Informações legais

Índice

Sobre este guia

O *Guia de Instalação* fornece informações sobre planejamento, instalação, licenciamento e configuração para o DRA (Directory and Resource Administrator) e seus componentes integrados.

Este livro orienta você durante o processo de instalação e o ajuda a tomar as decisões corretas para instalar e configurar o DRA.

Público-alvo

Este livro fornece informações para qualquer pessoa que esteja instalando o DRA.

Documentação adicional

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

Informações de contato

Aguardamos seus comentários e suas sugestões sobre este manual e sobre o restante da documentação que acompanha este produto. Você pode usar o link **comente sobre este tópico** na parte inferior de cada página na documentação online ou enviar 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 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 Directory and Resource Administrator fornece administração de identidade privilegiada segura e eficiente do Microsoft Active Directory (AD). O DRA realiza a delegação granular de "privilégios mínimos", de modo que administradores e usuários recebam apenas as permissões necessárias para concluir suas responsabilidades específicas. O DRA também impõe a adesão obrigatória à política, fornece auditoria e gerador de relatórios de atividades detalhadas e simplifica a conclusão de tarefas repetitivas com automação de processos de TI. Cada um desses recursos contribui para proteger os ambientes do AD e do Exchange de seus clientes contra o risco de escalonamento de privilégios, erros, atividade mal-intencionada e não conformidade com normas, ao mesmo tempo reduzindo o fardo do administrador ao oferecer recursos de autoatendimento a usuários, gerentes de negócios e pessoal de suporte técnico.

O DRA também amplia os eficientes recursos do Microsoft Exchange para fornecer gerenciamento contínuo de objetos do Exchange. Por meio de uma interface do usuário única e em comum, o DRA oferece administração baseada em 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 Active Directory local e no Azure, Exchange Server local, Skype for Business local, Exchange Online e Skype for Business Online.
- **Controles granulares de acesso de privilégio administrativo e do usuário:** A tecnologia patenteada ActiveView 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 Mecanismo de Workflow do Aegis 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)	Console de Configuração e Delegação	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 Configuração e Delegação

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

- **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.
- **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.).
- **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:

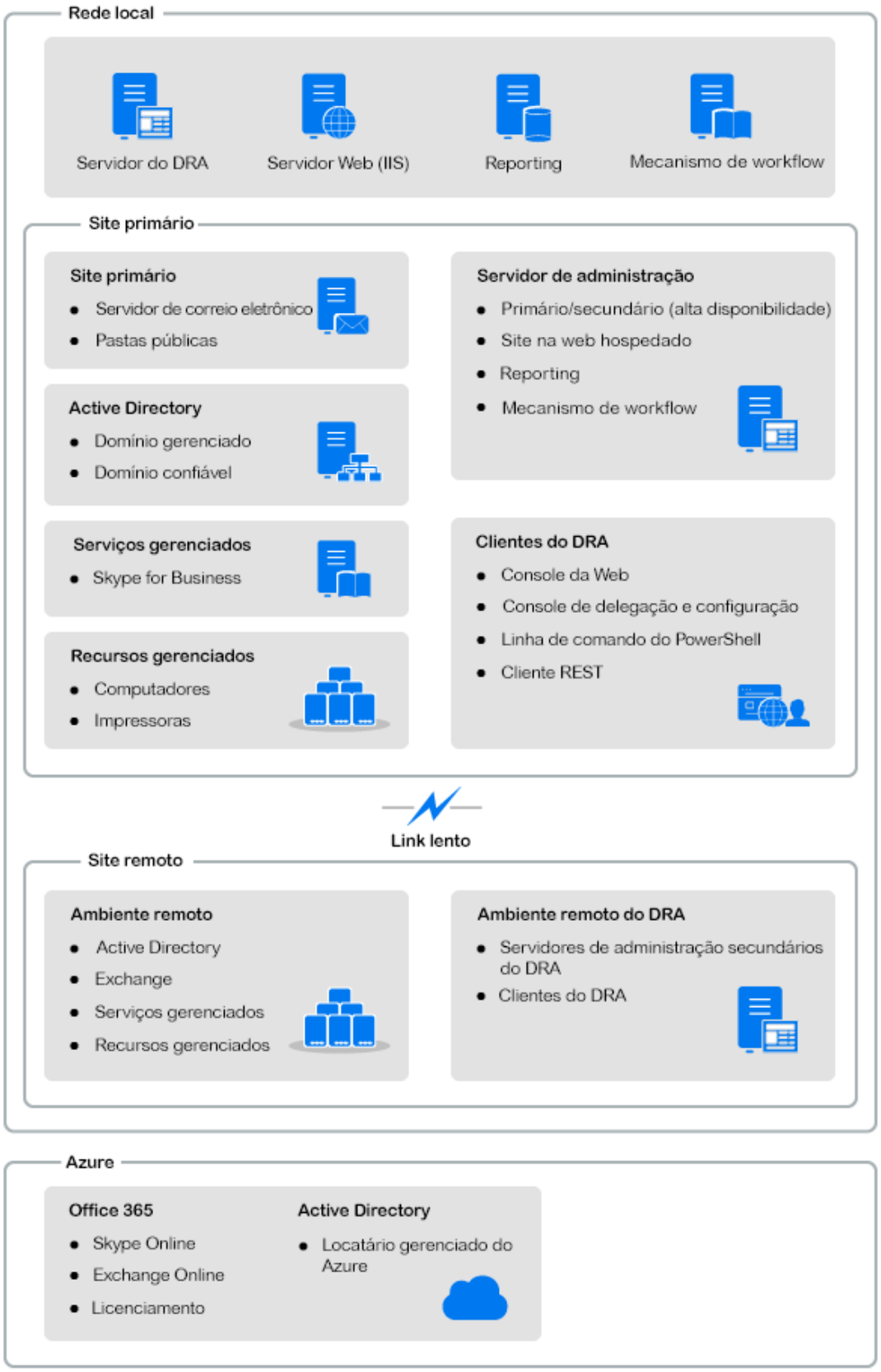
- Relatórios de recursos para objetos do Active Directory
- Relatórios de dados de objeto do Active Directory
- Relatórios de resumo do Active Directory
- Relatórios de configuração do DRA
- Relatórios de configuração do Exchange
- Relatórios do Exchange Online do Office 365
- Relatórios de tendências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

