servidores de Administração secundários

Ao fazer upgrade de servidores de Administração secundários, você pode fazer upgrade de cada servidor conforme necessário, dependendo de seus requisitos de administração. Considere também como planeja implantar as interfaces do usuário do DRA e fazer upgrade delas. Para obter mais informações, veja Implantar as interfaces do usuário do DRA.

Por exemplo, um caminho de upgrade típico pode incluir as seguintes etapas:

1. Faça upgrade de um servidor de Administração secundário.
2. Instrua os administradores assistentes que usam esse servidor a instalarem as interfaces do usuário apropriadas, como o console da Web.
3. Repita as etapas 1 e 2 acima até fazer o upgrade integral do MMS.

Antes de fazer upgrade, notifique a seus administradores assistentes quando você planeja iniciar esse processo. Se você dedicou um servidor de Administração secundário à execução de uma versão anterior do DRA, identifique também esse servidor para que os administradores assistentes possam continuar usando a versão anterior do DRA durante o upgrade. Quando você concluir o processo de

upgrade para esse MMS e todos os computadores cliente de administradores assistentes estiverem executando interfaces do usuário que receberam upgrade, coloque offline quaisquer servidores restantes com versões anteriores do DRA.

Atualizando a configuração do Console da Web – Após a instalação

Execute ambas as ações abaixo ou uma delas após a instalação do upgrade, se elas se aplicarem ao seu ambiente do DRA:

Conexão padrão com o servidor DRA

O componente de Serviço REST do DRA está consolidado com o Servidor DRA a partir do DRA 10.1. Se você tiver a conexão padrão com o Servidor DRA configurada antes de fazer upgrade de uma versão do DRA 10.0.x ou anterior, precisará rever essas configurações após o upgrade, pois agora há apenas uma configuração de conexão, a Conexão com o Servidor DRA. Você pode acessar esta configuração no Console da Web em **Administração** > **Configuração** > **Conexão com o Servidor DRA**.

Você também pode atualizar essas configurações após o upgrade no arquivo `web.config` em `C:\inetpub\wwwroot\DRAClient\rest` no servidor do Console da Web do DRA, da seguinte forma:

```
<restService useDefault="Never">
<serviceLocation address="<REST server name>" port="8755"/>
</restService>
```

Configuração de login do Console da Web

Ao fazer upgrade das versões DRA 10.0.x ou anteriores, se o Serviço REST do DRA for instalado sem o Servidor DRA, a desinstalação do Serviço REST do DRA será um pré-requisito para o upgrade. Uma cópia de arquivos que foram modificados antes do upgrade é feita em `C:\ProgramData\NetIQ\DRA\Backup\` no servidor. Você pode usar esses arquivos para fazer referência para atualizar quaisquer itens relevantes após o upgrade.

Fazendo upgrade do Workflow Automation

Para realizar um upgrade “in-place” em ambientes não agrupados de 64 bits, basta executar o programa de configuração do Workflow Automation em seus computadores existentes com Workflow Automation. Não é necessário parar nenhum serviço do Workflow Automation que possa estar em execução.

Quaisquer adaptadores do Workflow Automation que não estejam incorporados ao instalador do Workflow Automation devem ser desinstalados e reinstalados após o upgrade.

Para obter informações mais detalhadas sobre como fazer upgrade do Workflow Automation, consulte “Upgrading from a Previous Version” (Fazendo upgrade de uma versão anterior) no *Workflow Automation Administrator Guide* (Guia do Administrador do Workflow Automation).

Fazendo upgrade do Reporting

Antes de você fazer upgrade do DRA Reporting, verifique se o seu ambiente cumpre os requisitos mínimos para o NRC 3.3. Para obter mais informações sobre os requisitos de instalação e considerações sobre o upgrade, veja o *NetIQ Reporting Center Reporting Guide* (Guia de Geração de Relatórios do NetIQ Reporting Center).

Etapas	Mais informações
Desabilitar o suporte ao DRA Reporting	Para assegurar que os coletores do gerador de relatórios não sejam executados durante o processo de upgrade, desabilite o suporte ao DRA Reporting na janela Configuração do Serviço Gerador de Relatórios no Console de Delegação e Configuração.
Efetuar logon no servidor da instância do SQL com as credenciais aplicáveis	Efetue logon no servidor do Microsoft Windows em que você instalou a instância do SQL para os bancos de dados do gerador de relatórios com uma conta de administrador. Verifique se essa conta tem privilégios administrativos locais, além de privilégios de administrador do sistema no SQL Server.
Executar a configuração do DRA Reporting	Execute DRA`ReportingSetup.exe`. do kit de instalação e siga as instruções no assistente de instalação.
Habilitar o suporte ao DRA Reporting	Em seu servidor de Administração principal, habilite o gerador de relatórios no Console de Delegação e Configuração.

Se o seu ambiente usa integração SSRS, você precisa reimplantar os relatórios. Para mais informações sobre a reimplantação de relatórios, consulte o *Guia da Central do Gerador de Relatórios* no site da documentação na web.

III Modelo de delegação

O DRA permite que os administradores implementem um esquema de permissões de “privilégio mínimo”, fornecendo um conjunto flexível de controles para conceder poderes granulares a objetos gerenciados específicos na empresa. Por meio dessas delegações, os administradores podem garantir que os administradores assistentes recebam apenas as permissões necessárias para concluir suas funções e responsabilidades específicas.

6 Entendendo o modelo de delegação dinâmica

O DRA permite gerenciar o acesso administrativo à sua empresa no contexto de um modelo de delegação. O modelo de delegação permite que você configure acesso de “privilégio mínimo” para administradores assistentes por meio de um conjunto dinâmico de controles que podem se adaptar à medida que a empresa muda e evolui. O modelo de delegação fornece controle de acesso administrativo que representa mais de perto como sua empresa funciona:

- Com regras de escopo flexíveis, os administradores podem direcionar permissões para objetos gerenciados específicos com base nas necessidades comerciais, em vez da estrutura da empresa.
- A delegação baseada em funções garante que as permissões sejam concedidas de forma consistente e simplifica o aprovisionamento.
- A designação de privilégios pode ser administrada em domínios, locatários da nuvem e aplicativos gerenciados de um único local.
- Poderes granulares permitem que você personalize o acesso específico concedido aos administradores assistentes.

Controles do modelo de delegação

Os administradores usam os seguintes controles para provisionar o acesso por meio do modelo de delegação:

- **Delegação:** Os administradores provisionam acesso a usuários e grupos, atribuindo uma função que especificou permissões no contexto de uma Tela Ativa que fornece o escopo.
- **Telas Ativas:** Uma Tela Ativa representa um escopo específico de objetos gerenciados que são definidos por uma ou mais regras. Objetos gerenciados identificados por cada regra em uma Tela Ativa são agregados em um escopo unificado.
- **Regra da Tela Ativa:** As regras são definidas por expressões que correspondem a um conjunto de objetos gerenciados com base em várias condições, como tipo de objeto, local, nome e assim por diante.
- **Funções:** Uma função representa um conjunto específico de poderes (permissões) necessários para executar uma função de administração específica. O DRA fornece várias funções integradas para funções de negócios comuns e você pode definir funções personalizadas que melhor atendem às necessidades da sua organização.
- **Poderes:** Um poder define uma permissão específica para tarefas suportadas pelo objeto gerenciado, como exibir, modificar, criar, apagar e assim por diante. As permissões em torno da modificação de um objeto gerenciado podem ser subdivididas nas propriedades específicas que podem ser mudadas. O DRA fornece uma lista extensa de poderes incorporados para objetos gerenciados suportados e pode definir poderes personalizados para estender o que pode ser provisionado por meio do modelo de delegação.

Como o DRA processa solicitações

Quando o servidor de Administração recebe uma solicitação para uma ação, como mudar uma senha de usuário, ele usa o seguinte processo:

1. Pesquise por Telas Ativas que estão configuradas para gerenciar o objeto de destino da operação.
2. Valide os poderes atribuídos à conta que está solicitando a ação.
    a. Avalie todas as atribuições da Tela Ativa que contenham o administrador assistente solicitando a operação.
    b. Quando essa lista estiver concluída, crie uma lista de todas as Telas Ativas que contenham o objeto de destino e o administrador assistente.
    c. Compare os poderes com os poderes necessários para a operação solicitante.
3. *Se a conta tiver o poder correto*, o servidor de Administração permitirá que a ação seja executada.

    Se a conta não tiver o poder correto, o servidor de administração retornará um erro.
4. Atualize o Active Directory.

Exemplos de como o DRA processa atribuições de delegação

Os exemplos a seguir descrevem cenários comuns que surgem em como o DRA avalia o modelo de delegações ao processar uma solicitação:

Exemplo 1: Mudando a senha de um usuário

Quando um administrador assistente tenta definir uma nova senha para a conta do usuário JSmith, o servidor de Administração localiza todas as Telas Ativas que incluem JSmith. Essa pesquisa procura por qualquer Tela Ativa que especifique JSmith diretamente, por meio de uma regra curinga ou por meio da participação do grupo. Se uma Tela Ativa incluir outras Telas Ativas, o servidor de Administração também pesquisará essas Telas Ativas adicionais. O servidor de Administração determina se o administrador assistente tem o poder *Redefinir Senha da Conta do Usuário* em qualquer uma dessas Telas Ativas. Se o administrador assistente tiver o poder *Redefinir Senha da Conta do Usuário*, o servidor de Administração redefinirá a senha para JSmith. Se ele não tiver esse poder, o servidor de administração negará a solicitação.

Exemplo 2: Sobrepondo as Telas Ativas

Um poder define as propriedades de um objeto que um administrador assistente pode exibir, modificar ou criar em seu domínio gerenciado ou subárvore. Mais de uma Tela Ativa pode incluir o mesmo objeto. Esta configuração é chamada **sobrepondo Telas Ativas**.

Quando as Telas Ativas se sobrepõem, você pode acumular um conjunto de diferentes poderes sobre os mesmos objetos. Por exemplo, se uma Tela Ativa permitir que você adicione uma conta do usuário a um domínio e outra Tela Ativa permita apagar uma conta do usuário do mesmo domínio, você poderá adicionar ou apagar contas de usuário nesse domínio. Desta forma, os poderes que você tem sobre um determinado objeto são cumulativos.

É importante entender como as Telas Ativas podem se sobrepor e você pode ter mais poderes sobre os objetos incluídos nelas. Considere a configuração da Tela Ativa ilustrada na figura a seguir.

As guias brancas identificam as Telas Ativas por local *New York City* e *Houston*. As guias pretas identificam as Telas Ativas por sua função organizacional, *Vendas* e *Marketing*. As células mostram os grupos incluídos em cada Tela Ativa.

O grupo NYC_Sales e o grupo HOU_Sales são ambos representados na Tela Ativa de Vendas. Se você tiver poder na Tela Ativa de Vendas, poderá gerenciar qualquer membro dos grupos NYC_Sales e HOU_Sales. Se você também tiver poder na Tela Ativa de Nova York, esses poderes adicionais serão aplicados ao grupo NYC_Marketing. Dessa forma, os poderes se acumulam quando as Telas Ativas se sobrepõem.

A sobreposição de Telas Ativas pode fornecer um modelo de delegação eficiente e flexível. No entanto, esse recurso também pode ter consequências não intencionais. Planeje cuidadosamente suas Telas Ativas para garantir que cada administrador assistente tenha apenas os poderes que você pretende em cada conta do usuário, grupo, OU, contato ou recurso.

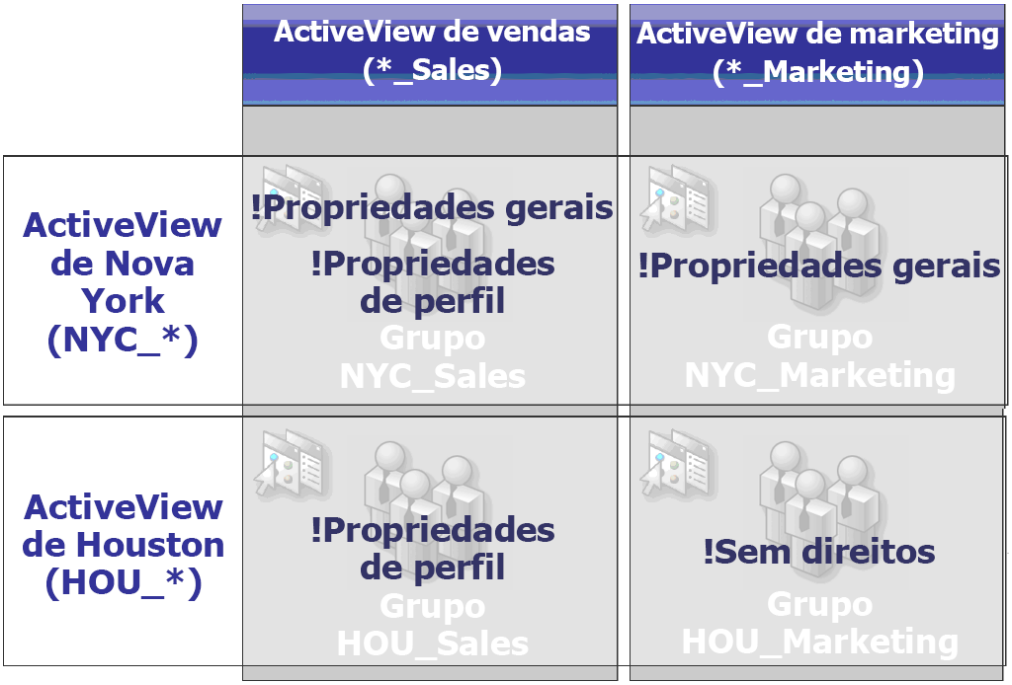
Grupos em várias Telas Ativas

Neste exemplo, o grupo NYC_Sales é representado em mais de uma Tela Ativa. Os membros do grupo NYC_Sales são representados na Tela Ativa de Nova York porque o nome do grupo corresponde à regra de Tela Ativa NYC_*. O grupo também está na Tela Ativa de Vendas porque o nome do grupo corresponde à regra de Tela Ativa *_Sales. Ao incluir o mesmo grupo em várias Telas Ativas, você pode permitir que diferentes administradores assistentes gerenciem os mesmos objetos de maneira diferente.

Usando poderes em várias Telas Ativas

Suponha que haja um administrador assistente, JSmith, que tenha o poder *Modificar Propriedades Gerais do Usuário* na Tela Ativa New York City. Esse primeiro poder permite que JSmith edite todas as propriedades na guia General (Geral) de uma janela de propriedades do usuário. JSmith tem o poder *Modificar Propriedades de Perfil do Usuário* na Tela Ativa de Vendas. Esse segundo poder permite que JSmith edite todas as propriedades na guia Perfil de uma janela de propriedades do usuário.

A figura a seguir indica os poderes que JSmith tem para cada grupo.



JSmith tem os seguintes poderes:

- Propriedades gerais na Tela Ativa NYC_*
- Propriedades de perfil na Tela Ativa *_Sales

A delegação de poder nessas Telas Ativas sobrepostas permite que JSmith modifique as propriedades General (Geral) e de Perfil do grupo NYC_Sales. Assim, JSmith tem todos os poderes concedidos em todas as Telas Ativas que representam o grupo NYC_Sales.

7 Telas Ativas

As Telas Ativas permitem que você implemente um modelo de delegação que tenha os seguintes recursos:

- É independente da sua estrutura do Active Directory
- Permite que você atribua poderes e defina políticas relacionadas aos seus workflows existentes
- Fornece automação para ajudar você a integrar e personalizar ainda mais sua empresa
- Responde dinamicamente à mudança

Uma Tela Ativa representa um conjunto de objetos em um ou mais domínios gerenciados. Você pode incluir um objeto em mais de uma Tela Ativa. Você também pode incluir muitos objetos de vários domínios ou OUs.

Telas Ativas integradas

Telas Ativas integradas são Telas Ativas padrão fornecidas pelo DRA. Essas Telas Ativas representam todos os objetos atuais e configurações de segurança. Assim, as Telas Ativas integradas fornecem acesso imediato a todos os seus objetos e configurações, bem como ao modelo de delegação padrão. Você pode usar essas Telas Ativas para gerenciar objetos, como contas de usuário e recursos, ou aplicar o modelo de delegação padrão à sua configuração corporativa atual.

O DRA fornece várias Telas Ativas integradas que podem representar seu modelo de delegação. O nó Tela Ativa integrada contém as seguintes Telas Ativas:

All Objects (Todos os objetos)

Inclui todos os objetos em todos os domínios gerenciados. Por meio dessa Tela Ativa, você pode gerenciar qualquer aspecto de sua empresa. Designe esta Tela Ativa ao administrador ou a um administrador assistente que precise de poderes de auditoria em toda a empresa.

Objects Current User Manages as Windows Administrator (Usuário atual dos objetos gerencia como administrador do Windows)

Inclui objetos do domínio gerenciado atual. Por meio dessa Tela Ativa, você pode gerenciar contas de usuários, grupos, contatos, OUs e recursos. Atribua essa Tela Ativa a administradores nativos responsáveis por objetos de conta e recurso no domínio gerenciado.

Administration Servers and Managed Domains (Servidores de administração e domínios gerenciados)

Inclui computadores do servidor de administração e domínios gerenciados. Por meio dessa Tela Ativa, você pode gerenciar a manutenção diária de seus servidores de administração. Designe esta Tela Ativa aos administradores assistentes cujas tarefas incluem monitorar o status de sincronização ou executar atualizações de cache.

DRA Policies and Automation Triggers (Políticas de DRA e Acionadores de Automação)

Inclui todos os objetos acionadores de política e automação em todos os domínios gerenciados. Por meio dessa Tela Ativa, você pode gerenciar as propriedades e o escopo da política, bem como as propriedades do acionador de automação. Designe esta Tela Ativa aos administradores assistentes responsáveis por criar e manter as políticas da sua empresa.

DRA Security Objects (Objetos de segurança do DRA)

Inclui todos os objetos de segurança. Por meio desta Tela Ativa, você pode gerenciar Telas Ativas, grupos de administradores assistentes e funções. Designe esta Tela Ativa aos administradores assistentes responsáveis por criar e manter seu modelo de segurança.

SPA Users from All Managed and Trusted Domains (Usuários do SPA de Todos os Domínios Gerenciados e Confiáveis)

Inclui todas as contas de usuário de domínios gerenciados e confiáveis. Por meio desta Tela Ativa, você pode gerenciar senhas de usuários por meio do Administrador de Senha Segura (SPA).

Acessando Telas Ativas integradas

Acesse Telas Ativas integradas para auditar o modelo de delegação padrão ou gerenciar suas próprias configurações de segurança.

Para acessar Telas Ativas integradas:

1. Acesse **Delegation Management** > **Manage ActiveViews** (Gerenciamento de Delegação > Gerenciar Telas Ativas).
2. Verifique se o campo de pesquisa está em branco e clique em **Find Now** (Localizar Agora) no painel **List items that match my criteria** (Listar itens que correspondem aos meus critérios).
3. Selecione a Tela Ativa apropriada.

Usando Telas Ativas integradas

Não é possível apagar, clonar ou modificar Telas Ativas integradas. No entanto, você pode incorporar essas Telas Ativas ao seu modelo de delegação existente ou usá-las para criar seu próprio modelo.

Você pode usar Telas Ativas integradas das seguintes maneiras:

- Designe as Telas Ativas incorporadas individuais aos grupos de administradores assistentes apropriados. Esta associação permite que os membros do grupo de administradores assistentes gerenciem o conjunto correspondente de objetos com os poderes apropriados.
- Consulte as regras e associações da Tela Ativa integrada como diretrizes para projetar e implementar seu modelo de delegação.

Para obter mais informações sobre como criar um modelo de delegação dinâmica, consulte Entendendo o modelo de delegação dinâmica.

Implementando uma Tela Ativa personalizada

Uma Tela Ativa fornece acesso em tempo real a objetos específicos dentro de um ou mais domínios ou OUs. Você pode adicionar ou remover objetos de uma Tela Ativa sem mudar o domínio subjacente ou a estrutura da OU.

Você pode pensar em uma Tela Ativa como um domínio virtual ou OU, ou os resultados de uma declaração de seleção ou exibição de banco de dados para um banco de dados relacional. As Telas Ativas podem incluir ou apagar qualquer conjunto de objetos, conter outras Telas Ativas e ter conteúdo sobreposto. As Telas Ativas podem conter objetos de diferentes domínios, árvores e florestas. Você pode configurar a Tela Ativa para atender a qualquer necessidade de gerenciamento corporativo.

As Telas Ativas podem incluir os seguintes tipos de objeto:

Contas:

- Usuários
- Grupos
- Computadores
- Contatos
- Grupos de distribuição dinâmica
- Conta de serviço gerenciado do grupo
- Published Printers (Impressoras publicadas)
- Trabalhos de impressão de impressoras publicadas
- Caixas de correio de recursos
- Caixas de correio compartilhadas
- Pastas públicas

Objetos do Diretório:

- Unidades organizacionais
- Domínios
- Servidores membros

Objetos de delegação:

- Telas Ativas
- Autoadministração
- Subordinados Diretos
- Grupos gerenciados

Recursos:

- Usuários conectados
- Dispositivos
- Registros de Eventos
- Arquivos abertos

- Impressoras
- Trabalhos de impressão
- Serviços
- Compartilhamentos

Objetos do Azure:

- Usuário do Azure
- Grupo do Azure
- Locatário do Azure
- Contato do Azure

À medida que sua empresa muda ou cresce, as Telas Ativas mudam para incluir ou apagar os novos objetos. Assim, você pode usar as Telas Ativas para reduzir a complexidade do seu modelo, fornecer a segurança de que precisa e oferecer muito mais flexibilidade do que outras ferramentas de organização empresarial.

Regras das Telas Ativas

Uma Tela Ativa pode consistir em regras que incluem ou excluem objetos, como contas do usuário, grupos, OUs, contatos, recursos, computadores, caixas de correio de recursos, caixas de correio compartilhadas, grupos de distribuição dinâmica, contas de serviço gerenciado do grupo e objetos do Azure, como usuários do Azure, usuários convidados do Azure, grupos do Azure e contatos do Azure. Essa flexibilidade torna as Telas Ativas dinâmicas.

Essas correspondências são chamadas de **curingas**. Por exemplo, você pode definir uma regra para incluir todos os computadores com nomes correspondentes `DOM*`. Essa especificação curinga pesquisará por qualquer conta de computador cujo nome comece com a string DOM. A correspondência de curingas torna a administração dinâmica porque as contas são incluídas automaticamente quando correspondem à regra. Assim, quando você usa curingas, não é necessário reconfigurar as Telas Ativas conforme a organização muda.

Outro exemplo é a definição de Telas Ativas com base na participação do grupo. Você pode definir uma regra que inclua todos os membros de grupos que começam com as letras NYC. Então, como os membros são adicionados a qualquer grupo que corresponda a essa regra, esses membros são automaticamente incluídos nesta Tela Ativa. À medida que sua empresa muda ou cresce, o DRA aplica novamente as regras para incluir ou apagar os novos objetos nas Telas Ativas adequadas.

8 Funções

Esta seção inclui uma lista com descrições das funções integradas ao DRA, como usar essas funções e informações sobre como criar e gerenciar funções personalizadas.

Para uma descrição das funções e seu uso em geral, consulte Controles do modelo de delegação.

Funções integradas

As funções de administrador assistente incorporadas fornecem acesso imediato a um conjunto de poderes comumente usados. Você pode estender sua configuração de segurança atual usando essas funções padrão para delegar poder a contas de usuários específicas ou outros grupos.

Essas funções contêm os poderes necessários para executar tarefas comuns de administração. Por exemplo, a função Administração do DRA contém todos os poderes necessários para gerenciar objetos. Para usar esses poderes, no entanto, a função deve estar associada a uma conta do usuário ou a um grupo de administradores assistentes e à Tela Ativa gerenciada.

Como as funções incorporadas fazem parte do modelo de delegação padrão, você pode usá-las para delegar capacidades rapidamente e implementar a segurança. Essas funções incorporadas abordam tarefas comuns que você pode executar por meio das interfaces de usuário do DRA. As seções a seguir descrevem cada função incorporada e resumem as capacidades associadas a essa função.

Gerenciamento do Exchange Online

Administração de contatos do Azure

Fornece todas as capacidades necessárias para criar, modificar, apagar e ver as propriedades de um contato do Azure. Você pode designar essa função a todos os administradores assistentes responsáveis pelo gerenciamento de contatos do Azure.

Administração do Grupo do Azure

Fornece todos os poderes necessários para gerenciar os grupos do Azure e a participação do Azure.

Administração do Usuário do Azure

Fornece todos os poderes necessários para criar, modificar, apagar, habilitar, desabilitar e ver propriedades de gerenciamento do usuário do Azure. Designe esta função aos administradores assistentes responsáveis pelo gerenciamento do usuário do Azure.

Administração

Administração de contato

Fornece todos os poderes necessários para criar um novo contato, modificar propriedades de contato ou apagar um contato. Designe esta função aos administradores assistentes responsáveis pelo gerenciamento de contatos.

Administração do DRA

Fornece todos os poderes para um administrador assistente. Essa função concede ao usuário as permissões para executar todas as tarefas de administração no DRA. Essa função é equivalente às permissões de um administrador. Um administrador assistente associado à função de Administração do DRA pode acessar todos os nós do Directory and Resource Administrator.

Administração de gMSA

Fornece as capacidades necessárias para criar, modificar, apagar e ver as propriedades de uma gMSA (conta de serviço gerenciado do grupo). Você pode designar essa função a todos os administradores assistentes responsáveis pelo gerenciamento de uma gMSA.

Gerenciar e executar ferramentas personalizadas

Fornece todos os poderes necessários para criar, gerenciar e executar ferramentas personalizadas. Designe esta função aos administradores assistentes responsáveis pelo gerenciamento de ferramentas personalizadas.

Gerenciar exceções de clone

Fornece todos os poderes necessários para criar e gerenciar exceções de clone.

Gerenciar políticas e acionadores de automação

Fornece todos os poderes necessários para definir políticas e acionadores de automação. Designe esta função aos administradores assistentes responsáveis por manter as políticas da empresa e automatizar os workflows.

Gerenciar Modelo de Segurança

Fornece todos os poderes necessários para definir as regras de Administração, incluindo Telas Ativas, administradores assistentes e funções. Designe esta função aos administradores assistentes responsáveis por implementar e manter seu modelo de segurança.

Gerenciar atributos virtuais

Fornece todos os poderes necessários para criar e gerenciar atributos virtuais. Designe esta função aos administradores assistentes responsáveis pelo gerenciamento de atributos virtuais.

Administração da OU

Fornece todos os poderes necessários para gerenciar unidades organizacionais. Designe esta função aos administradores assistentes responsáveis pelo gerenciamento da estrutura do Active Directory.

Administração da pasta pública

Fornece os poderes para criar, modificar, apagar, habilitar ou desabilitar e-mail e exibir as propriedades da sua pasta pública. Você pode designar essa função a todos os administradores assistentes responsáveis pelo gerenciamento da Pasta Pública.

Replicar arquivos

Fornece todos os poderes necessários para fazer upload, apagar e modificar informações de arquivos. Designe esta função aos administradores assistentes responsáveis por replicar arquivos do servidor de Administração principal para outros servidores de Administração nos computadores cliente do MMS e do DRA.

Redefinir senha do administrador local

Fornece todos os poderes para redefinir a senha da conta de administrador local e exibir o nome do administrador do computador. Designe esta função aos administradores assistentes responsáveis pelo gerenciamento de contas de administrador.

Autoadministração

Fornece todos os poderes necessários para modificar propriedades básicas, como números de telefone, de sua própria conta do usuário. Designe esta função aos administradores assistentes para permitir que eles gerenciem suas próprias informações pessoais.

Gerenciamento avançado de consultas

Executar consultas avançadas

Fornece todos os poderes necessários para executar consultas avançadas gravadas. Designe esta função aos administradores assistentes responsáveis pela execução de consultas avançadas.

Gerenciar consultas avançadas

Fornece todos os poderes necessários para criar, gerenciar e executar consultas avançadas. Designe esta função aos administradores assistentes responsáveis pelo gerenciamento de consultas avançadas.

Gerenciamento de auditoria

Auditar todos os objetos

Fornece todos os poderes necessários para ver propriedades de objetos, políticas e configurações em toda a sua empresa. Esta função não permite que um administrador assistente modifique propriedades. Designe esta função aos administradores assistentes responsáveis pelas ações de auditoria em toda a sua empresa. Permite que os administradores assistentes vejam todos os nós, exceto o nó de Ferramentas Personalizadas.

Conta limitada de auditoria e propriedades do recurso

Fornece poderes para todas as propriedades do objeto.

Recursos de auditoria

Fornece todos os poderes necessários para ver propriedades de recursos gerenciados. Designe esta função aos administradores assistentes responsáveis pela auditoria de objetos de recursos.

Auditar usuários e grupos

Fornece todos os poderes necessários para exibir a conta do usuário e as propriedades do grupo, mas sem poderes para modificar essas propriedades. Designe esta função aos administradores assistentes responsáveis pela auditoria de propriedades de contas.

Gerenciamento do computador

Administração do computador

Fornece todos os poderes necessários para modificar as propriedades do computador. Esta função permite que os administradores assistentes adicionem, apaguem e encerrem computadores, além de sincronizar os controladores de domínio. Designe esta função aos administradores assistentes responsáveis pelo gerenciamento de computadores na Tela Ativa.

Criar e apagar contas de computador

Fornece todos os poderes necessários para criar e apagar uma conta de computador. Designe esta função aos administradores assistentes responsáveis pelo gerenciamento de computadores.

Gerenciar propriedades do computador

Fornece todos os poderes necessários para gerenciar todas as propriedades de uma conta de computador. Designe esta função aos administradores assistentes responsáveis pelo gerenciamento de computadores.

Exibir todas as propriedades do computador

Fornece todos os poderes necessários para ver propriedades de uma conta de computador. Designe esta função aos administradores assistentes responsáveis pela auditoria de computadores.

Gerenciamento do Exchange

Clonar usuário com caixa de correio

Fornece todos os poderes necessários para clonar uma conta do usuário existente junto com a caixa de correio da conta. Designe esta função aos administradores assistentes responsáveis pelo gerenciamento de contas de usuários.

Observação: Para permitir que o administrador assistente adicione a nova conta do usuário a um grupo durante a tarefa de clonagem, designe também a função Gerenciar Associações de Grupo.

Criar e apagar caixa de correio de recursos

Fornece todos os poderes necessários para criar e apagar uma caixa de correio. Designe esta função aos administradores assistentes responsáveis pelo gerenciamento de caixas de correio.

Administração de caixa de correio

Fornece todos os poderes necessários para gerenciar as propriedades da caixa de correio do Microsoft Exchange. Se você usa o Microsoft Exchange, designe esta função aos administradores assistentes responsáveis pelo gerenciamento de caixas de correio do Microsoft Exchange.

Gerenciar os direitos da caixa de correio do Exchange

Fornece todos os poderes necessários para gerenciar a segurança e os direitos das caixas de correio do Microsoft Exchange. Se você usa o Microsoft Exchange, designe esta função aos administradores assistentes responsáveis pelo gerenciamento de permissões de caixa de correio do Microsoft Exchange.

Gerenciar e-mail do grupo

Fornece todos os poderes necessários para exibir, habilitar ou desabilitar o endereço de e-mail de um grupo. Designe esta função aos administradores assistentes responsáveis pelo gerenciamento de grupos ou endereços de e-mail para objetos conta.

Gerenciar solicitações de movimentação de caixa de correio

Fornece todos os poderes necessários para gerenciar solicitações de movimentação de caixa de correio.

Gerenciar propriedades da caixa de correio de recursos

Fornece todos os poderes necessários para gerenciar todas as propriedades de uma caixa de correio. Designe esta função aos administradores assistentes responsáveis pelo gerenciamento de caixas de correio.

Gerenciar e-mail do usuário

Fornece todos os poderes necessários para exibir, habilitar ou desabilitar o endereço de e-mail de uma conta do usuário. Designe esta função aos administradores assistentes responsáveis pelo gerenciamento de contas de usuários ou endereços de e-mail para objetos conta.

Redefinir as propriedades do PIN da colaboração unificada

Fornece todos os poderes necessários para redefinir as propriedades do PIN da colaboração unificada para contas do usuário.

Administração de caixa de correio de recursos

Fornece todos os poderes necessários para gerenciar caixas de correio de recursos.

Administração de caixa de correio compartilhadas

Fornece todos os poderes necessários para criar, modificar, apagar e exibir as propriedades de suas caixas de correio compartilhadas. Designe esta função a todos os administradores assistentes responsáveis pelo gerenciamento de caixas de correio compartilhadas.

Exibir todas as propriedades da caixa de correio de recursos

Fornece todos os poderes necessários para ver propriedades de uma caixa de correio de recursos. Designe esta função aos administradores assistentes responsáveis pela auditoria de caixas de correio dos recursos.

Gerenciamento de grupos

Criar e apagar grupos

Fornece todos os poderes necessários para criar e apagar um grupo. Designe esta função aos administradores assistentes responsáveis pelo gerenciamento de grupos.

Administração de grupo dinâmico

Fornece todos os poderes necessários para gerenciar grupos dinâmicos do Active Directory.

Administração do grupo

Fornece todos os poderes necessários para gerenciar grupos e associações a grupos e exibir as propriedades do usuário correspondentes. Designe esta função a administradores assistentes responsáveis pelo gerenciamento de grupos ou objetos de conta e recurso gerenciados por grupos.

Gerenciar grupos de distribuição dinâmica

Fornece todos os poderes necessários para gerenciar grupos distribuição dinâmica do Microsoft Exchange.

Gerenciar a segurança da participação do grupo

Fornece todos os poderes necessários para designar quem pode exibir e modificar associações de grupo do Microsoft Windows por meio do Microsoft Outlook

Gerenciar participações do grupo

Fornece todos os poderes necessários para adicionar e remover contas de usuários ou grupos de um grupo existente e exibir o grupo principal de uma conta do usuário ou computador. Designe esta função aos administradores assistentes responsáveis pelo gerenciamento de grupos e contas de usuários.

Gerenciar propriedades do grupo

Fornece todos os poderes necessários para gerenciar todas as propriedades de um grupo. Designe esta função aos administradores assistentes responsáveis pelo gerenciamento de grupos.

Gerenciar atribuições de grupo temporárias

Fornece todos os poderes necessários para criar e gerenciar atribuições de grupo temporárias. Designe esta função aos administradores assistentes responsáveis pelo gerenciamento de grupos.

Renomear grupo e modificar descrição

Fornece todos os poderes necessários para modificar o nome e a descrição de um grupo. Designe esta função aos administradores assistentes responsáveis pelo gerenciamento de grupos.

Exibir todas as propriedades do grupo

Fornece todos os poderes necessários para ver propriedades de um grupo. Designe esta função aos administradores assistentes responsáveis pela auditoria de grupos.

Gerenciamento do gerador de relatórios

Gerenciar Active Directory Collectors, DRA Collectors e Management Reporting Collectors

Fornece todos os poderes necessários para gerenciar Active Directory Collectors, DRA Collectors e Management Reporting Collectors para coleta de dados. Designe esta função aos administradores assistentes responsáveis pelo gerenciamento da configuração do gerador de relatórios.

Gerenciar Active Directory Collectors, DRA Collectors, Management Reporting Collectors e configuração do banco de dados

Fornece todos os poderes necessários para gerenciar Active Directory Collectors, DRA Collectors, Management Reporting Collectors e configuração de banco de dados para coleta de dados. Designe esta função aos administradores assistentes responsáveis pelo gerenciamento da configuração do banco de dados e do gerador de relatórios.

Gerenciar gerador de relatórios de UI

Fornece todos os poderes necessários para gerar e exportar relatórios de detalhes da atividade para usuários, grupos, contatos, computadores, unidades organizacionais, poderes, funções, Telas Ativas, impressoras publicadas e administradores assistentes. Designe esta função aos administradores assistentes responsáveis pela geração de relatórios.

Gerenciar configuração do banco de dados

Fornece todos os poderes necessários para gerenciar a configuração do banco de dados para relatórios de gerenciamento. Designe esta função aos administradores assistentes responsáveis pelo gerenciamento da configuração do banco de dados do gerador de relatórios.

Exibir Active Directory Collectors, DRA Collectors, Management Reporting Collectors e informações de configuração do banco de dados

Fornece todos os poderes necessários para exibir AD Collectors, AD Collectors, Management Reporting Collectors e informações de configuração do banco de dados.

Gerenciamento de recursos

Criar e apagar recursos

Fornece todos os poderes necessários para criar e apagar compartilhamentos e contas de computador e limpar registros de eventos. Designe esta função aos administradores assistentes responsáveis pelo gerenciamento de objetos de recursos e registros de eventos.

Gerenciar impressoras e trabalhos de impressão

Fornece todos os poderes necessários para gerenciar impressoras, filas de impressão e trabalhos de impressão. Para gerenciar trabalhos de impressão associados a uma conta do usuário, o serviço de impressão e a conta do usuário devem ser incluídos na mesma Tela Ativa. Designe esta função aos administradores assistentes responsáveis por manter as impressoras e gerenciar os trabalhos de impressão.

Gerenciar recursos para usuários gerenciados

Fornece todos os poderes necessários para gerenciar recursos associados a contas de usuários específicas. O administrador assistente e as contas de usuário devem ser incluídos na mesma Tela Ativa. Designe esta função aos administradores assistentes responsáveis pelo gerenciamento de objetos de recursos.

Gerenciar serviços

Fornece todos os poderes necessários para gerenciar serviços. Designe esta função aos administradores assistentes responsáveis pelo gerenciamento de serviços.

Gerenciar pastas compartilhadas

Fornece todos os poderes necessários para gerenciar pastas compartilhadas. Designe esta função aos administradores assistentes responsáveis pelo gerenciamento de pastas compartilhadas.

Administração de recurso

Fornece todos os poderes necessários para modificar propriedades de recursos gerenciados, incluindo recursos associados a qualquer conta do usuário. Designe esta função aos administradores assistentes responsáveis pelo gerenciamento de objetos de recursos.

Iniciar e parar recursos

Fornece todos os poderes necessários para pausar, iniciar, continuar ou parar um serviço, iniciar ou parar um dispositivo ou impressora, encerrar um computador ou sincronizar seus controladores de domínio. Também fornece todos os poderes necessários para pausar, continuar e iniciar serviços, parar dispositivos ou filas de impressão e encerrar computadores. Designe esta função aos administradores assistentes responsáveis pelo gerenciamento de objetos de recursos.

Gerenciamento de servidores

Programador integrado – somente uso interno

Fornece poderes para programar quando o DRA atualiza o cache.

Administração dos servidores do aplicativo

Fornece os poderes necessários para configurar, exibir e apagar configurações do servidor de aplicativos.

Configurar servidores e domínios

Fornece todos os poderes necessários para modificar as opções do servidor de administração e os domínios gerenciados. Também fornece os poderes necessários para configurar e gerenciar locatários do Azure. Designe esta função aos administradores assistentes responsáveis por monitorar e manter os servidores de Administração e gerenciar locatários do Azure.

Administração do servidor do histórico de mudança unificado

Fornece os poderes necessários para configurar, exibir e apagar configurações do servidor do histórico de mudança unificado.

Administração do servidor do Workflow Automation

Fornece os poderes necessários para configurar, exibir e apagar configurações do servidor do Workflow Automation.

Gerenciamento de contas do usuário

Criar e apagar contas de usuários

Fornece todos os poderes necessários para criar e apagar uma conta do usuário. Designe esta função aos administradores assistentes responsáveis pelo gerenciamento de contas de usuários.

Administração de Help Desk

Fornece todos os poderes necessários para exibir as propriedades da conta do usuário e mudar as senhas e as propriedades relacionadas à senha. Esta função também permite que os administradores assistentes desabilitem, habilitem e desbloqueiem contas de usuários. Designe esta função aos administradores assistentes responsáveis pelas funções do Suporte Técnico associadas à garantia de que os usuários tenham acesso adequado às suas contas.

Gerenciar discagem do usuário em propriedades

Fornece todos os poderes necessários para modificar a discagem nas propriedades de contas do usuário. Designe esta função aos administradores assistentes responsáveis pelo gerenciamento de contas de usuários que tenham acesso remoto à empresa.

Gerenciar senha do usuário e desbloquear conta

Fornece todos os poderes necessários para redefinir a senha, especificar configurações de senha e desbloquear uma conta do usuário. Designe esta função aos administradores assistentes responsáveis por manter o acesso à conta do usuário.

Gerenciar propriedades do usuário

Fornece todos os poderes necessários para gerenciar todas as propriedades de uma conta do usuário, incluindo as propriedades da caixa de correio do Microsoft Exchange. Designe esta função aos administradores assistentes responsáveis pelo gerenciamento de contas de usuários.

Renomear usuário e modificar descrição

Fornece todos os poderes necessários para modificar o nome e a descrição de uma conta do usuário. Designe esta função aos administradores assistentes responsáveis pelo gerenciamento de contas de usuários.

Redefinir senha

Fornece todos os poderes necessários para redefinir e modificar senhas. Designe esta função aos administradores assistentes responsáveis pelo gerenciamento de senhas.

Redefinir senha e desbloquear conta usando o SPA

Fornece todos os poderes necessários para usar o Administrador de Senha Segura para redefinir senhas e desbloquear contas do usuário.

Transformar um usuário

Fornece todos os poderes necessários para adicionar ou remover um usuário de grupos encontrados em uma conta de gabarito, incluindo a capacidade de modificar as propriedades do usuário enquanto transforma o usuário.

Administração de usuários

Fornece todos os poderes necessários para gerenciar contas do usuário, caixas de correio do Microsoft Exchange associadas e propriedade do grupo. Designe esta função aos administradores assistentes responsáveis pelo gerenciamento de contas de usuários.

Exibir todas as propriedades do usuário

Fornece todos os poderes necessários para ver propriedades de uma conta do usuário. Designe esta função aos administradores assistentes responsáveis pela auditoria de contas de usuários.

Administração do WTS

Gerenciar propriedades do ambiente WTS

Fornece todos os poderes necessários para mudar as propriedades do ambiente WTS para uma conta do usuário. Designe esta função aos administradores assistentes responsáveis por manter o ambiente WTS ou gerenciar contas de usuários.

Gerenciar propriedades do controle remoto do WTS

Fornece todos os poderes necessários para mudar as propriedades do controle remoto do WTS para uma conta do usuário. Designe esta função aos administradores assistentes responsáveis pela manutenção do acesso ao WTS ou pelo gerenciamento de contas de usuários.

Gerenciar propriedades da sessão do WTS

Fornece todos os poderes necessários para mudar as propriedades da sessão do WTS para uma conta do usuário. Designe esta função aos administradores assistentes responsáveis pela manutenção de sessões do WTS ou pelo gerenciamento de contas de usuários.

Gerenciar propriedades do terminal do WTS

Fornece todos os poderes necessários para mudar as propriedades do terminal do WTS para uma conta do usuário. Designe esta função aos administradores assistentes responsáveis pela manutenção de propriedades do terminal do WTS ou pelo gerenciamento de contas de usuários.

Administração do WTS

Fornece todos os poderes necessários para gerenciar as propriedades do Windows Terminal Server (WTS) para contas do usuário na Tela Ativa. Se você usa o WTS, designe esta função aos administradores assistentes responsáveis por manter as propriedades do WTS das contas de usuários.

Acessando funções integradas

Acesse funções integradas para auditar o modelo de delegação padrão ou gerenciar suas próprias configurações de segurança.

Para acessar funções integradas:

1. Acesse **Delegation Management** > **Manage Roles** (Gerenciamento de Delegação > Gerenciar Funções).
2. Verifique se o campo de pesquisa está em branco e clique em **Find Now** (Localizar Agora) no painel **List items that match my criteria** (Listar itens que correspondem aos meus critérios).
3. Selecione a função apropriada.

Usando funções integradas

Não é possível apagar nem modificar funções integradas. No entanto, você pode incorporar as funções integradas ao modelo de delegação existente ou usar essas funções para projetar e implementar seu próprio modelo.

Você pode usar funções integradas das seguintes maneiras:

- Associe uma função incorporada a uma conta do usuário ou um grupo de administradores assistentes. Essa associação fornece ao usuário ou aos membros do grupo de administradores assistentes os poderes apropriados para a tarefa.
- Clone uma função integrada e use esse clone como base para uma função personalizada. Você pode adicionar outras funções ou poderes a essa nova função e remover poderes originalmente incluídos na função integrada.

Para obter mais informações sobre como criar um modelo de delegação dinâmica, consulte Entendendo o modelo de delegação dinâmica.

Criando funções personalizadas

Ao criar uma função, você pode delegar rápida e facilmente um conjunto de poderes que representa uma tarefa administrativa ou um workflow. Você cria e gerencia funções do **Delegation Management** (Gerenciamento de Delegação) > nó **Funções** no console de Delegação e Configuração. Neste nó, você pode fazer o seguinte:

- Criar novas funções
- Clonar funções existentes
- Modificar propriedades da função
- Apagar funções
- Gerenciar atribuições de funções
  - Delegar uma nova designação
  - Remover uma designação existente
  - Ver propriedades de um administrador assistente atribuído
  - Ver propriedades de uma Tela Ativa atribuída
- Gerenciar as funções e os poderes em uma função (funções podem ser aninhadas)
- Gerar relatórios de mudança de função

O workflow geral para executar qualquer uma das ações identificadas nesta seção é selecionar o nó **Funções** e seguir um destes procedimentos:

- Use **Tarefas** ou o menu de clique com o botão direito do mouse para abrir o assistente ou a caixa de diálogo aplicável para executar a ação necessária.
- Localize o objeto da função no painel **List items that match my criteria** (Listar itens que correspondem aos meus critérios) e use **Tarefas** ou o menu de clique com o botão direito do mouse para selecionar e abrir o assistente ou a caixa de diálogo aplicável para executar a ação necessária.

Para executar qualquer uma das ações acima, você deve ter os poderes apropriados, como aqueles incluídos na função Gerenciar Modelo de Segurança.

9 Poderes

Os poderes são os blocos de construção iniciais para a administração de “privilégios mínimos”. Atribuir poderes aos usuários ajuda você a implementar e manter seu modelo de segurança dinâmico. Você executa esses procedimentos no console de Delegação e Configuração.

Poderes integrados

Existem mais de 390 poderes integrados para gerenciar objetos e executar tarefas administrativas comuns com as quais você pode trabalhar ao definir funções e fazer atribuições de delegação. Poderes integrados não podem ser apagados, mas você pode cloná-los para criar poderes personalizados. Alguns exemplos de poderes integrados estão incluídos abaixo:

Criar Grupo e Modificar Todas as Propriedades

Fornece o poder de criar grupos e especificar todas as propriedades durante a criação do grupo.

Apagar conta do usuário

Se a Lixeira estiver habilitada, fornecerá a capacidade de mover as contas do usuário para a Lixeira. Se a Lixeira estiver desabilitada, fornecerá a capacidade de apagar permanentemente as contas do usuário.

Modificar todas as propriedades do computador

Fornece o poder de modificar todas as propriedades para contas de computador.

Implementando poderes personalizados

Para criar um poder personalizado, você cria um novo poder ou clona um poder existente. Você pode usar um poder existente como um gabarito para novas delegações de poder. Um poder define as propriedades de um objeto que um administrador assistente pode exibir, modificar ou criar em seu domínio gerenciado ou subárvore. Poderes personalizados podem incluir acesso a várias propriedades, como o poder *Exibir Todas as Propriedades do Usuário*.

Observação: Não é possível clonar todos os poderes integrados.

Você implementa poderes personalizados do **Delegation Management** (Gerenciamento de Delegação) > nó **Poderes** no console de Delegação e configuração. Neste nó, você pode fazer o seguinte:

- Exibir todas as propriedades do poder
- Criar novos poderes
- Clonar poderes existentes
- Modificar poderes personalizados
- Gerar relatórios de mudança de poder

Para executar essas ações, você deve ter os poderes apropriados, como aqueles incluídos na função Gerenciar Modelo de Segurança.

Considere o seguinte processo antes de tentar criar um novo poder.

1. Revise os poderes fornecidos com o DRA.
2. Decida se você precisa de um poder personalizado. Se aplicável, você pode clonar um poder personalizada existente.
3. Conclua os procedimentos apropriados orientados por assistente. Por exemplo, conclua o assistente New Power (Novo Poder).
4. Veja seu novo poder.
5. Modifique seu novo poder, se necessário.

O workflow geral para executar qualquer uma das ações identificadas nesta seção é selecionar o nó **Capacidades** e realizar um dos seguintes procedimentos:

- Use Tarefas ou o menu de clique com o botão direito do mouse para abrir o assistente ou a caixa de diálogo aplicável para executar a ação necessária.
- Encontre o objeto de capacidade no painel **List items that match my criteria** (Listar itens que correspondem aos meus critérios) e use **Tarefas** ou o menu de clique com o botão direito do mouse para selecionar e abrir o assistente ou a caixa de diálogo aplicável para executar a ação necessária.

Estendendo poderes

Você pode adicionar permissões ou funcionalidades a um poder estendendo esse poder.

Por exemplo, para permitir que um administrador assistente crie uma conta do usuário, você pode designar o poder *Criar Usuário e Modificar Todas as Propriedades* ou o poder *Criar Usuário e Modificar Propriedades Limitadas*. Se você designar também o poder *Adicionar Novo Usuário ao Grupo*, o administrador assistente poderá adicionar essa nova conta do usuário a um grupo enquanto usa o assistente Criar Usuário. Neste caso, o poder *Adicionar Novo Usuário ao Grupo* fornece um recurso adicional do assistente. O poder *Adicionar Novo Usuário ao Grupo* é o **poder de extensão**.

Poderes de extensão não podem adicionar permissões ou funcionalidade por si mesmos. Para delegar com êxito uma tarefa que inclua uma extensão de poder, você deve atribuir o poder de extensão junto com o poder que deseja estender.

Observação

- Para criar um grupo com êxito e incluir o novo grupo em uma Tela Ativa, você deve ter o poder *Adicionar Novo Grupo à Tela Ativa* na Tela Ativa especificada. A Tela Ativa especificada também deve incluir a OU ou o container integrado que conterá o novo grupo.
- Para clonar com sucesso um grupo e incluir o novo grupo em uma Tela Ativa, você deve ter a capacidade *Add Cloned Group to ActiveView* (Adicionar o grupo clonado à Tela Ativa) na Tela Ativa especificada. A Tela Ativa especificada também deve incluir o grupo de origem, bem como a OU ou o container integrado que conterá o novo grupo.

A tabela a seguir lista alguns exemplos de ações que são configuráveis ao criar um novo poder ou modificar as propriedades de um poder existente:

Para delegar esta tarefa	**Atribuir esta capacidade**	**E esta capacidade de extensão**
Clonar um grupo e incluir o novo grupo em uma Tela Ativa especificada	Clonar Grupo e Modificar Todas as Propriedades	Adicionar Grupo Clonado à Tela Ativa
Criar um grupo e incluir o novo grupo em uma Tela Ativa especificada	Criar Grupo e Modificar Todas as Propriedades	Adicionar Novo Grupo à Tela Ativa
Criar um contato habilitado para e-mail	Criar Contato e Modificar Todas as Propriedades Criar Contato e Modificar Propriedades Limitadas	Habilitar E-mail para Novo Contato
Criar um grupo habilitado para e-mail	Criar Grupo e Modificar Todas as Propriedades	Habilitar E-mail para Novo Grupo
Criar uma conta do usuário habilitada para e-mail	Criar Usuário e Modificar Todas as Propriedades Criar Usuário e Modificar Propriedades Limitadas	Habilitar E-mail para novo Usuário
Criar uma conta do usuário e adicionar a nova conta a grupos específicos	Criar Usuário e Modificar Todas as Propriedades Criar Usuário e Modificar Propriedades Limitadas	Adicionar Novo Usuário ao Grupo

10 Designações de Delegação

Você gerencia as designações de delegação do nó **Delegation Management** (Gerenciamento de Delegação) > nó **Admin Assistente** no console de Delegação e Configuração. Neste nó, você pode ver os poderes e as funções atribuídos a administradores assistentes e gerenciar as atribuições de funções e Telas Ativas. Você também pode fazer o seguinte com os grupos de Admin Assistente:

- Adicionar membros ao grupo
- Criar grupos
- Clonar grupos
- Apagar grupos
- Modificar propriedades do grupo

Para exibir e gerenciar atribuições e fazer mudanças nos grupos de Admin Assistentes, você deve ter os poderes apropriados, como aqueles incluídos na função Gerenciar Modelo de Segurança.

O workflow geral para executar qualquer uma das ações identificadas nesta seção é selecionar o nó **Admins Assistentes** e executar uma das seguintes ações:

- Use Tarefas ou o menu de clique com o botão direito do mouse para abrir o assistente ou a caixa de diálogo aplicável para executar a ação necessária.
- Encontre o grupo ou administrador assistente no painel **List items that match my criteria** (Listar itens que correspondem aos meus critérios) e use **Tarefas** ou o menu de clique com o botão direito do mouse para selecionar e abrir o assistente ou a caixa de diálogo aplicável para executar a ação necessária.

IV Configuração de componentes e processos

Este capítulo fornece informações para configurar o DRA pela primeira vez, incluindo servidores e personalizações de servidores, consoles e personalizações de console, administração do Azure, administração de Pasta Pública e conexão com servidores.

11 Configuração inicial

Esta seção descreve as etapas de configuração necessárias se você estiver instalando o Directory and Resource Administrator pela primeira vez.

Lista de verificação de configuração

Use a lista de verificação a seguir para guiá-lo na configuração do DRA para a primeira utilização.

Etapas	Mais informações
Instalar uma licença do DRA	Use o Utilitário de Verificação de Saúde para aplicar uma licença do DRA. Para obter mais informações sobre licenças do DRA, veja Requisitos para licenciamento.
Configurar os recursos e os servidores DRA	Configure MMS, exceções de clone, replicação de arquivos, Marcação de Eventos, caching, AD LDS, grupos dinâmicos, Lixeira, gerador de relatórios, Histórico de Mudanças Unificado e Servidor de Workflow.
Configurar o Gerador de Relatórios de Histórico de Mudanças(opcional)	Configure o Gerador de Relatórios de Histórico de Mudanças se quiser integrar a um Servidor do Change Guardian para coletar dados de histórico de mudanças para eventos de usuários tanto internos quanto externos ao DRA.
Configurar os Serviços de DRA para uma conta gMSA(opcional)	Configure os Serviços do DRA para uma gMSA (Conta de Serviço Gerenciado do grupo) se quiser gerenciar o protocolo de autenticação em vários servidores versus um único servidor.
Configurar o Cliente de Delegação e Configuração	Configure o modo como os itens são acessados e exibidos no Cliente de Delegação e Configuração.
Configurar o Cliente da Web	Configure o logout automático, certificados, conexões de servidor e componentes de autenticação

Instalar ou fazer upgrade de licenças

O DRA requer um arquivo de chave de licença. Esse arquivo contém suas informações de licença e está instalado no servidor de Administração. Após instalar o servidor de administração, use o Utilitário de Verificação de Saúde para instalar sua licença comprada. Se necessário, uma chave de licença de avaliação (`TrialLicense.lic`) também é fornecida com o pacote de instalação que permite o gerenciamento de um número ilimitado de contas de usuário e caixas de correio por 30 dias.

Para fazer upgrade de uma licença de avaliação ou de uma licença existente, abra o Console de Delegação e Configuração e navegue até **Configuration Management** > **Update License** (Gerenciamento de Configurações > Atualizar Licença). Ao fazer upgrade da sua licença, faça upgrade do arquivo de licença em cada servidor de Administração.

Você pode ver sua licença do produto no Console de Delegação e Configuração. Para ver a licença do seu produto, acesse o menu **File** (Arquivo) > **DRA Properties** (Propriedades do DRA) > **License** (Licença).

Configurar os recursos e servidores do DRA

O gerenciamento de acesso com menos privilégios para tarefas do Active Directory usando o DRA tem muitos componentes e processos que precisam ser configurados. Isso inclui configurações gerais e de componentes do cliente. Esta seção fornece informações sobre os componentes e processos gerais que precisam ser configurados para o DRA.

Configurar o conjunto multimaster

Um ambiente MMS usa vários servidores de administração para gerenciar o mesmo conjunto de domínios e servidores membros. Um MMS consiste em um servidor de administração principal e vários servidores de administração secundários.

O modo padrão para o servidor de Administração é Principal. Ao adicionar servidores secundários ao seu ambiente MMS, lembre-se de que um servidor de Administração secundário pode pertencer a apenas um conjunto de servidores.

Para verificar se cada servidor no conjunto está gerenciando os mesmos dados, sincronize periodicamente os servidores secundários com o servidor de Administração principal. Para reduzir a manutenção, use a mesma conta de serviço para todos os servidores de Administração na floresta de domínio.

Importante

- Ao instalar o servidor secundário, selecione **Servidor de Administração Secundário** no instalador.
- A versão do DRA do novo servidor secundário deve ser a mesma do servidor principal do DRA de modo que todos os recursos que estão disponíveis no servidor principal também estejam disponíveis no servidor secundário.

- "Adicionando um servidor de administração secundário" na página 91
- "Promovendo um servidor de Administração secundário" na página 92
- "Retrocedendo um servidor de Administração principal" na página 93
- "Programando a sincronização" na página 93

Adicionando um servidor de administração secundário

Você pode adicionar um Servidor de administração secundário a um MMS existente no cliente de Delegação e Configuração.

Observação: Para adicionar com sucesso um novo servidor secundário, você precisa primeiro instalar o produto Directory and Resource Administrator no computador do servidor de Administração. Para obter mais informações, veja Instalar o Servidor de administração DRA.

Para adicionar um Servidor de administração secundário:

1. Clique o botão direito do mouse em **Administration Servers** (Servidores de administração) no nó Gerenciamento de Configurações e selecione **Add Secondary Server** (Adicionar um servidor secundário).
2. No Assistente Adicionar Servidor Secundário, clique em Próximo.
3. Na guia Servidor secundário, especifique o nome do Servidor de administração secundário que deseja adicionar ao MMS.

4 Na guia Conta de acesso, especifique uma conta de serviço do Servidor de administração secundário. O DRA usa essa conta apenas para adicionar o Servidor de administração secundário ao MMS.

5 Na guia Multi-Master access (Conta de acesso multimaster), especifique uma conta de acesso a ser usada pelo Servidor de administração primário para operações do MMS. Recomenda-se não usar a conta de serviço do Servidor de administração secundário como a Conta de acesso multimaster. Você pode especificar qualquer conta do usuário do domínio associado ao Servidor de administrador secundário. A Conta de acesso multimaster deve fazer parte do grupo de Administradores Locais no servidor secundário. Se a Conta de acesso multimaster não tiver privilégios suficientes para realizar operações de MMS, o Servidor DRA delegará automaticamente as capacidades necessárias para a Conta de acesso multimaster.

Promovendo um servidor de Administração secundário

Você pode promover um servidor de Administração secundário para um servidor de Administração principal. Quando você promove um servidor de Administração secundário para um servidor de Administração principal, o servidor de Administração principal existente se torna um servidor de Administração secundário no conjunto de servidores. Para promover um servidor de Administração secundário, você precisa ter os poderes apropriados, como aqueles incluídos na função Configurar Servidores e Domínios incorporados. Antes de promover um servidor de Administração secundário, sincronize o MMS para que ele tenha a configuração mais recente.

Para obter informações sobre como sincronizar o MMS, consulte Programando a sincronização.

Observação: Um servidor principal recém-promovido só pode se conectar a servidores secundários que estavam disponíveis durante o processo de promoção. Se um servidor secundário ficar não disponível durante o processo de promoção, entre em contato com o Suporte técnico.

Para promover um servidor de Administração secundário:

1 Navegue até o nó **Configuration Management** > **Administration Servers** (Gerenciamento de Configurações > Servidores de Administração).

2 No painel direito, selecione o servidor de Administração secundário que você deseja promover.

3 No menu Tarefas, clique em **Advanced** (Avançado) > **Promote Server** (Promover Servidor).

Importante: Quando a conta de Serviço do Servidor secundário é diferente do Servidor principal ou o Servidor secundário está instalado em um domínio diferente do Servidor principal (Domínios confiáveis/domínios não confiáveis) e você promove o Servidor secundário, delegue as seguintes funções antes de promover o Servidor secundário: **Audit All Objects** (Auditar Todos os Objetos), **Configure Servers and Domains** (Configurar Servidores e Domínios) e **Generate UI Reports** (Gerar Relatórios de Interface do Usuário). Em seguida, verifique se as sincronizações do MMS foram bem-sucedidas.

Retrocedendo um servidor de Administração principal

Você pode retroceder um servidor de Administração principal para um servidor de Administração secundário. Para retroceder um servidor de Administração principal, você deve ter os poderes apropriados, como aqueles incluídos na função integrada Configurar Servidores e Domínios.

Para retroceder um servidor de Administração principal:

1. Navegue até o nó **Configuration Management** > **Administration Servers** (Gerenciamento de Configurações > Servidores de Administração).
2. No painel direito, selecione o servidor de Administração principal que você deseja retroceder.
3. No menu Tarefas, clique em **Advanced** (Avançado) > **Demote Server** (Retroceder Servidor).
4. Especifique o computador que você deseja designar como o novo servidor de Administração principal e clique em **OK**.

Programando a sincronização

A sincronização garante que todos os servidores de Administração no MMS usem os mesmos dados de configuração. Embora você possa sincronizar manualmente os servidores a qualquer momento, a programação padrão é definida para sincronizar o MMS a cada 4 horas. Você modifica essa programação para adaptá-la às necessidades de sua empresa.

Para modificar a programação de sincronização ou para sincronizar manualmente os servidores do MMS, você precisa ter os poderes apropriados, como aqueles incluídos na função integrada Configurar Servidores e Domínios.

Para acessar a programação de sincronização ou para sincronizações manuais, acesse **Configuration Management** (Gerenciamento de Configurações) > **Administration Servers** (Servidores de Administração) e use o menu **Tarefas** ou clique o botão direito do mouse nas opções em um servidor selecionado. A programação de sincronização está nas Propriedades de um servidor selecionado.

Entendendo as opções de sincronização

Existem basicamente quatro opções diferentes para sincronizar servidores do MMS:

- Selecionar o servidor principal e sincronizar todos os servidores secundários “Synchronize All Servers” (Sincronizar Todos os Servidores)
- Selecionar um servidor secundário e sincronizar apenas esse servidor
- Configurar a programação de sincronização para servidores principais e secundários de modo independente
- Configure a programação de sincronização para todos os servidores. Essa opção é habilitada quando você tem a seguinte configuração selecionada na programação de sincronização do servidor principal:

  Configure secondary Administration servers when refreshing the primary Administration server (Configurar servidores de Administração secundários ao atualizar o servidor de Administração principal)

  Observação: Se você desmarcar essa opção, os arquivos de configuração serão copiados para os servidores secundários na programação principal, mas não serão carregados pelo secundário naquele momento; eles serão carregados com base na programação configurada no servidor

secundário. Isso é útil se os servidores estão em fusos horários diferentes. Por exemplo, você pode configurar todos os servidores para atualizar suas configurações no meio da noite, mesmo que esse seja um horário diferente por causa dos fusos horários.

Gerenciando exceções de clonagem

As exceções de clonagem permitem que você defina propriedades para usuários, grupos, contatos e computadores que não serão copiados quando um desses objetos for clonado.

Com os poderes apropriados, você pode gerenciar as exceções de clonagem. A função Manage Clone Exceptions (Gerenciar Exceções de Clonagem) concede poderes para ver, criar e apagar exceções de clonagem.

Para exibir ou apagar uma exceção de clonagem existente ou para criar uma nova exceção de clonagem, navegue até **Configuration Management** (Gerenciamento de Configurações) > **Clone Exceptions** (Exceções de Clonagem) > **Tarefas** ou até o menu de clique com o botão direito do mouse.

Replicação de arquivo

Quando você cria ferramentas personalizadas, pode ser necessário instalar arquivos de suporte usados pela ferramenta personalizada no computador do Console de Delegação e Configuração do DRA antes que ela possa ser executada. Você pode usar os recursos de replicação de arquivos DRA para replicar rápida e facilmente os arquivos de suporte de ferramentas personalizadas do servidor de Administração principal para os servidores de Administração secundários no MMS, bem como para os computadores cliente do DRA. A replicação de arquivos também pode ser usada para replicar scripts acionadores de servidores principais para secundários.

Os recursos Ferramentas personalizadas e Replicação de arquivos só estão disponíveis no Console de Delegação e Configuração.

Você pode usar ferramentas personalizadas e replicação de arquivos para verificar se os computadores cliente do DRA podem acessar arquivos de ferramentas personalizadas. O DRA replica arquivos de ferramentas personalizadas para servidores de Administração secundários para garantir que os computadores cliente do DRA conectando-se a servidores de Administração secundários possam acessar ferramentas personalizadas.

O DRA replica os arquivos da ferramenta personalizada no servidor de Administração principal para servidores de Administração secundários durante o processo de sincronização do MMS. O DRA faz o download dos arquivos de ferramentas personalizadas para computadores cliente do DRA quando eles se conectam aos servidores de Administração.

Observação: O DRA faz o download dos arquivos da ferramenta personalizada para o seguinte local nos computadores cliente do DRA:

{DRAInstallDir}\{MMS ID}\Download

MMSID é a identificação do conjunto multimaster do qual o DRA faz o download dos arquivos da ferramenta personalizada.

- "Fazendo upload de arquivos da ferramenta personalizada para replicação" na página 95
- "Replicando vários arquivos entre servidores de administração" na página 96
- "Replicando vários arquivos para computadores cliente do DRA" na página 96

Fazendo upload de arquivos da ferramenta personalizada para replicação

Ao fazer o upload de arquivos para o servidor de Administração principal, você especifica os arquivos dos quais deseja fazer upload e replicar entre o servidor de Administração principal e todos os servidores de Administração secundários no conjunto do MMS. O DRA permite fazer o upload de arquivos de biblioteca, arquivos de script e arquivos executáveis.

A função Replicar Arquivos permite replicar arquivos do servidor de Administração principal para os servidores de Administração secundários nos computadores cliente do DRA e também do MMS. A função Replicar Arquivo contém os seguintes poderes:

- **Apagar Arquivos do Servidor:** Esse poder permite que o DRA apague arquivos que não existem mais no servidor de Administração principal, em servidores de Administração secundários e em computadores cliente do DRA.
- **Definir Informações do Arquivo:** Esse poder permite que o DRA atualize as informações do arquivo para arquivos nos servidores de Administração secundários.
- **Fazer Upload dos Arquivos para o Servidor:** Esse poder permite que o DRA faça upload de arquivos do computador cliente do DRA para o servidor de Administração principal.

Observação: Você pode fazer upload de apenas um arquivo para replicação por vez usando a interface do usuário de Replicação de Arquivos no console de Delegação e Configuração.

Para fazer upload de um arquivo de ferramentas personalizadas para o servidor de Administração principal:

1. Navegue até **Configuration Management** (Gerenciamento de Configurações) > **File Replication** (Replicação de Arquivo).
2. No menu Tarefas, clique em **Upload File** (Fazer Upload do Arquivo).
3. Para pesquisar pelo arquivo cujo upload você deseja realizar e selecioná-lo, clique em **Browse** (Procurar).
4. *Se você deseja fazer download do arquivo selecionado para todos os computadores cliente do DRA*, marque a caixa de seleção **Download to all client computers** (Fazer download para todos os computadores cliente).
5. *Se você deseja registrar uma biblioteca COM*, marque a caixa de seleção **Register COM library** (Registrar biblioteca COM).
6. Clique em **OK**.

Observação

- O DRA faz upload do arquivo de script ou dos arquivos de suporte que precisam ser replicados para outros servidores de Administração secundários para a pasta *{DRAInstallDir}*\FileTransfer\Replicate no servidor de Administração principal. A pasta *{DRAInstallDir}*\FileTransfer\Replicate também é chamada de *{DRA_Replicated_Files_Path}*.
- O DRA carrega o arquivo de script ou os arquivos de suporte que precisam ser replicados para os computadores cliente do DRA para a pasta *{DRAInstallDir}* FileTransfer\Download no servidor de Administração principal.
- O arquivo de ferramenta personalizado carregado no servidor de Administração principal é distribuído aos servidores de Administração secundários durante a próxima sincronização programada ou por sincronização manual.

Replicando vários arquivos entre servidores de administração

Se tiver vários arquivos dos quais deseja fazer upload e que deseja replicar entre o servidor de Administração principal e os servidores de Administração secundários no MMS, você poderá fazer manualmente o upload desses arquivos para replicação copiando-os para o diretório de replicação do servidor de administração principal, que está no seguinte local:

{DRAInstallDir}\FileTransfer\Replicate

O diretório de replicação é criado quando o DRA é instalado.

O servidor de Administração identifica automaticamente os arquivos no diretório de replicação e os replica entre os servidores de Administração durante a próxima sincronização programada. Após a sincronização, o DRA exibe os arquivos carregados na janela File Replication (Replicação de Arquivos) no console de Delegação e Configuração.

Observação: Se você quiser replicar arquivos que contenham bibliotecas COM que devem ser registradas, não será possível copiar manualmente os arquivos para o diretório de replicação do servidor de Administração. Você precisa usar o console de Delegação e Configuração para fazer o upload de cada arquivo e registrar a biblioteca COM.

Replicando vários arquivos para computadores cliente do DRA

Se você tiver vários arquivos que deseja replicar entre o servidor de Administração principal e os computadores cliente do DRA, poderá copiá-los para o diretório de replicação do cliente no servidor de Administração principal, que está no seguinte local:

{DRAInstallDir}\FileTransfer\Download

O diretório de replicação do cliente é criado quando o DRA é instalado.

O servidor de Administração identifica automaticamente os arquivos na pasta Download e os replica para os servidores de Administração secundários durante a próxima sincronização programada. Após a sincronização, o DRA exibe os arquivos carregados na janela File Replication (Replicação de Arquivos) no console de Delegação e Configuração. O DRA faz o download dos arquivos replicados para os computadores cliente do DRA na primeira vez que esses computadores se conectam aos servidores de Administração após a replicação.

Observação: Se você quiser replicar arquivos que contenham bibliotecas COM que devem ser registradas, não será possível copiar os arquivos para o diretório de download do servidor de Administração. Você precisa usar o console de Delegação e Configuração para fazer o upload de cada arquivo e registrar a biblioteca COM.

Sincronização do Azure

A Sincronização do Azure permite assegurar o uso obrigatório de caracteres inválidos e de políticas de comprimento de caracteres para evitar falhas na sincronização de diretórios. A seleção desta opção garantirá que todas as propriedades sincronizadas com o Azure Active Directory restrinjam caracteres inválidos e assegurem o uso obrigatório de limites de comprimento de caracteres.

Para habilitar a Sincronização do Azure:

1. No painel esquerdo, clique em **Configuration Management** (Gerenciamento de Configurações).
2. Em Common Tasks (Tarefas Comuns) no painel direito, clique em **Update Administration Server Options** (Atualizar Opções do Servidor de Administração).
3. Na guia Sincronização do Azure, selecione **Assegurar o uso obrigatório de políticas de caixa de correio online para caracteres inválidos e comprimento de caracteres**.

Habilitando vários gerentes para grupos

Quando você habilita o suporte de vários gerentes para gerenciar um grupo, um dos dois atributos padrão é usado para armazenar os gerentes do grupo. O atributo ao executar o Microsoft Exchange é o atributo `msExchCoManagedByLink`. O atributo padrão, quando o Microsoft Exchange não está em execução, é o atributo `nonSecurityMember`. A última opção pode ser modificada. No entanto, recomendamos que você contate o suporte técnico para determinar um atributo apropriado se precisar mudar essa configuração.

Para habilitar o suporte a vários gerentes para grupos:

1. No painel esquerdo, clique em **Configuration Management** (Gerenciamento de Configurações).
2. Em Common Tasks (Tarefas Comuns) no painel direito, clique em **Update Administration Server Options** (Atualizar Opções do Servidor de Administração).
3. Na guia Enable Support for Group Multiple Managers (Habilitar Suporte para Gerentes de Vários Grupos), marque a caixa de seleção **Enable support for group's multiple managers** (Habilitar suporte para gerentes de vários grupos).

Comunicações criptografadas

Esta função permite habilitar ou desabilitar o uso de comunicação criptografada entre o cliente de Delegação e Configuração e o servidor de Administração. Por padrão, o DRA criptografa senhas de contas. Esse recurso não criptografa as comunicações do Cliente da Web nem do PowerShell, que são tratadas separadamente por certificados do servidor.

Usar comunicações criptografadas pode afetar o desempenho. A comunicação criptografada está desativada por padrão. Se você habilitar essa opção, os dados serão criptografados durante a comunicação entre as interfaces do usuário e o servidor de Administração. O DRA usa a criptografia padrão da Microsoft para a Chamada de Procedimento Remoto (RPC).

Para habilitar as comunicações criptografadas, acesse **Configuration Management** (Gerenciamento de Configurações) > **Update Administration Server Options** (Atualizar Opções do Servidor de Administração) > guia **General** (Geral) e marque a caixa de seleção **Encrypted Communications** (Comunicações Criptografadas).

Observação: Para criptografar todas as comunicações entre o servidor de Administração e as interfaces do usuário, você precisa ter os poderes apropriados, como aqueles na função integrada Configurar Servidores e Domínios.

Definindo atributos virtuais

Usando atributos virtuais, você pode criar novas propriedades e associá-las a usuários, grupos, grupos de distribuição dinâmica, contatos, computadores e unidades organizacionais. Os atributos virtuais permitem que você crie novas propriedades sem precisar estender o esquema do Active Directory.

Usando atributos virtuais, você pode adicionar novas propriedades a objetos no Active Directory. Você só pode criar, habilitar, desabilitar, associar e desassociar atributos virtuais no servidor de Administração principal. O DRA armazena os atributos virtuais criados no AD LDS. O DRA replica atributos virtuais no servidor de Administração principal para servidores de administração secundários durante o processo de sincronização do MMS.

Com os poderes apropriados, você pode gerenciar atributos virtuais. A função Gerenciar Atributos Virtuais confere poderes para criar, habilitar, associar, desassociar, desabilitar e exibir atributos virtuais.

- “Criando atributos virtuais” na página 98
- “Associando atributos virtuais a objetos” na página 98
- “Desassociando atributos virtuais” na página 99
- “Desabilitando atributos virtuais” na página 99

Criando atributos virtuais

Você precisa do poder *Criar Atributos Virtuais* para criar atributos virtuais e do poder *Exibir Atributos Virtuais* para exibir atributos virtuais.

Para criar um atributo virtual, acesse **Configuration Management** (Gerenciamento de Configurações) > **Virtual Attributes** (Atributos Virtuais) > nó **Managed Attributes** (Atributos Gerenciados) e clique em **New Virtual Attribute** (Novo Atributo Virtual) no menu Tarefas.

Associando atributos virtuais a objetos

Você pode associar somente atributos virtuais habilitados a objetos do Active Directory. Depois de associar um atributo virtual a um objeto, o atributo virtual fica disponível como parte das propriedades do objeto.

Para expor atributos virtuais por meio das interfaces do usuário do DRA, você precisa criar uma página de propriedades personalizada.

Para associar um atributo virtual a um objeto, acesse o nó **Configuration Management** (Gerenciamento de Configurações) > **Virtual Attributes** (Atributos Virtuais) > **Managed Attributes** (Atributos Gerenciados), clique o botão direito do mouse no atributo virtual que você deseja usar e selecione **Associate** (Associar) > (tipo de objeto).

Observação

- Você só pode associar atributos virtuais a usuários, grupos, grupos dinâmicos de distribuição, computadores, contatos e unidades organizacionais.
- Quando você associa um atributo virtual a um objeto, o DRA cria automaticamente dois poderes personalizados padrão. Administradores assistentes exigem esses poderes personalizados para gerenciar o atributo virtual.

Desassociando atributos virtuais

Você pode desassociar os atributos virtuais dos objetos do Active Directory. Nenhum novo objeto criado exibe o atributo virtual desassociado como parte das propriedades do objeto.

Para desassociar um atributo virtual de um objeto do Active Directory, acesse o nó **Configuration Management** > **Virtual Attributes** > **Managed Classes** (Gerenciamento de Configurações > Atributos Virtuais > Classes Gerenciadas) > (tipo de objeto). Clique o botão direito do mouse no atributo virtual e selecione **Disassociate** (Desassociar).

Desabilitando atributos virtuais

Você pode desabilitar atributos virtuais se eles não estiverem associados a um objeto do Active Directory. Quando você desabilita um atributo virtual, os administradores não podem exibir ou associar o atributo virtual a um objeto.

Para desabilitar um atributo virtual, acesse **Configuration Management** > **Managed Attributes** (Gerenciamento de Configurações > Atributos Gerenciados). Clique o botão direito do mouse no atributo desejado no painel de lista e selecione **Disable** (Desabilitar).

Configurando armazenamento em cache

O servidor de Administração cria e mantém um **cache de contas** que contém partes do Active Directory para os domínios gerenciados. O DRA usa o cache de contas para melhorar o desempenho ao gerenciar contas de usuários, grupos, contatos e contas de computador.

Para programar um horário de atualização do cache ou exibir o status do cache, você precisa ter os poderes apropriados, como aqueles incluídos na função integrada Configurar Servidores e Domínios.

Observação: Para executar atualizações de cache de contas incrementais em domínios que contenham subárvores gerenciadas, verifique se a conta de serviço tem acesso de leitura ao container Objetos Apagados, bem como a todos os objetos no domínio da subárvore. Você pode usar o utilitário de Objetos Apagados para verificar e delegar as permissões apropriadas.

- “Atualizações completas e incrementais” na página 100
- “Horários Programados Padrão” na página 101

Atualizações completas e incrementais

Uma atualização de cache de contas incrementais atualiza apenas os dados que foram mudados desde a última atualização. A atualização incremental fornece uma maneira simplificada de acompanhar suas mudanças no Active Directory. Use a atualização incremental para atualizar rapidamente o cache de contas e, ao mesmo tempo, gerar o menor impacto em sua empresa.

Importante: O Servidor da Microsoft limita o número de usuários simultâneos conectados à sessão do WinRM/WinRS a cinco e o número de shells por usuário a cinco de modo a garantir que a mesma conta do usuário seja limitada a cinco shells para servidores secundários do DRA.

Uma atualização incremental atualiza os seguintes dados:

- Objetos novos e clonados
- Objetos apagados e movidos
- Membros do grupo
- Todas as propriedades do objeto em cache para objetos modificados

Uma atualização completa do cache de contas recria o cache de contas do DRA para o domínio especificado.

Observação: Enquanto uma Atualização do Cache de Contas Completas estiver em execução, o domínio ficará não disponível para os usuários do DRA.

Executando uma atualização completa do cache de contas

Para atualizar o cache de contas, você precisa ter os poderes apropriados, como aqueles incluídos na função integrada “Configure Servers and Domains” (Configurar Servidores e Domínios).

Para executar uma atualização imediata do cache de contas completas:

1. Acesse **Configuration Management** (Gerenciamento de Configurações) > **Managed Domains** (Domínios Gerenciados).
2. Clique o botão direito do mouse no domínio desejado e selecione **Propriedades**.
3. Clique em **Refresh Now** (Atualizar Agora) na guia **Full refresh** (Atualização completa).

Horários Programados Padrão

A frequência com que você deve atualizar o cache de contas depende da frequência com que sua empresa muda. Use a atualização incremental para atualizar o cache de contas com frequência, garantindo que o DRA tenha as informações mais atualizadas sobre o Active Directory.

Por padrão, o servidor de Administração executa uma atualização de cache de contas incrementais nos seguintes horários:

Tipo do domínio	Horário de Atualização Programado Padrão
Domínios Gerenciados	A cada 5 minutos
Domínios de confiança	Todas as horas
Locatário do Azure	A cada 15 minutos

Não é possível programar um FACR; no entanto, o DRA executa um FACR automático nas seguintes circunstâncias:

- Após configurar um domínio gerenciado pela primeira vez.
- Após fazer upgrade do DRA para uma nova versão completa de uma versão anterior.
- Após instalar um pacote de serviço do DRA.

A execução de uma atualização completa do cache de contas pode levar vários minutos.

Considerações

Você precisa atualizar periodicamente o cache de contas para garantir que o DRA tenha as informações mais recentes. Antes de executar ou programar uma atualização do cache de contas, revise as seguintes considerações:

- Para executar uma atualização de cache de contas incrementais, a conta de serviço ou conta de acesso do servidor de Administração deve ter permissão para acessar objetos apagados no Active Directory do domínio gerenciado ou de confiança.
- Quando o DRA realiza uma atualização do cache de contas, o servidor de Administração não inclui grupos de segurança locais de domínio de domínios confiáveis. Como o cache não contém esses grupos, o DRA não permite adicionar um grupo de segurança local de domínio do domínio de confiança a um grupo local no servidor do membro gerenciado.
- Se você omitir um domínio de confiança de uma atualização do cache de contas, o servidor de Administração também omitirá esse domínio da atualização da configuração do domínio.
- Se você incluir um domínio de confiança anteriormente omitido na atualização do cache de contas, execute uma atualização completa do cache de contas para o domínio gerenciado. Isso garante que o cache de contas no servidor de Administração para o domínio gerenciado reflita corretamente os dados da participação do grupo em seus domínios gerenciados e confiáveis.
- Se você definir o intervalo de atualização do cache de contas incrementais como **Nunca**, o servidor de Administração executará somente atualizações de cache de contas completas. Uma atualização completa do cache da conta pode levar algum tempo, durante o qual não é possível gerenciar objetos nesse domínio.

- O DRA não pode determinar automaticamente quando as mudanças são feitas por meio de outras ferramentas, como o Microsoft Directory Services. Operações executadas fora do DRA podem afetar a precisão das informações em cache. Por exemplo, se você usar outra ferramenta para adicionar uma caixa de correio a uma conta do usuário, não será possível usar o Exchange para gerenciar essa caixa de correio até atualizar o cache de contas.
- A execução de uma atualização completa do cache de contas apaga as últimas estatísticas de logon mantidas no cache. O servidor de Administração então coleta as informações de logon mais recentes de todos os controladores de domínio.