Mecanismo de workflow

O DRA integra-se ao Mecanismo de Workflow do Aegis para automatizar tarefas de workflow por meio do Console da Web no qual administradores assistentes podem configurar o Servidor de Workflow, executar formulários de automação de workflow personalizados e então ver o status desses workflows. Para obter mais informações sobre o Mecanismo de Workflow, consulte 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 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 20
- "Servidor REST do DRA" na página 22
- "Console da Web (IIS)" na página 22
- "Console de administração e delegação do DRA" na página 23
- "Servidor de workflow" na página 23

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)
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)

Protocolo e porta	Direção	Destino	Uso
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
TCP 8898	Bidirecional	Servidores de administração DRA	Comunicação do Serviço de Replicação do DRA entre servidores do DRA para designações temporárias de grupos

Protocolo e porta	Direção	Destino	Uso
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 11192 * **	Saída	Serviço de host do DRA	Para comunicação entre o serviço REST do DRA e o serviço de administração do DRA
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, o PowerShell do DRA e o serviço de host 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 *Using Distributed COM with Firewalls* (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	Console de operações e 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
TCP 9900	Host local	Correlation Engine	Usado pelo Correlation Engine para comunicar-se com o Mecanismo de Workflow e o Provedor de Namespace

Protocolo e porta	Direção	Destino	Uso
TCP 10117	Host local	Provedor de namespace do 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: ◆ Skype for Business Online https://www.microsoft.com/en-us/download/details.aspx?id=39366 ◆ Azure Active Directory V2 (AzureAD) versão 2.0.2.4 ou posterior ◆ AzureRM.Profile versão 5.8.2 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 ◆ Microsoft Skype 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 ◆ Microsoft SQL Server 2017 ◆ Microsoft SQL Server 2019
Browsers da Web	◆ Microsoft Internet Explorer 11 ◆ Google Chrome ◆ Mozilla Firefox
Automação de workflow	◆ Microsoft Server 2012 R2 ◆ Microsoft Server 2016

Requisitos de extensões REST, Servidor de administração DRA e console da Web

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

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 ◆ Microsoft Windows 8.1 (x86 e x64), 10 (x86 e x64)
Instalador	◆ Microsoft .NET Framework 4.6.2 e superior
Servidor de Administração	**Directory and Resource Administrator:**
	◆ Microsoft .NET Framework 4.6.2 e superior ◆ Pacotes Redistribuíveis do Microsoft Visual C++ 2013 (x64) e Pacotes Redistribuíveis do Microsoft Visual C++ 2017 (Atualização 3) (x64 e x86) ◆ 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
	Administração do Microsoft Office 365/Exchange Online:
	◆ Módulo do Microsoft Azure Active Directory para o Windows PowerShell ◆ Skype for Business Online, módulo do Windows PowerShell
	Para obter mais informações, veja Plataformas suportadas.