Habilitando a coleta de Impressoras do Active Directory

A coleta de Impressoras do AD está desabilitada por padrão. Para habilitá-la, acesse **Configuration Management** (Gerenciamento de Configurações) > **Update Administration Server Options** (Atualizar Opções do Servidor de Administração) > guia **General** (Geral) e marque a caixa de seleção Collect Printers (Coletar Impressoras).

AD LDS

Você pode configurar a atualização de limpeza do AD LDS para ser executada em uma programação para domínios específicos. A configuração padrão é "Nunca" atualizar. Você também pode exibir o status de limpeza e exibir informações específicas relacionadas à configuração do AD LDS (ADAM).

Para configurar a programação ou ver o status da Limpeza do AD LDS, clique o botão direito do mouse no domínio desejado no nó **Account and Resource Management** (Gerenciamento de Recursos e de Contas) > **Todos os Meus Objetos Gerenciados** e selecione **Propriedades** > **Adlds Cleanup Refresh Schedule** (Programação de Atualização de Limpeza do Adlds) ou **Adlds Cleanup status** (Status de limpeza do Adlds), respectivamente.

Para exibir as informações de configuração do AD LDS (ADAM), acesse **Configuration Management** (Gerenciamento de Configurações) > **Update Server Options** (Atualizar Opções do Servidor) > **ADAM Configuration** (Configuração do ADAM).

Grupo Dinâmico

Um grupo dinâmico é aquele cuja participação muda com base em um conjunto definido de critérios que você configura nas propriedades do grupo. Em Propriedades do Domínio, você pode configurar a atualização do Grupo Dinâmico para ser executada em uma programação para domínios específicos. A configuração padrão é "Nunca" atualizar. Você também pode ver o status de atualização.

Para configurar a programação ou ver o status da atualização do Grupo Dinâmico, clique o botão direito do mouse no domínio desejado no nó **Account and Resource Management** (Gerenciamento de Recursos e de Contas) > **Todos os Meus Objetos Gerenciados** e selecione **Propriedades** > **Dynamic group refresh** (Atualização do grupo dinâmico) ou **Dynamic group status** (Status do grupo dinâmico), respectivamente.

Para mais informações sobre grupos dinâmicos, consulte Grupos dinâmicos do DRA.

Configurando a Lixeira

Você pode habilitar ou desabilitar a Lixeira para cada domínio ou objetos do Microsoft Windows em cada domínio e configurar quando e como deseja que a limpeza da Lixeira ocorra.

Para obter informações detalhadas sobre o uso da Lixeira, consulte Lixeira.

Habilitando a Lixeira

Você pode habilitar a Lixeira para domínios específicos do Microsoft Windows e para objetos dentro desses domínios. Por padrão, o DRA ativa a Lixeira para cada domínio gerenciado e todos os objetos do domínio. Você deve ser um membro do grupo Administradores do DRA ou Administradores de Configuração do DRA para habilitar a Lixeira.

Se o seu ambiente incluir a configuração a seguir, use o utilitário Recycle Bin para habilitar esse recurso:

- O DRA está gerenciando uma subárvore desse domínio.
- O serviço do servidor de Administração ou a conta de acesso não tem permissão para criar o container da Lixeira, mover contas para esse container e modificar contas nesse container.

Você também pode usar o utilitário Recycle Bin para verificar o serviço do servidor de Administração ou acessar as permissões da conta no container da Lixeira.

Para habilitar a Lixeira, clique o botão direito do mouse no domínio desejado no nó **Lixeira** e selecione **Enable Recycle Bin** (Habilitar Lixeira).

Desabilitando a Lixeira

Você pode desabilitar a Lixeira para domínios específicos do Microsoft Windows e para objetos dentro desses domínios. Se uma Lixeira desabilitada tiver contas, não será possível exibir, apagar permanentemente nem restaurar essas contas.

Você precisa ser um membro do grupo de Administradores do DRA ou Administradores assistentes de Configuração do DRA para desabilitar a Lixeira.

Para desabilitar a Lixeira, clique o botão direito do mouse no domínio desejado no nó **Lixeira** e selecione **Disable Recycle Bin** (Desabilitar Lixeira).

Configurando objetos da Lixeira e limpeza

A configuração padrão para a limpeza da Lixeira é diária. Você pode mudar essa configuração para limpar a Lixeira do domínio a cada x dias. Durante a limpeza programada, a Lixeira apaga objetos mais antigos do que o número de dias que você configurou para cada tipo de objeto. A configuração padrão para cada tipo é apagar objetos com mais de um dia. Você pode personalizar o comportamento da limpeza da Lixeira desabilitando, reabilitando e definindo a idade dos objetos a serem apagados para cada tipo de objeto.

Para configurar a limpeza da Lixeira, selecione o domínio desejado no console de Delegação e Configuração e acesse **Tarefas** > **Propriedades** > guia **Lixeira**.

Configuração do Gerador de Relatórios

As seções a seguir fornecem informações conceituais sobre os relatórios de Gerenciamento do DRA e os coletores de relatório que você pode habilitar. Para acessar o assistente em que você pode configurar os coletores, acesse **Configuration Management** (Gerenciamento de Configurações) > **Update Reporting Service Configuration** (Atualizar Configuração do Serviço Gerador de Relatórios).

Configurando o Active Directory Collector

O Active Directory Collector coleta um conjunto especificado de atributos do Active Directory para cada usuário gerenciado, grupo, contato, computador, OU e grupo de Distribuição Dinâmica no DRA. Esses atributos são armazenados no banco de dados do gerador de relatórios e são usados para gerar relatórios no Console Reporting (Gerador de Relatórios).

Você pode configurar o Active Directory Collector para especificar quais atributos são coletados e armazenados no banco de dados do gerador de relatórios. Você também pode configurar em qual servidor de Administração DRA o coletor será executado.

Configurando o DRA Collector

O DRA Collector coleta informações sobre sua configuração de DRA e armazena essas informações no banco de dados do gerador de relatórios, que é usado para gerar relatórios no console Reporting (Gerador de Relatórios).

Para habilitar o DRA Collector, você precisa especificar em qual servidor de Administração DRA o coletor será executado. Como prática recomendada, você deve programar o DRA Collector para ser executado após o Active Directory Collector ser executado com êxito e durante os períodos em que o servidor estiver menos carregado ou fora do horário normal de trabalho.

Configurando o Azure Tenant Collector

O Azure Tenant Collector coleta informações sobre usuários e grupos do Azure que estão sincronizados com o Azure Active Directory e armazena essas informações no banco de dados do gerador de relatórios, que é usado para gerar relatórios no Console do Gerador de Relatórios.

Para habilitar o Azure Tenant Coletor, você deve especificar em qual Servidor de administração DRA o coletor será executado.

Observação: O locatário do Azure só poderá executar uma coleta bem-sucedida após o Active Directory Collector do domínio correspondente ter executado uma coleta bem-sucedida.

Configurando o coletor de relatórios de gerenciamento

O Coletor de relatórios de gerenciamento coleta informações de auditoria de DRA e armazena essas informações no banco de dados do gerador de relatórios, que é usado para gerar relatórios no console Reporting (Gerador de Relatórios). Quando você habilita o coletor, é possível configurar com que frequência os dados são atualizados no banco de dados para que as consultas sejam executadas na ferramenta DRA Reporting.

Esta configuração exige que a conta de Serviço do DRA tenha a permissão **sysadmin** no SQL Server no servidor Gerador de Relatórios. As opções configuráveis são definidas abaixo:

- **Audit Export Data Interval** (Intervalo de Dados de Exportação de Auditoria): Esse é o intervalo em que os dados de auditoria do registro de rastreamento do DRA (LAS) são exportados para o banco de dados “SMCubeDepot” no SQL Server.
- **Management Report Summarization Interva:** (Intervalo de Resumo do Relatório de Gerenciamento) Esse é o intervalo em que os dados de auditoria do banco de dados do SMCubeDepot são enviados para o banco de dados do DRA Reporting, no qual podem ser consultados pela ferramenta DRA Reporting.

Coletando as últimas estatísticas de logon

Você pode configurar o DRA para coletar as estatísticas do último logon de todos os controladores de domínio no domínio gerenciado. Para habilitar e programar a coleta de estatísticas do último logon, você precisa ter os poderes apropriados, como aqueles incluídos na função integrada Configurar Servidores e Domínios.

Por padrão, o recurso de coleta de estatísticas do último logon está desabilitado. Se você deseja reunir dados estatísticos do último logon, deve habilitar esse recurso. Depois de habilitar a coleta de estatísticas do último logon, você pode exibir as estatísticas do último logon de um determinado usuário ou ver o status da última coleta de estatísticas de logon.

Para coletar as estatísticas do último logon:

1. Acesse **Configuration Management** (Gerenciamento de Configurações) > **Managed Domains** (Domínios Gerenciados).
2. Clique o botão direito do mouse no domínio desejado e selecione **Propriedades**.
3. Clique na guia **Last logon schedule** (Programação do último logon) para configurar a coleta de estatísticas do último logon.

Delegando Poderes de Configuração do Servidor do Workflow Automation

Para gerenciar o Workflow, designe a função de Administração do Servidor do Workflow Automation ou os poderes aplicáveis abaixo aos administradores assistentes:

- Criar um Evento de Workflow e Modificar Todas as Propriedades
- Apagar a configuração do Servidor do Workflow Automation
- Definir informações de configuração do servidor do Workflow Automation
- Iniciar o Workflow

- Ver Todas as Propriedades de Eventos de Workflow
- Ver Todas as Propriedades de Workflow
- Ver informações de configuração do servidor do Workflow Automation

Para delegar poderes de configuração do servidor do Workflow Automation:

1. Clique em **Poderes** no nó de Gerenciamento de Delegação e use o recurso de objetos de pesquisa para encontrar e selecionar os poderes de Workflow que você deseja.
2. Clique o botão direito do mouse em um dos poderes de Workflow selecionados e selecione **Delegar Funções e Poderes**.
3. Pesquise o usuário, o grupo ou o grupo de administradores assistentes específico ao qual você deseja delegar poderes.
4. Use o **Seletor de Objetos** para localizar e adicionar os objetos desejados e clique em **Roles and Powers** (Funções e Poderes) no **Assistente**.
5. Clique em **Telas Ativas** e use o **Seletor de Objetos** para encontrar e adicionar as Telas Ativas que você deseja.
6. Clique em **Next** (Próximo) e em **Finish** (Terminar) para concluir o processo de delegação.

Configurando o Servidor do Workflow Automation

Para usar o Workflow Automation no DRA, você precisa instalar o Workflow Automation Engine em um Servidor Windows e, em seguida, configurar o servidor do Workflow Automation por meio do console de Delegação e Configuração.

Para configurar o servidor do Workflow Automation:

1. Efetue login no Console de Delegação e Configuração.

   Para saber mais sobre os poderes do Workflow Automation, veja Delegando Poderes de Configuração do Servidor do Workflow Automation.
2. Expanda **Gerenciamento de Configurações** > **Servidores de Integração**.
3. Clique o botão direito do mouse em **Workflow Automation** e selecione **Novo Servidor do Workflow Automation**.
4. No assistente **Adicionar Servidor do Workflow Automation**, especifique os detalhes como nome do servidor, porta, protocolo e conta de acesso.
5. Teste a conexão do servidor e clique em **Terminar** para gravar a configuração.

Para obter informações sobre a instalação do Workflow Automation Engine, consulte o *Workflow Automation Administrator Guide* (Guia do Administrador do Workflow Automation) no DRA Documentation site (site de Documentação do DRA).

Delegando os Poderes da Pesquisa do LDAP

O DRA permite pesquisar objetos LDAP em domínios locais do Active Directory, como usuários, contatos, computadores, grupos e OUs do servidor LDAP. O servidor do DRA ainda lida com a operação e é o controlador de domínio em que a pesquisa é executada. Use os filtros de pesquisa para realizar pesquisas mais eficientes e eficazes. Além disso, você pode gravar a consulta de pesquisa para uso futuro e compartilhá-la com o público ou usá-la por sua conta, marcando-a como

particular. Você pode editar as consultas gravadas. A função Consultas Avançadas do LDAP concede aos administradores assistentes poderes para criar e gerenciar consultas da Pesquisa do LDAP. Use os seguintes poderes para delegar a criação e o gerenciamento de consultas de Pesquisa do LDAP:

- Criar Consulta Avançada Particular
- Criar Consulta Avançada Pública
- Apagar a Consulta Avançada Pública
- Executar uma consulta avançada
- Executar uma consulta avançada gravada
- Modificar a Consulta Pública
- Ver a Consulta Avançada

Para delegar poderes de Consulta LDAP:

1. Clique em **Poderes** no nó de Gerenciamento de Delegação e use o recurso de objetos de pesquisa para encontrar e selecionar os poderes das Consultas LDAP Avançadas que você deseja.
2. Clique o botão direito do mouse em um dos poderes LDAP selecionados e selecione **Delegar Funções e Poderes**.
3. Pesquise o usuário, o grupo ou o grupo de administradores assistentes específico ao qual você deseja delegar poderes.
4. Use o **Seletor de Objetos** para localizar e adicionar os objetos desejados e clique em **Roles and Powers** (Funções e Poderes) no **Assistente**.
5. Clique em **Telas Ativas** e use o **Seletor de Objetos** para encontrar e adicionar as Telas Ativas que você deseja.
6. Clique em **Next** (Próximo) e em **Finish** (Terminar) para concluir o processo de delegação.

Para acessar o recurso de pesquisa no Console da Web, navegue até **Gerenciamento > Pesquisa do LDAP**.

Configurando o Gerador de Relatórios de Histórico de Mudanças

O DRA habilita a delegação de mudanças gerenciadas em uma organização empresarial e o CG (Change Guardian) permite o monitoramento de mudanças gerenciadas e não gerenciadas que ocorrem no Active Directory. A integração do DRA com o CG fornece:

- Capacidade de ver o Administrador Assistente delegado do DRA que fez uma mudança no Active Directory em eventos do CG para mudanças feitas por meio do DRA.
- Capacidade de ver o histórico recente de mudanças para um objeto no DRA de ambas as mudanças feitas por meio de DRA e mudanças capturadas pelo CG que se originaram fora do DRA.
- As mudanças feitas por meio do DRA são designadas como mudanças “gerenciadas” no CG.

Para configurar o gerador de relatórios de histórico de mudanças do DRA, siga estas etapas:

1. Instale o agente do Windows do Change Guardian.

2. Adicione uma chave de licença do Active Directory.
3. Configure o Active Directory.
4. Crie e designe uma política do Active Directory.
5. Gerencie domínios do Active Directory.
6. Habilite a marcação de eventos.
7. Configure o Histórico de Mudanças Unificado.

Depois de concluir as etapas acima para instalar o Change Guardian e configurar a integração do DRA com o CG, os usuários podem gerar e ver relatórios UCH no Console da Web.

Para obter mais informações, consulte "Generating Change History Reports" (Gerando relatórios de histórico de mudanças) no *Directory and Resource Administrator User Guide* (Guia do Usuário do Directory and Resource Administrator).

Instalar o agente do Windows do Change Guardian

Antes de iniciar a integração do DRA com o CG, instale o agente do Windows do Change Guardian. Para obter mais informações, consulte o *Change Guardian Installation and Administration Guide* (Guia de Instalação e Administração do Change Guardian).

Adicione uma chave de licença do Active Directory

Você deve adicionar licenças para o servidor do Change Guardian e os aplicativos ou módulos que você planeja monitorar.

Adicionando uma chave de licença para o servidor

Você pode usar o Console de Administração ou a linha de comando para adicionar a chave de licença do servidor do Change Guardian.

Se estiver usando a chave da licença de avaliação, você deverá adicionar a chave de licença corporativa antes que a chave de avaliação expire, a fim de evitar qualquer interrupção na funcionalidade do Change Guardian. Para obter informações sobre como comprar a licença, consulte o site do produto Change Guardian na web.

Adicionando do Console de Administração

Para adicionar uma chave de licença:

1 No console da Web, clique em **ADMINISTRAÇÃO**.

2 Clique em **Ajuda > Sobre > Licenças > Add License** (Adicionar Licença).

3 Especifique a chave de licença e grave.

Observação: Quando uma licença expira, o console da Web do Change Guardian aparece em branco.

Adicionando da linha de comando

Para adicionar uma chave de licença usando a linha de comando:

1. Efetue login no servidor do Change Guardian como `root`.
2. Mude para o diretório `/opt/novell/sentinel/bin`.
3. Mude para o usuário da Novell:

   ```
   su novell
   ```
4. Execute o script `softwarekey.sh`:

   ```
   ./softwarekey.sh
   ```
5. Digite 1 para inserir a chave de licença.
6. Especifique a chave de licença e pressione Enter

Adicionando uma licença para aplicativos

O **Module Manager** (Gerenciador de Módulos) fornece informações sobre aplicativos licenciados e permite que você importe licenças de aplicativos para o Policy Editor.

Quando você instala o Change Guardian, todos os aplicativos disponíveis são instalados automaticamente no Policy Editor. No entanto, você deve adicionar um novo aplicativo ao Policy Editor. Para permitir que o Change Guardian comece a monitorar, importe a chave de licença para cada aplicativo.

Para adicionar um novo aplicativo ao Module Manager (Gerenciador de Módulos):

1. No **Module Manager** (Gerenciador de Módulos), clique em **Install > From Local Directory** (Instalar > Do Diretório Local).

Para importar uma licença:

1. Efetue login no Policy Editor, clique em **Change Guardian**.
2. Selecione **Module Manager** (Gerenciador de Módulos).
3. Clique em **Import License Key** (Importar a chave de licença).
4. Selecione a chave de licença para o aplicativo necessário.

Configurar o Active Directory

Para configurar o Active Directory para o Histórico de Mudanças, consulte as seguintes seções:

Configurando o registro de eventos de segurança

Configure o registro de eventos de segurança para garantir que os eventos do Active Directory permaneçam no registro de eventos até que o Change Guardian os processe.

Para configurar o registro de eventos de segurança:

1. Efetue login como administrador de um computador no domínio que deseja configurar.

2 Para abrir o Console de Gerenciamento de Políticas de Grupo, digite o seguinte no prompt de comando: `gpmc.msc`

3 Abra **Forest > Domains** > ***domainName***> **Domain Controllers** (Floresta > Domínios > domainName > Controladores de domínio).

4 Clique o botão direito do mouse em **Default Domain Controllers Policy** (Política de Controladores de Domínio Padrão) e, em seguida, clique em **Editar**.

Observação: Mudar a política padrão dos controladores de domínio é importante porque um GPO vinculado à unidade organizacional (OU) do controlador de domínio (DC) com uma ordem de vínculo mais alta pode anular essa configuração quando você reiniciar o computador ou executar o `gpUpdate` novamente. Se os padrões corporativos não permitirem que você modifique a política padrão dos controladores de domínio, crie um GPO para as configurações do Change Guardian, adicione essas configurações ao GPO e defina-as para ter a ordem de vínculo mais alta na OU dos Controladores de Domínio.

---

5 Expanda **Computer Configuration (Configuração do computador) > Policies (Políticas) > Windows Settings (Configurações do Windows) > Security Settings (Configurações de segurança)**.

6 Selecione **Registro de eventos** e defina:

- **Tamanho máximo do registro de segurança** para 10.240 KB (10 MB) ou mais
- **Método de retenção para registro de segurança** para **Sobregravar eventos conforme necessário**

7 Para atualizar as configurações da política, execute o comando `gpUpdate` no prompt de comando.

Para verificar se a configuração foi bem-sucedida:

1 Abra um prompt de comando como administrador no computador.

2 Inicie o Visualizador de Eventos: `eventvwr`

3 Em registros do Windows, clique o botão direito do mouse em **Segurança** e selecione **Propriedades**.

4 Verifique se as configurações mostram o tamanho máximo do registro de 10.240 KB (10 MB) ou mais e que está selecionado o item “Sobregravar eventos conforme necessário”.

Configurando a auditoria do AD

Configure a auditoria do AD para habilitar o registro de eventos do AD no registro de eventos de segurança.

Configure o GPO de política de controladores de domínio padrão com acesso ao serviço de Diretório de Auditoria para monitorar eventos de sucesso e de falha.

Para configurar a auditoria do AD:

1 Efetue login como administrador de um computador no domínio que deseja configurar.

2 Para abrir o Console de Gerenciamento de Políticas de Grupo, execute `gpmc.msc` no prompt de comando.

3 Expanda **Forest > Domains** > ***domainName*** > **Domain Controllers** (Floresta > Domínios > domainName > Controladores de domínio).

4 Clique o botão direito do mouse em **Default Domain Controllers Policy** (Política de Controladores de Domínio Padrão) e clique em **Editar**.

Observação: Mudar a política padrão dos controladores de domínio é importante porque um GPO vinculado à unidade organizacional (OU) do controlador de domínio (DC) com uma ordem de vínculo mais alta pode anular essa configuração quando você reiniciar o computador ou executar o `gpUpdate` novamente. Se os padrões corporativos não permitirem que você modifique a política padrão dos controladores de domínio, crie um GPO para as configurações do Change Guardian, adicione essas configurações ao GPO e defina-as para ter a ordem de vínculo mais alta na OU dos Controladores de Domínio.

---

5 Expanda **Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies** (Configuração do Computador > Políticas > Configurações do Windows > Configurações de Segurança > Configuração de Políticas Avançadas de Auditoria > Políticas de Auditoria).

5a Para configurar a política do AD e de grupo, em **Account Management** (Gerenciamento de Contas) e **Policy Change** (Mudança de Política), selecione o seguinte para cada subcategoria: **Configure the following audit events** (Configurar os seguintes eventos de auditoria), **Success** (Sucesso) e **Failure** (Falha).

5b Para configurar apenas o AD, em **DS Access** (Acesso DS), selecione o seguinte para cada subcategoria: **Configure the following audit events** (Configurar os seguintes eventos de auditoria), **Success** (Sucesso) e **Failure** (Falha).

6 Clique em **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options** (Configuração do computador > Políticas > Configurações do Windows > Configurações de segurança > Políticas locais > Opções de segurança) e habilite **Audit: Force audit policy subcategory settings... to override audit policy category settings** (Auditoria: forçar configurações de subcategorias de políticas de auditoria... para substituir configurações de categorias de políticas de auditoria).

7 Navegue até **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Audit Policy** (Configuração do computador > Políticas > Configurações do Windows > Configurações de segurança > Políticas locais > Política de auditoria).

8 Em **Audit account management** (Gerenciamento de contas de auditoria), **Audit directory service access** (Acesso ao serviço de diretório de auditoria) e **Audit policy change** (Mudança da política de auditoria), selecione o seguinte para cada subcategoria em Propriedades: **Define these policy settings** (Definir estas configurações de política), **Success** (Sucesso) e **Failure** (Falha).

9 Para atualizar as configurações da política, execute o comando `gpUpdate` no prompt de comando.

Para obter mais informações, consulte *Monitoring Active Directory for Signs of Compromise* (Monitorar o Active Directory em busca de sinais de comprometimento) no site de Documentação da Microsoft.

Configurando a auditoria de usuários e grupos

Configure a auditoria de usuários e grupos para auditar as seguintes atividades:

- Atividades de logon e logoff de usuários locais e usuários do Active Directory
- Configurações de usuários locais
- Configurações de grupo locais

Para configurar a auditoria de usuários e grupos:

1. Efetue login como administrador de um computador no domínio que deseja configurar.
2. Abra o Console de Gerenciamento da Microsoft, selecione **File (Arquivo) > Add/Remove Snap-in (Adicionar/remover snap-in)**.
3. Selecione **Group Policy Management Editor (Editor de Gerenciamento de Políticas de Grupo)** e clique em **Adicionar**.
4. Na janela Selecionar Objeto de Política de Grupo, clique em **Procurar**.
5. Selecione **Domain Controllers (Controladores de domínio).*FQDN***, em que *FQDN* é o Nome de Domínio Completo e Qualificado para o computador do controlador de domínio.
6. Selecione **Política de Controladores de Domínio Padrão**.
7. No console de gerenciamento da Microsoft, expanda **Default Domain Controllers Policy *FQDN* > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Audit Policy** (FQDN da Política de Controladores de Domínio Padrão > Configuração do Computador > Políticas > Configurações do Windows > Configurações de Segurança > Políticas Locais > Política de Auditoria).
8. Em **Audit Account Logon Events** (Eventos de logon da conta de auditoria) e **Audit Logon Events** (Eventos de logon de auditoria), selecione **Define these policy settings** (Definir essas configurações de política), **Success** (Sucesso) e **Failure** (Falha).
9. No Console de Gerenciamento da Microsoft, expanda **Default Domain Controllers Policy *FQDN* > Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies > Logon/Logoff** (FQDN da Política de Controladores de Domínio Padrão > Configuração do Computador > Políticas > Configurações do Windows > Configurações de Segurança > Configuração Avançada de Política de Auditoria > Políticas de Auditoria > Logon/Logoff).
10. Em **Audit Logon** (Logon de auditoria), selecione **Audit Logon** (Logon de auditoria), **Success** (Sucesso) e **Failure** (Falha).
11. Em **Audit Logoff** (Logoff de auditoria), selecione **Audit Logoff** (Logoff de auditoria), **Success** (Sucesso) e **Failure** (Falha).
12. Para atualizar as configurações da política, execute o comando `gpupdate /force` no prompt de comando.

Configurando listas de controles de acesso de segurança

Para monitorar todas as mudanças dos objetos atuais e futuros dentro do Active Directory, configure o nó de domínio.

Para configurar SACLs:

1. Efetue login como administrador de um computador no domínio que deseja configurar.
2. Para abrir a ferramenta de configuração Editor ADSI, execute `adsiedit.msc` no prompt de comando.
3. Clique o botão direito do mouse em **ADSI Edit** (Editor ADSI) e selecione **Connect to** (Conectar a).
4. Na janela Connection Settings (Configurações de conexão), faça o seguinte:
   - **Name** (Nome) como `Default naming context` (Contexto de nomeação padrão).
   - **Path** (Caminho) para o domínio a ser configurado.

- Se você estiver executando esta etapa pela primeira vez, selecione **Default naming context** (Contexto de nomeação padrão).
- Se você a estiver executando pela segunda vez, selecione **Schema** (Esquema).
- Se você a estiver executando pela terceira vez, selecione **Configuration** (Configuração).

Observação: Você deve executar a Etapa 4 até a Etapa 11 três vezes, para configurar pontos de conexão para **Default naming context** (Contexto de nomeação padrão), **Schema** (Esquema) e **Configuration** (Configuração).

---

5 Em **Connection Point** (Ponto de Conexão), defina **Select a well known Naming Context** (Selecionar um contexto de nomeação bem conhecido) como **Default naming context** (Contexto de nomeação padrão).

6 Na janela ADSI Edit (Editor ADSI), expanda **Default naming context** (Contexto de nomeação padrão).

7 Clique o botão direito do mouse no nó sob o ponto de conexão (começa com DC= ou CN=) e clique em **Propriedades**.

8 Na guia **Security** (Segurança), clique em **Advanced (Avançada) > Auditing (Auditoria) > Add (Adicionar)**.

9 Em **Applies to** (Aplica-se a) ou **Apply onto** (Aplicar em), selecione **This object and all descendant objects** (Este objeto e todos os objetos descendentes).

10 Configure a auditoria para monitorar cada usuário:

10a Clique em **Select a principal** (Selecionar um principal) e digite `everyone` (todos) em **Enter the object name to select** (Digite o nome do objeto a ser selecionado).

10b Especifique as seguintes opções:

- **Type** (Tipo) como **All** (Todos)
- Selecione **Permissions** (Permissões) como:
  - **Write All Properties** (Gravar Todas as Propriedades)
  - **Delete** (Apagar)
  - **Modify Permissions** (Modificar Permissões)
  - **Modify Owner** (Modificar Proprietário)
  - **Create All Child Objects** (Criar Todos os Objetos Filhos)

    Os outros nós relacionados a objetos filhos são selecionados automaticamente
  - **Delete All Child Objects** (Apagar Todos os Objetos Filhos)

    Os outros nós relacionados a objetos filhos são selecionados automaticamente

11 Anule a seleção da opção **Apply these auditing entries to objects and/or containers within this container only** (Aplicar essas entradas de auditoria a objetos e/ou containers somente neste container).

12 Repita o Etapa 4 até Etapa 11 mais duas vezes.

Criar e designar uma política do Active Directory

Você pode criar uma nova política sem configurações predefinidas.

Para criar uma política:

1. No Policy Editor, selecione um dos aplicativos, como o Active Directory.
2. Expanda a lista de políticas e selecione o tipo de política que deseja criar. Por exemplo, selecione **Active Directory Policies (Políticas do Active Directory) > AD Object (Objeto do AD)**.
3. Na tela Política de configuração, faça as mudanças apropriadas.
4. (Condicional) Se você quiser habilitar a política imediatamente, selecione **Enable this policy revision now** (Habilitar esta revisão de política agora).

Para designar uma política ou um conjunto de políticas a um bem:

1. Clique em **Change Guardian > Policy Assignment** (Designação de Política).
2. Selecione um bem ou um grupo de bens e clique em **Assign Policies** (Designar Políticas).
3. Selecione um conjunto de políticas ou uma política e clique em **Aplicar**.

Observação: Você não pode designar políticas usando **Asset Groups** (Grupos de Bens) para os seguintes tipos de bens: Azure AD, AWS for IAM, Dell EMC, Microsoft Exchange, Microsoft Office 365 e NetApp.

Gerenciar domínios do Active Directory

Para configurar um domínio no DRA como um Domínio gerenciado, consulte Gerenciando domínios do Active Directory.

Habilitar a marcação de eventos no DRA

Quando a auditoria dos Serviços de Domínio do AD está habilitada, os eventos do DRA são registrados como tendo sido gerados pela conta do Serviço DRA ou pela conta de Acesso ao Domínio, se houver uma configurada. A Marcação de Eventos leva esse recurso um passo adiante gerando um evento AD DS adicional que identifica o administrador assistente que executou a operação.

Para que esses eventos sejam gerados, você precisa configurar a auditoria do AD DS e habilitar a Marcação de Eventos no Servidor de administração DRA. Quando a opção Event Stamping (Marcação de Eventos) estiver habilitada, você poderá exibir as mudanças que os administradores assistentes fazem nos relatórios do Evento do Guardião de Mudanças.

- Para configurar a auditoria do AD DS, veja a documentação da Microsoft no *AD DS Auditing Step-by-Step Guide* (Guia passo a passo de Auditoria do AD DS).
- Para configurar a integração do Guardião de Mudanças, consulte Configurando servidores do Histórico de Mudanças Unificado.
- Para habilitar a Marcação de Eventos, abra o console de Delegação e Configuração como administrador do DRA e faça o seguinte:
    1. Acesse **Configuration Management** > **Update Administration Server Options** > **Event Stamping** (Gerenciamento de Configurações > Atualizar Opções do Servidor de Administração > Marcação de Eventos).
    2. Selecione um tipo de objeto e clique em **Update** (Atualizar).
    3. Selecione um atributo para usar para a Marcação de Eventos para esse tipo de objeto.

Atualmente, o DRA oferece suporte à Marcação de Eventos para usuários, grupos, contatos, computadores e unidades organizacionais.

O DRA também exige que os atributos existam no esquema do AD para cada um dos seus domínios gerenciados. Você deverá estar ciente disso se adicionar domínios gerenciados após configurar a Marcação de Eventos. Se você adicionasse um domínio gerenciado que não contivessem um atributo selecionado, as operações desse domínio não seriam auditadas com os dados da Marcação de Eventos.

O DRA modifica esses atributos, portanto, você precisa selecionar os atributos que não são usados pelo DRA ou por qualquer outro aplicativo em seu ambiente.

Para obter mais informações sobre a Marcação de Eventos, consulte Como funciona a marcação de eventos.

Configurar o Histórico de Mudanças Unificado

O recurso Servidor do UCH (Histórico de Mudanças Unificado) permite gerar relatórios para mudanças feitas fora do DRA.

Delegando os Poderes de Configuração do Servidor de Histórico de Mudanças Unificado

Para gerenciar o Servidor do Histórico de Mudanças Unificado, designe a função Administração do Servidor do Histórico de Mudanças Unificado ou os poderes aplicáveis abaixo aos administradores assistentes:

- Apagar configuração do servidor do histórico de mudanças unificado
- Definir informações de configuração do Histórico de Mudanças Unificado
- Exibir informações de configuração do Histórico de Mudanças Unificado

Para delegar poderes do Servidor de Histórico de Mudanças Unificado:

1. Clique em **Poderes** no nó de Gerenciamento de Delegação e use o recurso de objetos de pesquisa para encontrar e selecionar os poderes do UCH (Histórico de Mudanças Unificado) que você deseja.
2. Clique o botão direito do mouse em um dos poderes do UCH selecionados e selecione **Delegar Funções e Poderes**.
3. Pesquise o usuário, o grupo ou o grupo de administradores assistentes específico ao qual você deseja delegar poderes.
4. Use o **Seletor de Objetos** para localizar e adicionar os objetos desejados e clique em **Roles and Powers** (Funções e Poderes) no **Assistente**.
5. Clique em **Telas Ativas** e use o **Seletor de Objetos** para encontrar e adicionar as Telas Ativas que você deseja.
6. Clique em **Next** (Próximo) e em **Finish** (Terminar) para concluir o processo de delegação.

Configurando servidores do Histórico de Mudanças Unificado

Para configurar Servidores do Histórico de Mudanças Unificado:

1. Efetue login no Console de Delegação e Configuração.
2. Expanda **Gerenciamento de Configurações** > **Servidores de Integração**.
3. Clique o botão direito do mouse em **Histórico de Mudanças Unificado** e selecione **Novo Servidor do Histórico de Mudanças Unificado**.
4. Especifique o nome do servidor do UCH ou o endereço IP, o número da porta, o tipo de servidor e os detalhes da conta de acesso na configuração do Histórico de Mudanças Unificado.
5. Teste a conexão do servidor e clique em **Terminar** para gravar a configuração.
6. Adicione outros servidores, se necessário.

Acessar relatórios de Histórico de Mudanças Unificado

Para gerar e ver relatórios de histórico de mudanças unificados em objetos do Active Directory via Change Guardian, consulte "Generating Change History Reports" (Gerando relatórios de histórico de mudanças) no *Directory and Resource Administrator User Guide* (Guia do Usuário do Directory and Resource Administrator).

Configurando Serviços do DRA para uma Conta de Serviço Gerenciado do Grupo

Se necessário, você pode usar uma gMSA (Conta de Serviço Gerenciado do Grupo) para serviços do DRA. Para obter mais informações sobre como usar uma gMSA, consulte a referência da Microsoft *Group Managed Service Accounts Overview* (Visão geral de contas de serviço gerenciado do grupo). Esta seção explica como configurar o DRA para uma gMSA após ter adicionado a conta ao Active Directory.

Importante: Não use a gMSA como uma conta de serviço ao instalar o DRA.

Para configurar o servidor de Administração Principal do DRA para uma gMSA:

1. Adicione a gMSA como um membro dos seguintes grupos:
   - Grupo de Administradores Locais no servidor do DRA
   - Grupo do AD LDS no domínio gerenciado do DRA
2. Mude a conta de logon nas Propriedades do serviço para cada um dos serviços abaixo para a gMSA:
   - Serviço de Administração da NetIQ
   - Serviço de Auditoria do DRA da NetIQ
   - Serviço de BD de Cache do DRA da NetIQ

     Serviço de Cache do DRA da NetIQ
   - Serviço de Núcleo do DRA da NetIQ
   - Arquivo de Registro do DRA da NetIQ

- Serviço de Replicação do DRA da NetIQ
- Serviço REST do DRA da NetIQ
- Serviço Skype do DRA da NetIQ

3 Reinicie todos os serviços.

Para configurar um servidor de administração secundário do DRA para uma gMSA:

1 Instale o servidor secundário.
2 No servidor principal, designe a função **Configurar Servidores e Domínios** à Tela Ativa **Servidores de Administração e Domínios Gerenciados** para a conta de serviço do servidor secundário.
3 No servidor principal, adicione um novo servidor secundário e especifique a conta de serviço do servidor secundário.
4 Adicione a gMSA ao grupo de administradores locais no servidor de Administração Secundário do DRA.
5 No servidor secundário, mude a conta de logon de todos os serviços do DRA para a gMSA e, em seguida, reinicie os serviços do DRA.

Configurar o Cliente de Delegação e Configuração

O cliente de Delegação e Configuração fornece acesso a tarefas de configuração e delegação, atendendo às necessidades de gerenciamento corporativo, da administração distribuída até a imposição de políticas. Por meio do Console de Delegação e Configuração, você pode configurar o modelo de segurança e as configurações do servidor necessárias para gerenciar com eficiência sua empresa.

Para configurar o Cliente de Delegação e Configuração:

1 Inicie o cliente de Delegação e Configuração e acesse **Configuration Management** (Gerenciamento de Configurações) > **Update Administration Server Options** (Atualizar Opções do Servidor de Administração).
2 Clique na guia **Client Options** (Opções do Cliente) e defina suas configurações preferidas nas opções de configuração exibidas:
   - Permitir que os usuários pesquisem pela Tela Ativa
   - Ocultar objetos somente de origem nas listas de console
   - Mostrar objetos avançados do Active Directory
   - Mostrar comando de segurança
   - Mostrar recursos e caixas de correio compartilhadas ao pesquisar usuários
   - Sufixo UPN do Usuário padrão para o domínio atual
   - Máximo de itens editáveis por vez (seleção múltipla)
   - Opções de pesquisa
   - Opção de retorno de carro
   - Unidades de limites de armazenamento da caixa de correio do Exchange

Configurando o Cliente Web

Você pode configurar o Console da Web para autenticar usando cartões inteligentes ou autenticação de vários fatores e também personalizar a marca com seu próprio logotipo e título do aplicativo.

Iniciando o console da Web

Você pode iniciar o Console da Web de qualquer computador, dispositivo iOS ou dispositivo Android que esteja executando browser da Web. Para iniciar o Console, 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/draclient` no campo de endereço do seu browser da Web.

Observação: Para exibir as informações mais atualizadas da conta e 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.

Logout automático

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, navegue até **Administração** > **Configuração** > **Efetuar Logout Automático**.

Conexão com o 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: ◆ Usar descoberta automática (no domínio fornecido) ◆ Servidor principal para esse domínio ◆ Pesquisar um servidor DRA (no domínio fornecido)

Para configurar a conexão do servidor DRA no Console da Web, navegue até **Administração** > **Configuração** > **Conexão com o Servidor DRA**.

Autenticação

Esta seção contém informações para configurar a Autenticação do Smart Card, do Windows e de vários fatores usando a integração de Advanced Authentication.

- "Autenticação do Smart Card" na página 119
- "Autenticação do Windows" na página 121
- "Autenticação Multifator com a Advanced Authentication" na página 122

Autenticação do Smart Card

Para configurar o Console da Web para aceitar um usuário com base nas credenciais do cliente de seu smart card, você precisa configurar o IIS (Serviços de Informações da Internet) e o arquivo de configuração de serviços REST.

Importante: Verifique se os certificados no smart card também estão instalados no armazenamento de certificados raiz no servidor Web, pois o IIS precisa encontrar certificados que correspondam aos que estão no cartão.

1 Instale os componentes de autenticação no servidor web.

1a Inicie o Gerenciador do Servidor.

1b Clique em **Servidor Web (IIS)**.

1c Acesse a seção Serviços de Função e clique em **Adicionar Serviços de Função**.

1d Acesse o nó Serviços de função de segurança e selecione**Autenticação do Windows** e **Autenticação de Mapeamento do Certificado do Cliente**.

2 Habilite a autenticação no servidor web.

2a Inicie o **Gerente IIS**.

2b Selecione seu servidor web.

2c Localize o ícone **Autenticação** na seção IIS e clique duas vezes nele.

2d Habilite “Autenticação de Certificado do Cliente do Active Directory” e “Autenticação do Windows”.

3 Configure o cliente DRA.

3a Selecione seu cliente DRA.

3b Localize o ícone **Autenticação** na seção IIS e clique duas vezes nele.

3c Habilite “Autenticação do Windows” e desabilite “Autenticação Anônima”.

4 Habilite os certificados SSL e do cliente no cliente DRA.

4a Localize o ícone **Serviços SSL** na seção IIS e clique duas vezes nele.

4b Selecione **Exigir SSL** e **Exigir** nos certificados do Cliente.

Dica: Se a opção estiver disponível, selecione **Exigir SSL de 128 bits**.

---

5 Configure o aplicativo web de serviços REST.

5a Selecione seu aplicativo web de serviços REST.

5b Localize o ícone **Autenticação** na seção IIS e clique duas vezes nele.

5c Habilite “Autenticação do Windows” e desabilite “Autenticação Anônima”.

6 Habilite os certificados SSL e do cliente no aplicativo web de serviços REST.

6a Localize o ícone **Serviços SSL** na seção IIS e clique duas vezes nele.

6b Selecione **Exigir SSL** e **Exigir** nos certificados do Cliente.

Dica: Se a opção estiver disponível, selecione **Exigir SSL de 128 bits**.

---

7 Configure o arquivo de serviço da Web do WCF.

7a Selecione seu aplicativo web de serviços REST e alterne para ão de Conteúdo.

7b Localize o arquivo `.svc` e clique o botão direito do mouse nele.

7c Selecione **Alternar para ão de Recursos**.

7d Localize o ícone **Autenticação** na seção IIS e clique duas vezes nele.

7e Habilite a “Autenticação Anônima” e desabilite todos os outros métodos de autenticação.

8 Edite o arquivo de configuração dos serviços REST.

8a Use um editor de texto para abrir o arquivo `C:\inetpub\wwwroot\DRAClient\rest\web.config`.

8b Localize a linha `<authentication mode="None" />` e apague-a.

8c Remova o comentário das linhas especificadas abaixo:

- Abaixo da linha `<system.serviceModel>`:

```
<services> <service name="NetIQ.DRA.DRARestProxy.RestProxy">
<endpoint address="" binding="webHttpBinding"
bindingConfiguration="webHttpEndpointBinding"
name="webHttpEndpoint"
contract="NetIQ.DRA.DRARestProxy.IRestProxy" /> </service> </
services>
```

- Abaixo da linha `<serviceDebug includeExceptionDetailInFaults="false"/>`:

```
<serviceAuthorization impersonateCallerForAllOperations="true" /
> <serviceCredentials> <clientCertificate> <authentication
mapClientCertificateToWindowsAccount="true" /> </
clientCertificate> </serviceCredentials>
```

- Acima da linha `<serviceHostingEnvironment multipleSiteBindingsEnabled="true" />`:

```
<bindings> <webHttpBinding> <binding
name="webHttpEndpointBinding"> <security mode="Transport">
<transport clientCredentialType="Certificate" /> </security> </
binding> </webHttpBinding> </bindings>
```

9. Grave o arquivo e reinicie o servidor IIS.

Autenticação do Windows

Para habilitar a autenticação do Windows no Console da Web, você deve configurar o IIS (Serviços de Informações da Internet) e o arquivo de configuração de serviços REST.

1. Abra o Gerente do IIS.
2. No painel Conexões, localize o aplicativo web Serviços REST e selecione-o.
3. No painel direito, acesse a seção IIS e clique duas vezes em **Autenticação**.
4. Habilite **Autenticação do Windows** e desabilite todos os outros métodos de autenticação.
5. Uma vez habilitada a Autenticação do Windows, a opção **Providers** (Provedores) é adicionada ao menu de clique com o botão direito do mouse e ao painel Ações no lado direito da janela do gerenciador. Abra a caixa de diálogo Provedores e mova o **NTLM** para o topo da lista.
6. Use um editor de texto para abrir o arquivo `C:\inetpub\wwwroot\DRAClient\rest\web.config` e localize a linha `<authentication mode="None" />`.
7. Mude `"Nenhum"` para `"Windows"` e grave o arquivo.
8. Reinicie o servidor IIS.

Autenticação Multifator com a Advanced Authentication

O AAF (Advanced Authentication Framework) é o nosso pacote de software principal, que permite ir além de um simples nome de usuário e senha para uma maneira mais segura de proteger suas informações confidenciais usando a autenticação multifator.

O Advanced Authentication suporta os seguintes protocolos de comunicação para segurança:

- TLS 1.2 (configuração padrão), TLS 1.1, TLS 1.0
- SSL 3.0

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.

Existem três tipos de categorias de autenticação ou fatores:

- *Conhecimento*. Esta categoria exige que você conheça uma informação específica, como uma senha ou um código de ativação.
- *Posse*. Esta categoria exige que você tenha um dispositivo de autenticação, como um smart card ou smartphone.
- *Corpo*. Essa categoria exige que você use uma parte de sua anatomia, como sua impressão digital, como método de verificação.

Cada fator de autenticação contém pelo menos um método de autenticação. Um método de autenticação é uma técnica específica que você pode usar para estabelecer a identidade de um usuário, por exemplo, usando uma impressão digital ou exigindo uma senha.

Você poderá considerar que um processo de autenticação é forte se ele usar mais de um tipo de método de autenticação, por exemplo, exigir uma senha e uma impressão digital.

O Advanced Authentication suporta os seguintes métodos de autenticação:

- Senha LDAP
- Serviço do Usuário de Discagem de Autenticação Remota (RADIUS)
- Smartphone

Dica: O método Smartphone exige que o usuário faça download de um aplicativo para iOS ou Android. Para mais informações, consulte o *Guia do Usuário para Advanced Authentication – Aplicativos de Smartphone*, que está disponível no site na Web de Documentação da NetIQ.

Use as informações nas seções a seguir para configurar o Console da Web para usar a autenticação multifator.

Importante: Enquanto algumas das etapas nas seções a seguir ocorrem dentro do console da Web, a maioria do processo de configuração de autenticação multifator exige acesso ao AAF. Esses procedimentos pressupõem que você já tenha instalado o AAF e tenha acesso à documentação de ajuda do AAF.

Adicionando repositórios à Advanced Authentication Framework

A primeira etapa na configuração do Console da Web para usar a autenticação multifator para adicionar todos os domínios do Active Directory que contêm os administradores de DRA e os administradores assistentes gerenciados pelo DRA ao AAF. Esses domínios são chamados de repositórios e contêm os atributos de identidade dos usuários e grupos que você deseja autenticar.

1. Efetue login no portal de administração do AAF com um nome de usuário e senha em nível de administrador.
2. Acesse o painel esquerdo e clique em **Repositórios**.
3. Clique em **Adicionar**.
4. Preencha o formulário.

   Dica: O **tipo LDAP** é **AD**.

   Dica: Digite um nome de usuário e senha em nível de administrador nos campos correspondentes.
5. Clique em **Adicionar Servidor**.
6. Digite o endereço IP do servidor LDAP no campo **Endereço**.
7. Clique em **Gravar**.
8. Repita as etapas de 3 a 7 para todos os outros repositórios do AD gerenciados pelo DRA.
9. Para cada repositório listado na página Repositórios, clique em **Sincronizar agora** para sincronizá-lo com o servidor AAF.

Criando cadeias de autenticação

Uma cadeia de autenticação contém pelo menos um método de autenticação. Os métodos na cadeia serão invocados na ordem em que foram adicionados a ela. Para que um usuário seja autenticado, ele deve ser aprovado em todos os métodos na cadeia. Por exemplo, você pode criar uma cadeia que contenha o método de senha LDAP e o método SMS. Quando uma usuária tenta autenticar-se usando esta cadeia, ela deve primeiro autenticar usando sua senha LDAP. Após, uma mensagem de texto será enviada para o celular dela com uma senha para único uso. Após ela digitar a senha, todos os métodos na cadeia serão atendidos e a autenticação será bem-sucedida. Uma cadeia de autenticação pode ser atribuída a um usuário ou grupo específico.

Para criar uma cadeia de autenticação:

1. Efetue login no portal de administração do AAF com um nome de usuário e senha em nível de administrador.
2. Acesse o painel esquerdo e clique em **Cadeias**. O painel direito exibe uma lista da cadeias atualmente disponíveis.
3. Clique em **Adicionar**.
4. Preencha o formulário. Todos os campos são obrigatórios.

   Importante: Adicione os métodos na ordem em que devem ser invocados, ou seja, se você quiser que o usuário digite primeiro uma senha LDAP, adicione primeiro a senha LDAP à cadeia.

Importante: Verifique se o switch **Aplicar se usada pelo proprietário de endpoint** está DESATIVADO.

5 Alterne a opção **Está habilitado** para ATIVADA.

6 Digite os nomes das funções ou grupos a serem submetidos à solicitação de autenticação no campo **Funções e Grupos**.

Dica: Se você quiser que a cadeia se aplique a todos os usuários, digite `all users` no campo **Funções e Grupos** e selecione **Todos os Usuários** na lista suspensa resultante.

Qualquer usuário ou grupo selecionado será adicionado abaixo do campo **Funções e Grupos**.

7 Clique em **Gravar**.

Criando eventos de autenticação

Um evento de autenticação é acionado por um aplicativo, neste caso, o Console da Web, que deseja autenticar um usuário. Pelo menos uma cadeia de autenticação deve ser atribuída ao evento para que, quando o evento for acionado, os métodos na cadeia associada ao evento sejam chamados para autenticar o usuário.

Um endpoint é o dispositivo real – como um computador ou um smartphone – que está executando o software que aciona o evento de autenticação. O DRA registrará o endpoint com o AAF após você criar o evento.

Você pode usar a caixa de lista de permissões do endpoint para restringir o acesso a um evento a endpoints específicos ou pode permitir que todos os endpoints acessem o evento.

Para criar um evento de autenticação:

1 Efetue login no portal de administração do AAF com um nome de usuário e senha em nível de administrador.

2 Acesse o painel esquerdo e clique em **Eventos**. O painel direito exibe uma lista dos eventos atualmente disponíveis.

3 Clique em **Adicionar**.

4 Preencha o formulário. Todos os campos são obrigatórios.

Importante: Verifique se o switch **Está habilitado** está ATIVADO.

5 Se você quiser restringir o acesso a endpoints específicos, acesse a seção de lista de permissões de Endpoints e mova os endpoints de destino da lista *Disponível* para a lista *Usado*.

Dica: Se não houver endpoints na lista*Usado*, o evento ficará disponível para todos os endpoints.

Habilitando o console da Web

Após configurar cadeias e eventos, você pode efetuar login no Console da Web como um administrador e habilitar o Advanced Authentication.

Depois que a autenticação for habilitada, todos os usuários precisarão se autenticar por meio do AAF antes de receberem acesso ao console da Web.

Importante: Antes de habilitar o Console da Web, você já deve estar inscrito nos métodos de autenticação que o Console da Web usará para autenticar usuários. Consulte o *Advanced Authentication Framework User Guide* (Guia do Usuário da Advanced Authentication Framework) para saber mais sobre como se registrar em métodos de autenticação.

Para habilitar o Advanced Authentication, efetue login no Console da Web e acesse **Administração** > **Configuração** > **Advanced Authentication**. Selecione a caixa de seleção **Habilitado** e configure o formulário de acordo com as instruções fornecidas para cada campo.

Dica: Após gravar a configuração, o endpoint será criado no AAF. Para exibi-lo ou editá-lo, faça logon no portal de administração do AAF com um nome de usuário e senha de nível de administrador e clique em **Endpoints** no painel esquerdo.

Etapas finais

1. Faça logon no portal de administração do AAF com um nome de usuário e senha em nível de administrador e clique em **Eventos** no painel esquerdo.
2. Edite cada um dos eventos do Console da Web:
   - **2a** Abra o evento para edição.
   - **2b** Acesse a seção de lista de permissões de endpoints e mova o endpoint que você criou quando configurou o console da Web da lista **Disponível** para a lista **Usado**. Isso garantirá que apenas o console da Web possa usar esses eventos.
3. Clique em **Gravar**.

12 Conectando sistemas gerenciados

Esta seção fornece informações para conexão e configuração de sistemas gerenciados relacionados a domínios e componentes do Microsoft Exchange que incluem Public Folder, Exchange, Office 365 e Skype for Business Online.

Gerenciando domínios do Active Directory

Você pode adicionar novos domínios gerenciados e computadores por meio do cliente de Delegação e Configuração após instalar o servidor de Administração. Você também pode adicionar subárvores e domínios confiáveis e configurar o domínio e as contas de acesso do Exchange para eles. Para adicionar domínios gerenciados e computadores, você deve ter os poderes apropriados, como aqueles incluídos na função integrada Configurar Servidores e Domínios.

Observação: Após você terminar de adicionar domínios gerenciados, verifique se as programações de atualização de cache das contas para esses domínios estão corretas.

Adicionando Domínios Gerenciados e Computadores

Para adicionar um computador ou domínio gerenciado:

1 Acesse **Configuration Management** > **New Managed Domain** (Gerenciamento de Configurações > Novo Domínio Gerenciado).

2 Especifique o componente que você está adicionando, selecionando o botão de opção aplicável e fornecendo o domínio ou o nome do computador:

- **Gerenciar um domínio**
  - Se você deseja gerenciar a subárvore de um domínio, veja Adicionando uma subárvore gerenciada.
  - Se você está adicionando um novo domínio com LDAP seguro habilitado em seus controladores de domínio e deseja que o DRA use SSL para se comunicar com seus controladores de domínio, selecione **Este domínio está configurado para LDAP por SSL**. Para obter mais informações, veja Configurando o DRA para executar o Active Directory Seguro.
- **Gerenciar um computador**

Clique em **Próximo** após terminar a configuração.

3 Na guia **Acesso ao domínio**, especifique as credenciais da conta que você deseja que o DRA use para acessar esse domínio ou computador. Por padrão, o DRA usa a conta de serviço do servidor de Administração.

4 Revise o resumo e clique em **Finish** (Terminar).

5 Para começar a gerenciar objetos deste domínio ou computador, atualize a configuração do domínio.

Especificando contas de acesso ao domínio

Para cada domínio gerenciado ou subárvore, você pode especificar uma conta para usar em vez da conta de serviço do servidor de Administração para acessar esse domínio. Essa conta alternativa é chamada de conta de acesso. Para configurar uma conta de acesso, você precisa ter os poderes apropriados, como aqueles incluídos na função integrada Configurar Servidores e Domínios.

Para especificar uma conta de acesso para um servidor membro, você precisa ter permissão para gerenciar o domínio no qual o membro do domínio existe. Você só pode gerenciar membros do domínio se eles existirem em um domínio gerenciado que você possa acessar por meio do servidor de Administração.

Para especificar uma conta de acesso:

1 Acesse **Configuration Management** (Gerenciamento de Configurações) > nó **Managed Domains** (Domínios Gerenciados).

2 Clique o botão direito do mouse no domínio ou na subárvore para a qual você deseja especificar uma conta de acesso e clique em **Propriedades**.

3 Na guia Domain access account (Conta de acesso do domínio), clique em **Use the following account to access this domain** (Usar a seguinte conta para acessar este domínio).

4 Especifique e confirme as credenciais para esta conta e clique em **OK**.

Para obter informações sobre como configurar essa conta com menos privilégios, consulte Contas de acesso do DRA com privilégios mínimos.

Especificando contas de acesso do Exchange

Para cada domínio no DRA, você pode gerenciar objetos do Exchange usando a conta de acesso ao domínio do DRA ou uma conta de acesso separada do Exchange. Para configurar uma conta de acesso do Exchange, você deve ter os poderes apropriados, como aqueles incluídos na função integrada Configurar Servidores e Domínios.

Importante: O Servidor da Microsoft limita o número de usuários simultâneos conectados à sessão do WinRM/WinRS a cinco e o número de shells por usuário a cinco de modo a garantir que a mesma conta do usuário seja limitada a cinco shells para servidores secundários do DRA.

Para especificar uma conta de acesso do Exchange:

1. Acesse **Configuration Management** (Gerenciamento de Configurações) > nó **Managed Domains** (Domínios Gerenciados).
2. Clique o botão direito do mouse no domínio ou na subárvore para a qual você deseja especificar uma conta de acesso e clique em **Propriedades**.
3. Na guia Exchange access account (Conta de acesso do Exchange), clique em **Use the following account to access all Exchange servers** (Usar a seguinte conta para acessar todos os servidores do Exchange).
4. Especifique e confirme as credenciais para esta conta e clique em **OK**.

Para obter informações sobre como configurar essa conta com menos privilégios, consulte Contas de acesso do DRA com privilégios mínimos.

Adicionando uma subárvore gerenciada

Você pode adicionar subárvores gerenciadas e ausentes de domínios específicos do Microsoft Windows após instalar o servidor de Administração. Para adicionar uma subárvore gerenciada, você precisa ter os poderes apropriados, como aqueles incluídos na função integrada Configurar Servidores e Domínios.

Para obter informações sobre as versões suportadas do Microsoft Windows, consulte Requisitos do Servidor de Administração e do Console da Web do DRA.

Ao gerenciar uma subárvore de um domínio do Windows, você pode usar o DRA para proteger um departamento ou uma divisão dentro de um domínio corporativo maior.

Por exemplo, você pode especificar a subárvore de Houston no domínio SOUTHWEST, permitindo que o DRA gerencie com segurança somente os objetos contidos na OU de Houston e suas OUs filho. Essa flexibilidade permite gerenciar uma ou mais subárvores sem exigir permissões administrativas para todo o domínio.

Observação

- Para verificar se a conta especificada tem permissões para gerenciar essa subárvore e realizar atualizações de cache de contas incrementais, use o Utilitário Objetos Apagados para verificar e delegar as permissões apropriadas.
- Após você terminar de adicionar subárvores gerenciadas, verifique se as programações de atualização de cache das contas para os domínios correspondentes estão corretas.

Para adicionar uma subárvore gerenciada:

1. Acesse **Gerenciamento de Configuração** > **Novo Domínio Gerenciado**.
2. Na guia Domain or server (Domínio ou servidor), clique em **Manage a domain** (Gerenciar um domínio) e especifique o domínio da subárvore que você deseja gerenciar.
3. Especifique o domínio da subárvore que você deseja gerenciar.
4. Selecione **Manage a subtree of this domain** (Gerenciar uma subárvore deste domínio) e clique em **Next** (Próximo).
5. Na guia Subtrees (Subárvores), clique em **Adicionar** para especificar a subárvore que você deseja gerenciar. Você pode especificar mais de uma subárvore.
6. Na guia Conta de acesso, especifique as credenciais da conta que você deseja que o DRA use para acessar essa subárvore. Por padrão, o DRA usa a conta de serviço do servidor de Administração.
7. Revise o resumo e clique em **Finish** (Terminar).
8. Para começar a gerenciar objetos desta subárvore, atualize a configuração do domínio.

Adicionando um domínio de confiança

Domínios confiáveis permitem a autenticação do usuário em sistemas gerenciados em todo o ambiente gerenciado. Depois de adicionar um domínio de confiança, você pode especificar contas de acesso ao domínio e ao Exchange, programar atualizações de cache e realizar outras ações nas propriedades do domínio, da mesma forma que um domínio gerenciado.

Para adicionar um domínio de confiança:

1. No nó **Configuration Management** > **Managed Domains** (Gerenciamento de Configurações > Domínios Gerenciados), selecione o domínio gerenciado que tenha um domínio confiável associado.
2. Clique em **Trusted domains** (Domínios confiáveis) no painel Mais informações. O painel Mais informações deve ser ativado no menu Ver.
3. Clique o botão direito do mouse no domínio de confiança e selecione **Propriedades**.
4. Desmarque **Ignore this trusted domain** (Ignorar este domínio confiável) e aplique suas mudanças.

Observação: Adicionar um domínio de confiança iniciará uma atualização completa do cache de contas, mas você será notificado disso com um prompt de confirmação ao clicar em **Aplicar**.

Configurando o DRA para executar o Active Directory Seguro

O Active Directory Seguro é definido por um ambiente DRA configurado para execução usando o protocolo LDAPS (LDAP por SSL) para criptografar as comunicações entre o DRA e o Active Directory para fornecer um ambiente mais seguro.

Ao fazer upgrade para uma versão 10.x de uma versão 9.x do DRA, o LDAPS precisa ser habilitado após o upgrade para usar o Active Directory Seguro. O recurso de Descoberta Automática para detectar e conectar-se com os servidores do DRA e REST também precisa ser configurado para esse recurso.

Habilitar LDAP Por SSL (LDAPS)

Se você está fazendo upgrade para a versão 10.x de uma versão 9.x do DRA, siga as etapas abaixo. Se você está configurando o DRA para uma nova instalação, veja Adicionando Domínios Gerenciados e Computadores.

1. Navegue até **Configuration Management** > **Managed Domains** (Gerenciamento de Configurações > Domínios Gerenciados) no console de Delegação e Configuração do DRA.
2. Clique o botão direito do mouse no domínio e abra Propriedades.
3. Habilite **Este domínio está configurado para LDAP por SSL** na guia Geral e clique em **OK**.
4. Reinicie o Serviço de Administração da NetIQ.

Observação: Se você também estiver configurando a Descoberta Automática para usar o Active Directory Seguro, poderá esperar para reiniciar os serviços após terminar a configuração. Para obter mais informações, veja Configurar a Descoberta Automática para LDAPS.

Configurar a Descoberta Automática para LDAPS

A Descoberta Automática é o mecanismo usado pelo cliente para conectar-se automaticamente com o ambiente DRA disponível.

Para configurar o DRA para um ambiente executando o Active Directory Seguro, configure a chave de Registro `ClientSSLAllDomains`:

1. Inicie o utilitário do Editor do Registro.
2. Clique o botão direito do mouse no nó `HKEY_LOCAL_MACHINE SOFTWARE\Wow6432Node\Mission Critical Software\RestExtentions`.
3. Selecione **Novo** > **Valor DWORD (32 bits)**.
4. Nomeie a nova chave como `ClientSSLAllDomains`.
5. Defina o valor da chave de Registro como 1.
6. Após adicionar a chave de registro `ClientSSLAllDomains`, reinicie os seguintes serviços:
   - Serviço de Publicação na World Wide Web
   - Serviço REST do DRA da NetIQ

Conectando pastas públicas

O DRA permite gerenciar pastas públicas do Microsoft Exchange. Você pode gerenciar algumas das propriedades de Pastas Públicas usando o DRA, configurando domínios de floresta de Pasta Pública e concedendo poderes a administradores assistentes.

Importante: Para gerenciar a administração de pastas públicas, você precisa primeiro habilitar o suporte do Microsoft Exchange no DRA e ter os poderes aplicáveis.

- Para obter informações sobre como habilitar o Microsoft Exchange, consulte Habilitando o Microsoft Exchange.
- Para obter informações sobre permissões de conta, consulte Contas de acesso do DRA com privilégios mínimos.

Para configurar o suporte à Pasta Pública do Exchange:

1. Clique o botão direito do mouse em **Managed Public Folder Forests** (Florestas de Pastas Públicas Gerenciadas) no nó Configuration and Management (Configuração e Gerenciamento) e clique em **New Public Folder Forest** (Nova Floresta de Pastas Públicas).
2. Clique em **Forest Domain** (Domínio de Floresta), especifique a floresta do Active Directory em que os objetos de pasta pública estão localizados e clique em **Next** (Próximo).
3. No **Acesso ao domínio**, especifique a conta de acesso.

   Importante: Se você estiver usando o Servidor Secundário, a opção **Usar a conta de acesso ao domínio do Servidor de Administração Principal** ficará disponível.

   ---
4. Em **Acesso ao Exchange**, especifique a conta que você deseja que o DRA use para acesso seguro aos servidores do Exchange.

   Importante: Se você estiver usando o servidor secundário, a opção **Use the Primary Administration Server Exchange access account** (Usar a conta de acesso do Exchange do Servidor de Administração Principal) ficará disponível.

   ---
5. No **Servidor do Exchange**, selecione o Exchange Server que você deseja que o DRA use para gerenciar pastas públicas.
6. Em **Summary** (Resumo), revise mais informações da conta e mais informações do Exchange Server e clique em **Finish** (Terminar) para concluir o processo.

   O servidor DRA executa a atualização do cache de contas completas na pasta pública. A nova floresta de Pastas Públicas aparecerá no console após a conclusão da atualização do cache, o que pode levar alguns minutos.

Observação: Você pode remover um domínio de floresta de pasta pública selecionado por meio de **Tarefas** ou do menu aberto clicando o botão direito do mouse.

- "Exibindo e modificando propriedades de domínio de pasta pública" na página 133
- "Delegando poderes de pasta pública" na página 133

Exibindo e modificando propriedades de domínio de pasta pública

Para exibir ou modificar propriedades do domínio de pasta pública:

1. Clique em **Managed Public Folder Forests** (Florestas de Pastas Públicas Gerenciadas) no nó Configuration Management (Gerenciamento de Configurações) para exibir as pastas públicas.
2. Clique o botão direito do mouse na conta de pasta pública que você deseja exibir e selecione **Propriedades**.
3. Nas propriedades **Floresta da Pasta Pública**, você pode executar as seguintes ações:
   - **Geral:** Ver mais informações da conta de pasta pública e atualizar o campo **Exchange Server**, que é usado pelo servidor DRA para executar a atividade do Exchange no servidor de pasta pública.
   - **Estatísticas:** Ver o número de pastas públicas e o número de pastas públicas habilitadas para e-mail.
   - **Incremental Status (Status Incremental):** Ver ou atualizar o status do cache de contas incrementais.
   - **Incremental schedule (Programação incremental):** Ver a programação de atualização de cache incremental e reprogramar uma atualização de cache.
   - **Full status (Status completo):** Ver o status completo da atualização do cache da conta.
   - **Full refresh (Atualização completa):** Executar uma atualização completa do cache da conta imediatamente.

     A NetIQ recomenda que você execute uma **Full refresh** (Atualização completa) somente se os dados do cache da Pasta Pública estiverem corrompidos.
   - **Domain access (Acesso ao domínio):** Ver mais informações da conta de serviço DRA ou anular contas de acesso.
   - **Exchange access (Acesso ao Exchange):** Ver ou atualizar o acesso seguro aos servidores do Exchange.

Delegando poderes de pasta pública

Use as Telas Ativas para definir poderes e gerenciar a delegação de Pasta Pública. Você pode especificar regras para adicionar objetos gerenciados, escolher domínios e designar poderes e, em seguida, delegar esses poderes de Pasta Pública a administradores assistentes.

Para criar uma Tela Ativa e delegar poderes de Pasta Pública:

1. No nó **Delegation Management** (Gerenciamento de Delegação), clique em **ActiveViews** (Telas Ativas).
2. Clique em **Next** (Próximo) no **Assistente > Create ActiveView** (Criar Tela Ativa), selecione a regra necessária na lista suspensa **Adicionar** e escolha Pastas Públicas como o tipo de objeto. Por exemplo, para criar uma regra de correspondência de objetos, selecione **Objects that match a rule** (Objetos que correspondem a uma regra) e escolha **Pastas Públicas** como o tipo de objeto.
3. Especifique a regra de Tela Ativa que você deseja adicionar à Pasta Pública e clique em **Próximo**.
4. Especifique o nome da Tela Ativa e clique em **Terminar**.

5 Clique o botão direito do mouse em **ActiveViews** (Telas Ativas) e acesse **Delegate Administration** (Delegar Administração) > **Admins Assistentes** e especifique o tipo de Admin na lista expansível **Adicionar** em **Assistente**.

6 Pesquise o usuário, o grupo ou o grupo de administradores assistentes específico ao qual você deseja delegar poderes.

7 Use o **Seletor de Objetos** para localizar e adicionar os objetos desejados e clique em **Roles and Powers** (Funções e Poderes) no **Assistente**.

8 Selecione **Funções** na lista suspensa **Adicionar** e pesquise e adicione a função Administração de Pasta Pública.

9 Selecione Poderes na lista suspensa **Adicionar** e, em seguida, localize e adicione quaisquer poderes adicionais que você deseje atribuir a seus administradores assistentes que não fazem parte da função Administração de Pasta Pública.

10 Clique em **Next** (Próximo) e em **Finish** (Terminar) para concluir o processo de delegação.

Após concluir a delegação de poderes da Pasta Pública, os usuários autorizados poderão executar operações de criar, ler, atualizar e apagar nas propriedades da Pasta Pública em domínios configurados usando o Console da Web.

Habilitando o Microsoft Exchange

Habilitar o Microsoft Exchange permite que você aproveite os recursos do Exchange e do Exchange Online, para incluir políticas do Microsoft Exchange, caixa de correio integrada e gerenciamento de objetos habilitados para correio. Você pode habilitar ou desabilitar o suporte do Microsoft Exchange em cada servidor de Administração do Microsoft Exchange Server 2013 e versões posteriores.

Para habilitar o Exchange, você precisa dos privilégios necessários, como aqueles incluídos na função incorporada Gerenciar Políticas e Acionadores de Automação, e sua licença deve suportar o produto Exchange. Para obter mais informações sobre os requisitos do Microsoft Exchange, consulte Plataformas suportadas.

Para habilitar o suporte para o Microsoft Exchange e o Exchange Online:

1 Navegue até **Policy and Automation Management** > **Configure Exchange Policies** (Gerenciamento de Políticas e Automação > Configurar Políticas do Exchange) no console de Delegação e Configuração.

2 Selecione **Habilitar a Política do Exchange** e clique em **Aplicar**.

Configurando Locatários do Azure

Com uma conta ativa do Azure e um ou mais locatários do Azure, você pode configurar o DRA para trabalhar com o Azure Active Directory para gerenciar objetos usuário e grupo. Esses objetos incluem usuários e grupos criados no Azure e usuários e grupos sincronizados com o locatário do Azure de domínios gerenciados do DRA.

Os módulos do Azure PowerShell, o Azure Active Directory e o Perfil do Azure Resource Manager são necessários para gerenciar tarefas do Azure. Você também precisa de uma conta no Azure Active Directory. Para obter informações sobre permissões de conta de acesso de locatário do Azure, veja Contas de acesso do DRA com privilégios mínimos.

Importante: Operações em objetos do Azure como criar, modificar, apagar, desabilitar e habilitar não são suportadas no Console de Delegação e Configuração.

- "Delegando Funções e Poderes" na página 135
- "Criando um Aplicativo do Azure e Adicionando um Locatário do Azure" na página 136
- "Redefinindo uma Senha de Aplicativo do Azure" na página 138

Delegando Funções e Poderes

Você pode usar o Administrador do DRA ou um administrador assistente com a função delegada "Configurar Servidores e Domínios" para gerenciar locatários do Azure e as funções incorporadas do Azure são necessárias para gerenciar objetos do Azure.

Funções Incorporadas do Azure

Para delegar objetos do Azure, designe as seguintes funções do Azure:

- **Administração do Grupo do Azure:** Fornece todos os poderes necessários para gerenciar os grupos do Azure e a participação no grupo do Azure.
- **Administração do Usuário do Azure:** Fornece todos os poderes necessários para gerenciar usuários do Azure.
- **Administração de contatos do Azure:** Fornece todas as capacidades necessárias para gerenciar contatos do Azure.

Capacidades do Azure

Use as seguintes capacidades para delegar a criação e o gerenciamento de usuários, grupos e contatos do Azure.

Poderes da Conta do Usuário do Azure:

- Criar Usuário do Azure e Modificar Todas as Propriedades
- Apagar Permanentemente a Conta do Usuário do Azure
- Gerenciar Entrada para Usuários do Azure
- Gerenciar Entrada para Usuários do Azure Sincronizados com o Locatário do Azure
- Modificar Todas as Propriedades de Usuário do Azure
- Redefinir a Senha da Conta do Usuário do Azure
- Ver Todas as Propriedades de Usuário do Azure

Poderes do Grupo do Azure:

- Adicionar Objeto ao Grupo do Azure
- Criar Grupo do Azure e Modificar Todas as Propriedades
- Apagar a Conta do Grupo do Azure
- Modificar Todas as Propriedades de Grupo do Azure
- Remover o Objeto do Grupo do Azure
- Ver Todas as Propriedades de Grupo do Azure

Capacidades de contato do Azure:

- Criar contato do Azure e Modificar todas as propriedades
- Apagar a conta do contato do Azure
- Modificar todas as propriedades do contato do Azure
- Ver todas as propriedades do contato do Azure

Para gerenciar propriedades em nível granular para usuários do Azure, você pode criar capacidades personalizadas selecionando atributos de objetos especificados.

Objetos do Azure Suportados

Os seguintes tipos de grupos do Azure são suportados:

- Lista de Distribuição
- Segurança habilitada para correio
- Office 365
- Segurança

Observação: Usuários convidados criados no Azure não são suportados.

Criando um Aplicativo do Azure e Adicionando um Locatário do Azure

Para gerenciar um novo locatário do Azure, adicione o novo locatário concluindo um aplicativo do Azure no Console de Delegação e Configuração. O DRA suporta a criação do aplicativo do Azure online e offline e requer um aplicativo do Azure com as seguintes permissões para gerenciar objetos no locatário:

- Leia e grave os perfis completos de todos os usuários
- Leia e grave todos os grupos
- Leia os dados do diretório

Essas permissões serão concedidas automaticamente ao aplicativo do Azure, tanto na abordagem Online quanto Offline.

Para criar um Aplicativo do Azure online e adicionar um locatário:

1. Navegue até **Gerenciamento de Configurações** > **Locatários do Azure** no Console de Delegação e Configuração.
2. Clique o botão direito do mouse em **Locatários do Azure** e selecione Novo Locatário do Azure.
3. (Opcional) Especifique o atributo de âncora de origem usado para mapear seus objetos do Active Directory para o Azure durante a sincronização.
4. Especifique a conta usada para acessar o locatário do Azure e valide as credenciais.

   Para obter informações sobre permissões de conta de acesso de locatário do Azure, veja Contas de acesso do DRA com privilégios mínimos.
5. Selecione a opção **Permitir que o DRA crie o aplicativo do Azure**.

6 Especifique as credenciais para uma conta do usuário com a função de Administrador da Empresa do Azure AD e valide as credenciais.

7 Clique em **Terminar**.

A adição do locatário do Azure pode levar alguns minutos. Depois que o locatário é adicionado com êxito, o DRA executa uma atualização completa do cache de contas para o locatário e o locatário adicionado é exibido no painel de exibição Locatários do Azure.

Observação: Após a conclusão da atualização, se você quiser verificar o status da conta de todos os locatários gerenciados do Azure, instale o módulo `msonline` do PowerShell e execute a verificação **Tenant Accounts Overview** (Visão Geral das Contas de Locatários) no Utilitário de Verificação de Saúde. Para instalar o módulo, execute o comando `install-module msonline` no PowerShell.

Para criar um aplicativo do Azure offline para o DRA e adicionar um locatário:

1 Navegue até **Gerenciamento de Configurações** > **Locatários do Azure** no Console de Delegação e Configuração.

2 Clique o botão direito do mouse em **Locatários do Azure** e selecione **Novo Locatário do Azure**.

3 (Opcional) Especifique o atributo de âncora de origem usado para mapear seus objetos do Active Directory para o Azure durante a sincronização.

4 Especifique a conta usada para acessar o locatário do Azure e valide as credenciais.

5 Selecione a opção **Criar o aplicativo do Azure offline**.

6 Inicie uma sessão do PowerShell no Servidor de administração DRA e navegue até `C:\Program Files (x86)\NetIQ\DRA\SupportingFiles`

7 Execute `. .\NewDraAzureApplication.ps1` para carregar o PowerShell.

8 Execute o cmdlet `New-DRAAzureApplication` para solicitar parâmetros.

9 Especifique os parâmetros a seguir para `New-DraAzureApplication`:

- <name> – Nome do aplicativo do assistente de locatário.

  Importante: A Micro Focus recomenda que você use o nome especificado no console do DRA.

- (Opcional) <ambiente> – Especifique AzureCloud, AzureChinaCloud, AzureGermanyCloud ou AzureUSGovernment, dependendo de qual locatário você está usando.

10 Na caixa de diálogo Credencial, especifique as credenciais de Administrador da Empresa.

O ID do aplicativo e a senha do Azure são gerados.

11 Copie o ID e a senha do aplicativo no console do DRA (assistente de locatário **Credenciais do Aplicativo do Azure do DRA**) e valide as credenciais.

12 Clique em **Terminar**.

A adição do locatário do Azure pode levar alguns minutos. Depois que o locatário é adicionado com êxito, o DRA executa uma atualização completa do cache de contas para o locatário e o locatário adicionado é exibido no painel de exibição Locatários do Azure.

Observação: Após a conclusão da atualização, se você quiser verificar o status da conta de todos os locatários gerenciados do Azure, instale o módulo `msonline` do PowerShell e execute a verificação **Tenant Accounts Overview** (Visão Geral das Contas de Locatários) no Utilitário de Verificação de Saúde. Para instalar o módulo, execute o comando `install-module msonline` no PowerShell.

Redefinindo uma Senha de Aplicativo do Azure

Siga as etapas abaixo se precisar redefinir uma senha do Azure, online ou offline, conforme aplicável.

Para redefinir uma senha de aplicativo do Azure para DRA usando Credenciais do Azure:

1. Navegue até **Gerenciamento de Configurações** > **Locatários do Azure** no Console de Delegação e Configuração.
2. Clique o botão direito do mouse no locatário gerenciado do Azure e selecione **Propriedades**.
3. Clique em **Aplicativo do Azure** na página de Propriedades.
4. Escolha a opção **Allow DRA to reset the password using your Azure Credentials** (Permitir que o DRA redefina a senha usando suas Credenciais do Azure) e, então, especifique as credenciais do Azure.
5. Aplique as mudanças.

Para redefinir uma senha de aplicativo do Azure para o DRA offline:

1. Inicie uma sessão do PowerShell no Servidor de administração DRA e navegue até `C:\Program Files (x86)\NetIQ\DRA\SupportingFiles`
2. Execute `. .\ResetDraAzureApplicationPassword.ps1` para carregar o PowerShell.
3. Execute o cmdlet `. .\ResetDraAzureApplicationPassword` para solicitar parâmetros.
4. Especifique os parâmetros a seguir para `Reset-DRAAzureApplicationPassword`:
   - <name> – Nome do aplicativo do assistente de locatário.

     Importante: A Micro Focus recomenda que você use o nome especificado no console do DRA.

   - (Opcional) <ambiente> – Especifique AzureCloud, AzureChinaCloud, AzureGermanyCloud ou AzureUSGovernment, dependendo de qual locatário você está usando.
5. Na caixa de diálogo Credencial, especifique as credenciais de Administrador da Empresa.

   O ID do aplicativo e a senha do Azure são gerados.
6. Copie o ID e a senha do aplicativo no console do DRA (assistente de locatário **Credenciais do Aplicativo do Azure do DRA**) e valide as credenciais.
7. Abra o Console de Delegação e Configuração e navegue até **Gerenciamento de Configurações** > **Locatários do Azure**.
8. Clique o botão direito do mouse em um locatário do Azure e acesse **Propriedades** > **Aplicativo do Azure**.
9. Escolha a opção **Redefinir a senha offline** usando a opção de script fornecida e cole a senha do aplicativo do Azure que é gerada do script.
10. Aplique as mudanças.

Gerenciando senhas para contas de acesso

Você pode redefinir senhas para contas de acesso que são usadas para gerenciar um domínio, servidor secundário, Exchange ou locatário do Azure do DRA. Se a senha de qualquer uma dessas contas de acesso estiver prestes a expirar ou se você esquecer a senha, poderá redefinir a senha da conta de acesso das seguintes maneiras:

- Redefinir a senha manualmente no Console de Delegação e Configuração.
- Programar uma tarefa para monitorar o vencimento de senhas para contas de acesso e redefinir a senha para contas de acesso que estão prestes a expirar.

Você pode redefinir a senha para contas de acesso tanto do servidor principal quanto do servidor secundário. Se a mesma conta de acesso for usada em várias instâncias no mesmo domínio, por exemplo, para gerenciar uma caixa de correio do Exchange ou um servidor secundário, o servidor DRA atualizará automaticamente a senha para todas as instâncias do uso da conta de acesso, eliminando assim a necessidade de atualizar manualmente a senha para cada instância. Se o Servidor de administração secundário usar a conta de acesso de domínio do Servidor de administração primário, o servidor DRA atualizará automaticamente a senha da conta de acesso no Servidor de administração secundário.

- “Redefinir a senha manualmente” na página 139
- “Programar uma tarefa para redefinir senha” na página 140

Redefinir a senha manualmente

Use o Console de Delegação e Configuração para redefinir manualmente a senha de uma conta de acesso.

Para redefinir manualmente a senha de uma conta de acesso:

1. No console de Delegação e Configuração, clique em **Configuration Management** (Gerenciamento de Configurações).
2. Selecione um domínio gerenciado ou um locatário do Azure e veja as propriedades.
3. Na página de propriedades, especifique as seguintes informações:
   - Para atualizar a senha de uma conta de acesso de domínio, na guia Acesso de domínio, especifique uma nova senha para a conta de acesso de domínio. Selecione **Update password in Active Directory** (Atualizar a senha no Active Directory).
   - Para atualizar a senha de uma conta de acesso do Exchange, na guia de acesso do Exchange, especifique uma nova senha para a conta de acesso do Exchange. Selecione **Update password in Active Directory** (Atualizar a senha no Active Directory).
   - Para atualizar a senha de uma conta de acesso do locatário do Azure, na guia de acesso do Locatário, especifique uma nova senha para a conta de acesso do locatário. Selecione **Update Azure tenant access account password** (Atualizar a senha da conta de acesso do locatário do Azure).
   - Para atualizar a senha de uma conta de acesso para um Servidor de administração secundário, selecione **Configuration Management** > **Administration Servers** (Gerenciamento de Configurações > Servidores de Administração) no Servidor de administração primário. Selecione o Servidor de administração secundário cuja senha deseja atualizar, clique o

botão direito do mouse nele e selecione **Propriedades**. Na guia Conta de acesso, especifique uma nova senha para a conta de acesso. Selecione **Update password in Active Directory** (Atualizar a senha no Active Directory).