Componente	Pré-requisitos
Interface do Usuário	**Interfaces do DRA:** ◆ Microsoft .NET Framework 4.6.2 ◆ Pacotes redistribuíveis (x64 e x86) do Microsoft Visual C++ 2017 (Atualização 3)
Serviço de host do DRA	◆ Microsoft .NET Framework 4.6.2 ◆ Servidor de administração DRA
Serviço e endpoint REST do DRA	◆ Microsoft .NET Framework 4.6.2
Extensões do PowerShell	◆ Microsoft .NET Framework 4.6.2 ◆ 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 **Componentes do Microsoft IIS:** ◆ Servidor Web ◆ Recursos HTTP comuns ◆ Conteúdo estático ◆ Documento padrão ◆ Browser do diretório ◆ Erros HTTP ◆ Desenvolvimento de Aplicativo ◆ ASP ◆ Saúde e diagnóstico ◆ Registro HTTP ◆ Monitor de solicitações ◆ Segurança ◆ Autenticação básica ◆ Desempenho ◆ Compressão de conteúdo estático ◆ Ferramentas de gerenciamento de servidor Web

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 de Grupo para DRA, veja: “Configurando Serviços do DRA para uma conta de Serviço Gerenciado de Grupo”

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 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 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 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.
- Se o Servidor REST não estiver instalado no mesmo servidor que o Servidor de administração DRA, a conta de Serviço REST em execução deverá ter controle total sobre o Servidor REST no Active Directory. Por exemplo, definir controle TOTAL sobre `CN=DRARestServer,CN=System,DC=myDomain,DC=com`

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 com o mínimo de privilégios “Permissão Total” em 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: Após os domínios necessários terem sido adicionados ou estarem sendo gerenciados pelo DRA, execute os seguintes comandos:

- 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
NetIQ Reporting Center (v3.2)	**Banco de dados:** ◆ Microsoft SQL Server 2016, 2017, 2019 ◆ Microsoft SQL Server Reporting Services **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.
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.
- **Endpoints e Serviço REST:** Fornece as interfaces RESTful que habilitam o console da Web do DRA e clientes não DRA para solicitar operações do DRA. Este serviço precisa ser executado em um computador que tenha um console do DRA ou que tenha o Serviço de Administração do DRA instalado.
- **Interfaces do Usuário:** A interface de cliente da Web que é primariamente usada por 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 que você especifique de modo granular e designe acesso a recursos e tarefas gerenciados a Administradores Assistentes.
  - **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 de cliente da Web que é primariamente usada por 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 **Instalar o DRA** e em **Avançar** 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 ◆ SDK do DRA **Serviços REST** **Interfaces do Usuário** ◆ Provedor ADSI ◆ Interface de linha de comando ◆ Delegação e Configuração ◆ Extensões do PowerShell ◆ Console da Web
Verificar pré-requisitos	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.
Aceitar o contrato de licença EULA	Aceite os termos do Contrato de Licença por Usuário Final.
Selecione o modo de operação do servidor	Selecione **Principal** para instalar o Servidor de administração DRA em um conjunto com vários masters (poderá haver apenas um principal em uma implantação) ou **Secundário** para ingressar um novo Servidor de administração DRA em um conjunto com vários masters existente. Para obter informações sobre um conjunto multimaster, consulte “Configuring the Multi-Master Set” (Configurando o conjunto multimaster) no *Directory and Resource Administrator Guide* (Guia do Directory and Resource Administrator).

Etapa	Mais informações
Especifique as contas de instalação e as credenciais	◆ Conta de serviço do DRA ◆ Grupo AD LDS ◆ Administrador do DRA Para obter mais informações, veja: Requisitos de extensões REST, Servidor de administração DRA e console da Web.
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.
Especifique o certificado SSL do serviço REST	Selecione o certificado SSL que você usará para o serviço REST e especifique as portas para o REST e para o serviço de host.
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 Servidor de Workflow

Para obter informações sobre como instalar o Servidor de Workflow, consulte o*Guia do Administrador de Automação do Workflow*.

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.

Etapas	Mais informações
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 aos ActiveViews incorporados.
  - 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, consulte “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, 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).