Observação

- Verifique se a conta de acesso do Servidor de administração secundário não é a conta de serviço do Servidor de administração secundário. A conta de acesso deve fazer parte do grupo de Administradores Locais no Servidor de administração secundário.
- Caso você use a conta de menor privilégio como a conta de acesso, verifique se a conta recebeu a permissão “Redefinir Senha” para si mesma no Active Directory para que a redefinição de senha seja bem-sucedida no DRA.

Programar uma tarefa para redefinir senha

Você pode programar a tarefa Redefinir senha para ser executada em um intervalo predefinido para redefinir senha para suas contas de acesso que estão expirando. A tarefa redefinirá todas as senhas de contas de acesso que estão prestes a expirar antes da próxima vez que a tarefa for agendada para ser executada. Uma nova senha será gerada automaticamente de acordo com a política de senha.

A tarefa está desabilitada por padrão. Você pode programar a tarefa uma vez por semana ou em um intervalo específico, de acordo com sua exigência. Em um ambiente MMS, se você configurar a tarefa no servidor principal, verifique se ela está configurada em todos os servidores no MMS.

Para configurar a tarefa:

1. No servidor em que deseja programar a tarefa, acesse a entrada de registro `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Mission Critical Software\OnePoint\Administration\Modules\Accounts\UpdateAccessAccPWD.Freq`.
2. Clique o botão direito do mouse e selecione **Modificar**.
3. No campo **Value data** (Dados do valor), especifique a frequência com que deseja que a tarefa seja executada.
   - Para programar uma tarefa semanal, especifique a frequência no formato `Weekly <Dia da semana> <Hora no formato de 24 horas>`. Por exemplo, para programar a tarefa para ser executada todos os sábados às 18:00, digite:

     `Weekly 06 18:00`

     Em que 6 indica o dia da semana e `18:00` indica a hora no formato de 24 horas.
   - Para programar a tarefa para ser executada em um intervalo específico, especifique a frequência no formato `Interval <Hora no formato de 24 horas>`. Por exemplo, para programar a tarefa para ser executada a cada 8 horas, digite:

     `Interval 08:00`

   Recomenda-se programar a tarefa para ser executada nos finais de semana.

Observação: A tarefa Redefinir a senha não suporta frequência diária. Se você configurar a frequência diária, o Servidor DRA redefinirá automaticamente a programação para `Weekly 06 00:00` quando você reiniciar o NetIQ Administration Service.

4 Clique em **OK**.

5 Reinicie o **Serviço de Administração da NetIQ** para que as mudanças entrem em vigor.

Observação: Para cada locatário do Azure configurado, a tarefa cria a seguinte chave de registro para a política de senha padrão com validade de 90 dias: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Mission Critical Software\OnePoint\Administration\Modules\Accounts\<tenantName>.ValidityPeriod`. A data de validade da senha da conta de acesso do locatário é calculada com base no prazo de validade do locatário. Quando a senha está prestes a expirar, a tarefa redefine a senha da conta de acesso do locatário.

Habilitar a autenticação de anulação de LDAP

Você pode configurar uma autenticação de anulação de LDAP para modificações da sub-rotina personalizada do LDAP no Console da Web. Com esse recurso habilitado, você pode definir que o tipo de autenticação para sub-rotinas de consulta do LDAP personalizadas exigirá a conta de anulação de LDAP para autenticação de conexão.

Para habilitar esse recurso:

1 Navegue até **Configuration Management** > **Update Administration Server Options** (Gerenciamento de Configurações > Atualizar as Opções do Servidor de Administração) no Console de Delegação e Configuração.

2 Selecione a guia **Conta de Anulação de LDAP** na janela Opções do servidor de administração.

3 Forneça o nome da conta, o domínio e a senha e aplique as mudanças.

Por exemplo: `nome@domínio` ou `domínio\nome`

Para obter informações sobre o uso deste recurso em personalizações do Console da Web, consulte Etapas básicas para criar uma sub-rotina personalizada.

V Automação de políticas e processos

Este capítulo fornece informações para ajudá-lo a entender como as políticas funcionam no ambiente do DRA e quais são essas opções de política. Também explica como os acionadores e o workflow automatizado são usados para automatizar processos ao trabalhar com objetos no Active Directory.

13 Entendendo a política do DRA

O DRA permite que você configure várias políticas que ajudam a proteger sua empresa e evitar danos aos dados. Essas políticas funcionam dentro do contexto do modelo de segurança dinâmica, garantindo que a aplicação da política acompanhe automaticamente sua empresa em constante mudança. O estabelecimento de políticas, como convenções de nomenclatura, limites de uso de disco e validação de propriedade, permite assegurar o uso obrigatório de regras que ajudam a manter a integridade de seus dados corporativos.

No DRA, você pode definir rapidamente as regras de política para estas áreas de gerenciamento corporativo:

- Microsoft Exchange
- Office 365 Licença
- Diretório Pessoal
- Geração de senha

O DRA também fornece políticas integradas para grupos, contas do usuário e computadores.

Para gerenciar ou definir políticas, você deve ter os poderes adequados, como aqueles incluídos nas funções Admins do DRA ou Gerenciar Políticas e Acionadores de Automação. Para ajudar você a gerenciar suas políticas, o DRA fornece o relatório Mais Informações da Política. Este relatório fornece as seguintes informações:

- Indica se a política está habilitada
- Relaciona operações associadas
- Relaciona objetos governados por esta política
- Fornece mais informações do escopo de política

Você pode usar esse relatório para verificar se suas políticas são definidas corretamente. Você também pode usar esse relatório para comparar as propriedades da política, capturando conflitos e aplicando melhor as políticas em toda a empresa.

Como o servidor de administração aplica a política

Você pode associar cada tarefa ou operação de administração a uma ou mais políticas. Quando você executa uma operação associada a uma política, o servidor de Administração executa a política e impõe as regras especificadas. Se o servidor detectar uma violação de política, ele retornará uma mensagem de erro. Se o servidor não detectar uma violação de política, a operação será concluída. Você pode limitar o escopo de uma política, associando-a a determinadas Telas Ativas ou grupos de Admin Assistentes.

Se uma operação estiver associada a mais de uma política, o servidor de Administração aplicará as políticas em ordem alfabética. Ou seja, a Política A será aplicada antes da Política B, independentemente das regras especificadas.

Para verificar se suas políticas não entram em conflito entre si, use as seguintes diretrizes:

- Nomeie as políticas para que elas sejam executadas na ordem correta
- Verifique se cada política não interfere nas validações ou ações realizadas por outras políticas
- Teste detalhadamente as políticas personalizadas antes de implementá-las em seu ambiente de produção

O servidor de Administração insere o status da política no registro de auditoria sempre que uma política é executada. Essas entradas de log registram o código de retorno, as operações associadas, os objetos executados e se a política personalizada foi bem-sucedida.

Aviso: As políticas são executadas usando a conta de serviço Administração. Como a conta de serviço tem permissões de administrador, as políticas têm acesso total a todos os dados corporativos. Assim, os administradores assistentes associados à função incorporada Gerenciar Políticas e Acionadores de Automação poderiam obter mais poder do que você pretendia.

Política integrada

Políticas integradas são implementadas quando você instala o servidor de Administração. Ao trabalhar com essas políticas, você pode encontrar os seguintes termos:

Escopo da política

Define os objetos ou propriedades aos quais o DRA aplica a política. Por exemplo, algumas políticas permitem que você aplique uma política a administradores assistentes específicos em Telas Ativas específicas. Algumas políticas permitem escolher entre diferentes classes de objetos, como contas do usuário ou grupos.

Políticas globais

Assegure o uso obrigatório regras de política a todos os objetos da classe ou tipo especificado nos domínios gerenciados. As políticas globais não permitem limitar o escopo dos objetos aos quais a política se aplica.

Relacionamento da política

Define se a política se aplica em conjunto ou por si só. Para estabelecer um relacionamento de política, defina duas ou mais regras que se aplicam à mesma ação e escolha o membro de uma opção do grupo de políticas. Se os parâmetros ou as propriedades da operação corresponderem a qualquer uma das regras, a operação será bem-sucedida.

Tópicos da política incorporada:

- “Entendendo políticas integradas” na página 147
- “Políticas disponíveis” na página 148
- “Usando política integrada” na página 150

Entendendo políticas integradas

Políticas integradas fornecem regras de negócios para abordar problemas comuns de segurança e integridade de dados. Essas políticas fazem parte do modelo de segurança padrão, permitindo integrar recursos de segurança do DRA em sua configuração corporativa existente.

O DRA fornece duas maneiras de assegurar o uso obrigatório da política. Você pode criar políticas personalizadas ou escolher entre várias políticas integradas. Políticas integradas facilitam a aplicação de políticas sem necessidade de desenvolver scripts personalizados. Se você precisar implementar uma política personalizada, poderá adaptar uma política integrada existente para atender às suas necessidades. A maioria das políticas permite modificar o texto da mensagem de erro, renomear a política, adicionar uma descrição e especificar como aplicar a política.

Várias políticas integradas são habilitadas quando você instala o DRA. As políticas a seguir são implementadas por padrão. Se você não quiser assegurar o uso obrigatório dessas políticas, poderá desabilitá-las ou apagá-las.

Nome da Política	Valor Padrão	Descrição
$ComputerNameLengthPolicy	64 15 (anterior ao Windows 2000)	Limita o número de caracteres no nome do computador ou no nome do computador anterior ao Windows 2000
$GroupNameLengthPolicy	64 20 (anterior ao Windows 2000)	Limita o número de caracteres no nome do grupo ou no nome do grupo anterior ao Windows 2000
$GroupSizePolicy	5000	Limita o número de membros em um grupo
$NameUniquenessPolicy	Nenhum	Garante que os nomes anteriores ao Windows 2000 e CN sejam exclusivos em todos os domínios gerenciados
$SpecialGroupsPolicy	Nenhum	Impede o escalonamento não verificado de poderes no ambiente.
$UCPowerConflictPolicy	Nenhum	Evita a escalada de poder, tornando os Clones do Usuário e os poderes de Criação de Usuários mutuamente exclusivos
$UPNUniquenessPolicy	Nenhum	Garante que os nomes UPN sejam únicos em todos os domínios gerenciados
$UserNameLengthPolicy	64 20 (nome de logon de baixo nível)	Limita o número de caracteres no nome de logon do usuário ou no nome de logon de baixo nível

Políticas disponíveis

O DRA fornece várias políticas que você pode personalizar para o seu modelo de segurança.

Observação: Você pode criar uma política que exija uma entrada para uma propriedade que não esteja atualmente disponível nas interfaces de usuário do DRA. Se uma entrada for exigida pela política e a interface do usuário não fornecer um campo para digitar o valor, como um departamento para uma nova conta do usuário, não será possível criar nem gerenciar o objeto. Para evitar esse problema, configure políticas que exigem apenas as propriedades que podem ser acessadas nas interfaces do usuário.

Criar uma política personalizada

Permite vincular um script ou executável a uma operação de DRA ou Exchange. Políticas personalizadas permitem que você valide todas as operações escolhidas.

Assegurar o uso obrigatório de um comprimento máximo de nome

Permite assegurar o uso obrigatório globalmente do comprimento máximo de nome para contas do usuário, grupos, OUs, contatos ou computadores.

A política verifica o container de nomes (nome comum ou CN) e o nome anterior ao Windows 2000 (nome de logon do usuário).

Assegurar o uso obrigatório do número máximo de membros do grupo

Permite que você assegure o uso obrigatório limites globais ao número de membros de um grupo.

Assegurar o uso obrigatório de nomes de conta exclusivos anteriores ao Windows 2000

Verifica se um nome anterior ao Windows 2000 é exclusivo em todos os domínios gerenciados. Nos domínios do Microsoft Windows, os nomes anteriores ao Windows 2000 devem ser exclusivos em um domínio. Essa política global impõe essa regra em todos os domínios gerenciados.

Assegurar o uso obrigatório de nomes principais de usuário (UPNs) exclusivos

Verifica se um nome principal de usuário (UPN) é exclusivo em todos os domínios gerenciados. Nos domínios do Microsoft Windows, os UPNs devem ser exclusivos em um domínio. Essa política impõe essa regra em todos os domínios gerenciados. Como esta é uma política global, o DRA fornece o nome da política, a descrição e o relacionamento de política.

Limite de ações em membros de grupos especiais

Impede você de gerenciar membros de um grupo de administradores, a menos que você seja um membro desse grupo de administradores. Essa política global está habilitada por padrão.

Quando você limita ações em membros dos grupos de administradores, o Assistente Create Policy (Criar Política) não requer informações adicionais. Você pode especificar uma mensagem de erro personalizada. Como esta é uma política global, o DRA fornece o nome da política, a descrição e o relacionamento de política.

Impedir que administradores assistentes Criem e Clonem Usuários na Mesma Tela Ativa

Impede a possível escalada de poderes. Quando esta política está habilitada, você pode criar contas do usuário ou clonar contas de usuário, mas não pode ter ambos os poderes. Essa política global garante que você não possa criar e clonar contas de usuário na mesma Tela Ativa.

Esta política não requer informações adicionais.

Definir política de convenção de nomenclatura

Permite estabelecer convenções de nomenclatura que se aplicam a administradores assistentes específicos, Telas Ativas e classes de objetos, como conta do usuário ou grupos.

Você também pode especificar os nomes exatos monitorados por esta política.

Criar uma política para validar uma propriedade específica

Permite que você crie uma política para validar qualquer propriedade de uma OU ou um objeto de conta. Você pode especificar um valor padrão, uma máscara de formato de propriedade e valores e intervalos válidos.

Use essa política para assegurar o uso obrigatório da integridade de dados validando determinados campos de entrada ao criar, clonar ou modificar propriedades de objetos específicos. Essa política oferece enorme flexibilidade e poder para validar entradas, fornecer entradas padrão e limitar as opções de entrada para vários campos de propriedade. Ao usar essa política, você pode exigir que uma entrada correta seja feita antes que a tarefa seja concluída, mantendo, assim, a integridade dos dados nos seus domínios gerenciados.

Por exemplo, suponha que você tenha três departamentos: Manufatura, Vendas e Administração. Você pode limitar as entradas que o DRA aceitará apenas para esses três valores. Você também pode usar essa política para assegurar o uso obrigatório de formatos de números de telefone apropriados, fornecer uma faixa de dados válidos ou exigir uma entrada para o campo de endereço de e-mail. Para especificar máscaras de vários formatos para um número de telefone, como `(123)456 7890`, assim como`456 7890`, defina a máscara de formato da propriedade como `(###)### ####,### ####`.

Criar política para assegurar o uso obrigatório de licenças do Office 365

Permite que você crie uma política para atribuir licenças do Office 365 com base na participação do grupo do Active Directory. Essa política também impõe a remoção de licenças do Office 365 quando um membro é removido do grupo relevante do Active Directory.

Se um usuário que não está sincronizado com a nuvem for adicionado ao grupo do Active Directory, o usuário será sincronizado antes de uma licença do Office 365 ser atribuída ao usuário.

Durante a criação da política, você pode especificar várias propriedades e configurações, como o nome da política e a redação da mensagem de erro que aparece quando um administrador assistente tenta realizar uma ação que viola essa política.

A configuração **Assegurar que apenas as licenças designadas pelas políticas do DRA estão habilitadas nas contas. Todas as outras licenças serão removidas.** está incluída na página Propriedades do Locatário, que pode ser configurada por locatário. Esta configuração é usada nas políticas de licença do Office 365 do DRA para configurar como será assegurado o uso obrigatório das designações de licença:

Quando esta configuração está habilitada, assegurar o uso obrigatório da licença do DRA garante que apenas as licenças designadas pelas políticas do DRA sejam provisionadas para as contas (as licenças designadas fora do DRA serão removidas das contas designadas à política de licença). Quando essa configuração estiver desabilitada (padrão), assegurar o uso obrigatório da

licença do DRA garantirá somente que as licenças específicas incluídas nas políticas do Office 365 sejam provisionadas para contas (se uma conta tiver sua designação a uma política de licença removida, apenas as licenças designadas por essa política terão o provisionamento cancelado).

Usando política integrada

Como a política integrada é parte do modelo de segurança padrão, você pode usar essas políticas para assegurar o uso obrigatório de seu modelo de segurança atual ou modificá-las para atender melhor às suas necessidades. Você pode mudar o nome, as configurações de regra, o escopo, o relacionamento de política e a mensagem de erro de várias políticas integradas. Você pode habilitar ou desabilitar cada política integrada.

Você também pode criar facilmente novas políticas.

Implementando uma política personalizada

As políticas personalizadas permitem que você explore totalmente o poder e a flexibilidade do modelo de segurança padrão. Ao usar políticas personalizadas, você pode integrar o DRA a componentes corporativos existentes, garantindo que suas regras proprietárias sejam aplicadas. Você pode usar o recurso de política personalizada para estender suas políticas corporativas.

Você cria e assegura o uso obrigatório de políticas personalizadas associando um executável ou um script a uma operação de administração. Por exemplo, um script de política associado à operação `UserCreate` pode verificar seu banco de dados de recursos humanos para ver se o funcionário especificado existe. Se o funcionário existir no banco de dados de recursos humanos e não tiver uma conta existente, o script recuperará o ID do funcionário, o primeiro nome e o sobrenome do banco de dados. A operação é concluída com êxito e preenche a janela de propriedades da conta do usuário com as informações adequadas. No entanto, se o funcionário já tiver uma conta, a operação falhará.

Os scripts oferecem uma enorme flexibilidade e poder. Para criar seus próprios scripts de políticas, você pode usar os cmdlets do provedor de ADSI do Directory e Administrador de Recurso (provedor ADSI), SDK (Software Development Kit) e PowerShell. Para obter mais informações sobre como criar seus próprios scripts de política, consulte a seção Referência no site Documentação do DRA.

Restringindo grupos de segurança integrados nativos

Para fornecer um ambiente mais seguro, o DRA permite limitar os poderes dados aos grupos de segurança integrados do Microsoft Windows. A capacidade de modificar a participação do grupo, as propriedades integradas do grupo de segurança ou as propriedades dos membros do grupo podem ter importantes implicações de segurança. Por exemplo, se você puder mudar a senha de um usuário no grupo Operadores de Servidor, poderá fazer logon como esse usuário e exercer os poderes delegados a esse grupo de segurança integrado.

O DRA impede esse problema de segurança fornecendo uma política que verifica os poderes que você tem para um grupo de segurança integrado nativo e seus membros. Essa validação garante que suas ações solicitadas não escalem esses poderes. Após habilitar esta política, um administrador assistente que seja membro de um grupo de segurança incorporado, como o grupo Operadores de Servidor, só poderá gerenciar outros membros do mesmo grupo.

Grupos de segurança integrados nativos que você pode restringir

Você pode restringir os poderes dos seguintes grupos de segurança integrados do Microsoft Windows usando políticas do DRA:

- Operadores de conta
- Administradores
- Operadores de Backup
- Editores de Certificados
- Admins do DNS
- Admins de Domínio
- Admins Corporativos
- Proprietários do Criador de Política de Grupo
- Operadores de Impressão
- Admins de Esquema

Observação: DRA refere-se aos grupos de segurança integrados por seus identificadores internos. Como resultado, o DRA suporta esses grupos mesmo que eles sejam renomeados. Esse recurso garante que o DRA suporte grupos de segurança integrados com nomes diferentes em países diferentes. Por exemplo, o DRA refere-se ao grupo Administradores e ao grupo *Administrar* com o mesmo identificador interno.

Restringindo ações em grupos de segurança integrados nativos

O DRA usa uma política para limitar os grupos de segurança integrados nativos e seus membros podem se exercitar. Essa política, chamada `$SpecialGroupsPolicy`, restringe as ações que um membro de um grupo de segurança integrado nativo pode executar em outros membros ou outros grupos de segurança integrados nativos. O DRA habilita essa política por padrão. Se você não quiser restringir ações em grupos de segurança integrados nativos e seus membros, poderá desabilitar essa política.

Quando esta política está habilitada, o DRA usa os seguintes testes de validação para determinar se uma ação é permitida em um grupo de segurança integrado nativo ou em seus membros:

- Se você for um administrador do Microsoft Windows, poderá executar ações em grupos de segurança integrados nativos e seus membros para os quais você tem os poderes apropriados.
- Se você for um membro de um grupo de segurança integrado, poderá executar ações no mesmo grupo de segurança integrado e em seus membros, contanto que tenha os poderes apropriados.
- Se você não for membro de um grupo de segurança integrado, não poderá modificar um grupo de segurança integrado ou seus membros.

Por exemplo, se você for um membro dos grupos Operadores de Servidor e Operadores de Conta e tiver os poderes apropriados, poderá executar ações em membros do grupo Operadores de Servidor, membros do grupo Operadores de Contas ou membros de ambos os grupos. No entanto, você não pode executar ações em uma conta do usuário que seja membro do grupo Operadores de impressão e do grupo Operadores de conta.

O DRA o impede de executar as seguintes ações em grupos de segurança integrados nativos:

- Clonar um grupo
- Criando um grupo
- Apagar um grupo
- Adicionar um membro a um grupo
- Remover um membro de um grupo
- Mover um grupo para uma OU
- Modificar propriedades de um grupo
- Copiar uma caixa de correio
- Remover uma caixa de correio
- Clonar uma conta do usuário
- Criar uma conta do usuário
- Apagar uma conta do usuário
- Mover uma conta do usuário para uma OU
- Modificar as propriedades da conta do usuário

O DRA também restringe ações para garantir que você não tenha poderes sobre um objeto. Por exemplo, quando você adiciona uma conta do usuário a um grupo, o DRA verifica se você não obtém poderes adicionais sobre a conta do usuário, pois é membro desse grupo. Essa validação ajuda a proteger contra uma escalada de poder.

Gerenciando Políticas

Por meio do nó Policy and Automation Management (Gerenciamento de Política e Automação), você pode acessar as políticas do Microsoft Exchange e do diretório pessoal, bem como políticas integradas e personalizadas. Use as seguintes tarefas comuns para melhorar sua segurança corporativa e integridade de dados.

Configure Exchange Policies (Configurar Políticas do Exchange)

Permite que você defina regras de configuração do Microsoft Exchange, políticas de caixa de correio, nomeação automática e geração de proxy. Estas regras podem definir como as caixas de correio são gerenciadas quando um administrador assistente cria, modifica ou apaga uma conta do usuário.

Configurar Políticas do Diretório Pessoal

Permite que você crie, renomeie ou apague automaticamente os diretórios e os compartilhamentos da página inicial quando um administrador assistente cria, renomeia ou apaga uma conta do usuário. A política de diretório pessoal também permite habilitar ou desabilitar o suporte a cotas de disco para diretórios pessoais em servidores Microsoft Windows, bem como em servidores que não são Windows.

Configure Password Generation Policies (Configurar Políticas de Geração de Senha)

Permite definir os requisitos para senhas geradas pelo DRA.

Para obter informações mais detalhadas sobre o gerenciamento de políticas no DRA, consulte as seguintes seções:

Política do Microsoft Exchange

O Exchange fornece várias políticas para ajudá-lo a gerenciar com mais eficiência os objetos do Microsoft Exchange. A política do Microsoft Exchange permite que você automatize o gerenciamento de caixa de correio, assegure o uso obrigatório de convenções de nomenclatura para aliases e armazenamentos de caixa de correio e gere automaticamente endereços de e-mail.

Essas políticas podem ajudar você a otimizar seus workflows e manter a integridade dos dados. Por exemplo, você pode especificar como o Exchange gerencia as caixas de correio quando você cria, modifica ou apaga contas do usuário. Para definir e gerenciar as políticas do Microsoft Exchange, você deve ter os poderes apropriados, como aqueles incluídos na função Gerenciar Políticas e Acionadores de Automação.

Especificando uma política de endereço de e-mail padrão

Para especificar a política de endereço de e-mail padrão, você deve ter os poderes apropriados, como aqueles incluídos na função Gerenciar Políticas e Acionadores de Automação integrados, e sua licença deve suportar o produto Exchange.

Para especificar uma política de endereço de e-mail padrão:

1. Acesse **Policy and Automation Management** (Política e Gerenciamento de Automação) > **Configure Exchange Policies** (Configurar Políticas do Exchange) > **Proxy Generation** (Geração de Proxy).
2. Especifique o domínio do servidor do Microsoft Exchange.
   - **2a** Clique em **Procurar**.
   - **2b** Especifique critérios de pesquisa adicionais, conforme necessário, e clique em **Find Now** (Localizar Agora).
   - **2c** Selecione o domínio a ser configurado e clique em **OK**.
3. Especifique as regras de geração de proxy para o domínio selecionado.
   - **3a** Clique em **Adicionar**.
   - **3b** Selecione um tipo de proxy. Por exemplo, clique em **Endereço de Internet**.
   - **3c** Aceite o valor padrão ou digite uma nova regra de geração de proxy e clique em **OK**.

     Para obter mais informações sobre strings de substituição suportadas para regras de geração de proxy, consulte Política do cliente de Delegação e Configuração

4 Clique em **Atributos personalizados** para editar o nome personalizado de propriedades de caixa de correio personalizadas.

   4a Selecione o atributo e clique no botão **Editar**.

   4b Na janela Attribute Properties (Propriedades do Atributo), digite o nome do atributo no campo **Custom name** (Nome personalizado) e clique em **OK**.

5 Clique em **OK**.

Observação: O Admin da Política do DRA deve ter o poder *Gerenciar Ferramentas Personalizadas* para modificar atributos personalizados na política do Microsoft Exchange.

Regras da caixa de correio

As regras da caixa de correio permitem especificar como o Exchange gerencia as caixas de correio quando os administradores assistentes criam, clonam, modificam ou apagam contas de usuários. As regras da caixa de correio gerenciam automaticamente caixas de correio do Microsoft Exchange com base em como o administrador assistente gerencia as contas de usuários associadas.

Observação: Ao habilitar a opção **Do not allow Assistant Admins to create a user account without a mailbox** (Não permitir que os Admins Assistentes criem uma conta do usuário sem uma caixa de correio) nos domínios do Microsoft Windows, verifique se o administrador assistente tem capacidade para clonar ou criar uma conta do usuário. A habilitação desta opção exige que os administradores assistentes criem contas de usuários do Windows com uma caixa de correio.

Para especificar regras da caixa de correio do Microsoft Exchange, você deve ter os poderes apropriados, como aqueles incluídos na função Gerenciar Políticas e Acionadores de Automação integrados, e sua licença deve suportar o produto Exchange.

Para especificar as regras da caixa de correio do Exchange:

1 Acesse **Policy and Automation Management** (Política e Gerenciamento de Automação) > **Configure Exchange Policies** (Configurar Políticas do Exchange) > **Mailbox Rules** (Regras da Caixa de Correio).

2 Selecione as políticas de caixa de correio cujo uso obrigatório você deseja que o Exchange assegure ao criar ou modificar contas do usuário.

3 Clique em **OK**.

Política de Licença do Office 365

Para especificar políticas de licença do Office 365, você deve ter os poderes apropriados, como aqueles incluídos na função incorporada Gerenciar Políticas e Acionadores de Automação. Sua licença também deve suportar o produto Microsoft Exchange.

Permitindo que o DRA gerencie suas licenças do Office 365 (opcional)

Se você quiser permitir que o DRA gerencie suas licenças do Office 365, faça o seguinte:

- Crie uma política de imposição de licença.
- Habilite a **License update schedule** (Programação de atualização de licença) na página de propriedades do locatário.

Criando uma política para assegurar o uso obrigatório de licenças do Office 365

Para criar uma política para assegurar o uso obrigatório de licenças do Office 365, clique no nó **Policy and Automation Management** (Política e Gerenciamento de Automação) no console de Delegação e Configuração e selecione **New Policy** > **Create New Policy to Enforce Office 365 Licenses** (Nova Política > Criar Nova Política para Assegurar o Uso Obrigatório de Licenças do Office 365).

Quando a política é imposta e um usuário é adicionado ao Active Directory, o DRA usa participação do grupo para atribuir automaticamente a licença do Office 365 ao usuário.

Programação de atualização de licença do Office 365

As políticas criadas para assegurar o uso obrigatório de licenças do Office 365 não são aplicadas quando as mudanças são feitas fora do DRA, a menos que você também habilite a **License update schedule** (Programação de atualização de licença) na página de propriedades do locatário. A tarefa de atualização de licença garante que as licenças do Office 365 atribuídas aos usuários correspondam às políticas de licença do Office 365.

A tarefa de atualização de licença e as políticas de licença do Office 365 trabalham juntas para garantir que todos os usuários gerenciados recebam apenas as licenças do Office 365 que deveriam ter.

Observação

- O DRA não gerencia licenças do Office 365 para contas do usuário somente online. Para que o DRA gerencie seus usuários com licenças do Office 365, esses usuários devem ser sincronizados com o Active Directory.
- Se você optar por usar o DRA para gerenciar as licenças do Office 365, o DRA anulará quaisquer mudanças manuais nas licenças do Office 365 feitas fora do DRA na próxima vez em que a tarefa de atualização da licença for executada.
- Se você habilitar a tarefa de atualização da licença do Office 365 antes de garantir que as políticas de licença do Office 365 estejam configuradas corretamente, as licenças atribuídas poderão estar incorretas após a execução da tarefa de atualização da licença.

Criando e implementando a política de diretório pessoal

Quando você gerencia um grande número de contas do usuário, criar e manter esses diretórios pessoais e compartilhamentos pode exigir muito tempo e ser uma fonte de erros na segurança. Manutenção adicional pode ser necessária sempre que um usuário é criado, renomeado ou apagado. As políticas de diretório pessoal ajudam você a gerenciar o diretório pessoal e na manutenção de compartilhamento pessoal.

O DRA permite automatizar a criação e a manutenção de diretórios pessoais do usuário. Por exemplo, você pode configurar facilmente o DRA para que o servidor de Administração crie um diretório pessoal ao criar uma conta do usuário. Nesse caso, se você especificar um caminho de diretório pessoal ao criar a conta do usuário, o servidor criará automaticamente o diretório pessoal de acordo com o caminho especificado. Se você não especificar um caminho, o servidor não criará o diretório pessoal.

O DRA suporta caminhos do Sistema de Arquivos Distribuídos (DFS) durante a criação de diretórios pessoais de usuários ou a configuração de políticas de diretórios pessoais para usuários em caminhos pai permitidos. Você pode criar, renomear e apagar diretórios pessoais em Netapp Filers e caminhos ou partições DFS.

Configurando políticas do diretório pessoal

Para configurar políticas de cota de disco de diretório pessoal, compartilhamento e volume, você deve ter os poderes apropriados, como aqueles incluídos na função Gerenciar Políticas e Acionadores de Automação integrados. Cada política gerencia automaticamente os diretórios de usuário, compartilhamento e volume de cota de disco com base em como você gerencia as contas de usuário associadas.

Para configurar políticas de diretório pessoal, acesse **Policy and Automation Management** (Política e Gerenciamento de Automação) > **Configure Home Directory Policies** (Configurar Políticas do Diretório Pessoal) >

- Diretório pessoal
- Compartilhamento pessoal
- Cota de Disco do Volume Pessoal

Requisitos do Servidor de Administração

Para cada computador em que você precise criar um compartilhamento pessoal, a conta de serviço ou conta de acesso do servidor de Administração deverá ser um administrador nesse computador ou um membro do grupo Administradores no domínio correspondente.

Um compartilhamento de administração, como C$ ou D$, deve existir para cada unidade na qual o DRA gerencia e armazena diretórios pessoais. O DRA usa os compartilhamentos de administração para executar algumas tarefas de automação de diretório pessoal e compartilhamento pessoal. Se esses compartilhamentos não existirem, o DRA não poderá fornecer automação de compartilhamento pessoal e diretório pessoal.

Configurando caminhos permitidos do diretório pessoal para o NetApp Filers

Para configurar os Allowable Parent Paths (Caminhos Pai Permitidos) para um NetApp Filer:

1. Acesse **Policy and Automation Management** (Política e Gerenciamento de Automação) > **Configure Home Directory Policies** (Configurar Políticas do Diretório Pessoal).
2. Na caixa de texto **Allowable parent paths** (Caminhos pai permitidos), digite um dos caminhos permitidos na tabela a seguir:

Tipo de compartilhamento	Caminho permitido
Windows	(*FileName**adminshare:**volumerootpath**directorypath*)
Não Windows	*não windows**compartilhamento*

3. Clique em **Adicionar**.
4. Repita as etapas de 1 a 3 para cada caminho pai permitido onde quer que você queira aplicar as políticas de diretório pessoal.

Compreendendo a política de diretório pessoal

Para ser consistente com as políticas de segurança adequadas do Microsoft Windows, o DRA cria restrições de controle de acesso apenas no nível do diretório. Impor restrições de controle de acesso no nível de nome de compartilhamento e no nível de objeto de diretório ou arquivo geralmente leva a um esquema de acesso confuso para administradores e usuários.

Quando você muda uma restrição de controle de acesso para um compartilhamento pessoal, o DRA não muda a segurança existente para esse diretório. Nesse caso, você deve garantir que as contas do usuário tenham o acesso apropriado aos seus próprios diretórios pessoais.

Automação e regras do diretório pessoal

O DRA automatiza as tarefas de manutenção de diretório pessoal, gerenciando diretórios pessoais quando você modifica uma conta do usuário. O DRA pode executar ações diferentes quando uma conta do usuário é criada, clonada, modificada, renomeada ou apagada.

Para implementar com sucesso sua política de diretório pessoal, considere as seguintes diretrizes:

- Verifique se o caminho especificado usa o formato correto.
  - Para especificar um caminho para um único diretório pessoal, use um dos modelos da tabela a seguir:

Tipo de Compartilhamento	Gabarito do Caminho
Windows	*computador**compartilhamento*\. Por exemplo, se você quiser que o DRA crie automaticamente um diretório pessoal na pasta `Compartilhamento Pessoal`, no computador de server01, digite `\\server01HomeShare\`
Não Windows	*não windows**compartilhamento*

- Para padronizar a administração do diretório pessoal no diretório raiz do compartilhamento pessoal correspondente, use a sintaxe UNC (Universal Naming Convention), como *nome do servidor**C:**caminho para o diretório raiz*.
- Para especificar um caminho para diretórios pessoais aninhados, use um dos modelos da tabela a seguir:

Tipo de Compartilhamento	Gabarito do Caminho
Windows	*computador**compartilhamento**primeiro diretório**segundo diretório*\ Por exemplo, se você quiser que o DRA crie automaticamente um diretório pessoal em `JSmith\Home directory`, na pasta Home Share do computador do `server01`, digite `\\server01\Home Share\JSmith\Home`.
Não Windows	*não windows**compartilhamento**primeiro diretório**segundo diretório*\

Observação: O DRA também suporta os seguintes formatos: *computador**compartilhamento**nome de usuário* e *computador**compartilhamento**%nome de usuário%*. Em cada caso, o DRA cria automaticamente um diretório pessoal para a conta do usuário associada.

- Quando você define uma política ou acionador de automação para gerenciar diretórios pessoais em um NetApp Filer, é necessário usar um formato diferente para a especificação do diretório.
  - Se você estiver usando o NetApp Filers, especifique o diretório pai no seguinte formato: *FilerName**adminshare:**volumerootpat*h*directorypath*
  - A variável adminshare é o compartilhamento oculto mapeado para o volume raiz no NetApp Filer, como *c$*. Por exemplo, se o caminho local do compartilhamento em um NetApp Filer, chamado usfiler, for `c$\vol\vol0\mydirectory`, você poderá especificar um caminho raiz de `\\usfiler\c:\vol\vol0\mydirectory` para o NetApp Filer.
- Para especificar um caminho DFS enquanto você cria diretórios pessoais do usuário ou configura políticas de diretório pessoal para usuários, use *servidor**raiz*\<*vínculo*> `formato`, em que a raiz pode ser o domínio gerenciado ou um diretório raiz independente no seguinte formato: *FilerName**adminshare**volumerootpath**directorypath* .

- Crie um diretório compartilhado para armazenar o diretório pessoal para essa conta do usuário.
- Verifique se o DRA pode acessar o computador ou compartilhar o mencionado no caminho.

Criar um diretório pessoal quando a conta do usuário é criada

Essa regra permite que o DRA crie diretórios pessoais automaticamente para novas contas do usuário. Quando o DRA cria um diretório pessoal, o servidor de Administração usa o caminho especificado no campo **Diretório pessoal** no Assistente Criar Usuário. Posteriormente, você pode modificar esse caminho usando a guia Perfil da janela de propriedades do usuário e o DRA moverá o diretório pessoal para o novo local. Se você não especificar valores para esses campos, o DRA não criará um diretório pessoal para essa conta do usuário.

O DRA define a segurança para o novo diretório com base nas opções **Permissões do diretório pessoal**. Essas opções permitem controlar o acesso geral de todos os diretórios pessoais.

Por exemplo, você pode especificar que os membros do grupo Administradores tenham controle total e os membros do grupo de Suporte Técnico tenham acesso de leitura ao compartilhamento no qual os diretórios pessoais do usuário são criados. Em seguida, quando o DRA criar um diretório pessoal do usuário, o novo diretório pessoal poderá herdar esses direitos do diretório pai. Portanto, os membros do grupo Administradores têm controle total sobre todos os diretórios pessoais do usuário e os membros do grupo de suporte técnico têm acesso de leitura a todos os diretórios pessoais do usuário.

Se o diretório pessoal especificado já existir, o DRA não criará o diretório pessoal e não modificará as permissões do diretório existente.

Renomear o diretório pessoal quando a conta do usuário é renomeada

Essa regra permite que o DRA execute automaticamente as seguintes ações:

- Criar um diretório pessoal quando você especifica um novo caminho de diretório pessoal
- Mover o conteúdo do diretório pessoal quando você muda o caminho de diretório pessoal
- Renomear um diretório pessoal quando você renomeia a conta do usuário

Quando você renomeia uma conta do usuário, o DRA renomeia o diretório pessoal existente com base no novo nome da conta. Se o diretório pessoal existente estiver em uso no momento, o DRA criará um novo diretório pessoal com o novo nome e não mudará o diretório pessoal existente.

Quando você muda o caminho de diretório pessoal, o DRA tenta criar o diretório pessoal especificado e mover o conteúdo do diretório pessoal para o novo local. Você também pode configurar a política de Diretório Pessoal para criar um diretório pessoal sem mover o conteúdo do diretório pessoal existente. O DRA também aplica as ACLs atribuídas do diretório anterior ao novo diretório. Se o diretório pessoal especificado já existir, o DRA não criará esse novo diretório e não modificará as permissões do diretório existente. Se o diretório pessoal não estiver bloqueado, o DRA o apagará.

Quando o DRA não renomeia o diretório pessoal, o DRA tenta criar um novo diretório pessoal com um novo nome e copiar o conteúdo do diretório pessoal para o novo diretório pessoal. O DRA então tenta apagar o diretório pessoal anterior. Você pode configurar o DRA para não

copiar o conteúdo do diretório pessoal anterior para o novo diretório pessoal e mover manualmente o conteúdo do diretório pessoal para o novo diretório pessoal para evitar problemas, como copiar arquivos abertos.

Ao apagar o diretório pessoal, o DRA requer permissão explícita para apagar arquivos e subdiretórios apenas leitura do diretório pessoal anterior. Você pode fornecer ao DRA a permissão para apagar explicitamente os arquivos e subdiretórios apenas leitura do diretório pessoal anterior.

Permitir diretório pai ou caminho para um compartilhamento pessoal

O DRA permite que você especifique os diretórios ou caminhos pai permitidos para compartilhamentos pessoais em servidores de arquivos. Se você tiver muitos caminhos de diretório ou de servidor de arquivos para especificar, poderá exportar esses caminhos para um arquivo CSV e adicionar esses caminhos ao DRA usando o console DRA. O DRA usa as informações inseridas no campo **Allowable parent paths** (Caminhos pai permitidos) para garantir:

- O DRA não apaga o diretório pai no servidor de arquivos quando os administradores assistentes apagam uma conta do usuário e o diretório pessoal da conta do usuário.
- O DRA move o diretório pessoal para um caminho ou diretório pai válido no servidor de arquivos quando você renomeia uma conta do usuário ou muda o caminho de diretório pessoal para uma conta do usuário.

Apagar o diretório pessoal quando a conta do usuário é apagada

Essa regra permite que o DRA apague automaticamente um diretório pessoal quando você apaga a conta do usuário associada. Se você habilitar a Lixeira, o DRA não apagará o diretório pessoal até que você apague a conta do usuário da Lixeira. Ao apagar o diretório pessoal, o DRA exige permissão explícita para apagar arquivos e subdiretórios apenas leitura do diretório pessoal anterior. Você pode fornecer ao DRA a permissão para apagar explicitamente os arquivos e subdiretórios apenas leitura do diretório pessoal anterior.

Regras e automação do compartilhamento pessoal

O DRA automatiza as tarefas de manutenção de compartilhamento pessoal, gerenciando compartilhamentos pessoais quando você modifica uma conta do usuário ou gerencia diretórios pessoais. O DRA pode executar ações diferentes quando uma conta do usuário é criada, clonada, modificada, renomeada ou apagada.

Para ser consistente com as políticas de segurança adequadas do Microsoft Windows, o DRA não cria restrições de controle de acesso no nível do nome do compartilhamento. Em vez disso, o DRA cria restrições de controle de acesso somente no nível do diretório. Impor restrições de controle de acesso no nível de nome de compartilhamento e no nível de objeto de diretório ou arquivo geralmente leva a um esquema de acesso confuso para administradores e usuários.