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.
Dedique um servidor secundário para 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.

Etapas	Mais informações
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 de 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 43
- "Sincronizar seu conjunto de servidores com versão anterior do DRA" na página 44
- "Fazer backup do registro de servidor de administração" na página 45

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 de Automação do Workflow 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 Managing Tenants (Gerenciando locatários) 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).

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

Etapas	Mais informações
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 Managing Tenants (Gerenciando locatários) no *DRA Administrator Guide* (Guia do Administrador do DRA).

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.

Fazendo upgrade do Reporting

Antes de você fazer upgrade do DRA Reporting, verifique se o seu ambiente cumpre os requisitos mínimos para o NRC 3.2. 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 Configuração e Delegação.
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 Configuração e Delegação.

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 Configuração do produto

Este capítulo descreve as etapas e os procedimentos de configuração necessários se você está instalando o Directory and Resource Administrator pela primeira vez.

6 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
Aplicar 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.
Abrir Delegação e Configuração	Usando a conta do serviço DRA, efetue logon em um computador em que o Console de Configuração e Delegação esteja instalado. Abra o console.
Adicionar o primeiro domínio gerenciado ao DRA	Adicione o primeiro domínio gerenciado ao DRA. **Observação:** Você pode começar a delegar poderes após a conclusão da primeira Atualização de Conta Completa.
Adicionar domínios gerenciados e subárvores	*Opcional:* Adicione domínios gerenciados adicionais e subárvores ao DRA. Para obter mais informações sobre domínios gerenciados, veja Adicionar domínios gerenciados.
Definir as configurações do DCOM	*Opcional:* Defina as configurações do DCOM. Para obter mais informações sobre as configurações do DCOM, veja Definir configurações de DCOM.
Configurar os controladores de domínio e os servidores de Administração	Configure o computador cliente executando o console de Delegação e Configuração para cada controlador de domínio e cada servidor de Administração. Para obter mais informações, consulte Configurar o controlador de domínio e o servidor de Administração.
Configurar os Serviços de DRA para uma gMSA	*Opcional:* Configure os serviços de DRA para uma gMSA (Conta de Serviço Gerenciado de Grupo). Para obter mais informações, consulte Configurando Serviços do DRA para uma Conta de Serviço Gerenciado de Grupo.

7 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 **Gerenciamento de Configurações**> **Atualizar Licença**. Ao fazer upgrade da sua licença, faça upgrade do arquivo de licença em cada servidor de Administração.

8 Adicionar domínios gerenciados

Você pode adicionar domínios gerenciados, servidores ou estações de trabalho após instalar o servidor de Administração. Quando você adiciona o primeiro domínio gerenciado, precisa efetuar logon usando a conta do serviço DRA em um computador no qual o Console de Configuração e Delegação está instalado. Você também precisa ter direitos administrativos no domínio, assim como os direitos concedidos ao grupo de Administradores do Domínio. Para adicionar domínios gerenciados e computadores após instalar o primeiro domínio gerenciado, você precisa ter os poderes adequados, como aqueles inclusos na função incorporada 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. Para obter mais informações sobre como modificar a programação de atualização de cache das contas, veja "Configuring Caching" (Configurando o caching) no *DRA Administrator Guide* (Guia do Administrador do DRA).

---

9 Adicionando subárvores gerenciadas

Você pode adicionar subárvores gerenciadas ou ausentes de domínios específicos do Microsoft Windows após instalar o servidor de Administração. Essas funções são executadas no Console de Delegação e Configuração do nó **Gerenciamento de Configurações** > **Domínios Gerenciados**. Para adicionar subárvores gerenciadas após instalar o servidor de Administração, você precisa ter os poderes adequados, como aqueles inclusos na função incorporada Configurar Servidores e Domínios. Para assegurar que a conta de acesso especificada tenha as permissões para gerenciar essa subárvore e realizar atualizações de cache incrementais nas contas, use o utilitário Objetos Apagados para verificar e delegar as permissões adequadas.

Para obter mais informações sobre como usar esse utilitário, veja "Deleted Objects Utility" (Utilitário Objetos Apagados) no *DRA Administrator Guide* (Guia do Administrador do DRA).

Para obter mais informações sobre como configurar a conta de acesso, veja "Specifying Domain Access Accounts" (Especificando contas de acesso ao domínio) no *DRA Administrator Guide* (Guia do Administrador do DRA).

Observação: Após você terminar de adicionar subárvores gerenciadas, verifique se as programações de atualização de cache das contas para os domínios correspondentes estão corretas. Para obter mais informações sobre como modificar a programação de atualização de cache das contas, veja "Configuring Caching" (Configurando o caching) no *DRA Administrator Guide* (Guia do Administrador do DRA).

---

10 Definir configurações de DCOM

Defina as configurações de DCOM em seu servidor de Administração principal se ainda não permitiu que o programa de configuração configure o DCOM para você.

Se você tiver selecionado a opção de não configurar o COM Distribuído durante o processo de instalação do DRA, deverá atualizar a participação no grupo “Usuários de COM Distribuído” para incluir todas as contas de usuário que usam o DRA. Essa participação deve incluir a Conta do Serviço DRA, todos os Admins Assistentes e a conta usada para gerenciar o REST do DRA, o Host do DRA e os serviços de Admin do DRA.

Para configurar o grupo “Usuários de COM Distribuído”:

1. Efetue logon em um computador de Administração como um administrador do DRA.
2. Inicie o console de Configuração e Delegação. Se o console não se conectar automaticamente ao servidor de Administração, estabeleça a conexão manualmente.

   Observação: Você poderá não conseguir se conectar ao servidor de Administração se o grupo “Usuários de COM Distribuído” não contiver nenhuma conta de Admin Assistente. Se for o caso, configure o grupo “Usuários de COM Distribuído” usando o snap-in Usuários e Computadores do Active Directory. Para obter mais informações sobre como usar o snap-in Usuários e Computadores do Active Directory, veja o site na web da Microsoft.
3. No painel esquerdo, expanda **Gerenciamento de Recursos e de Contas**.
4. Expanda **Todos os Meus Objetos Gerenciados**.
5. Expanda o nó de domínio para cada domínio em que você tem um controlador de domínio.
6. Clique no container **Incorporado**.
7. Pesquise pelo grupo “Usuários de COM Distribuído”.
8. Na lista de resultados da pesquisa, clique no grupo **Usuários de COM Distribuído**.
9. Clique em **Membros** no painel inferior, depois clique em **Adicionar Membros**.
10. Adicione usuários e grupos que usarão o DRA. Adicione a conta de serviço do DRA a este grupo.
11. Clique em **OK**.

11 Configurar o controlador de domínio e o servidor de Administração

Após configurar o computador cliente executando o console de Configuração e Delegação, você deve configurar cada controlador de domínio e cada servidor de Administração.

Para configurar o controlador de domínio e o servidor de Administração:

1. Do menu Iniciar, acesse **Painel de Controle** > **Sistema e Segurança**.
2. Abra Ferramentas Administrativas e então Serviços de Componente.
3. Expanda **Serviços de Componente** > **Computadores** > **Meu Computador** > **Config DCOM**.
4. Selecione **Serviço de Administração MCS OnePoint** no servidor de Administração.
5. No menu Ação, clique em **Propriedades**.
6. Na guia Geral, na área de Nível de Autenticação, selecione **Pacote**.
7. Na guia Segurança na área Permissões de Acesso, selecione **Personalizar** e, em seguida, clique em **Editar**.
8. Verifique se o grupo “Usuários de COM Distribuído” está disponível. Se ele não estiver disponível, adicione-o. Se o grupo “Todos” estiver disponível, remova-o.
9. Verifique se o grupo “Usuários de COM Distribuído” tem as permissões de acesso Remoto e Local.
10. Na guia Segurança na área Permissões de Início e Ativação, selecione **Personalizar** e, em seguida, clique em **Editar**.
11. Verifique se o grupo “Usuários de COM Distribuído” está disponível. Se ele não estiver disponível, adicione-o. Se o grupo “Todos” estiver disponível, remova-o.
12. Verifique se o grupo “Usuários de COM Distribuído” tem as seguintes permissões:
    - Início local
    - Início remoto
    - Ativação local
    - Ativação remota
13. Aplique as mudanças.

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

Se necessário, você pode usar uma gMSA (Conta de Serviço Gerenciado de 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 gerenciadas de grupo). Esta seção explica como configurar o DRA para uma Conta de Serviço Gerenciado de Grupo após ter adicionado previamente 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 Cache do DRA da NetIQ
   - Serviço de Núcleo do DRA da NetIQ
   - Serviço de Host 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** ao ActiveView **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 login de todos os serviços do DRA para a gMSA e então reinicie os serviços do DRA.