Observação: O local especificado deve ter um compartilhamento pessoal comum, como `HOMEDIRS`, em um nível acima dos diretórios pessoais.

Por exemplo, o caminho a seguir é válido: `\\`*`HOUSERV1`*`\`*`HOMEDIRS`*`\%username%`

O caminho a seguir é inválido: `\\`*`HOUSERV1`*`\%username%`

Especificando nomes de compartilhamento pessoal

Ao definir as regras de automação de compartilhamento pessoal, você pode especificar um prefixo e um sufixo para cada compartilhamento pessoal criado automaticamente. Ao especificar um prefixo ou sufixo, você pode assegurar o uso obrigatório de uma convenção de nomenclatura para compartilhamentos pessoais.

Por exemplo, você habilita Criar diretório pessoal e Criar regras de automação de compartilhamento pessoal. Para o compartilhamento pessoal, você especifica um prefixo de sublinhado e um sufixo de sinal de dólar. Quando você cria um usuário chamado TomS, mapeia seu novo diretório para a unidade U e especifica `\\HOUSERV1\HOMEDIRS\%username%` como o caminho de diretório. Neste exemplo, o DRA cria um compartilhamento de rede chamado `_TomS$` que aponta para `\\HOUSERV1\HOMEDIRS\TomS directory`.

Criando compartilhamentos pessoais para novas contas do usuário

Quando o DRA cria um compartilhamento pessoal, o servidor de Administração usa o caminho especificado no campo **Diretório pessoal** no Assistente Criar Usuário. Posteriormente, você pode modificar esse caminho usando a guia Perfil da janela de propriedades do usuário.

O DRA cria o nome do compartilhamento adicionando o prefixo e o sufixo especificados, se houver, ao nome de usuário. Se você usar nomes longos de contas do usuário, o DRA poderá não conseguir adicionar o prefixo e o sufixo do compartilhamento pessoal especificado. O prefixo e o sufixo, assim como o número de conexões permitidas, são baseados nas opções de criação de compartilhamento pessoal selecionadas.

Criando compartilhamentos pessoais para contas de usuários clonados

Se o nome de compartilhamento pessoal gerado do nome da conta do usuário recém-criada já existir, o DRA apagará o compartilhamento existente e criará um novo compartilhamento no diretório pessoal especificado.

Ao clonar uma conta do usuário, o nome do compartilhamento da conta do usuário existente deve existir atualmente. Quando você clona uma conta do usuário, o DRA também clona as informações do diretório pessoal e personaliza essas informações para o novo usuário.

Modificando as propriedades do compartilhamento pessoal

Quando você muda o local do diretório pessoal, o DRA apaga o compartilhamento existente e cria um novo compartilhamento no novo diretório pessoal. Se o diretório pessoal original estiver vazio, o DRA apagará o diretório original.

Renomeando compartilhamentos pessoais para contas de usuários renomeadas

Quando você renomeia uma conta do usuário, o DRA apaga o compartilhamento pessoal existente e cria um novo compartilhamento com base no novo nome da conta. O novo compartilhamento aponta para o diretório pessoal existente.

Apagando compartilhamentos pessoais para contas de usuário apagadas

Quando você apaga permanentemente uma conta do usuário, o DRA apaga o compartilhamento pessoal.

Regras de gerenciamento de cota de disco do volume pessoal

O DRA permite gerenciar cotas de disco para volumes pessoais. Você pode implementar essa política em domínios nativos nos quais o diretório pessoal reside em um computador Microsoft Windows. Ao implementar essa política, você deve especificar uma cota de disco de pelo menos 25 MB para permitir um amplo espaço.

Habilitando geração de senhas

Esse recurso permite especificar as configurações de política para senhas geradas pelo DRA. O DRA não assegura o uso obrigatório dessas configurações nas senhas que os usuários criam. Ao configurar as propriedades da Política de Senha, o tamanho da senha deve ter entre 6 e 127 caracteres, todos os valores podem ser definidos como zero, exceto pelo tamanho da senha e pelo limite máximo.

Para configurar as Políticas de Geração de Senhas, acesse **Policy and Automation Management** (Política e Gerenciamento de Automação) > **Configure Password Generation Policies** (Configurar Políticas de Geração de Senhas) e marque a caixa de seleção **Enable Password Policy** (Habilitar Política de Senha). Clique em **Password Settings** (Configurações de Senha) e configure as propriedade da Política de Senha.

Tarefas de Política

Para apagar, habilitar ou desabilitar políticas, você deve ter os poderes apropriados, como aqueles incluídos na função Gerenciar Políticas e Acionadores de Automação integrados.

Para realizar uma destas ações, acesse **Policy and Automation Management** (Política e Gerenciamento de Automação) > **Política**. Clique o botão direito do mouse na política que você deseja apagar, habilitar ou desabilitar no painel direito e selecione a ação desejada.

Implementando políticas integradas

Para implementar políticas integradas, você deve ter os poderes apropriados, como aqueles incluídos na função Gerenciar Políticas e Acionadores de Automação integrados. Para mais informações sobre políticas integradas, consulte Entendendo políticas integradas.

Observação: Antes de associar a política incorporada a um administrador assistente e a uma Tela Ativa, primeiro verifique se o administrador assistente está designado a essa Tela Ativa.

Para implementar políticas integradas:

1. Acesse **Policy and Automation Management** (Política e Gerenciamento de Automação) > **Política**.
2. No menu Tarefas, clique em **New Policy** (Nova Política) e selecione o tipo de política integrada que você deseja criar.
3. Em cada janela do assistente, especifique os valores apropriados e clique em **Next** (Próximo). Por exemplo, você pode associar essa nova política a uma Tela Ativa específica, permitindo que o DRA assegure o uso obrigatório dessa política a objetos incluídos por essa Tela Ativa.
4. Revise o resumo e clique em **Finish** (Terminar).

Implementando políticas personalizadas

Para implementar uma política personalizada, você deve ter os poderes apropriados, como aqueles incluídos na função integrada Gerenciar Políticas e Disparadores de Automação.

Para implementar com êxito uma política personalizada, você deve escrever um script que seja executado durante uma operação específica (tarefa administrativa). Você pode associar um executável ou um script à operação. O DRA suporta tanto o script do PowerShell de 32 bits quanto o script do PowerShell de 64 bits. No script de política personalizada, você pode definir mensagens de erro para exibir sempre que uma ação violar a política. Você também pode especificar uma mensagem de erro padrão por meio do Assistente Create Policy (Criar Política).

Para obter mais informações sobre como gravar políticas personalizadas, exibir uma lista de operações de administração ou usar matrizes de argumentos, consulte o SDK. Para obter mais informações, veja Gravando scripts ou executáveis de política personalizada.

Observação

- Antes de associar a política personalizada a um administrador assistente e a uma Tela Ativa, primeiro verifique se o administrador assistente está designado a essa Tela Ativa.
- Se o caminho do script ou executável da política personalizada contiver espaços, especifique com aspas (") ao redor do caminho.

Para implementar uma política personalizada:

1. Grave um executável ou script de política.
2. Efetue logon em um computador cliente do DRA com uma conta à qual esteja atribuída a função Gerenciar Políticas e Acionadores de Automação integrados no domínio gerenciado.
3. Inicie o Console de Delegação e Configuração.
4. Conecte-se ao servidor de Administração principal.
5. No painel esquerdo, expanda **Policy and Automation Management** (Política e Gerenciamento de Automação).
6. Clique em **Política**.
7. No menu Tarefas, clique em **New Policy > Create a Custom Policy** (Nova Política > Criar uma Política Personalizada).
8. Em cada janela do assistente, especifique os valores apropriados e clique em **Next** (Próximo). Por exemplo, você pode associar essa nova política a uma Tela Ativa específica, permitindo que o DRA assegure o uso obrigatório dessa política a objetos incluídos por essa Tela Ativa.
9. Revise o resumo e clique em **Finish** (Terminar).

Modificando propriedades da política

Para modificar todas as propriedades de uma política, você deve ter os poderes apropriados, como aqueles incluídos na função Gerenciar Políticas e Acionadores de Automação integrados.

Para modificar propriedades da política:

1. Acesse **Policy and Automation Management** (Política e Gerenciamento de Automação) > **Política**.

2 Clique o botão direito do mouse na política que você deseja modificar e selecione **Propriedades**.

3 Modifique as propriedades e as configurações apropriadas para esta política.

Gravando scripts ou executáveis de política personalizada

Para obter mais informações sobre como gravar scripts de políticas personalizadas ou executáveis, consulte o SDK.

Para acessar o SDK:

1 Verifique se instalou o SDK no seu computador. O programa de configuração cria um atalho para o SDK no grupo de programa Directory and Resource Administrator. Para mais informações, consulte a lista de verificação da instalação em Instalar o Servidor de administração DRA.

2 Clique no atalho do SDK no grupo de programas do Directory and Resource Administrator.

Política do cliente de Delegação e Configuração

A política de nomenclatura automática inclui três configurações de política nas Políticas do Exchange exclusivas do cliente de Delegação e Configuração, o que significa que é uma política do lado do cliente.

A política de nomeação automática permite que você especifique regras de nomenclatura automáticas para propriedades específicas de uma caixa de correio. Essas opções permitem estabelecer convenções de nomenclatura e gerar rapidamente valores padrão para o nome para exibição, nome do diretório e propriedades de álias. O Exchange permite que você especifique cadeias de substituição, como `%First` e `%Last` para várias opções de nomenclatura automatizadas.

Quando o Exchange gera um nome de diretório ou álias, ele verifica se o valor gerado é exclusivo. Se o valor gerado não for exclusivo, o Exchange anexará um hífen (-) e um número de dois dígitos, começando com `-01` para fazer o valor exclusivo. Quando o Exchange gera um nome de exibição, ele não verifica se o valor é exclusivo.

O Exchange suporta as seguintes strings de substituição para políticas automáticas de geração de nomes e proxy:

`%First`	**Indica o valor da propriedade Primeiro nome para a conta do usuário associada.**
`%Último`	Indica o valor da propriedade Sobrenome para a conta do usuário associada.
`%Initials`	Indica o valor da propriedade Iniciais da conta do usuário associada.
`%Álias`	Indica o valor da propriedade da caixa de correio Álias.
`%DirNam`	Indica o valor da propriedade da caixa de correio do nome do diretório. Ao gerar endereços de e-mail para caixas de correio do Microsoft Exchange, o Exchange não suporta strings de geração de proxy que especifiquem a variável `%DirName`.
`%Nome de usuário`	Indica o valor da propriedade Nome de usuário para a conta do usuário associada.

Você também pode especificar um número entre o sinal de porcentagem (%) e o nome da string de substituição para indicar o número de caracteres a serem incluídos nesse valor. Por exemplo, `%2First` indica os primeiros dois caracteres da propriedade do nome **First** da conta do usuário.

Cada regra de nomenclatura automática ou política de geração de proxy pode conter uma ou mais strings de substituição. Você também pode especificar caracteres em cada regra como um prefixo ou sufixo para uma string de substituição específica, como um ponto e espaço (`.`) seguindo a string de substituição `%Initials`. Se a propriedade da string de caracteres de substituição estiver em branco, o Exchange não incluirá o sufixo dessa propriedade.

Por exemplo, considere a seguinte regra de nomenclatura automática para a propriedade de nome **Display**:

```
%First %1Initials. %Last
```

Se a propriedade **First** name for `Susan`, a propriedade **Initials** for `May` e a propriedade **Last** name for `Smith`, o Exchange definirá a propriedade do nome **Display** como `Susan M. Smith`.

Se a propriedade **First** name for `Michael`, a propriedade **Initials** estiver vazia e a propriedade **Last** name for `Jones`, o Exchange definirá a propriedade do nome **Display** como `Michael Jones`.

Especificando uma política de nomenclatura de caixa de correio automatizada

Para especificar opções de nomeação automatizada de caixa de correio, você deve ter os poderes apropriados, como aqueles incluídos na função Gerenciar Políticas e Acionadores de Automação integrados, e sua licença deve oferecer suporte ao produto Exchange.

Para especificar uma política de nomenclatura automatizada de caixa de correio:

1. Acesse **Policy and Automation Management** (Política e Gerenciamento de Automação) > **Configure Exchange Policies** (Configurar Políticas do Exchange) > **Alias naming** (Nomenclatura do álias).
2. Especifique as informações apropriadas de geração de nome.
3. Selecione **Enforce alias naming rules during mailbox updates** (Assegurar o uso obrigatório de regras de nomenclatura de álias durante atualizações de caixa de correio).
4. Clique em **OK**.

Especificando uma política de nomenclatura de recursos

Para especificar opções de nomenclatura de recursos, você deve ter os poderes apropriados, como aqueles incluídos na função Gerenciar Políticas e Acionadores de Automação integrados, e sua licença deve suportar o produto Exchange.

Para especificar uma política de nomenclatura de recursos:

1. Acesse **Policy and Automation Management** (Política e Gerenciamento de Automação) > **Configure Exchange Policies** (Configurar Políticas do Exchange) > **Resource naming** (Nomenclatura de recursos).
2. Especifique as informações apropriadas de geração da nomenclatura de recurso.

3 Selecione **Enforce resource naming rules during mailbox updates** (Assegurar o uso obrigatório de regras de nomenclatura de recursos durante atualizações de caixa de correio).

4 Clique em **OK**.

Especificando uma política de nomenclatura do arquivo

Para especificar opções de nomenclatura do arquivo, você deve ter os poderes apropriados, como aqueles incluídos na função Gerenciar Políticas e Acionadores de Automação integrados, e sua licença deve suportar o produto Exchange.

Para especificar uma política de nomenclatura de arquivo:

1 Acesse **Policy and Automation Management** (Política e Gerenciamento de Automação) > **Configure Exchange Policies** (Configurar Políticas do Exchange) > **Archive naming** (Nomenclatura do arquivo).

2 Especifique as informações apropriadas de geração de nomenclatura de arquivo para contas do usuário.

3 Selecione **Enforce archive naming rules during mailbox updates** (Assegurar o uso obrigatório de regras de nomenclatura de arquivo durante atualizações da caixa de correio).

4 Clique em **OK**.

14 Pré e pós-automação do acionador da tarefa

Um acionador de automação é uma regra que associa um script ou arquivo executável a uma ou mais operações. Por meio do script ou arquivo executável, você pode automatizar um workflow existente e estabelecer uma ponte de informações entre o DRA e outros repositórios de dados. Os acionadores de automação permitem estender a funcionalidade e a segurança que o DRA oferece.

Ao definir um acionador de automação, você define os parâmetros da regra, quais operações devem ser associadas ao acionador, qual script ou executável deve ser executado e, se aplicável, quais Telas Ativas ou administradores assistentes devem ser associados a esse acionador. Essas regras determinam como o servidor de administração aplica seu acionador.

Você também pode especificar um script de desfazer ou executável para o seu acionador. Um **script desfazer** permite realizar o rollback de suas mudanças se a operação falhar.

O DRA suporta scripts do VBScript e do PowerShell.

Como o servidor de administração automatiza processos

Além da administração baseada em regras da Tela Ativa, o DRA permite que você automatize seus workflows existentes e execute automaticamente tarefas relacionadas por meio de acionadores de automação. A automação de workflows existentes pode ajudar você a simplificar sua empresa, fornecendo serviços melhores e mais rápidos.

Quando o servidor de Administração executa a operação associada ao acionador de automação, o servidor também executa o script ou o executável do acionador. Se o seu acionador for um acionador pré-tarefa, o servidor executará o script ou o executável antes de executar a operação. Se seu acionador for um acionador pós-tarefa, o servidor executará o script ou o executável após executar a operação. Esse processo é chamado de transação. Uma **transação** representa o ciclo de implementação completo para cada tarefa ou operação que o servidor de Administração executa. Uma transação inclui as ações necessárias para concluir uma operação, juntamente com as ações de desfazer que o servidor de Administração deve executar se a operação falhar.

O servidor de Administração insere o status do acionador no registro de auditoria sempre que um acionador de automação é executado. Essas entradas de registro registram o código de retorno, as operações associadas, os objetos atuados e se o script do acionador foi bem-sucedido.

Aviso: Os acionadores de automação são executados usando a conta de serviço do servidor de administração. Como a conta de serviço tem permissões de administrador, as políticas e os acionadores de automação têm acesso total a todos os dados corporativos. Para definir acionadores de automação, você deve ter os poderes adequados, como aqueles incluídos na função Gerenciar Políticas e Acionadores de Automação integrados. Esses acionadores de automação serão executados no contexto de segurança da conta de serviço. Assim, os administradores assistentes associados à função incorporada Gerenciar Políticas e Acionadores de Automação poderiam obter mais poder do que você pretendia.

Implementando um acionador de automação

Para implementar acionadores de automação, você deve primeiro escrever scripts de acionador ou executáveis e ter os poderes apropriados, como aqueles incluídos na função Gerenciar Políticas e Acionadores de Automação integrados.

Para implementar com êxito um acionador personalizado, você deve gravar um script que seja executado durante uma operação específica (tarefa administrativa). Você pode associar um executável ou um script à operação. O DRA suporta tanto o script do PowerShell de 32 bits quanto o script do PowerShell de 64 bits. Você pode especificar se o DRA aplica o acionador antes (pré-tarefa) ou após (pós-tarefa) de uma operação. No script do acionador, você pode definir mensagens de erro a serem exibidas sempre que o acionador falhar. Você também pode especificar uma mensagem de erro padrão por meio do Assistente Create Automation Trigger (Criar Acionador de Automação).

Para obter mais informações sobre como gravar acionadores personalizados, exibir uma lista de operações de administração ou usar matrizes de argumentos, consulte o *SDK*.

Observação

- Antes de associar o acionador de automação personalizado a um administrador assistente e a uma Tela Ativa, primeiro verifique se o administrador assistente está designado a essa Tela Ativa.
- Se o caminho do script ou executável do acionador personalizado contiver espaços, especifique com aspas (") ao redor do caminho.
- No momento, se a operação **UserSetInfo** for usada para um acionador de automação de script e um atributo do usuário for mudado (executando o acionador), o atributo mudado não será proliferado na empresa até após a execução de uma operação **Localizar Agora** no objeto usuário.

Para implementar um acionador de automação:

1. Grave um script de acionador ou arquivo executável.
2. Efetue logon em um computador cliente do DRA com uma conta à qual esteja atribuída a função incorporada **Manage Policies and Automation Triggers** (Gerenciar políticas e acionadores de automação) no domínio gerenciado.
3. Inicie o Console de Delegação e Configuração.
4. Conecte-se a um servidor de administração principal.
5. Use Replicação de arquivo para fazer upload do arquivo acionador nos servidores primário e secundário do DRA.

   O caminho da pasta já deve existir em todos os servidores do DRA no domínio gerenciado. Esse caminho, incluindo o arquivo, será usado em **Caminho do arquivo DO** do assistente do Acionador de Automação.
6. No painel esquerdo, expanda **Policy and Automation Management** (Política e Gerenciamento de Automação).
7. Clique em **Automation Triggers** (Acionadores de Automação).
8. No menu Tarefas, clique em **New Trigger** (Novo Acionador).

9 Em cada janela do assistente, especifique os valores apropriados e clique em **Next** (Próximo). Por exemplo, você pode associar esse novo acionador a uma Tela Ativa específica, permitindo que o DRA aplique esse acionador a objetos gerenciar de administradores assistentes incluídos por essa Tela Ativa.

10 Revise o resumo e clique em **Finish** (Terminar).

Importante: Se você tiver mais de uma Tela Ativa configurada para um acionador, ao adicionar uma vírgula entre as Telas Ativas, elas serão bifurcadas no acionador ao fazer o upgrade para uma nova versão do DRA, e o acionador não será executado. Para que a operação seja executada após o upgrade, o acionador precisará ser reconfigurado ou um acionador precisará ser criado.

---

15 Workflow automatizado

Usando o Workflow Automation, você pode automatizar os processos de TI criando formulários de workflow personalizados que são executados de um workflow ou quando acionados por um evento de workflow nomeado criado no servidor do Workflow Automation. Quando você cria um formulário de workflow, você define os grupos de Admin que podem exibir o formulário. A submissão de formulários ou execução de processos de workflow depende dos poderes delegados ao grupo ou grupos incluídos ao criar o formulário de workflow.

Os formulários de workflow, quando criados ou modificados, são gravados no servidor Web. Os administradores assistentes que efetuam logon no Console da Web para esse servidor terão acesso aos formulários com base em como você configurar o formulário. Geralmente, os formulários estão disponíveis para todos os usuários com credenciais de servidor Web. Você limita o acesso a um formulário específico adicionando grupos de Admin Assistentes e ocultando o formulário de outros usuários. A capacidade de enviar o formulário requer um dos seguintes poderes:

- Create Workflow Event and Modify All Properties (Criar um evento de workflow e modificar todas as propriedades)
- Iniciar workflow

Iniciando o formulário de workflow: Os workflows são criados no Servidor do Workflow Automation, que deve ser integrado ao DRA por meio do Console de Delegação e Configuração. 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 solicitações de workflow configuradas com Iniciar Workflow Específico terão um histórico de execução que pode ser consultado no painel de pesquisa principal em **Tarefas** > **Solicitações**.

Você pode modificar uma solicitação existente ou criar uma solicitação. Para modificar uma solicitação existente, navegue até **Tarefas** > **Solicitações**.

Para criar uma solicitação de workflow, navegue até **Administração** > **Personalização** > **Solicitações**.

Para criar uma solicitação, siga estas etapas básicas:

1. Configure a solicitação para executar um *workflow especificado* quando o formulário for submetido ou configure a solicitação para ser executada ao ser acionada por um *evento nomeado* predefinido.

2. Escolha o grupo ou os grupos de Admins Assistentes que estão incluídos no processo de workflow e habilite a opção **Formulário oculto** na guia **Geral** para restringir o acesso aos formulários a esses usuários.
3. Adicione quaisquer campos de propriedade obrigatórios ou páginas de propriedades adicionais ao formulário.
4. Se aplicável, crie manipuladores personalizados para definir melhor o processo de fluxo de workflow e como ele é executado.

   Observação: Opções de sub-rotinas personalizadas não são expostas para uma nova solicitação de workflow até que a solicitação seja gravada inicialmente. Você pode acessar, criar e modificar sub-rotinas personalizadas em **Propriedades do Formulário**.

   ---
5. Desabilite a opção **Formulário oculto** para permitir que os usuários vejam os formulários.

Para obter informações sobre como configurar o servidor do Workflow Automation, veja Configurando o Servidor do Workflow Automation. Para personalizar solicitações de workflow, veja Personalizando Formulários de Solicitação.

VI Auditando e gerando relatórios

A auditoria das ações do usuário está entre os aspectos mais importantes de uma sólida implementação de segurança. Para permitir que você revise e relate as ações do administrador assistente, o DRA registra todas as operações do usuário no arquivo de registros no computador do servidor de Administração. O DRA fornece geração de relatórios claros e abrangentes que incluem valores antes e após os eventos auditados para que você possa ver exatamente o que mudou.

16 Auditando atividades

A auditoria de atividade nos registros de eventos pode ajudar você a isolar, diagnosticar e resolver problemas em seu ambiente. Esta seção fornece informações para ajudá-lo a habilitar e entender o registro de eventos e como trabalhar com arquivos de registro.

Registro de eventos do Windows nativo

Para permitir que você revise e relate as ações do administrador assistente, o DRA registra todas as operações do usuário no arquivo de registros no computador do servidor de Administração. As operações do usuário incluem todas as tentativas de mudar definições, como atualizar contas de usuários, 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.

Habilitando e desabilitando a auditoria de registro de eventos do Windows para DRA

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 mais informações, consulte a Ajuda do Editor do Registro do Windows.

Para habilitar a auditoria de evento:

1. Clique em **Iniciar > Executar**.
2. Digite `regedit` no campo **Abrir** e clique em **OK**.

3 Expanda a seguinte chave de Registro: `HKLM\Software\WOW6432Node\Mission Critical Software\OnePoint\Administration\Modules\ServerConfiguration\`.

4 Clique em **Editar > Novo > Valor DWORD**.

5 Digite `IsNTAuditEnabled` como o nome da chave.

6 Clique em **Editar > Modificar**.

7 Digite `1` no campo **Dados do valor** e clique em **OK**.

8 Feche o editor de registro.

Para desabilitar auditoria de eventos:

1 Clique em **Iniciar > Executar**.

2 Digite `regedit` no campo **Abrir** e clique em **OK**.

3 Expanda a seguinte chave de Registro: `HKLM\Software\WOW6432Node\Mission Critical Software\OnePoint\Administration\Modules\ServerConfiguration\`.

4 Selecione a chave `IsNTAuditEnabled`.

5 Clique em **Editar > Modificar**.

6 Digite `0` no campo **Dados do valor** e clique em **OK**.

7 Feche o editor de registro.

Garantindo a integridade da auditoria

Para verificar se todas as ações do usuário são auditadas, o DRA fornece métodos de registro alternativos quando o produto não pode verificar a atividade de registro. Quando você instala o DRA, a chave e o caminho AuditFailsFilePath são adicionados ao seu registro para garantir as seguintes ações:

- Se o DRA detectar que os eventos de auditoria não estão mais sendo registrados em um arquivo de registros, o DRA registrará os eventos de auditoria em um arquivo local no servidor de Administração.
- Se o DRA não puder gravar eventos de auditoria em um arquivo local, o DRA gravará eventos de auditoria no registro de eventos do Windows.
- Se o DRA não puder gravar eventos de auditoria no registro de eventos do Windows, o produto gravará eventos de auditoria no registro do DRA.
- Se o DRA detectar que os eventos de auditoria não estão sendo registrados, ele bloqueará outras operações do usuário.

Para habilitar operações de gravação quando o arquivo de registro não está disponível, você também deve definir um valor de chave do Registro para a chave AllowOperationsOnAuditFailure.

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 mais informações, consulte a Ajuda do Editor do Registro do Windows.

Para habilitar operações de gravação:

1 Clique em **Iniciar > Executar**.

2 Digite `regedit` no campo **Abrir** e clique em **OK**.

3 Expanda a seguinte chave de registro: `HKLM\Software\WOW6432Node\Mission Critical Software\OnePoint\Administration\Audit\`.

4 Clique em **Editar > Novo > Valor DWORD**.

5 Digite `AllowOperationsOnAuditFailure` como o nome da chave.

6 Clique em **Editar > Modificar**.

7 Digite 736458265 no campo **Dados do valor**.

8 Selecione **Decimal** no campo **Base** e clique em **OK**.

9 Feche o editor de registro.

Entendendo arquivos de registro

O DRA registra os dados de atividade do usuário nos arquivos de registro no servidor de Administração. O DRA cria as partições de arquivo de registro diárias para armazenar dados coletados e normalizados naquele dia. O DRA usa a data na hora local no servidor de administração (*AAAAMMDD*) como a convenção de nomenclatura para partições do arquivo de registro diárias.

Se você tiver habilitado o Coletor de Relatórios de Gerenciamento, o DRA exportará os dados de arquivo de registro para um banco de dados do SQL Server como a origem dos relatórios de Gerenciamento do DRA.

Inicialmente, o DRA retém os dados de registro no arquivo de registro indefinidamente por padrão. O tamanho do arquivo de registro pode atingir um tamanho máximo determinado no momento da instalação com base no espaço disponível no disco rígido. Quando o arquivo de registro excede esse tamanho máximo, nenhum novo evento de auditoria é armazenado. Você pode definir um limite de tempo para a retenção de dados, e o DRA remove os dados mais antigos para liberar espaço para dados mais recentes por meio de um processo chamado grooming. Verifique se você tem uma estratégia de backup em vigor antes de habilitar o grooming. Você pode configurar o período de retenção do arquivo de registro usando o utilitário Configuração do Arquivo de Registro. Para obter mais informações, veja Modificando as configurações de preparação do arquivo de registro.

Usando o utilitário Log Archive Viewer

Você usa o utilitário Log Archive Viewer para exibir dados armazenados em arquivos de registro. O Kit de Recursos de Arquivo de Registro do NetIQ DRA (LARK), que você pode optar por instalar com o DRA, fornece o utilitário Log Archive Viewer. Para mais informações, consulte a *Referência Técnica do Kit de Recursos do Arquivo de Registro do NetIQ DRA*.

Fazendo backup de arquivos de registro

Um **arquivo de registro** é uma coleção de blocos de registros. Como arquivos de registro são arquivos binários compactados que estão localizados fora de um banco de dados físico, você não precisa usar o Microsoft SQL Server Management Studio para fazer backup de arquivos de registro. Se você tiver um sistema de backup de arquivos automatizado, seus arquivos de registros serão copiados automaticamente como qualquer outro arquivo.

Tenha em mente as seguintes melhores práticas ao planejar sua estratégia de backup:

- Uma única partição é criada a cada dia que contém dados do evento para esse dia. Quando você habilita o grooming, o Serviço de Arquivo de Registro prepara os dados dessas partições automaticamente a cada 90 dias, por padrão. A estratégia de backup deve levar em conta a programação de preparação para determinar a frequência dos backups. Quando as partições de arquivo de registro são preparadas, o DRA apaga os arquivos binários. Não é possível recuperar dados de grooming. Você deve restaurar os dados de grooming de um backup. Para obter mais informações, veja Modificando as configurações de preparação do arquivo de registro.
- Você só deve fazer o backup das partições após terem sido fechadas. Em condições normais, uma partição é fechada dentro de 2 horas da meia-noite do próximo dia.
- Efetue backup e restaure as pastas de partição e todas as suas subpastas como uma unidade. Efetue backup do arquivo `VolumeInfo.xml` como parte do backup de partição.
- Se você deseja restaurar partições de arquivo de registro para relatórios, verifique se os arquivos de registro de backup mantêm ou podem ser restaurados para o formato original.
- Ao configurar seu processo para efetuar backup de arquivos de registro, NetIQ recomenda apagar ambas as subpastas `index_data` e `CubeExport` localizadas na pasta de arquivo de registro principal. Essas subpastas contêm dados temporários e não devem ter backup.

Modificando as configurações de preparação do arquivo de registro

Quando você instala o DRA, a limpeza do arquivo de registro fica desabilitada por padrão. Quando você estabelece procedimentos de backup regulares para seus arquivos de registro, você deve habilitar o grooming do arquivo de registro para economizar espaço em disco. Você modifica o número de dias antes que as partições do arquivo de registro sejam preparadas usando o utilitário Configuração de Arquivo de Registro.

Para mudar o número de dias antes de as partições de arquivo de registro serem preparadas:

1. Efetue logon no servidor de administração usando uma conta que seja membro do grupo Administradores locais.
2. Inicie a **Configuração de Arquivo de Registro** no grupo do programa da Administração da NetIQ.
3. Clique em **Log Archive Server Settings** (Configurações do Servidor do Arquivo de Registro).
4. *Se você quiser habilitar o grooming de partição,* defina o valor do campo **Partition Grooming Enabled** (Limpeza de Partição Habilitada) como True.
5. Digite o número de dias que você deseja manter as partições do arquivo de registro antes do grooming no campo **Number of Days before Grooming** (Número de Dias Antes do Grooming).
6. Clique em **Aplicar**.
7. Clique em **Sim**.

8 Clique em **Fechar**.

9 Localize o caminho para a pasta *NetIQLogArchiveData*\<*Nome da Partição*>, geralmente: `C:\ProgramData\NetIQ\DRA\NetIQLogArchiveData`

Se o atributo “Arquivo está pronto para arquivamento” nos arquivos ou nas pastas dentro das partições especificadas não estiver marcado (nas propriedades do arquivo ou da pasta), você deverá editar o arquivo CONFIG para habilitar a limpeza do arquivo de registro. Para entender por que esse atributo pode ou não ser verificado, consulte a seção **Informações Adicionais** no artigo da Base de Conhecimento *Como configurar o período de retenção de dados para os Dados do DRA Logarchival?*.

Se o valor for	
Marcada	Clique em **Sim** na mensagem de confirmação para reiniciar o serviço Arquivo de Registro do NetIQ Security Manager. **Observação:** Se você modificar qualquer configuração do arquivo de registro, deverá reiniciar o serviço Arquivo de Registro para que a mudança entre em vigor.
Não verificado	Clique em **Não** na mensagem de confirmação. Consulte Para permitir que o Servidor do Arquivo de Registro do DRA prepare dados não arquivados:.

Para permitir que o Servidor do Arquivo de Registro do DRA prepare dados não arquivados:

1 Efetue logon localmente em cada console do Windows do servidor DRA como membro do grupo de administradores locais.

2 Use o editor de texto para abrir o arquivo `C:\ProgramData\NetIQ\Directory Resource Administrator\LogArchiveConfiguration.config` e localize a linha `<Property name="GroomUnarchivedData" value="false" />`.

3 Mude `"false"` para `"true"` e grave o arquivo.

4 Reinicie o Serviço Arquivo de Registro NetIQ DRA.

Observação: Se você modificar qualquer configuração do arquivo de registro, deverá reiniciar o serviço Arquivo de Registro para que a mudança entre em vigor.

17 Gerador de relatórios

Esta seção fornece informações para entender e habilitar o DRA Reporting, coleta de dados de geração de relatórios, coleta e geração de relatórios do Analisador da Tela Ativa e para acessar relatórios integrados.

O DRA desabilita funções e relatórios que a 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.

Relatórios de Detalhes da atividade estarão disponíveis no console de Delegação e Configuração logo que você instalar o DRA para fornecer as informações mais recentes sobre as mudanças na rede.

- "Gerenciando a coleta de dados para o gerador de relatórios" na página 181
- "Relatórios integrados" na página 183

Gerenciando a coleta de dados para o gerador de relatórios

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 recurso, grupo e conta do usuário em seu domínio.

Relatórios de detalhes da atividade

Acessados por meio do console de Delegação e Configuração, esses relatórios fornecem informações sobre mudanças 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. A geração de relatórios também permite ver mais informações sobre o modelo de segurança do DRA, como as definições da Tela Ativa e do grupo de administradores assistentes.

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 Configuração do Gerador de Relatórios.

Visualizando o status dos coletores

Você pode ver mais informações de cada coletor de dados na guia Collectors Status (Status dos Coletores).

Para ver o status dos coletores:

1. Expanda **Configuration Management** (Gerenciamento de Configurações) e clique em **Update Reporting Service Configuration** (Atualizar Configuração do Serviço Gerador de Relatórios).
2. Na guia Collectors Status (Status dos Coletores), clique em cada entrada para ver informações adicionais sobre coleta de dados, como quando os dados foram coletados pela última vez e se a última coleta de dados foi bem-sucedida.
3. Se você não vir nenhum dado na lista Servidor, clique em **Atualizar**.

Habilitando o gerador de relatórios e a coleta de dados

Após instalar os componentes do DRA Reporting, habilite e configure a coleta de dados de geração de relatórios para acessar os relatórios do Centro do Gerador de Relatórios.

Para habilitar o gerador de relatórios e a coleta de dados:

1. Acesse **Configuration Management** (Gerenciamento de Configurações) > **Update Reporting Service Configuration** (Atualizar Configuração do Serviço Gerador de Relatórios).
2. Na guia SQL Server, selecione **Enable DRA Reporting support** (Habilitar suporte do DRA Reporting).
3. Clique em **Browse** (Procurar) no campo Nome do Servidor e selecione o computador em que o SQL Server está instalado.
4. Na guia Credentials (Credenciais), especifique as credenciais apropriadas a serem usadas nas interações do SQL Server.
5. Se esta for a mesma conta que pode ser usada para criar o banco de dados e inicializar o esquema, marque a caixa de seleção Use the above credentials for creating a database and initializing the database schema (Usar as credenciais acima para criar um banco de dados e inicializar o esquema do banco de dados).
6. Se você quiser especificar uma conta diferente para criar um banco de dados, na guia Admin Credentials (Credenciais do Admin), especifique essa conta do usuário e senha.
7. Clique em **OK**.

Para obter informações sobre como configurar coletores específicos, consulte Configuração do Gerador de Relatórios.

Relatórios integrados

Os relatórios integrados permitem gerar relatórios sobre mudanças de objetos, listas de objetos e mais informações de objetos. Esses relatórios não fazem parte do DRA Reporting Services e nenhuma configuração é necessária para habilitar os relatórios de histórico de mudanças incorporados. Consulte os tópicos desta seção para saber como acessar esses relatórios.

Observação: Os relatórios do histórico de mudanças também podem ser acessados para eventos fora do DRA quando o DRA é integrado ao Change Guardian. Para obter informações sobre esse tipo de relatórios e como configurar um servidor do Change Guardian, veja "Configurar o Histórico de Mudanças Unificado" na página 115.

Gerando relatórios sobre mudanças de objetos

Você pode ver informações de mudança em tempo real para objetos em seus domínios, gerando relatórios de detalhes da atividade. Por exemplo, você pode ver uma lista de mudanças feitas em um objeto ou por um objeto durante um período de tempo especificado. Você também pode exportar e imprimir relatórios de detalhes da atividade.

Para relatar mudanças de objeto:

1. Encontre os objetos que correspondam aos seus critérios.
2. Clique o botão direito do mouse em um objeto e selecione **Reporting > Changes made to objectName** (Gerador de Relatórios > Mudanças feitas ao objectName) ou **Reporting > Changes made by objectName** (Gerador de Relatórios > Mudanças feitas por objectName).
3. Selecione as datas de início e término para especificar as mudanças que você deseja ver.
4. *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.

   ---
5. *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.
6. Clique em **OK**.

Gerador de relatórios em listas de objetos

Você pode exportar ou imprimir dados de listas de objetos. Com esse recurso, você pode relatar e distribuir de maneira rápida e fácil informações gerais sobre seus objetos gerenciados.

Ao exportar uma lista de objetos, você pode especificar o local, o nome e o formato do arquivo. O DRA oferece suporte aos formatos HTML, CSV e XML, portanto, você pode exportar essas informações para aplicativos de banco de dados ou publicar resultados de lista em uma página da Web

Observação: Você também pode selecionar vários itens em uma lista e, em seguida, copiar esses itens para um aplicativo de texto, como o Bloco de Notas.

Para relatar listas de objetos:

1. Encontre os objetos que correspondam aos seus critérios.
2. Para exportar esta lista de objetos, clique em **Export List** (Exportar Lista) no menu Arquivo.
3. Para imprimir esta lista de objetos, clique em **Print List** (Imprimir Lista) no menu Arquivo.
4. Especifique as informações apropriadas para gravar ou imprimir essa lista.

Gerando relatórios sobre mais informações do objeto

Você pode exportar ou imprimir dados de guias de mais informações que listam atributos de objetos, como membros de grupos. Com esse recurso, você pode relatar e distribuir com rapidez e facilidade mais informações frequentemente necessárias sobre objetos específicos.

Ao exportar uma guia de mais informações do objeto, você pode especificar o local, o nome e o formato do arquivo. O DRA oferece suporte aos formatos HTML, CSV e XML, portanto, você pode exportar essas informações para aplicativos de banco de dados ou publicar resultados de lista em uma página da Web.

Para relatar mais informações do objeto:

1. Encontre o objeto que corresponde aos seus critérios.
2. No menu Ver, clique em **Mais informações**.
3. No painel de mais informações, selecione a guia apropriada.
4. Para exportar mais informações do objeto, clique na Lista **Export Details** (Exportar Mais Informações) no menu Arquivo.
5. Para imprimir mais informações do objeto, clique em **Print Details List** (Imprimir Lista de Mais Informações) no menu Arquivo.
6. Especifique as informações apropriadas para gravar ou imprimir essa lista.

VII Recursos adicionais

Atribuições de grupo temporárias, grupos dinâmicos, marcação de eventos e senha de recuperação do BitLocker são recursos adicionais no DRA que você pode empregar em seu ambiente corporativo.

18 Atribuições temporárias de grupo

O DRA permite criar atribuições de grupo temporárias que fornecem aos usuários autorizados acesso temporário aos recursos. Os administradores assistentes podem usar atribuições de grupo temporárias para atribuir usuários a um grupo de destino por um período de tempo específico. No final do período de tempo, o DRA remove automaticamente os usuários do grupo.

A função Gerenciar Designações Temporárias de Grupos concede aos administradores assistentes poderes para criar e gerenciar designações temporárias de grupos.

Os administradores assistentes podem ver apenas designações temporárias de grupos para grupos nos quais o administrador assistente tem a capacidade de adicionar ou remover membros.

Use os seguintes poderes para delegar a criação e o gerenciamento de atribuições de grupo temporárias:

- Criar atribuições de grupo temporárias
- Apagar Designações Temporárias de Grupos
- Modificar Designações Temporárias de Grupos
- Redefinir o Estado das Designações Temporárias de Grupos
- Ver as Designações Temporárias de Grupos
- Adicionar objeto ao grupo
- Remover objeto do grupo

O grupo de destino e os usuários devem pertencer à mesma Tela Ativa.

Observação

- Não é possível criar uma designação de grupo temporária para um usuário que já é membro do grupo de destino. Se você tentar criar uma designação de grupo temporária para um usuário que já seja membro do grupo de destino, o DRA exibirá uma mensagem de aviso e não permitirá a criação de uma designação de grupo temporária para o usuário.
- Se você criar uma designação de grupo temporária para um usuário que não seja membro do grupo de destino, o DRA removerá o usuário do grupo quando a designação de grupo temporário expirar.

Exemplo:

Bob, o gerente de RH, notifica John, um administrador de suporte técnico, que a empresa contratou um funcionário temporário chamado Joe por um período específico para concluir um projeto. John faz o seguinte:

- Cria uma TGA (designação temporária de grupo)
- Adiciona um grupo de RH para funcionários temporários à TGA

- Adiciona Joe como membro do grupo de funcionários temporários
- Define a duração da TGA para um mês (de 03/07/2019 a 02/08/2019)

Resultado esperado:

Por padrão, quando a TGA expirar, a participação de Joe será removida do grupo de RH. A TGA permanecerá disponível por sete dias, a menos que John tenha selecionado a opção **Mantenha esta designação temporária de grupo para uso futuro**.

Para obter mais informações sobre como criar e usar designações temporárias de grupos, consulte o *DRA User Guide* (Guia do Usuário do DRA).

19 Grupos dinâmicos do DRA

Um grupo dinâmico é aquele cuja participação muda com base em um conjunto definido de critérios que você configura nas propriedades do grupo. Você pode tornar qualquer grupo dinâmico ou remover o filtro dinâmico de qualquer grupo que o tenha configurado. Esse recurso também fornece a capacidade de adicionar membros do grupo a uma lista estática ou a uma lista apagada. Os membros do grupo nessas listas não serão afetados pelos critérios dinâmicos.

Se você reverter um grupo dinâmico de volta para um grupo normal, todos os membros da lista de membros estáticos serão adicionados à participação de grupos e os membros apagados e os filtros dinâmicos serão ignorados. Você pode dinamizar grupos existentes ou criar um novo grupo dinâmico no Console de Delegação e Configuração e no Console da Web.

Para tornar um grupo dinâmico:

1. Localize o grupo no console aplicável.
   - Delegação e Configuração: Acesse **Todos os Meus Objetos Gerenciados** > **Find now** (Localizar Agora).

     Observação: Para habilitar o Query Builder, clique em **Browse** (Procurar) e selecione um domínio, container ou OU.

   - Console da Web: Acesse **Gerenciamento** > **Pesquisar**.
2. Abra as propriedades do grupo e selecione **Tornar grupo dinâmico** na guia Filtro Dinâmico de Membros.
3. Adicione o LDAP desejado e os atributos virtuais para filtrar a participação do grupo.
4. Adicione todos os membros estáticos ou apagados desejados ao grupo dinâmico e aplique suas mudanças.

Para tornar um novo grupo dinâmico:

- **Delegação e Configuração:** Clique o botão direito do mouse no domínio ou subnó em Todos os Meus Objetos Gerenciados e selecione **Novo** > **Grupo Dinâmico**.
- **Console da Web:** Acesse **Gerenciamento** > **Criar** > **Grupo Dinâmico**.

20 Como funciona a marcação de eventos

Quando você configura um atributo para um tipo de objeto e o DRA executa uma das operações suportadas, esse atributo será atualizado (marcado) com informações específicas do DRA, incluindo quem executou a operação. Isso faz com que o AD gere um evento de auditoria para essa mudança de atributo.

Como exemplo, suponha que você tenha selecionado o atributo `extensionAttribute1` como seu atributo de usuário e você tenha a auditoria do AD DS configurada. Sempre que um administrador assistente atualizar um usuário, o DRA atualizará o atributo `extensionAttribute1` com os dados da Marcação de Eventos. Isso significa que, juntamente com os eventos do AD DS para cada atributo que o administrador assistente atualizou (por exemplo: descrição, nome etc.) haverá um evento do AD DS adicional para o atributo `extensionAttribute1`.

Cada um desses eventos contém um ID de Correlação que é o mesmo para cada atributo mudado que foi mudado quando o usuário foi atualizado. É assim que os aplicativos podem associar os dados da Marcação de Eventos aos outros atributos que foram atualizados.

Para obter etapas para habilitar a Marcação de Eventos, consulte Habilitar a marcação de eventos no DRA.

Para obter um exemplo de evento do AD DS e tipos de operação suportados, consulte os seguintes:

- “O evento AD DS” na página 191
- “Operações suportadas” na página 192

O evento AD DS

Você verá um evento como este no registro de eventos do Windows Security sempre que o DRA executar uma operação suportada.

Nome de exibição do LDAP:	**`extensionAttribute1`**
Sintaxe (OID): 2.5.5.12	2.5.5.12
Valor:	<dra-event **user**="DRDOM300\drauseradmin" **sid**="S-1-5-21-53918190-1560392134-2889063332-1914" **tid**="E0E257E6B4D24744A9B0FE3F86EC7038" **SubjectUserSid**="S-1-5-21-4224976940-2944197837-1672139851-500" **ObjectDN**="CN=admin_113,OU=Vino_113,DC=DRDOM113,DC=LAB"/ >+a+02ROO+bJbhyPbR4leJpKWCGTp/ KXdqI7S3EBhVyniE7iXvxIT6eB6IdcXQ5StkbIAHJgKzLN5FCOM5fZcITxyAPLWhbstaA7ZA0VbVC9MGlVIaAcjl3z7mpF9GKXsfDogbSeNlmHliXvH5KpOX3/29AKMPj/zvf6Yuczoos=

O valor do evento consiste em duas partes. A primeira é uma string XML contendo os dados de Marcação de Eventos. A segunda é uma autenticação dos dados que podem ser usados para validar que os dados foram realmente gerados pelo DRA. Para validar a autenticação, um aplicativo deve ter a chave pública para a autenticação.

A string XML consiste nas seguintes informações:

Usuário	O administrador assistente que executou a operação
Sid	O SID do administrador assistente que executou a operação
Tid	O ID de transação de auditoria do DRA para verificar se cada evento é exclusivo
SubjectUserSid	O SID da conta de serviço ou conta de acesso do DRA que realmente atualizou o AD
ObjectDN	O nome exclusivo do objeto que foi modificado

Operações suportadas

Usuário	◆ Criar ◆ Renomear ◆ Modificar ◆ Clonar
Grupo	◆ Criar ◆ Renomear ◆ Modificar ◆ Clonar
Contato	◆ Criar ◆ Renomear ◆ Modificar ◆ Clonar
Computador	◆ Criar ◆ Habilitar ◆ Desabilitar ◆ Renomear ◆ Modificar
Unidade Organizacional	◆ Criar ◆ Renomear ◆ Clonar

21 Senha de recuperação do BitLocker

O Microsoft BitLocker armazena suas senhas de recuperação no Active Directory. Usando o recurso Recuperação de BitLocker DRA, você pode delegar poderes a administradores assistentes 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 o BitLocker está habilitado.

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 **Delegação e Configuração** e expanda a estrutura de exibição em árvore.
2. No nó **Account and Resource Management** (Gerenciamento de Recursos e de Contas), acesse **Todos os Meus Objetos Gerenciados** > **Domínio** > **Computadores**.
3. Na lista de computadores, clique o botão direito do mouse no computador desejado e selecione **Propriedades**.
4. Clique na guia **Senha de Recuperação do BitLocker** para exibir a senha de recuperação do BitLocker.
5. Clique o botão direito do mouse na senha de recuperação do BitLocker, clique em **Copiar** e cole o texto no arquivo texto ou planilha desejada.

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 **Delegação e Configuração** e expanda a estrutura de exibição em árvore.
2. No nó **Account and Resource Management** (Gerenciamento de Recursos e de Contas), acesse **Todos os Meus Objetos Gerenciados**, clique o botão direito do mouse no **Domínio Gerenciado** e clique em **Localizar 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**.

22 Lixeira

Você pode habilitar ou desabilitar a Lixeira para cada domínio ou objetos do Microsoft Windows nesses domínios, controlando o gerenciamento de contas em toda a sua empresa. Se você habilitar a Lixeira e depois apagar uma conta do usuário, grupo, grupo dinâmico de distribuição, grupo dinâmico, caixa de correio de recurso, contato ou conta de computador, o Servidor de Administração desabilitará a conta selecionada e a moverá para o container Lixeira. Depois que o DRA move a conta para a Lixeira, a conta não é exibida nas Telas Ativas às quais ela pertencia. Se você apagar uma conta do usuário, grupo, contato ou conta de computador quando a Lixeira estiver desabilitada, o servidor de Administração apagará permanentemente a conta selecionada. Você pode desabilitar uma Lixeira que contenha contas apagadas anteriormente. No entanto, depois que a Lixeira é desabilitada, essas contas não estão mais disponíveis no nó Lixeira.

Atribuindo poderes à Lixeira

Para permitir que um administrador assistente apague permanentemente contas do nó Todos os Meus Objetos Gerenciados, bem como da Lixeira, atribua a energia relevante da lista a seguir:

- Apagar Permanentemente a Conta do Usuário
- Apagar grupo permanentemente
- Apagar computador permanentemente
- Apagar contato permanentemente
- Apagar Grupo de Distribuição Dinâmica Permanentemente
- Apagar Grupo Dinâmico Permanentemente
- Apagar Permanentemente a Caixa de Correio de Recursos

Se vários servidores de Administração gerenciarem subárvores diferentes no mesmo domínio do Microsoft Windows, você poderá usar a Lixeira para exibir qualquer conta apagada desse domínio, independentemente de qual Servidor de administração gerencia essa conta.

Usando a Lixeira

Use a Lixeira para apagar permanentemente contas, restaurar contas ou ver propriedades de contas apagadas. Você também pode pesquisar contas específicas e acompanhar quantos dias uma conta apagada está na Lixeira. Uma guia Lixeira também é incluída na janela Propriedades de um domínio selecionado. Nessa guia, você pode desabilitar ou habilitar a Lixeira para todo o domínio ou para objetos específicos, bem como programar uma limpeza da Lixeira.

Use as opções **Restore All** (Restaurar Tudo) ou **Empty Recycle Bin** (Esvaziar Lixeira) para, de modo rápido e fácil, restaurar ou apagar essas contas.

Quando você restaura uma conta, o DRA restabelece a conta, incluindo todas as permissões, delegações de energia, atribuições de política, associações a grupos e membros da Tela Ativa. Se você apagar permanentemente uma conta, o DRA removerá essa conta do Active Directory.

Para garantir o apagamento seguro da conta, somente os administradores assistentes com os seguintes poderes podem apagar permanentemente as contas da Lixeira:

- Apagar Permanentemente a Conta do Usuário
- Apagar usuário da Lixeira
- Apagar permanentemente a conta do grupo
- Apagar grupo da Lixeira
- Apagar conta de computador permanentemente
- Apagar computador da Lixeira
- Apagar conta de contato permanentemente
- Apagar contato da Lixeira
- Apagar Grupo de Distribuição Dinâmica Permanentemente
- Apagar grupo de distribuição dinâmica da Lixeira
- Apagar Grupo Dinâmico Permanentemente
- Apagar grupo dinâmico da Lixeira
- Apagar Permanentemente a Caixa de Correio de Recursos
- Apagar caixa de correio de recursos da Lixeira
- Exibir todos os Objetos da Lixeira

Para restaurar uma conta da Lixeira, os administradores assistentes devem ter os seguintes poderes na OU que contém a conta:

- Restaurar usuário da Lixeira
- Restaurar grupo da Lixeira
- Restaurar grupo de distribuição dinâmica da Lixeira
- Restaurar grupo dinâmico da Lixeira
- Restaurar a caixa de correio de recursos da Lixeira
- Restaurar o computador da Lixeira
- Restaurar contato da Lixeira
- Exibir todos os Objetos da Lixeira

Observação

- Se você apagar uma conta do administrador assistente enviando-a para a Lixeira, o DRA continuará a exibir as designações da Tela Ativa e das funções dessa conta. Em vez de exibir o nome da conta do administrador assistente apagada, o DRA exibe o SID (identificador de segurança). Você pode remover essas designações antes de apagar permanentemente a conta do administrador assistente.
- O DRA apaga o diretório pessoal após apagar a conta do usuário da Lixeira.
- Se você apagar um usuário que tiver uma licença do Office 365, a conta do usuário será enviada para a Lixeira e a licença será removida. Se você restaurar posteriormente a conta do usuário, a licença do Office 365 também será restaurada.

VIII Personalização do cliente

Você pode personalizar o cliente de Delegação e Configuração e o Console da Web. O primeiro requer acesso remoto ou físico e credenciais de conta. O último requer o URL do servidor e as credenciais da conta para efetuar login em um browser da Web.

23 Cliente de Delegação e Configuração

Esta seção inclui informações para ajudá-lo a personalizar o cliente de Delegação e Configuração, que inclui o entendimento de como criar páginas de propriedades personalizadas, como criar ferramentas personalizadas no DRA que podem ser executadas em computadores cliente e servidor na rede e como personalizar a configuração da interface do usuário.

Personalizando páginas de propriedades

Você pode personalizar e estender o console de Delegação e Configuração implementando propriedades personalizadas. As propriedades personalizadas permitem que você adicione contas proprietárias e propriedades da OU, como extensões de esquema do Active Directory e atributos virtuais, a assistentes e janelas de propriedades específicos. Essas extensões permitem que você personalize o DRA para atender aos seus requisitos específicos. Usando o assistente New Custom Page (Nova Página Personalizada) no console de Delegação e Configuração, você pode criar uma página personalizada de modo rápido e fácil para estender a interface do usuário apropriada.

Se seus administradores assistentes precisarem de poderes exclusivos para gerenciar com segurança a página personalizada, você também poderá criar e delegar poderes personalizados. Por exemplo, você pode querer limitar o gerenciamento de contas do usuário somente às propriedades na página personalizada. Para obter mais informações, veja Implementando poderes personalizados.

Como funcionam as páginas de propriedades personalizadas

As extensões da interface do usuário são exibições do DRA de páginas personalizadas nas janelas apropriadas de assistente e de propriedades. Você pode configurar páginas personalizadas para expor atributos do Active Directory, extensões de esquema e atributos virtuais no console de Delegação e Configuração.

Quando você seleciona qualquer atributo suportado, uma extensão do esquema ou um atributo virtual do Active Directory, você pode usar páginas personalizadas das seguintes formas:

- Limite os administradores assistentes para gerenciar um conjunto bem-definido e controlado de propriedades. Este conjunto de propriedades pode incluir *propriedades padrão* e extensões de esquema. As propriedades padrão são atributos do Active Directory expostos por padrão no console de Gerenciamento de Recursos e de Contas.
- Exponha os atributos do Active Directory que não sejam as propriedades padrão gerenciadas pelo DRA.
- Estenda o console de Delegação e Configuração para incluir propriedades proprietárias.

Você também pode configurar como o DRA exibe e aplica essas propriedades. Por exemplo, você pode definir controles de interface do usuário com valores de propriedade padrão.

O DRA aplica páginas personalizadas a todos os objetos gerenciados aplicáveis em sua empresa. Por exemplo, se você criar uma página personalizada para adicionar extensões de esquema do Active Directory à janela Group Properties (Propriedades do Grupo), o DRA aplicará as propriedades nessa página a cada grupo gerenciado em um domínio que suporte as extensões de esquema especificadas. Cada página personalizada requer um conjunto exclusivo de propriedades. Não é possível adicionar um atributo do Active Directory a mais de uma página personalizada.

Você não pode desabilitar janelas ou guias individuais na interface do usuário existente. Um administrador assistente pode selecionar um valor de propriedade usando a interface do usuário padrão ou uma página personalizada. O DRA aplica o valor selecionado mais recentemente para uma propriedade.

O DRA fornece uma trilha de auditoria completa para propriedades personalizadas. O DRA registra os seguintes dados no registro de eventos do Aplicativo:

- Mudanças em páginas personalizadas

  Importante: Você deve configurar manualmente a Auditoria de Registro do Aplicativo do Windows. Para obter mais informações, veja Habilitando e desabilitando a auditoria de registro de eventos do Windows para DRA.

- Criação e apagamento de páginas personalizadas
- Extensão do esquema exposta, atributos do Active Directory e atributos virtuais incluídos em páginas personalizadas

Você também pode executar relatórios de atividades de mudanças para monitorar as mudanças de configuração das propriedades personalizadas.

Implemente e modifique páginas personalizadas no servidor de administração principal. Durante a sincronização, o DRA replica configurações de página personalizadas no Conjunto Multimaster. Para obter mais informações, veja Configurar o conjunto multimaster.

Páginas personalizadas suportadas

Cada página personalizada que você cria permite que você selecione um conjunto de propriedades do Active Directory, extensões de esquema ou atributos virtuais e exponha essas propriedades como uma guia personalizada. Você pode criar os seguintes tipos de páginas personalizadas:

Página de Usuário Personalizada

Permite que você exiba guias personalizadas nas seguintes janelas:

- Janela User Properties (Propriedades do Usuário)
- Criar Assistente do Usuário
- Clonar Assistente do Usuário

Página de Grupos Personalizada

Permite que você exiba guias personalizadas nas seguintes janelas:

- Janela Group Properties (Propriedades do Grupo)
- Assistente Criar Grupo
- Assistente Clonar Grupo

Página de Computador Personalizada

Permite que você exiba guias personalizadas nas seguintes janelas:

- Janela Propriedades do Computador
- Assistente Criar Computador

Página de Contato Personalizada

Permite que você exiba guias personalizadas nas seguintes janelas:

- Janela Propriedades do Contato
- Assistente Criar Contato
- Assistente Clonar Contato

Página da OU Personalizada

Permite que você exiba guias personalizadas nas seguintes janelas:

- Janela Propriedades da OU
- Assistente Criar OU
- Assistente Clonar OU

Página da Caixa de Correio de Recursos Personalizada

Permite que você exiba guias personalizadas nas seguintes janelas:

- Janela Propriedades da Caixa de Correio de Recursos
- Assistente Criar Caixa de Correio de Recursos
- Assistente Clonar Caixa de Correio de Recursos

Página do Grupo de Distribuição Dinâmica Personalizada

Permite que você exiba guias personalizadas nas seguintes janelas:

- Janela Propriedades do Grupo de Distribuição Dinâmica

- Assistente Criar Grupo de Distribuição Dinâmica
- Assistente Clonar Grupo de Distribuição Dinâmica

Página da caixa de correio compartilhada personalizada

Permite que você exiba guias personalizadas nas seguintes janelas:

- Janela Propriedades da caixa de correio compartilhada
- Assistente Criar caixa de correio compartilhada
- Assistente Clonar caixa de correio compartilhada

Controles de propriedades personalizadas suportados

Quando você adiciona um atributo do Active Directory, uma extensão do esquema ou um atributo virtual a uma página personalizada, também configura o controle da interface do usuário com o qual um administrador assistente insere o valor de propriedade. Por exemplo, você pode especificar valores de propriedade das seguintes maneiras:

- Definir intervalos de valores específicos
- Definir valores de propriedade padrão
- Indicar se uma propriedade é obrigatória

Você também pode configurar o controle da interface do usuário para exibir informações ou instruções proprietárias. Por exemplo, se você definir uma faixa específica para um número de identificação de funcionário, poderá configurar o rótulo de controle da caixa de texto para exibir **Especificar número de identificação do funcionário (001 a 100)**.

Cada controle de interface do usuário fornece suporte para um único atributo do Active Directory, uma extensão do esquema ou um atributo virtual. Configure os seguintes controles da interface do usuário com base no tipo de propriedade:

Tipo de atributo do Active Directory	Controles da interface do usuário suportados
Booliano	Caixa de seleção
Data	Controle de calendário
Inteiro	Caixa de texto (padrão) Lista de seleção
String	Caixa de texto (padrão) Lista de seleção Seletor de objetos
String multivalores	Lista de seleção

Trabalhando com páginas personalizadas

Você pode criar páginas personalizadas usando o nó User Interface Extensions (Extensões da Interface do Usuário). Depois que uma página é criada, você pode adicionar ou remover propriedades do atributo do AD e desabilitar ou apagar a página. Para cada personalização que você

deseja configurar, crie uma página personalizada e designe o poder ou a função apropriada ao administrador assistente. Considere as melhores práticas abaixo ao começar a trabalhar com páginas personalizadas:

1. Para verificar se o DRA reconhece seus atributos do Active Directory, atributos de extensão do esquema ou atributos virtuais, reinicie o serviço do Serviço de Administração NetIQ em cada servidor de Administração.
2. Identifique o tipo de página personalizada que você deseja criar e as propriedades que você deseja que os administradores assistentes gerenciem com essa página personalizada. Você pode selecionar qualquer atributo do Active Directory, incluindo atributos de extensão do esquema e atributos existentes em assistentes de DRA e janelas de propriedades ou qualquer atributo virtual criado. No entanto, cada página personalizada requer um conjunto exclusivo de propriedades. Não é possível adicionar um atributo do Active Directory a mais de uma página personalizada.

   Páginas personalizadas não substituem a interface do usuário existente. Para obter mais informações, consulte a Como funcionam as páginas de propriedades personalizadas e o Páginas personalizadas suportadas.
3. Determine como você deseja que os administradores assistentes especifiquem essas propriedades. Por exemplo, você pode querer limitar uma propriedade especificada a três valores possíveis. Você pode definir um controle de interface do usuário apropriado para cada propriedade. Para obter mais informações, veja Controles de propriedades personalizadas suportados.
4. Determine se seus administradores assistentes precisam de informações proprietárias ou de instruções para gerenciar com êxito essas propriedades. Por exemplo, determine se o Active Directory exige uma sintaxe para o valor de propriedade, como um nome exclusivo (DN) ou um caminho LDAP.
5. Identifique a ordem em que essas propriedades devem ser exibidas na página personalizada. Você pode mudar a ordem de exibição a qualquer momento.
6. Determine como o DRA deve usar essa página personalizada. Por exemplo, você pode adicionar uma página personalizada do usuário ao assistente New User (Novo usuário) e à janela User Properties (Propriedades do Usuário).
7. Use a guia Designações no painel de mais informações do Admin Assistente para verificar se os seus administradores assistentes têm os poderes apropriados para o conjunto correto de objetos. Se você criou poderes personalizados para essa página personalizada, delegue-os aos administradores assistentes apropriados.
8. Determine se seus administradores assistentes precisam de um poder personalizado para gerenciar as propriedades nessa página. Por exemplo, se você adicionar uma página personalizada à janela Propriedades do Usuário, delegar o poder *Modificar Todas as Propriedades do Usuário* poderá dar a um administrador assistente muito poder. Crie todos os poderes personalizados necessários para implementar sua página personalizada. Para obter mais informações, veja Implementando poderes personalizados.
9. Usando suas respostas das etapas acima, crie as páginas personalizadas apropriadas.
10. Distribua as informações sobre as páginas de propriedades personalizadas que você implementou para os administradores assistentes apropriados, como o Suporte Técnico.

Para implementar a personalização de propriedade, você deve ter os poderes incluídos na função Administração do DRA. Para mais informações sobre as páginas de personalização, consulte Como funcionam as páginas de propriedades personalizadas.

Criando páginas de propriedades personalizadas

Você pode criar diferentes propriedades personalizadas criando diferentes páginas personalizadas. Por padrão, novas páginas personalizadas estão habilitadas.

Quando você cria uma página personalizada, pode desabilitá-la. Desabilitar uma página personalizada a oculta da interface do usuário. Se você estiver criando várias páginas personalizadas, poderá desabilitar as páginas até que as personalizações sejam testadas e concluídas.

Observação: Contas de computador herdam atributos do Active Directory de contas de usuário. Se você estender o esquema do Active Directory para incluir atributos adicionais para contas de usuário, poderá selecionar esses atributos quando criar uma página personalizada para gerenciar contas de computador.

Para criar uma página de propriedades personalizada:

1. Navegue até o nó **Configuration Management** > **User Interface Extensions** (Gerenciamento de Configurações > Extensões da Interface do Usuário).
2. No menu Tarefas, clique em **Novo** e, em seguida, clique no item de menu apropriado para a página personalizada que você deseja criar.
3. Na guia General (Geral), digite o nome dessa página personalizada e clique em **OK**. Se você quiser desabilitar esta página, limpe a caixa de seleção **Habilitado**.
4. Para cada propriedade que você deseja incluir nessa página personalizada, conclua as etapas a seguir:
   - **4a** Na guia Propriedade, clique em **Adicionar**.
   - **4b** Para selecionar uma propriedade, clique em **Browse** (Procurar).
   - **4c** No campo **Control label** (Rótulo de controle), digite o nome da propriedade que o DRA deve usar como rótulo para o controle da interface do usuário. Verifique se o rótulo de controle é amigável ao usuário e altamente descritivo. Você também pode incluir instruções, intervalos de valores válidos e exemplos de sintaxe.
   - **4d** Selecione o controle de interface do usuário apropriado no menu **Control type** Tipo de controle.
   - **4e** Selecione em que local no console de Delegação e Configuração você deseja que o DRA exiba esta página personalizada.
   - **4f** Para especificar atributos adicionais, como comprimento mínimo ou valores padrão, clique em**Advanced** (Avançado).
   - **4g** Clique em **OK**.
5. Para mudar a ordem na qual o DRA exibe essas propriedades na página personalizada, selecione a propriedade apropriada e clique em **Mover para Cima** ou **Mover para Baixo**.
6. Clique em **OK**.

Modificando propriedades personalizadas

Você pode mudar uma página personalizada modificando as propriedades personalizadas.

Para modificar propriedades personalizadas:

1. Navegue até o nó **Configuration Management** > **User Interface Extensions** (Gerenciamento de Configurações > Extensões da Interface do Usuário).
2. No painel de lista, selecione a página personalizada desejada.
3. No menu Tarefas, clique em **Propriedades**.
4. Modifique as propriedades e configurações apropriadas para esta página personalizada.
5. Clique em **OK**.

Identificando atributos do Active Directory gerenciados com páginas personalizadas

Você pode identificar rapidamente quais propriedades do Active Directory, extensões de esquema ou atributos virtuais são gerenciados usando uma determinada página personalizada.

Para identificar as propriedades do Active Directory gerenciadas usando páginas personalizadas:

1. Navegue até o nó **Configuration Management** > **User Interface Extensions** (Gerenciamento de Configurações > Extensões da Interface do Usuário).
2. No painel de lista, selecione a página personalizada desejada.
3. No painel de mais informações, clique na guia**Propriedades**. Para ver o painel de mais informações, clique em **Mais informações** no menu Ver.
4. Para verificar como o DRA exibe e aplica uma propriedade, selecione o atributo apropriado do Active Directory, a extensão do esquema ou o atributo virtual na lista e clique no ícone **Propriedades**.

Habilitando, desabilitando e apagando páginas personalizadas

Quando você habilita uma página personalizada, o DRA adiciona essa página personalizada aos assistentes e janelas associados. Para especificar quais assistentes e janelas exibem uma página personalizada, modifique as propriedades da página personalizada.

Observação: Para verificar se cada página personalizada expõe um conjunto exclusivo de propriedades, o DRA não habilita páginas personalizadas que contenham propriedades expostas em outras páginas personalizadas.

Quando você desabilita uma página personalizada, o DRA remove a página personalizada dos assistentes e janelas associados. O DRA não apaga a página personalizada. Para garantir que uma página personalizada nunca seja exibida na interface do usuário, apague a página personalizada.

Quando você apaga uma página personalizada, o DRA remove a página personalizada dos assistentes e janelas associados. Você não pode restaurar uma página personalizada apagada. Para remover temporariamente uma página personalizada da interface do usuário, desabilite a página personalizada.

Para habilitar, desabilitar ou apagar uma página personalizada, navegue até o nó **Configuration Management** > **User Interface Extensions** (Gerenciamento de Configurações > Extensões da Interface do Usuário) e selecione a ação desejada em Tarefas ou no menu de clique com o botão direito do mouse.

Interface de linha de comando

A CLI permite que você acesse e aplique recursos avançados de produtos de administração usando comandos ou arquivos em lote. Com a CLI, você pode emitir um comando para implementar mudanças em vários objetos.

Por exemplo, se você precisar realocar os diretórios pessoais de 200 funcionários para um novo servidor, usando a CLI, poderá digitar o seguinte comando único para mudar todas as 200 contas de usuário:

```
EA USER @GroupUsers(HOU_SALES),@GroupUsers(HOU_MIS) UPDATE
HOMEDIR:\\HOU2\USERS\@Target()
```

Esse comando direciona o DRA a mudar o campo de diretório pessoal de cada uma das 200 contas de usuário nos grupos `HOU_SALES` e `HOU_MIS` para `\\HOU2\USERS\`*user_id*. Para realizar essa tarefa com as ferramentas de administração nativas do Microsoft Windows, você precisaria realizar pelo menos 200 ações separadas.

Observação: A ferramenta CLI será descontinuada em versões futuras à medida que mais recursos forem adicionados ao PowerShell.

Ferramentas personalizadas

Ferramentas personalizadas podem ser usadas para chamar qualquer aplicativo a ser executado em computadores clientes e servidores na rede, selecionando qualquer conta do Active Directory gerenciada no DRA.

O DRA suporta dois tipos de ferramentas personalizadas:

- Ferramentas personalizadas que iniciam utilitários de área de trabalho comuns, como o Microsoft Office
- Ferramentas personalizadas que você cria e distribui para cada computador cliente do DRA

Você pode criar uma ferramenta personalizada que inicia uma verificação antivírus de todos os computadores em que o cliente DRA está instalado. Você também pode criar uma ferramenta personalizada que inicie um aplicativo externo ou uma ferramenta que exija que o DRA atualize um script periodicamente. Essas atualizações periódicas podem ser mudanças na configuração ou mudanças na regra de negócios. Posteriormente, após as atualizações periódicas, o DRA replica as ferramentas personalizadas do servidor de administração principal para qualquer servidor de administração secundário e computador cliente DRA.

Para entender como as ferramentas personalizadas são replicadas no conjunto multimaster do servidor, consulte Replicação de arquivo.

Criando ferramentas personalizadas

Você pode criar ferramentas personalizadas no servidor principal do DRA associando a um objeto do Active Directory selecionado ou a todos os objetos do Active Directory exibidos nesse assistente de criação de ferramenta personalizada. O mesmo será replicado para servidores secundários no MMS e para os clientes DRA por meio da replicação de arquivos.

Uma nova ferramenta personalizada criará um menu e um submenu, se necessário, para invocar a operação contra os objetos do Active Directory associados no DRA.

Você pode delegar poderes a administradores assistentes para criar e executar ferramentas personalizadas e para acessar e executar o aplicativo.

Ao criar uma ferramenta personalizada, você precisa inserir os parâmetros da seguinte forma:

Guia General (Geral)

1. **Nome:** Qualquer nome de cliente necessário para a ferramenta.
2. **Menu e Submenu:** Para criar um item de menu para uma nova ferramenta personalizada, digite o título do menu no campo **Menu and Submenu Structure** (Estrutura do Menu e Submenu). Quando você cria uma ferramenta personalizada e seleciona o objeto, o DRA exibe o item de menu da ferramenta personalizada usando o menu e a estrutura do submenu especificados no menu Tarefas, no menu de Atalho e na barra de ferramentas DRA.

   Estrutura de amostra de Menu e Submenu: Digite o nome do item de menu, um caractere de barra invertida (\) e, em seguida, o nome do item de submenu.

   Para ter uma tecla de atalho: Digite um caractere e comercial (&) antes do nome do item de menu.

   a. Exemplo: `SendEmail\ApproveAction` ---- `SendEmail` é o menu e `ApproveAction` é o submenu com a primeira letra “A” em `ApproveAction` sendo a tecla de atalho habilitada.
3. **Habilitado:** Marque esta caixa para ativar a ferramenta personalizada.
4. **Descrição:** Você pode adicionar qualquer valor de descrição necessário.
5. **Comentário:** Você pode adicionar qualquer comentário necessário à ferramenta personalizada.

Guia Supported Objects (Objetos Suportados)

Selecione o objeto AD necessário ou todos os objetos do AD aos quais a ferramenta personalizada criada deve ser associada.

As opções atuais de ferramentas personalizadas suportadas incluem: Domínio Gerenciado, containeres, Usuários, Contatos, Grupos, Computadores, Unidade Organizacional e Published Printers (Impressoras Publicadas).

Observação: Outros objetos recém-apresentados, como Caixa de correio de recursos, Grupo dinâmico e Exchange Dynamic Group (Grupo Dinâmico do Exchange) não são suportados com Ferramentas personalizadas.

Guia Application Settings (Configurações do Aplicativo)

Location of the application: (Localização do aplicativo) Você precisa fornecer o caminho/local em que o aplicativo está instalado copiando e colando o caminho exato do aplicativo ou usando a opção **Inserir**.

Esse mesmo caminho já deve existir em todos os servidores do DRA no MMS. Se necessário, você pode usar Replicação de arquivo para fazer upload e replicar um arquivo em um caminho utilizável nos servidores do MMS antes de criar uma ferramenta personalizada.

Você também pode usar variáveis DRA, variáveis de ambiente e valores de registro para especificar o local do aplicativo externo no campo Location of the application (Localização do aplicativo). Para usar essas variáveis, clique em **Inserir** e selecione a variável que deseja usar.

Após inserir a variável, digite um caractere de barra invertida (\) e especifique o restante do caminho do aplicativo, incluindo o nome do arquivo executável do aplicativo.

Exemplos:

- *Exemplo 1:* Para especificar o local de um aplicativo externo que a ferramenta personalizada executará, selecione a variável de ambiente {%PROGRAMFILES%} e, em seguida, especifique o restante do caminho do aplicativo no campo Location of the application (Localização do aplicativo): {%PROGRAMFILES%}\ABC Associates\VirusScan\Scan32.exe

  ---

  Observação: O DRA fornece o valor do registro do diretório de instalação do Office como uma amostra. Para especificar uma chave de registro que contenha um caminho como um valor, use a seguinte sintaxe:
  {HKEY_LOCAL_MACHINE\SOFTWARE\MyProduct\SomeKey\(Default)}

- *Exemplo 2:* Para especificar o local de um arquivo de script personalizado que a ferramenta personalizada executará, selecione a variável do DRA {DRA_Replicated_Files_Path} e, em seguida, especifique o restante do caminho do arquivo de script no campo Location of the application (Localização do aplicativo): {DRA_Replicated_Files_Path}\cscript.vbs; em que {DRA_Replicated_Files_Path} é o caminho de arquivo replicado ou a pasta {DRAInstallDir}\FileTransfer\Replicate no Servidor de administração.

  Observação: Antes de criar a ferramenta personalizada, faça o upload do arquivo de script no servidor de administração primário usando o recurso de replicação de arquivo. O recurso de replicação de arquivos faz o upload do arquivo de script para a pasta {DRAInstallDir}\FileTransfer\Replicate no servidor de administração principal.

- *Exemplo 3:* Para especificar o local de um utilitário do DRA que a ferramenta personalizada executará, selecione a variável do DRA {DRA_Application_Path} e, em seguida, especifique o restante do caminho do utilitário no campo Location of the application (Localização do aplicativo): {DRA_Application_Path}\DRADiagnosticUtil.exe; em que {DRA_Application_Path} é o local em que o DRA está instalado.
- *Exemplo 4:* Basta copiar e colar o local do aplicativo junto com o nome do arquivo do aplicativo com extensão.

Parameters to pass to the application: (Parâmetros a passar para o aplicativo) Para definir um parâmetro a ser passado para um aplicativo externo, copie e cole ou digite um ou mais parâmetros no campo Parameters to pass to the application (Parâmetros para passar para o aplicativo). O DRA fornece parâmetros que você pode usar no campo Parameters to pass to the application (

Parâmetros para passar para o aplicativo). Para usar esses parâmetros, clique em Inserir e selecione o parâmetro ou parâmetros que você deseja usar. Ao fornecer a propriedade do objeto como um parâmetro, verifique se o administrador assistente tem a permissão de Leitura necessária na propriedade do objeto, juntamente com o poder *Executar Ferramentas Personalizadas* para executar a ferramenta personalizada.

Exemplos:

- *Exemplo 1:* Para passar o nome do grupo e o nome do domínio como parâmetros para um aplicativo externo ou script, selecione os parâmetros Object Property Name (Nome da Propriedade do Objeto) e Domain Property Name (Nome da Propriedade do Domínio) e especifique os nomes dos parâmetros no campo Parameters to pass to the application (Parâmetros a serem passados para o aplicativo): `"{Object.Name}" "{Domain.$McsName}"`
- *Exemplo 2:* Para passar o parâmetro de entrada “ipconfig” para o aplicativo “C:\Windows\SysWOW64\cmd.exe”, basta digitar `"{C:\Windows\SysWOW64\cmd.exe}" "{ipconfig}"` nesse campo.

Directory where the application will run (Diretório em que o aplicativo será executado): Este é o local em que o aplicativo precisa ser executado na máquina cliente ou servidor. Você precisa passar o caminho no qual o aplicativo deve ser executado. Você também pode usar a opção “Inserir” da mesma maneira que passamos o parâmetro para o campo "Location of the application" (“Localização do aplicativo”). Outros parâmetros nesta guia são suficientemente explícitos para explicar seu uso.

Personalizando a interface do usuário

Existem várias opções para personalizar o modo de configuração do Console de Delegação e Configuração. A maioria dessas opções fornece a capacidade de ocultar, mostrar ou reconfigurar recursos nos diferentes painéis de recursos no aplicativo. Você também pode ocultar ou mostrar a barra de ferramentas, personalizar o título do aplicativo e adicionar, remover ou reordenar colunas. Todas essas opções de personalização estão localizadas no menu **Ver**.

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 opções apropriadas e clique em **OK**. Para mais informações, clique no **?**.

Personalizando Colunas da Lista

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

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**.

24 Web Client

No Web Client, você pode personalizar as propriedades do objeto, os formulários do Workflow Automation e a marca da interface do usuário. Quando implementadas corretamente, as personalizações de propriedade e workflow ajudarão a automatizar as tarefas do administrador assistente durante o gerenciamento de objetos e as submissões de workflow automatizado.

Personalizando Páginas de Propriedades

Você pode personalizar os formulários de propriedade do objeto que os seus administradores assistentes usam em suas funções 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 propriedade estão claramente definidos na lista Personalização > Páginas de Propriedades 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 como administrador 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: 
- Criar sub-rotinas personalizadas para propriedades usando scripts, caixas de mensagens ou consultas (LDAP, DRA ou REST)

  Para obter mais informações sobre o uso de sub-rotinas personalizadas, consulte Adicionando manipuladores personalizados.

Definindo filtros personalizados

Você pode usar filtros para personalizar as informações exibidas para cada tipo de objeto adicionando o campo **Browser de objeto gerenciado** a uma página de propriedades. Ao definir as configurações do campo, você pode adicionar filtros a elas usando a guia Opções do Browser de objeto gerenciado. Ao definir filtros personalizados, você pode restringir as informações mostradas em browsers de objeto para administradores assistentes. Os administradores assistentes poderão ver apenas os objetos que atendam às condições do filtro que você definiu.

Para definir um filtro, na guia Opções do Browser de objeto gerenciado, habilite a caixa de seleção **Especificar filtros de objeto**. Para cada condição do filtro, especifique o tipo de objeto, o atributo a ser filtrado, a condição do filtro e o valor de atributo que será usado para filtrar as informações. Quando você cria vários filtros para o mesmo tipo de objeto, eles são combinados com o operador AND. Com todos os filtros predefinidos no browser de objeto gerenciado, os administradores assistentes podem executar a operação de pesquisa.

Observação

- Apenas atributos em cache podem ser usados para definir filtros.
- Se você criar uma sub-rotina personalizada usando um script personalizado para o filtro personalizado, deverá definir também o filtro personalizado manualmente na guia **Opção do Browser de Objeto Gerenciado** para que a sub-rotina personalizada funcione.

Criando uma nova página de propriedades do objeto

Para criar uma nova página de propriedades do objeto:

1 Efetue login no console da Web como administrador do DRA.

2 Navegue até **Administração** > **Personalização** > **Páginas de Propriedade**.

3 Clique em + **Criar**.

4 Crie o formulário inicial de propriedades do objeto definindo nome da ação, ícone, tipo de objeto e configuração de operação.

   As ações de criação 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.

5 Personalize o novo formulário conforme necessário. Consulte Personalizando uma página de propriedades do objeto.

Personalizando Formulários de Solicitação

Os formulários de solicitação, quando criados ou modificados, são gravados no Servidor Web. O administrador do DRA os gerencia por meio de **Administração** > **Personalização** > **Solicitações**. Administradores assistentes os gerenciam por meio de **Tarefas** > **Solicitações**. Esses formulários são usados para enviar workflows automatizados criados no servidor do Workflow Automation. Os criadores de formulários usam essas solicitações para automatizar e aprimorar ainda mais as tarefas de gerenciamento de objetos.

Você pode adicionar e modificar propriedades de formulário e sub-rotinas personalizadas existentes. O comportamento da interface para adicionar e personalizar propriedades geralmente é o mesmo em um formulário do Workflow Automation e na personalização de propriedades de objetos, com exceção das opções de configuração e dos controles de workflow para quem pode usar o formulário. Faça referência aos tópicos abaixo para obter mais informações sobre como adicionar e modificar propriedades, adicionar manipuladores personalizados e entender o Workflow Automation.

- Personalizando Páginas de Propriedades (Web Client)
- Adicionando manipuladores personalizados
- Workflow automatizado

Adicionando manipuladores personalizados

Os manipuladores personalizados são usados no DRA para que os atributos de propriedade interajam entre si para realizar uma tarefa de workflow e para Carregar e Enviar personalizações em um workflow, propriedade ou formulário de criação.

Sub-rotinas personalizadas de propriedades

Alguns exemplos de sub-rotinas personalizadas de propriedades incluem:

- consultar o valor de outros campos
- atualizar valores do campo
- alternar o estado apenas leitura de um campo
- mostrar ou ocultar campos com base em variáveis configuradas

Sub-rotinas de carregamento de página

As sub-rotinas de carregamento de página normalmente executam a inicialização e são usadas principalmente em páginas de propriedade personalizadas. Elas só são executadas na primeira vez que uma página é selecionada e, no caso de páginas de propriedade, são executadas após o carregamento de dados do servidor.

Sub-rotinas de carregamento de formulário

Sub-rotinas de carregamento de formulário normalmente executam controles de inicialização. Elas são executadas apenas uma vez quando o formulário é carregado inicialmente. No caso de páginas de propriedades, elas são executadas antes que o servidor seja consultado quanto às propriedades do objeto selecionado.

Sub-rotinas de envio de formulário

As sub-rotinas de envio de formulário permitirão que os usuários façam algum tipo de validação e cancelem a submissão de formulários caso algo não esteja certo.

Observação: Como uma melhor prática, evite configurar sub-rotinas de mudança na página e sub-rotinas de formulários que modificam os valores dos campos que estão em páginas diferentes (guias) daquela em que você criou a sub-rotina. Neste cenário, os dados em uma página diferente daquela da sub-rotina não serão carregados até que o administrador assistente acesse essa página, o que pode causar conflito com o valor definido pela sub-rotina de mudança.

Para obter exemplos detalhados do uso de sub-rotinas personalizadas e personalizações no Console da Web, consulte as seções “Web Console Customization” (Personalização do Console da Web) e “Workflow Customization” (Personalização do workflow) na referência *Product Customization* (Personalização do produto) na Página de documentação do DRA.

Veja os tópicos a seguir para obter mais informações sobre o comportamento da sub-rotina personalizada e como criá-las:

- “Etapas básicas para criar uma sub-rotina personalizada” na página 214
- “Habilitando JavaScript Personalizado” na página 217
- “Usando o editor de script” na página 217
- “Sobre a execução de sub-rotinas personalizadas” na página 218

Etapas básicas para criar uma sub-rotina personalizada

Antes de tentar criar uma sub-rotina personalizada, verifique se o JavaScript personalizado está habilitado na configuração do console. Para obter mais informações, veja Habilitando JavaScript Personalizado.

As etapas abaixo começam em uma página da sub-rotina personalizada pré-selecionada. Para chegar a esse ponto, você navega para diferentes sub-rotinas da seguinte forma:

- Sub-rotinas personalizadas de propriedades do objeto: Clique no ícone de edição em um campo de propriedade.

- Sub-rotinas de carregamento de página: Selecione as propriedades da página. Por exemplo, **Geral** > ▪▪▪ **Mais opções** > **Propriedades**.
- Sub-rotinas de Carregamento de Formulário ou Envio de Formulário: Clique no botão **Propriedades do Formulário** em um formulário de workflow selecionado, uma página Criar Objeto ou uma página Editar Propriedades.

Criando uma sub-rotina personalizada:

1. Selecione a guia da sub-rotina aplicável com base na propriedade ou na página que você está personalizando:
   - Sub-rotinas personalizadas
   - Sub-rotinas de carregamento de página
   - Manipuladores de carga de formulários
   - Manipuladores de envio de formulários
2. Habilite a página da sub-rotina  e siga um destes procedimentos:
   - **Sub-rotina personalizada do campo de propriedade:**
     1. Selecione um tempo de execução. Normalmente, você usaria a segunda opção.

        O tempo de execução controla quando as sub-rotinas de mudança são executadas em resposta à entrada do usuário. Observe que esta configuração não se aplica quando o valor do campo é atualizado por outra sub-rotina personalizada usando a interface draApi.fieldValues.
     2. Clique em **+ Adicionar** e escolha uma sub-rotina personalizada do menu **Adicionar Sub-rotina Personalizada**.
   - **Sub-rotina de formulário ou página:** Clique em **+ Adicionar** e escolha uma sub-rotina personalizada no menu **Adicionar Sub-rotina Personalizada**.

   Observação: Normalmente, você precisa de apenas uma sub-rotina personalizada, mas pode usar mais de uma. Várias sub-rotinas são executadas sequencialmente na ordem listada. Se você deseja mudar a ordem das sub-rotinas ou ignorar uma sub-rotina desnecessária, adicione APIs de controle de fluxo ao script.

   ---

3. Você precisará configurar cada sub-rotina personalizada que adicionar à página. As opções de configuração variam de acordo com o tipo de sub-rotina. O editor de scripts tem Ajuda incorporada e assistência dinâmica de conclusão de código Intellisense, que também faz referência a snippets da Ajuda. Para obter mais informações sobre como usar esses recursos, consulte Usando o editor de script.

   Você pode criar seus próprios tipos de sub-rotinas.

   - **Sub-rotinas de consulta LDAP ou REST:**
     1. Se desejar que sua consulta seja baseada em valores estáticos, defina as **Informações de Conexão** e os **Parâmetros de Consulta**.

        Observação: Para consultas LDAP, você pode exigir um tipo de autenticação específico nas configurações de informações de conexão:

        - **Conta Padrão:** Autentica com um login do Servidor DRA.

- **Conta de Anulação do Domínio Gerenciado:** Autentica no Active Directory por meio da conta de anulação do domínio gerenciado existente.
- **Conta de Anulação de LDAP:** Autentica por meio de uma conta de anulação de LDAP, em oposição a uma conta de domínio de um domínio gerenciado. Para usar esta opção, a conta deve primeiro ser habilitada no Console de Delegação e Configuração. Para obter mais informações, veja Habilitar a autenticação de anulação de LDAP.

Se desejar que sua consulta seja dinâmica, digite os valores do marcador de espaço nos campos obrigatórios. Isso é necessário para que a sub-rotina seja executada. O script anulará os valores do marcador de espaço.

Observação: Você também pode configurar Cabeçalhos e Cookies para a Consulta REST.

---

2. Em Ação de Pré-consulta, use o editor de scripts para escrever o código JavaScript personalizado que será executado antes da submissão da consulta. Este script tem acesso a todas as informações de conexão e parâmetros de consulta e pode modificar qualquer um deles para personalizar a consulta. Por exemplo, definindo parâmetros de consulta com base nos valores que o usuário inseriu no formulário.
3. Na Ação Pós-consulta, inclua script para processar os resultados da consulta. As tarefas comuns incluem verificação de erros, atualização dos valores do formulário com base nos resultados retornados e validação da exclusividade do objeto com base no número de objetos retornados pela consulta.

- **Script:** Insira o código JavaScript personalizado para criar o script.
- **Consulta do DRA:** Especifique o payload JSON na guia Parâmetros de Consulta. O formato do payload deve corresponder à chave VarSet ou aos pares de valores que serão enviados ao servidor do DRA. De modo semelhante às consultas REST e LDAP, você pode especificar uma Ação de Pré-consulta que pode ser usada para modificar o payload antes de ser submetida ao servidor e uma Ação Pós-consulta para processar os resultados.
- **Sub-rotinas da Caixa de Mensagem:** Depois de definir as propriedades da própria caixa de mensagem, você também pode gravar os segmentos de JavaScript para **Ação Antes de Mostrar** e **Ação Após o Fechamento**.

  Essas ações são opcionais. A ação Antes de Mostrar é usada para personalizar qualquer uma das propriedades da caixa de mensagem antes de ser mostrada ao usuário e a ação Após o Fechamento é usada para processar a seleção de botões do usuário e executar qualquer lógica adicional baseada nela.

4 Clique em **OK** para gravar a sub-rotina.

Para obter exemplos detalhados do uso de sub-rotinas personalizadas e personalizações no Console da Web, consulte as seções “Web Console Customization” (Personalização do Console da Web) e “Workflow Customization” (Personalização do workflow) na referência *Product Customization* (Personalização do produto) na Página de documentação do DRA

Habilitando JavaScript Personalizado

Por motivos de segurança, o JavaScript personalizado está desabilitado por padrão. Habilitar o JavaScript personalizado permite que os administradores escrevam snippets de código JavaScript que serão executados pelo console da Web no estado em que se encontram. Você só deverá habilitar essa exceção se entender e aceitar os riscos.

Para habilitar personalizações para incluir código JavaScript personalizado:

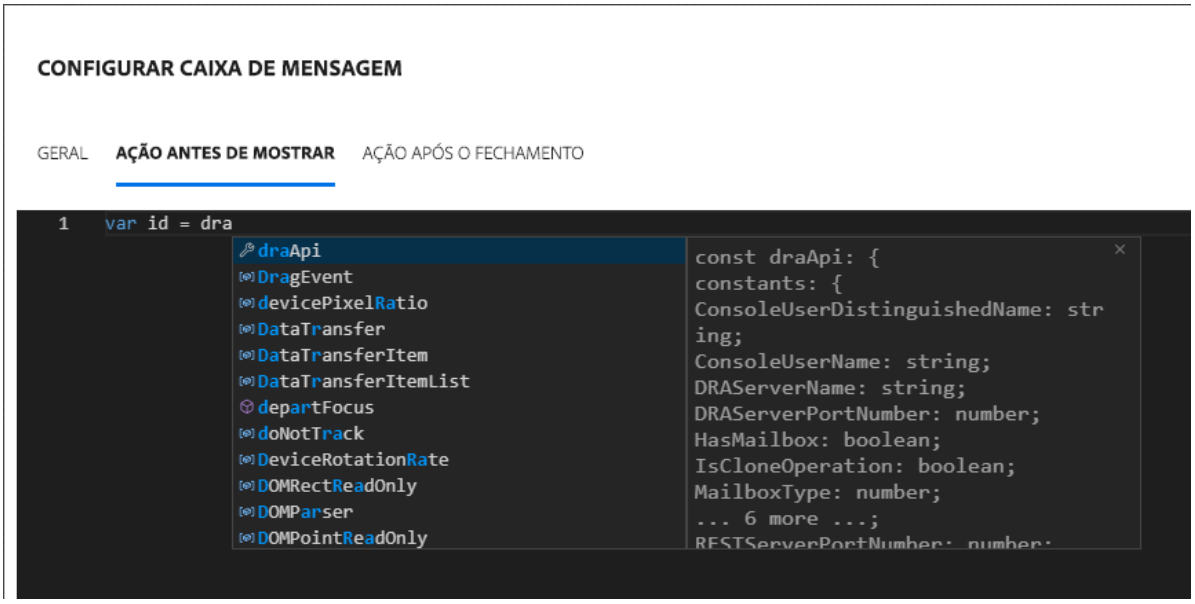
1. Navegue até o local `C:\ProgramData\NetIQ\DRARESTProxy`.
2. Abra o arquivo `restProxy.config`.
3. Adicione `allowCustomJavaScript="true"` ao elemento `<consoleConfiguration>`.

Usando o editor de script

O editor de script permite digitação livre e colagem de métodos JavaScript usando APIs do DRA para criar sub-rotinas personalizadas no DRA. O editor inclui a conclusão dinâmica do código Intellisense e um painel suspenso de Ajuda para ajudá-lo na hora de escrever o script.

Conclusão do Código Intellisense

O Intellisense no editor de script fornece snippets selecionáveis de conclusão de código, preenchimento de guias e painéis suspensos de resumos de API com descrições das APIs.



Observação: A conclusão do código Intellisense é dinâmica. Isso significa que ele pode fornecer-lhe opções de sintaxe com base no tipo de sub-rotina para a qual você está definindo o script, mas também armazena strings anteriormente inseridas pelo usuário e fornece a elas prompts também.

Ajuda do editor de scripts

Quando você clica na opção AJUDA no editor de scripts, abre-se um painel que explica o propósito geral das APIs personalizadas da sub-rotina, onde elas são usadas e também lista as APIs com descrições de suas funções pelo tipo de API:

- As APIs globais incluem:
  - Acesso ao formulário
  - Controle de fluxo
  - Constantes
- As APIs da caixa de mensagem incluem:
  - Ação antes de mostrar
  - Ação após o fechamento
- As APIs de consulta incluem:
  - Resultados da consulta
  - Consulta do DRA
  - Consulta de LDAP
  - Consulta de REST

Sobre a execução de sub-rotinas personalizadas

O DRA fornece a capacidade de personalizar o comportamento do formulário web em vários pontos do ciclo de vida de execução dos formulários por meio de sub-rotinas personalizadas. Cada tipo de sub-rotina personalizada tem uma janela de execução específica que, por sua vez, afeta o escopo dos dados do objeto disponíveis durante a execução da personalização, da seguinte forma:

1. *Sub-rotinas de carregamento de formulário*. Executadas quando o formulário é carregado antes da coleta de atributos do objeto ao qual o formulário está conectado. Essas sub-rotinas não têm acesso a valores de atributos para o objeto de destino.
2. *Sub-rotinas de carregamento de página*. O DRA executa sub-rotinas de carregamento de página na primeira vez que uma página de um formulário é acessada. Essas sub-rotinas têm acesso garantido aos valores de atributos do objeto de destino que estão contidos nessa página.
3. *Sub-rotinas de atributos*. O DRA executa sub-rotinas de atributos quando um valor de atributo no formulário é acessado. Além disso, cada atributo de formulário pode ser configurado para executar suas sub-rotinas personalizadas em um de três pontos específicos durante a interação dos usuários: (1) imediatamente (quando o atributo ganha foco), (2) quando o atributo perde o foco ou (3) uma quantidade especificada de tempo após o atributo perder o foco.
4. *Sub-rotinas de envio de formulário*. As sub-rotinas de envio de formulários são executadas quando o formulário é gravado ou mudanças são aplicadas a ele.

Personalizando a marca da interface do usuário

Você pode personalizar a barra de título do Console da Web do DRA com seu próprio título e imagem do logo. O posicionamento é diretamente à direita do nome do produto DRA. Como esse local também é usado para navegação de nível superior, ele é oculto pelos links de navegação do DRA de nível superior após o login. No entanto, a guia do browser continua exibindo o título personalizado.

Para personalizar a marca do Console da Web do DRA:

1. Efetue login no Console da Web como administrador do DRA.
2. Navegue até **Administração** > **Configuração** > **Marca**.
3. Se você está adicionando uma imagem do logo da empresa, grave a imagem do logo no Servidor Web em `inetpub\wwwroot\DRAClient\assets`.
4. Atualize a configuração, conforme aplicável, para os blocos Cabeçalho e Login.

   Se você quiser adicionar um aviso para administradores assistentes no login, ative o botão **Mostrar um modal de notificação ao efetuar login**. Atualize a configuração para essa notificação e clique em **VISUALIZAR** para ver como será essa notificação no login.
5. Quando todas as mudanças estiverem concluídas, clique em **Gravar**.

IX Ferramentas e Utilitários

Estas seções trazem informações sobre o Utilitário Analisador da Tela Ativa, o Utilitário de Diagnóstico, o Utilitário de Objeto Apagado, o Utilitário de Verificação de Saúde e o Utilitário de Lixeira fornecidos com o DRA.

25 Utilitário Analisador da Tela Ativa

Cada Tela Ativa do DRA contém uma ou mais regras que se aplicam aos objetos do Active Directory (AD) gerenciados por um conjunto multimaster do DRA. O Utilitário Analisador da Tela Ativa é usado para monitorar o tempo de processamento de cada regra da Tela Ativa do DRA, aplicada a objetos do AD em uma operação específica do DRA. Durante uma operação do DRA, o servidor do DRA compara os objetos de destino dessa operação com todas as regras em todas as Telas Ativas. O DRA cria uma lista de resultados contendo todas as regras correspondentes. O Analisador da Tela Ativa calcula quanto tempo foi usado no processamento de cada regra aplicada a uma operação do DRA.

Com essas informações, você pode diagnosticar problemas da Tela Ativa verificando anomalias no tempo de processamento da Tela Ativa, incluindo o tempo usado no processamento de Telas Ativas não utilizadas. O utilitário também simplifica a localização de Telas Ativas duplicadas.

Após executar uma coleta de dados e visualizar um relatório, você pode achar necessário modificar as regras de uma ou mais Telas Ativas.

Você pode acessar o Utilitário Analisador da Tela Ativa de qualquer Servidor de administração DRA. No entanto, você deve executar o Utilitário da Tela Ativa no servidor de Administração no qual você está enfrentando o problema.

Para acessar o Utilitário Analisador da Tela Ativa, efetue logon no servidor de Administração com privilégios de função de Administração do DRA e navegue até **Administração da NetIQ** > **Utilitário Analisador da Tela Ativa** no menu Iniciar. Você também pode iniciar o `ActiveViewAnalyzer.exe` do caminho instalado pelo DRA `Arquivos de Programas (x86)\NetIQ\DRA\X64`.

Use este utilitário para executar o seguinte:

- Coletar dados nas Telas Ativas
- Gerar um relatório do analisador

Exemplo

Paul, Administrador Assistente, avisa a Bob, administrador do DRA, que a criação de usuários parece estar demorando mais que o normal. Bob decide iniciar o analisador da Tela Ativa no objeto usuário de Paul e, então, pede que Paul crie um usuário. Após a coleta, Bob gera um relatório de análise e nota que uma regra chamada Compartilhar MBX leva 50 ms para enumerar. Bob identifica a Tela Ativa que contém a regra e, após mudar a regra, observa que o problema foi resolvido.

Iniciando uma coleta de dados da Tela Ativa

Com o Utilitário Analisador da Tela Ativa, você pode coletar dados nas Telas Ativas de ações executadas nelas por administradores assistentes. Esses dados podem ser vistos em um relatório do Analisador. Para coletar os dados, você precisa especificar o administrador assistente para coletar dados e, em seguida, iniciar uma coleta da Tela Ativa.

Observação: O administrador assistente no qual você deseja coletar dados deve estar conectado ao mesmo servidor DRA em que o Analisador está sendo executado.

Para iniciar uma coleta da Tela Ativa:

1. Clique em **Iniciar** > **Administração da NetIQ** > **Utilitário Analisador da Tela Ativa**.
2. Na página do Analisador da Tela Ativa, especifique o seguinte:
   - 2a **Servidor do DRA de Destino:** O servidor do DRA que coleta dados de desempenho nas operações do Admin Assistente.
   - 2b **Administrador Assistente de Destino:** Clique em Procurar e selecione um administrador assistente sobre o qual você deseja coletar dados.
   - 2c **Monitorando a Duração:** Especifique o número total de horas necessárias para coletar dados do analisador. Após exceder o tempo especificado, a coleta de dados será interrompida.
3. Clique em **Iniciar Coleta** para coletar dados da Tela Ativa.

   Depois de iniciar a coleta de dados da Tela Ativa, o utilitário limpa os dados existentes e exibe o status mais recente.
4. (Opcional) Você pode parar a coleta de dados manualmente antes que a duração agendada tenha terminado e ainda gerar um relatório. Clique em **Parar Coleta** para interromper a gravação de operações do Admin Assistente nas Telas Ativas.
5. (Opcional) Para obter o status mais recente, clique em **Status da Coleta**.

Importante: Se você parar a coleta e mudar o administrador assistente ou reiniciar uma coleta de dados para o mesmo administrador assistente, o Analisador da Tela Ativa limpará os dados existentes. Você só pode ter dados do Analisador para um administrador assistente no banco de dados por vez.

Gerando um Relatório do Analisador

Antes de gerar um relatório do analisador, pare de coletar dados.

Na página do Analisador da Tela Ativa é mostrada a lista de operações executadas pelo assistente administrador. Para gerar um relatório do analisador:

1. Clique em **Selecionar Relatório** e escolha o relatório que você deseja ver.
2. Clique em **Gerar Relatório** para gerar um relatório de análise com os detalhes da operação da Tela Ativa, como objetos do AD afetados pela operação, o gerenciamento dos objetos listados, com e sem correspondência, pela Tela Ativa e a duração para processar cada regra individual da Tela Ativa.

   Ao utilizar o relatório, você pode analisar quais regras levam mais tempo para executar operações e, então, decidir se alguma delas deve ser modificada ou apagada de suas respectivas Telas Ativas.
3. (Opcional) Passe o mouse sobre a grade, clique o botão direito do mouse e use o menu copiar para copiar o relatório para uma área de transferência. Na área de transferência, os cabeçalhos e os dados das colunas podem ser colados em outro aplicativo, como o Bloco de Notas ou o Excel.

Identificando o Desempenho dos Objetos

Para identificar o desempenho de todos os objetos gerenciados por uma Tela Ativa ou uma regra:

1. Inicie o Console de Delegação e Configuração.
2. Acesse **Gerenciamento de Delegação** e clique em **Gerenciar Telas Ativas**.
3. Execute uma pesquisa para localizar uma Tela Ativa específica.

   Daqui em diante, você pode encontrar a regra ou o objeto com problema e fazer modificações.

   - Clique duas vezes na Tela Ativa e selecione **Regras** para listar as regras. Você pode modificar uma regra específica do menu de clique com o botão direito do mouse.
   - Clique o botão direito do mouse na Tela Ativa e selecione **Mostrar Objetos Gerenciados** para listar os objetos. Você pode modificar um objeto com o botão direito do mouse > **Propriedades**.
4. Faça mudanças na regra ou no objeto gerenciado e verifique se essas mudanças resolvem o problema.

26 Utilitário de diagnóstico

O Utilitário de Diagnóstico reúne informações de seu servidor de Administração para ajudar a diagnosticar problemas com o DRA. Use este utilitário para fornecer arquivos de registro ao seu representante de suporte técnico. O Utilitário de Diagnóstico fornece uma interface de assistente que o orienta na configuração de níveis de registro e na coleta de informações de diagnóstico.

Você pode acessar o utilitário de diagnóstico em qualquer computador do servidor de administração. No entanto, você deve executar o utilitário de diagnóstico no servidor de administração no qual você está enfrentando o problema.

Para acessar o Utilitário de Diagnóstico, efetue logon no computador do servidor de Administração usando uma conta de administrador que tenha direitos de administrador local e abra o utilitário no grupo de programas Administração da NetIQ no menu Iniciar do Windows.

Para obter mais informações sobre como usar esse utilitário, entre em contato com o suporte técnico.

27 Utilitário de objetos apagados

Esse utilitário permite que você ative o suporte à atualização de cache de contas incrementais para um domínio específico quando a conta de acesso ao domínio não é um administrador. Se a conta de acesso ao domínio não tiver permissões de leitura no container Objetos Apagados no domínio, o DRA não poderá executar uma atualização do cache de contas incrementais.

Você pode usar esse utilitário para executar as seguintes tarefas:

- Verifique se a conta do usuário ou grupo especificado tem permissões de leitura no container Objetos Apagados no domínio especificado
- Delegar ou remover permissões de leitura para uma conta do usuário ou grupo especificado
- Delegar ou remover o direito de usuário Sincronizar dados do serviço de diretório para uma conta do usuário
- Exibir configurações de segurança para o container Objetos Apagados

Você pode executar o arquivo do Utilitário de Objetos Apagados (`DraDelObjsUtil.exe`) na pasta `Arquivos de Programa (x86)\NetIQ\DRA` no seu Servidor de Administração.

Permissões necessárias para o utilitário de objetos apagados

Para usar este utilitário, você deve ter as seguintes permissões:

Se você deseja...	**Você precisa desta permissão...**
Verificar as permissões da conta	Acesso com Permissões de Leitura ao container Objetos Apagados
Delegar permissões de leitura no container Objetos Apagados	Permissões de administrador no domínio em que o container Objetos Apagados está localizado
Delegar o direito de usuário Sincronizar dados do serviço de diretório	Permissões de administrador no domínio em que o container Objetos Apagados está localizado
Remover permissões anteriormente delegadas	Permissões de administrador no domínio em que o container Objetos Apagados está localizado
Exibir configurações de segurança para o container Objetos Apagados	Acesso com Permissões de Leitura ao container Objetos Apagados

Sintaxe para o utilitário de objetos apagados

```
DRADELOBJSUTIL /DOMAIN:DOMAINNAME [/DC:COMPUTERNAME] {/
DELEGATE:ACCOUNTNAME | /VERIFY:ACCOUNTNAME | /REMOVE:ACCOUNTNAME | /
DISPLAY [/RIGHT]}
```

Opções para o utilitário de objetos apagados

Você pode especificar as seguintes opções:

/DOMAIN:*domain*	Especifica o nome NETBIOS ou DNS do domínio em que o container Objetos Apagados está localizado.
/SERVER:*computername*	Especifica o nome ou endereço IP do controlador de domínio para o domínio especificado.
/DELEGATE:*accountname*	Delega permissões para a conta do usuário ou grupo especificado.
/REMOVE:*accountname*	Remove as permissões anteriormente delegadas à conta do usuário ou grupo especificado
/VERIFY:*accountname*	Verifica as permissões do grupo ou da conta do usuário especificado.
/DISPLAY	Exibe as configurações de segurança para o container Objetos Apagados no domínio especificado
/RIGHT	Garante que a conta do usuário ou grupo especificado tenha o direito de usuário Sincronizar dados do serviço de diretório. Você pode usar essa opção para delegar ou verificar esse direito. O direito de usuário Sincronizar dados do serviço de diretório permite que a conta leia todos os objetos e propriedades no Active Directory.

Observação

- Se o nome do grupo ou conta do usuário que você deseja especificar contiver um espaço, coloque o nome da conta entre aspas. Por exemplo, se você quiser especificar o grupo de TI Houston, digite “Houston IT”.
- Ao especificar um grupo, use o nome anterior ao Windows 2000 para esse grupo.

Exemplos para o utilitário de objetos apagados

Os exemplos a seguir demonstram comandos de amostra para cenários comuns.

Exemplo 1

Para verificar se a conta do usuário `MYCOMPANY\JSmith` tem permissões de leitura no container Objetos Apagados no domínio `hou.mycompany.com`, digite:

```
DRADELOBJSUTIL /DOMAIN:HOU.MYCOMPANY.COM /VERIFY:MYCOMPANY\JSMITH
```

Exemplo 2

Para delegar permissões de leitura no container Objetos Apagados no domínio `MYCOMPANY` para o grupo `MYCOMPANY\DraAdmins`, digite:

```
DRADELOBJSUTIL /DOMAIN:MYCOMPANY /DELEGATE:MYCOMPANY\DRAADMINS
```

Exemplo 3

Para delegar permissões de leitura no container Objetos apagados e no direito de usuário Sincronizar dados do serviço de diretório no domínio MYCOMPANY para a conta do usuário MYCOMPANY\JSmith, digite:

```
DRADELOBJSUTIL /DOMAIN:MYCOMPANY /DELEGATE:MYCOMPANY\JSMITH /RIGHT
```

Exemplo 4

Para exibir as configurações de segurança do container Objetos apagados no domínio hou.mycompany.com usando o controlador de domínio HQDC, digite:

```
DRADELOBJSUTIL /DOMAIN:HOU.MYCOMPANY.COM /DC:HQDC /DISPLAY
```

Exemplo 5

Para remover permissões de leitura no container Objetos Apagados no domínioMYCOMPANY do grupo MYCOMPANY\DraAdmins, digite:

```
DRADELOBJSUTIL /DOMAIN:MYCOMPANY /REMOVE:MYCOMPANY\DRAADMINS
```

28 Utilitário de verificação de integridade

O Utilitário de verificação de integridade do DRA é um aplicativo independente fornecido com o kit de instalação do DRA. Você usa a instalação pós-atualização do Utilitário Verificação de Integridade e pré e pós-upgrade para verificar, validar e informar o status de componentes e processos para o Servidor DRA, o Site na Web do DRA e os Clientes DRA. Você também pode usá-lo para instalar ou atualizar uma licença de produto, fazer backup da Instância do AD LDS antes de um upgrade de produto, exibir descrições das verificações e corrigir problemas ou identificar ações que precisam ser tomadas para corrigir problemas e revalidá-los.

O Utilitário de verificação de integridade está acessível na pasta do programa DRA após executar o instalador`NetIQAdminInstallationKit.msi`.

Você pode executar o Utilitário de verificação de integridade a qualquer momento, executando o arquivo `NetIQ.DRA.HealthCheckUI.exe`. Quando o aplicativo é aberto, você pode optar por fazer uma operação específica, executar verificações em componentes específicos ou executar verificações em todos os componentes. Veja abaixo as funções úteis que você executa usando o Utilitário de Verificação de Integridade:

Função	Ações do usuário
Selecionar tudo ou desmarcar tudo	Use a barra de ferramentas ou as opções do menu Arquivo para **Selecionar** ou **Desmarcar** todos os itens de seleção ou marque as caixas de seleção individuais para executar verificações específicas.
Executar verificações selecionadas	Use esta barra de ferramentas ou a opção de menu Arquivo para executar as verificações selecionadas (todas ou específicas).
Gravar resultados	Use esta barra de ferramentas ou a opção de menu Arquivo para criar e gravar um relatório detalhado para a verificação que é executada.
Executar esta verificação	Selecione um título de item para ver uma descrição da verificação e clique no ícone da barra de ferramentas para executar a verificação. Por exemplo, para executar uma das seguintes operações: ◆ Validação de Licença (Instalar ou atualizar uma licença do produto) ◆ Backup da Instância do AD LDS (Fazer backup da instância do AD LDS) ◆ Replicação (Validar o banco de dados de Replicação)
Corrigir esta questão	Selecione um título de item e use essa opção da barra de ferramentas quando a verificação falhar. Se a execução da verificação novamente não corrigir o problema, a descrição deverá incluir informações ou ações que você possa tomar para resolver o problema.

29 Utilitário Recycle Bin

Esse utilitário permite que você ative o suporte da Lixeira quando estiver gerenciando uma subárvore de um domínio. Se a conta de acesso ao domínio não tiver permissões no container NetIQRecycleBin oculto no domínio especificado, o DRA não poderá mover as contas apagadas para a Lixeira.

Observação: Após usar esse utilitário para habilitar a Lixeira, execute uma atualização completa do cache das contas para garantir que o servidor de Administração aplique essa mudança.

Você pode usar esse utilitário para executar as seguintes tarefas:

- Verificar se a conta especificada tem permissões de leitura no container NetIQRecycleBin no domínio especificado
- Delegar permissões de leitura a uma conta especificada
- Exibir configurações de segurança para o container NetIQRecycleBin

Permissões necessárias para o utilitário Recycle Bin

Para usar este utilitário, você deve ter as seguintes permissões:

Se você deseja...	Você precisa desta permissão...
Verificar as permissões da conta	Acesso com Permissões de Leitura ao container NetIQRecycleBin
Delegar permissões de leitura no container NetIQRecycleBin	Permissões de administrador no domínio especificado
Exibir configurações de segurança para o container NetIQRecycleBin	Acesso com Permissões de Leitura ao container NetIQRecycleBin

Sintaxe para o utilitário Recycle Bin

```
DRARECYCLEBINUTIL /DOMAIN:DOMAINNAME [/DC:COMPUTERNAME] {/
DELEGATE:ACCOUNTNAME | /VERIFY:ACCOUNTNAME | /DISPLAY}
```

Opções para o utilitário Recycle Bin

As opções a seguir permitem configurar o Utilitário Recycle Bin:

/DOMAIN:domain — Especifica o nome NETBIOS ou DNS do domínio em que a Lixeira está localizada.

/SERVER:*computername*	Especifica o nome ou endereço IP do controlador de domínio para o domínio especificado.
/DELEGATE:*accountname*	Delega as permissões para a conta especificada.
/VERIFY:*accountname*	Verifica as permissões da conta especificada.
/DISPLAY	Exibe as configurações de segurança para o container NetIQRecycleBin no domínio especificado.

Exemplos para o utilitário Recycle Bin

Os exemplos a seguir demonstram comandos de amostra para cenários comuns.

Exemplo 1

Para verificar se a conta do usuário `MYCOMPANY\JSmith` tem permissões de leitura no container NetIQRecycleBin no domínio `hou.mycompany.com`, digite:

```
DRARECYCLEBINUTIL /DOMAIN:HOU.MYCOMPANY.COM /VERIFY:MYCOMPANY\JSMITH
```

Exemplo 2

Para delegar permissões de leitura no container NetIQRecycleBin no domínio `MYCOMPANY` para o grupo `MYCOMPANY\DraAdmins`, digite:

```
DRARECYCLEBINUTIL /DOMAIN:MYCOMPANY /DELEGATE:MYCOMPANY\DRAADMINS
```

Exemplo 3

Para exibir as configurações de segurança do container NetIQRecycleBin no domínio `hou.mycompany.com` usando o controlador de domínio `HQDC`, digite:

```
DRARECYCLEBINUTIL /DOMAIN:HOU.MYCOMPANY.COM /DC:HQDC /DISPLAY
```

A Apêndice

Este apêndice fornece informações sobre os Serviços do DRA e como solucionar problemas com o Serviço REST do DRA.

Serviços do DRA

Esta tabela fornece informações sobre os serviços do DRA. Isso ajuda os administradores do DRA a decidir se podem desabilitar um serviço com segurança sem afetar nenhuma funcionalidade do DRA.

Serviço do DRA	Descrição	Seguro para desabilitar
Serviço de Administração da NetIQ	Este serviço realiza todas as operações do DRA e gerencia os processos internos do servidor DRA.	Não
Serviço de Auditoria do DRA da NetIQ	Este serviço lida com as solicitações de Histórico de Mudanças Unificado do Console da Web. Quando você desabilitar este serviço: ◆ A funcionalidade do DRA não será afetada. ◆ Você poderá gerar relatórios de Histórico de Mudanças Unificado do Console de Delegação e Configuração. ◆ Você não poderá gerar relatórios de Histórico de Mudanças Unificado do Console da Web.	Sim
Serviço de BD de Cache do DRA da NetIQ	Este serviço gerencia o banco de dados de cache do DRA da NetIQ.	Não
Serviço de Cache do DRA da NetIQ	Este serviço funciona como um cache persistente para o Servidor de Administração da NetIQ.	Não
Serviço de Núcleo do DRA da NetIQ	Este serviço gera relatórios para consoles do DRA e programa as tarefas do Active Directory, Office365, DRA e Resource Collector. Quando você desabilitar este serviço: ◆ A funcionalidade do DRA não será afetada. ◆ As tarefas do coletor não serão executadas para que os dados dos relatórios do NRC não sejam coletados. ◆ Você não poderá gerar relatórios de Histórico de Mudanças Unificado de nenhum console do DRA.	Sim

Serviço do DRA	Descrição	Seguro para desabilitar
Arquivo de Registro do DRA da NetIQ	Este serviço armazena todos os eventos de auditoria do DRA de modo seguro para suportar relatórios de auditoria.	Não
Serviço de Replicação do DRA da NetIQ	Este serviço suporta o recurso TGA (Temporary Group Assignment, designação temporária de grupo) do DRA. As TGAs não estarão disponíveis em nenhum servidor DRA do qual este serviço for removido ou interrompido.	Sim
Serviço REST do DRA da NetIQ	Os clientes do Console da Web e do PowerShell usam este serviço para se comunicar com o Servidor de Administração da NetIQ.	Não
Armazenamento Seguro do DRA da NetIQ	Este serviço gerencia a instância do AD LDS do DRA que armazena a configuração do DRA. Ele também replica esses dados de configuração em toda a configuração do MMS.	Não
Serviço Skype do DRA da NetIQ	Este serviço gerencia todas as tarefas do Skype. Quando você desabilitar este serviço: ◆ A funcionalidade do DRA não será afetada. ◆ As operações do Skype não serão processadas.	Sim

Solução de problemas dos Serviços de REST do DRA

Esta seção contém informações de solução de problemas para os seguintes tópicos:

Lidando com certificados para as extensões REST do DRA

O serviço de endpoint do DRA requer uma vinculação de certificado na porta de comunicação. Durante a instalação, o instalador executará os comandos para vincular a porta ao certificado. O objetivo desta seção é descrever como validar a vinculação e como adicionar ou remover uma vinculação, se necessário.

Informações Básicas

Porta de serviço de endpoint padrão: 8755

ID do aplicativo para extensões REST do DRA: 8031ba52-3c9d-4193-800a-d620b3e98508

Hash do Certificado: Mostrado na página de Certificados SSL do Gerenciador do IIS

Verificando se há vinculações existentes

Em uma janela CMD, execute este comando: `netsh http show sslcert`

Isso exibirá uma lista de vinculações de certificados para este computador. Veja a lista para o ID do aplicativo das Extensões REST do DRA. O número da porta deve corresponder à porta de configuração. O hash do certificado deve corresponder ao hash de certificado exibido no Gerenciador do IIS.

```
IP:port                 : 0.0.0.0:8755
Certificate Hash        : d095304df3d3c8eecf64c25df7931414c9d8802c
Application ID          : {8031ba52-3c9d-4193-800a-d620b3e98508}
Certificate Store Name  : (null)
Verify Client Certificate Revocation    : Enabled
Verify Revocation Using Cached Client Certificate Only    : Disabled
Usage Check             : Enabled
Revocation Freshness Time : 0
URL Retrieval Timeout   : 0
Ctl Identifier          : (null)
Ctl Store Name          : (null)
DS Mapper Usage         : Disabled
Negotiate Client Certificate    : Disabled
```

Removendo uma vinculação

Para remover uma vinculação existente, digite este comando em uma janela CMD:

```
netsh http delete sslcert ipport=0.0.0.0:9999
```

Em que 9999 é o número da porta a ser removida. O comando `netsh` exibirá uma mensagem indicando que o Certificado SSL foi removido com sucesso.

Adicionando uma vinculação

Para adicionar uma nova vinculação, digite o seguinte comando em uma janela CMD:

```
netsh http add sslcert ipport=0.0.0.0:9999 certhash=[HashValue]
appid={8031ba52-3c9d-4193-800a-d620b3e98508}
```

Em que 9999 = o número de porta do serviço de endpoint e `[HashValue]` = o valor hash do certificado mostrado no Gerenciador do IIS.

Erros de gestão do servidor DRA

Veja o tópico seguir se você receber um erro ao criar um objeto habilitado para e-mail:

Falha na operação de devolução do EnableEmail

Ao criar um objeto habilitado para e-mail ou chamar um dos endpoints do EnableEmail, você pode obter um erro do servidor DRA, como "*Server failed to complete the requested operation workflow successfully. Operation UserEnableEmail failed*" (O servidor não conseguiu concluir com sucesso o

workflow da operação solicitado. Falha no UserEnableEmail da Operação). Isso pode ser causado pela inclusão de uma propriedade `mailNickname` no payload que não está em conformidade com a política definida no servidor.

Remova a propriedade `mailNickname` do payload e deixe que o servidor DRA gere o valor do álias de e-mail de acordo com a política definida.

Todos os resultados do comando PowerShell em erro PSInvalidOperation

Quando o serviço REST do DRA estiver vinculado a um certificado autoassinado, os cmdlets do PowerShell retornarão o seguinte erro:

```
Get-DRAServerInfo: One or more errors occurred.
An error occurred while sending the request.
The underlying connection was closed: Could not establish trust
relationship for the SSL/TLS secure channel.
The remote certificate is invalid according to the validation procedure.
```

Em cada comando, você precisará incluir o parâmetro `-IgnoreCertificateErrors`. Para também suprimir a mensagem de confirmação, adicione o parâmetro `-Force`.

Registro de rastreamento WCF

Caso as suas solicitações REST estejam resultando em erros que não podem ser resolvidos lendo os registros de serviço REST, talvez seja necessário aumentar o nível de registro de rastreamento WCF para ver detalhes sobre como a solicitação está viajando pela camada WCF. O volume de dados gerados por esse nível do rastreamento pode ser significativo, então o nível de registro enviado é definido como “Critical, Error”.

Um exemplo de quando isso pode ser útil é se as solicitações estão resultando em exceções de valor nulo, mesmo que você esteja enviando os objetos no payload. Outro caso seria se o REST não respondesse.

Para aumentar o registro de rastreamento WCF, você precisa editar o arquivo de configuração para o serviço que está sob escrutínio. É provável que as exceções de payload sejam evidentes ao revisar o registro de rastreamento WCF para o Serviço REST.

Etapas para habilitar o registro detalhado

1. No explorador de arquivos do Windows, navegue até a pasta de instalação de extensões do DRA. Normalmente, será `C:\Arquivos de programas (x86)\NetIQ\DRA`.
2. Abra o arquivo `NetIQ.DRA.RestService.exe.config`.
3. Localize o elemento `<source>` no seguinte caminho xml: `<system.diagnostics><sources>`.
4. No elemento de origem, mude o valor do atributo `switchValue` de `"Critical, Error"` para `"Verbose, ActivityTracing"`.
5. Grave o arquivo e reinicie o Serviço REST do DRA da NetIQ.

Falha na operação de devolução do EnableEmail

Os dados de rastreamento WCF são escritos em um formato proprietário. Você pode ler o traces.svslog usando o utilitário SvcTraceViewer.exe. Você pode encontrar mais informações sobre este utilitário aqui: