Instalando e configurando o VMware Identity Manager

VMware Identity Manager 2.9.1

vmware®

Você pode encontrar a documentação técnica mais atualizada no site da VMware, em:

https://docs.vmware.com/br/

O site da VMware também fornece as atualizações mais recentes de produtos.

Caso tenha comentários sobre esta documentação, envie seu feedback para:

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Conteúdo

Sobre “Instalando e configurando o VMware Identity Manager "

O guia *Instalando e configurando o VMware Identity Manager* fornece informações sobre o processo de instalação e configuração do appliance do VMware Identity Manager. Quando a instalação for concluída, você poderá usar o console de administração para autorizar aos usuários o acesso com vários dispositivos gerenciados aos aplicativos da organização, incluindo aplicativos do Windows, aplicativos de software como serviço (SaaS) e desktops do View ou do Horizon. O guia também explica como configurar a sua implantação para alta disponibilidade.

Público-alvo

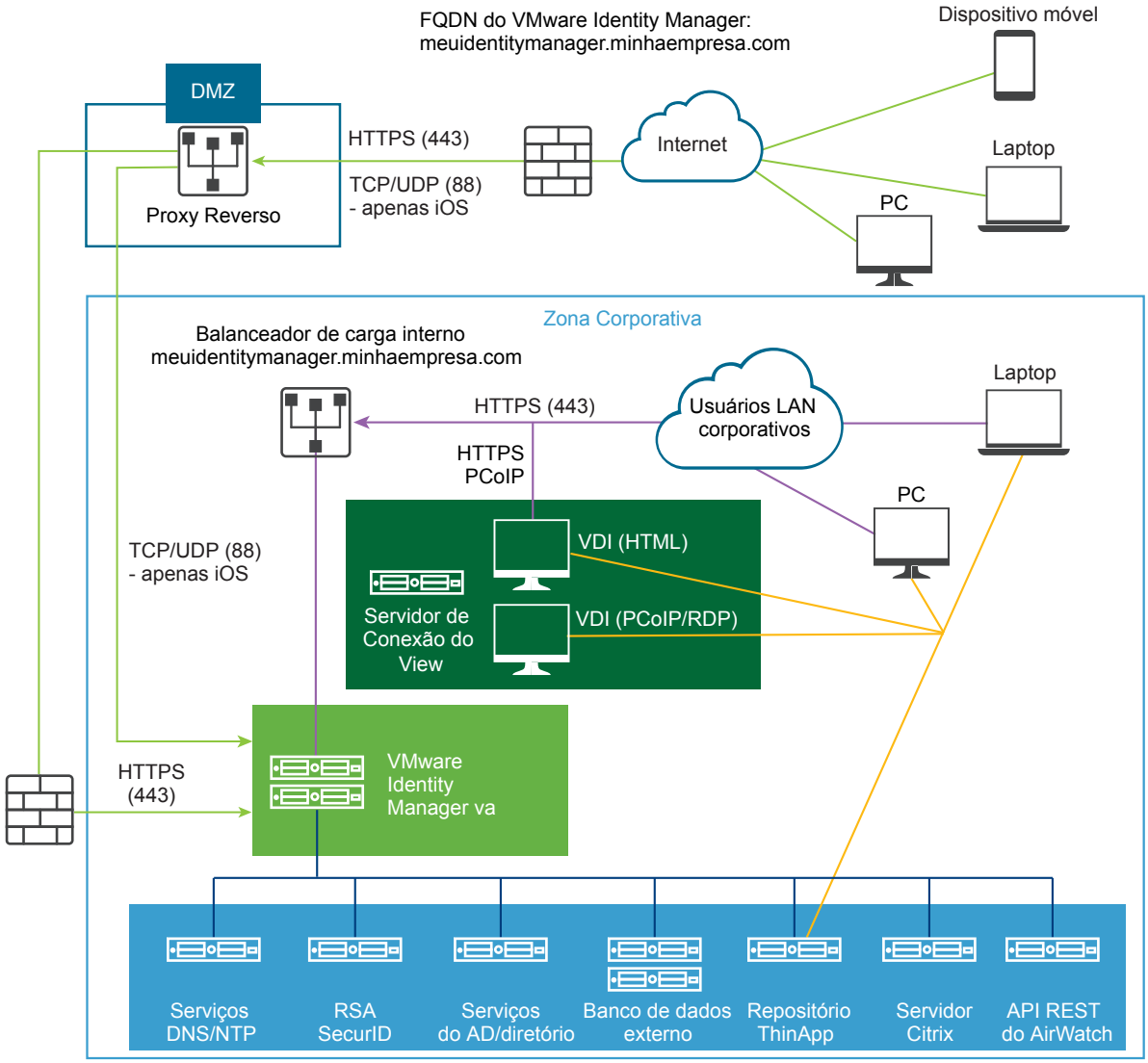
Estas informações destinam-se aos administradores do VMware Identity Manager. As informações são escritos para administradores de sistema Windows e Linux experientes que estão familiarizados com as tecnologias da VMware, especialmente o vCenter™, o ESX™, o vSphere® e o View™, conceitos de rede, servidores Active Directory, bancos de dados, procedimentos de backup e restauração, protocolo SMTP e servidores NTP. O SUSE Linux 11 é o sistema operacional subjacente do appliance virtual. O conhecimento de outras tecnologias, como o VMware ThinApp® e o RSA SecurID, será útil se você pretende implementar esses recursos.

Preparando a instalação do VMware Identity Manager

1

As tarefas para implantar e instalar o VMware Identity Manager exigem que você atenda aos pré-requisitos, implante o arquivo OVA do VMware Identity Manager e conclua a configuração pelo assistente de Instalação do VMware Identity Manager.

Figura 1-1. Diagrama da arquitetura do VMware Identity Manager para implantações típicas



Observação Se você planeja habilitar a autenticação com base em cartão inteligente ou em certificado, use a configuração de passagem de SSL no balanceador de carga, em vez da configuração SSL de término. Essa configuração garante que o handshake de SSL esteja entre o conector, um componente do VMware Identity Manager e o cliente.

Observação Dependendo da localização da implantação do AirWatch, as APIs REST do AirWatch podem estar na nuvem ou nas instalações.

Este capítulo inclui os seguintes tópicos:

- "Requisitos de configuração do sistema e da rede", na página 11
- "Preparando-se para implantar o VMware Identity Manager", na página 15
- "Programa de aperfeiçoamento da experiência do cliente", na página 18

Requisitos de configuração do sistema e da rede

Considere a sua implantação inteira, incluindo como você integra recursos, ao tomar decisões sobre requisitos de hardware, recursos e rede.

Versões compatíveis do vSphere e do ESX

As seguintes versões do vSphere e do ESX Server são compatíveis:

- 5.0 U2 e posteriores
- 5.1 e posteriores
- 5.5 e posterior
- 6.0 e posteriores

Observação Você deve ativar a sincronização de tempo no nível do host ESX usando um servidor NTP. Caso contrário, haverá um deslocamento de tempo entre os appliances virtuais.

Se você implantar vários appliances virtuais em hosts diferentes, considere desativar a opção Sincronizar para o Host para sincronização de tempo e configurar o servidor NTP diretamente em cada appliance virtual para garantir que não ocorra um deslocamento de tempo entre os appliances virtuais.

Requisitos de hardware

Certifique-se de que você atende aos requisitos para a quantidade de appliances virtuais do VMware Identity Manager e os recursos alocados a cada appliance.

Quantidade de usuários	Até 1.000	1.000-10.000	10.000-25.000	25.000-50.000	50.000-100.000
Quantidade de servidores do VMware Identity Manager	1 servidor	3 servidores com balanceamento de carga	3 servidores com balanceamento de carga	3 servidores com balanceamento de carga	3 servidores com balanceamento de carga
CPU (por servidor)	2 CPUs	2 CPUs	4 CPUs	8 CPUs	8 CPUs
RAM (por servidor)	6 GB	6 GB	8 GB	16 GB	32 GB
Espaço em disco (por servidor)	60 GB	100 GB	100 GB	100 GB	100 GB

Se você instalar appliances virtuais de conector externo, adicional, certifique-se de que atende aos seguintes requisitos.

Quantidade de usuários	Até 1.000	1.000-10.000	10.000-25.000	25.000-50.000	50.000-100.1000
Quantidade de servidores de conector	1 servidor	2 servidores com balanceamento de carga	2 servidores com balanceamento de carga	2 servidores com balanceamento de carga	2 servidores com balanceamento de carga
CPU (por servidor)	2 CPUs	4 CPUs	4 CPUs	4 CPUs	4 CPUs

Quantidade de usuários	Até 1.000	1.000-10.000	10.000-25.000	25.000-50.000	50.000-100.1000
RAM (por servidor)	6 GB	6 GB	8 GB	16 GB	16 GB
Espaço em disco (por servidor)	60 GB	60 GB	60 GB	60 GB	60 GB

Requisitos de banco de dados

Configure o VMware Identity Manager com um banco de dados externo para armazenar e organizar os dados do servidor. Um banco de dados interno do PostgreSQL está incorporado no appliance virtual, mas ele não é recomendado para uso com implantações de produção.

Para obter informações sobre as versões do banco de dados e as configurações de service pack suportadas, consulte Matrizes de interoperabilidade de produtos da VMware em https://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Os seguintes requisitos se aplicam a um banco de dados de SQL Server externo.

Quantidade de usuários	Até 1.000	1.000-10.000	10.000-25.000	25.000-50.000	50.000-100.000
CPU	2 CPUs	2 CPUs	4 CPUs	8 CPUs	8 CPUs
RAM	4 GB	4 GB	8 GB	16 GB	32 GB
Espaço em disco	50 GB	50 GB	50 GB	100 GB	100 GB

Requisitos de configuração de rede

Componente	Requisito mínimo
Registro DNS e endereço IP	Endereço IP e registro DNS
Porta do firewall	Certifique-se de que a porta 443 do firewall de entrada está aberta para os usuários fora da rede para a instância do VMware Identity Manager ou o balanceador de carga.
Proxy Reverso	Implante um proxy reverso, como o F5 Access Policy Manager na DMZ, para permitir que os usuários acessem o portal do usuário do VMware Identity Manager remotamente.

Requisitos de porta

As portas usadas na configuração do servidor estão descritas aqui. A implantação pode incluir somente um subconjunto dessas portas. Por exemplo:

- Para sincronizar usuários e grupos do Active Directory, o VMware Identity Manager deve se conectar ao Active Directory.
- Para sincronizar com o ThinApp, o VMware Identity Manager deve ingressar no domínio do Active Directory e se conectar ao compartilhamento Repositório do ThinApp.

Porta	Portal	Origem	Target	Descrição
443	HTTPS	Balanceador de Carga	Appliance virtual do VMware Identity Manager	
443	HTTPS	Appliance virtual do VMware Identity Manager	Appliance virtual do VMware Identity Manager	

Porta	Portal	Origem	Target	Descrição
443	HTTPS	Navegadores	Appliance virtual do VMware Identity Manager	
443	HTTPS	Appliance virtual do VMware Identity Manager	vapp-updates.vmware.com	Acesso ao servidor de atualização
8443	HTTPS	Navegadores	Appliance virtual do VMware Identity Manager	Porta do administrador
25	SMTP	Appliance virtual do VMware Identity Manager	SMTP	Porta para transmitir mensagens de saída
389 636 3268 3269	LDAP LDAPS MSFT-GC MSFT-GC-SSL	Appliance virtual do VMware Identity Manager	Active Directory	Os valores padrão aparecem. Essas portas são configuráveis.
445	TCP	Appliance virtual do VMware Identity Manager	Repositório do VMware ThinApp	Acesso ao repositório do ThinApp
5500	UDP	Appliance virtual do VMware Identity Manager	Sistema RSA SecurID	O valor padrão é mostrado. Essa porta é configurável.
53	TCP/UDP	Appliance virtual do VMware Identity Manager	Servidor DNS	Todos os appliances virtuais devem ter acesso ao servidor DNS na porta 53 e permitir o tráfego SSH de entrada na porta 22.
88, 464, 135	TCP/UDP	Appliance virtual do VMware Identity Manager	Controlador de domínio	
9300–9400 54328	TCP UDP	Appliance virtual do VMware Identity Manager	Appliance virtual do VMware Identity Manager	Necessidades de auditoria
1433, 5432, 1521	TCP	Appliance virtual do VMware Identity Manager	Banco de dados	A porta padrão do Microsoft SQL é a 1433 A porta padrão do Oracle é 1521
443		Appliance virtual do VMware Identity Manager	Servidor do View	Acesso ao servidor do View
80, 443	TCP	Appliance virtual do VMware Identity Manager	Servidor do Citrix Integration Broker	Conexão com o Citrix Integration Broker. A opção de porta depende do fato de um certificado estar instalado no servidor do Integration Broker
443	HTTPS	Appliance virtual do VMware Identity Manager	API REST do AirWatch	Para a verificação de conformidade de dispositivo e para o método de autenticação de senha do AirWatch Cloud Connector, se for usado.

Porta	Portal	Origem	Target	Descrição
88	UDP	Unified Access Gateway	Appliance virtual do VMware Identity Manager	Porta UDP a ser aberta para SSO móvel
5262	TCP	Dispositivo móvel Android	Serviço de proxy HTTPS do AirWatch	O cliente do AirWatch Tunnel encaminha o tráfego para o proxy HTTPS de dispositivos Android.
88	UDP	Dispositivo móvel iOS	Appliance virtual do VMware Identity Manager	A porta usada para o tráfego Kerberos de dispositivos iOS para o serviço do KDC hospedado na nuvem.
443	HTTPS/TCP			

Active Directory

O VMware Identity Manager suporta o Active Directory no Windows 2008, 2008 R2, 2012 e 2012 R2, com um nível funcional de Domínio e nível funcional de Floresta do Windows 2003 e posterior.

Navegadores da Web suportados para acessar o console de administração

O console de administração do VMware Identity Manager é um aplicativo baseado na Web que você usa para gerenciar seu tenant. Você pode acessar o console de administração nos seguintes navegadores.

- Internet Explorer 11 para sistemas do Windows
- Google Chrome 42.0 ou versões posteriores para sistemas do Windows e Mac
- Mozilla Firefox 40 ou versões posteriores para sistemas do Windows e Mac
- Safari 6.2.8 e versões posteriores para sistemas Mac

Observação No Internet Explorer 11, deve-se habilitar o JavaScript e se permitir cookies para a autenticação pelo VMware Identity Manager.

Navegadores suportados para acessar o portal do Workspace ONE

Os usuários finais podem acessar o portal do Workspace ONE nos seguintes navegadores.

- Mozilla Firefox (mais recente)
- Google Chrome (mais recente)
- Safari (mais recente)
- Internet Explorer 11
- Navegador Microsoft Edge
- Navegador nativo e Google Chrome em dispositivos Android
- Safari em dispositivos iOS

Observação No Internet Explorer 11, deve-se habilitar o JavaScript e se permitir cookies para a autenticação pelo VMware Identity Manager.

Preparando-se para implantar o VMware Identity Manager

Antes de implantar o VMware Identity Manager, você deve preparar o seu ambiente. Essa preparação inclui o download do arquivo OVA do VMware Identity Manager, a criação de registros DNS e a obtenção de endereços IP.

Pré-requisitos

Antes de começar a instalar o VMware Identity Manager, conclua as tarefas de pré-requisito.

- Você precisa de um ou mais servidores ESX para implantar o appliance virtual do VMware Identity Manager.

  Observação Para obter informações sobre as versões compatíveis do VMware vSphere e do ESX, consulte as Matrizes de interoperabilidade entre produtos VMware em http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

- O VMware vSphere Client ou o vSphere Web Client é necessário para implantar o arquivo OVA e acessar o appliance virtual implantado remotamente para configurar a rede.
- Faça download do arquivo OVA do VMware Identity Manager no site da VMware.

Criar registros DNS e endereços IP

Uma entrada DNS e um endereço IP estático devem estar disponíveis para o appliance virtual do VMware Identity Manager. Como cada empresa administra os próprios endereços IP e registros DNS de forma diferente, solicite o registro DNS e os endereços IP a serem usados antes de começar a instalação.

A configuração da pesquisa inversa é opcional. Ao implementar a pesquisa inversa, você deve definir um registro PTR no servidor DNS para que o appliance virtual use a configuração de rede correta.

Você pode usar a lista de amostra de registros DNS ao conversar com o administrador da rede. Substitua as informações de amostra por informações do seu ambiente. Este exemplo mostra os registros DNS e os endereços IP encaminhados.

Tabela 1-1. Exemplos de registros DNS e endereços IP encaminhados

Nome do domínio	Tipo de Recurso	Endereço IP
meuidentitymanager.empresa.com	Um	10.28.128.3

Este exemplo mostra os registros DNS e endereços IP reversos.

Tabela 1-2. Exemplos de registros DNS e endereços IP reversos

Endereço IP	Tipo de Recurso	Nome do Host
10.28.128.3	PTR	meuidentitymanager.empresa.com

Depois de concluir a configuração do DNS, verifique se a pesquisa de DNS reverso está configurada corretamente. Por exemplo, o comando do appliance virtual `host IPaddress` deve ser resolvido para a pesquisa de nome de DNS.

Usando um servidor DNS baseado em Unix/Linux

Se você estiver usando um servidor DNS baseado em Linux ou Unix e pretende ingressar o VMware Identity Manager no domínio do Active Directory, certifique-se de que os registros de recurso do serviço (SRV) adequados sejam criados para cada controlador de domínio do Active Directory.

Observação Caso você tenha um balanceador de carga com um endereço IP virtual (VIP) na frente dos servidores DNS, observe que o VMware Identity Manager não oferece para suporta usar um VIP. Você pode especificar vários servidores DNS separados por vírgula.

Opções de banco de dados com o VMware Identity Manager

Configure o VMware Identity Manager com um banco de dados externo para armazenar e organizar os dados do servidor. Um banco de dados PostgreSQL interno é incorporado no appliance, mas não é recomendado para uso com implantações de produção.

Para usar um banco de dados externo, o administrador de banco de dados deve preparar um banco de dados externo vazio e um esquema antes de se conectar ao banco de dados externo no Assistente de Instalação. Os usuários licenciados podem usar um servidor do banco de dados Microsoft SQL ou um servidor do banco de dados Oracle para configurar um ambiente de banco de dados externo de alta disponibilidade. Consulte "Conectando-se ao banco de dados", na página 32.

Conectando ao seu diretório empresarial

O VMware Identity Manager usa sua infraestrutura de diretório empresarial para autenticação e gerenciamento de usuários. Você pode integrar o serviço do VMware Identity Manager a um ambiente Active Directory, que consiste em um único domínio do Active Directory, vários domínios em uma única floresta do Active Directory ou vários domínios em várias florestas do Active Directory. Você também pode integrar o VMware Identity Manager a um diretório LDAP. Para sincronizar usuários e grupos, o appliance virtual do VMware Identity Manager precisa se conectar ao diretório.

Seu diretório deve ser acessíveis na mesma rede LAN do appliance virtual do VMware Identity Manager.

Consulte Capítulo 4, "Integrando ao seu Diretório Corporativo", na página 43 para obter mais informações.

Listas de verificação de implantação

Você pode usar a lista de verificação de implantação para reunir as informações necessárias para instalar o appliance virtual do VMware Identity Manager.

Informações do nome de domínio totalmente qualificado

Tabela 1-3. Lista de verificação de informações do nome de domínio totalmente qualificado (FQDN)

Informações a reunir	Listar as informações
FQDN do VMware Identity Manager	

Informações de rede do appliance virtual do VMware Identity Manager

Tabela 1-4. Lista de verificação de informações de rede

Informações a reunir	Listar as informações
Endereço IP	Você deve usar um endereço IP estático e ele deve ter um PTR e um registro A definido no DNS.
Nome DNS desse appliance virtual	

Tabela 1-4. Lista de verificação de informações de rede (Continuação)

Informações a reunir	Listar as informações
Endereço do gateway padrão	
Máscara de rede ou prefixo	

Informações do diretório

O VMware Identity Manager é compatível com a integração aos ambientes Active Directory ou diretório LDAP.

Tabela 1-5. Lista de verificação de informações do controlador de domínio do Active Directory

Informações a reunir	Listar as informações
Nome do servidor Active Directory	
Nome do domínio do Active Directory	
DN base	
Para o Active Directory sobre LDAP, o nome de usuário e a senha do DN Bind	
Para o Active Directory com Autenticação Integrada do Windows, o nome de usuário e a senha da conta com privilégios para ingressar computadores no domínio.	

Tabela 1-6. Lista de verificação de informações do servidor do diretório LDAP

Informações a reunir	Listar as informações
Nome ou endereço IP do servidor do diretório LDAP	
Número da porta do servidor do diretório LDAP	
DN base	
Nome de usuário e senha do DN Bind	
Filtros de pesquisa LDAP para objetos de grupo, objetos do usuário bind e objetos de usuário	
Nomes de atributo LDAP para associação, UUID do objeto e nome distinto	

Certificados SSL

Você pode adicionar um certificado SSL depois de implantar o appliance virtual do VMware Identity Manager.

Tabela 1-7. Lista de verificação de informações do certificado SSL

Informações a reunir	Listar as informações
certificado SSL	
Chave privada	

Chave de Licença

Tabela 1-8. Lista de verificação de informações da chave de licença do VMware Identity Manager

Informações a reunir	Listar as informações
Chave de licença	

Observação As informações de Chave de Licença são inseridas no console de administração na página **Configurações do Appliance > Licença** após a conclusão da instalação.

Banco de dados externo

Tabela 1-9. Lista de verificação de informações do banco de dados externo

Informações a reunir	Listar as informações
Nome do host do banco de dados	
Porta	
Nome de usuário	
Senha	

Programa de aperfeiçoamento da experiência do cliente

Ao instalar o appliance virtual do VMware Identity Manager, é possível escolher participar do programa de experiência do cliente VMware.

Caso você participe do programa, a VMware coleta dados anônimos sobre sua implantação para melhorar a resposta da VMware às necessidades do usuário. Não coletamos nenhum dado que identifique sua organização.

Antes de coletar os dados, a VMware torna anônimos todos os campos que contêm informações específicas sobre sua organização.

Observação Caso sua rede esteja configurada para acessar a Internet por meio do proxy HTTP, para enviar essa informação, será necessário ajustar as configurações do proxy no appliance virtual do VMware Identity Manager. Consulte "Definindo as configurações do servidor proxy para o VMware Identity Manager", na página 30.

Implantando o VMware Identity Manager 2

Para implantar o VMware Identity Manager, implante o modelo OVF usando o vSphere Client ou o vSphere Web Client, ligue o appliance virtual do VMware Identity Manager e defina as configurações.

Após a implantação do appliance virtual do VMware Identity Manager, use o Assistente de Instalação para configurar o ambiente VMware Identity Manager.

Use as informações na lista de verificação de implantação para concluir a instalação. Consulte "Listas de verificação de implantação", na página 16.

Este capítulo inclui os seguintes tópicos:

Instalar o arquivo OVA do VMware Identity Manager

Implante o arquivo OVA do VMware Identity Manager usando o vSphere Client ou o vSphere Web Client. Você pode fazer download e implantar o arquivo OVA de uma localização local acessível ao vSphere Client ou implantá-lo de uma URL Web.

Observação Se você estiver usando o vSphere Web Client, use o navegador Firefox ou Chrome para implementar o arquivo OVA. Não use o Internet Explorer.

Pré-requisitos

Revise Capítulo 1, "Preparando a instalação do VMware Identity Manager", na página 9.

Procedimentos

1 Faça download do arquivo OVA VMware Identity Manager no My VMware.

2 Faça login no vSphere Client ou no vSphere Web Client.

3 Selecione **Arquivo > Implementar Modelo OVF**.

4 No assistente Implantar Modelo OVF, especifique as informações a seguir.

Página	Descrição
Origem	Navegue até a localização do pacote OVA ou insira uma URL específica.
Detalhes do Modelo OVF	Revise os detalhes do produto, incluindo a versão e os requisitos de tamanho.
Contrato de Licença de Usuário Final	Leia o contrato de licença de usuário final e clique em **Aceitar**.
Nome e localização	Insira um nome para o appliance virtual do VMware Identity Manager. O nome deve ser exclusivo na pasta de inventário e pode conter até 80 caracteres. Os nomes diferenciam maiúsculas de minúsculas. Insira uma localização para o appliance virtual.
Host/Cluster	Selecione o host ou o cluster no qual executar o aplicativo virtual.
Pool de recursos	Selecione o pool de recursos.
Armazenamento	Selecione o armazenamento dos arquivos do appliance virtual. Você também pode selecionar um Perfil de Repositório de VM.
Formato do disco	Selecione o formato do disco para os arquivos. Para ambientes de produção, selecione um dos formatos de Provisionamento Estático. Use o formato Provisionamento Dinâmico para avaliação e testes. No formato Provisionamento Estático, todo o espaço necessário para o disco virtual é alocado durante a implantação. No formato Provisionamento Dinâmico, o disco usa somente a quantidade de espaço de armazenamento que necessita para as operações iniciais.
Mapeamento de rede	Mapeie as redes usadas no VMware Identity Manager para as redes no seu inventário.
Propriedades	a No campo **Configuração de fuso horário**, selecione o fuso horário correto. b A caixa de seleção **Programa de Aperfeiçoamento da Experiência do Usuário** está marcada por padrão. A VMware coleta dados anônimos sobre sua implantação para melhorar a resposta da VMware às necessidades do usuário. Desmarque a caixa de seleção se você não desejar que os dados sejam coletados. c Na caixa de texto **Nome do Host (FQDN)**, insira o nome do host a ser usado. Se estiver em branco, o DNS reverso será usado para procurar o nome do host. d Configure as propriedades de rede. ■ Para configurar um endereço IP estático do VMware Identity Manager, insira o endereço dos campos **Gateway Padrão**, **DNS**, **Endereço IP** e **Máscara de Rede**. **Observação** Caso você tenha um balanceador de carga com um endereço IP virtual (VIP) na frente dos servidores DNS, observe que o VMware Identity Manager não oferece para suporta usar um VIP. Você pode especificar vários servidores DNS separados por vírgula. **Importante** Se qualquer um dos quatro campos de endereço, incluindo **Nome do Host**, for deixado em branco, DHCP será usado. ■ Para configurar o DHCP, deixe os campos de endereço em branco. **Observação** Os campos **Nome do Domínio** e **Caminho de Pesquisa de Domínio** não são usados. Você pode deixá-los em branco. (Opcional) Depois que o VMware Identity Manager for instalado, você poderá configurar Pools de IP. Consulte "(Opcional) Adicionar pools de IPs", na página 21.
Pronto para ser concluído	Revise as seleções e clique em **Finalizar**.

Dependendo da velocidade da rede, a implantação pode levar vários minutos. Você pode exibir o andamento na caixa de diálogo de andamento que é exibida.

5 Quando a implantação estiver concluída, clique em **Fechar** na caixa de diálogo de andamento.

6 Selecione o appliance virtual do VMware Identity Manager implanta, clique com o botão direito do mouse e selecione **Ligar > Ligar**.

O appliance virtual do VMware Identity Manager é inicializado. Você pode ir até a guia **Console** para ver os detalhes. Quando a inicialização do dispositivo virtual é concluída, a tela do console exibe a versão, o endereço IP e as URLs do VMware Identity Manager para fazer login na interface Web do VMware Identity Manager e para concluir a configuração.

Próximo passo

- (Opcional) Adicione Pools de IP.
- Configure as definições do VMware Identity Manager, incluindo a conexão com o diretório do Active Directory ou LDAP, e selecione usuários e grupos a serem sincronizados com o VMware Identity Manager.

(Opcional) Adicionar pools de IPs

A configuração de rede com pools de IPs é opcional no VMware Identity Manager. Você pode adicionar manualmente pools de IPs ao appliance virtual do VMware Identity Manager depois de instalá-lo.

Os Pools de IP agem como servidores DHCP para atribuir endereços IP do pool ao appliance virtual do VMware Identity Manager. Para usar Pools de IPs, edite as propriedades de rede do appliance virtual para alterar as propriedades para propriedades dinâmicas e definir as configurações de máscara de rede, gateway e DNS.

Pré-requisitos

O appliance virtual deve estar desligado.

Procedimentos

1 No vSphere Client ou no vSphere Web Client, clique com o botão direito do mouse no appliance virtual do VMware Identity Manager e selecione **Editar Configurações**.

2 Selecione a guia **Opções**.

3 Em **Opções do vApp**, clique em **Avançado**.

4 Na seção Propriedades à direita, clique no botão **Propriedades**.

5 Na caixa de diálogo Configuração Avançada de Propriedade, configure as seguintes chaves:

- vami.DNS.WorkspacePortal
- vami.netmask0.WorkspacePortal
- vami.gateway.WorkspacePortal

a Selecione uma das chaves e clique em **Editar**.

b Na caixa de diálogo Editar Configurações de Propriedade, ao lado do campo **Tipo**, clique em **Editar**.

c Na caixa de diálogo Editar Tipo de Propriedade, selecione **Propriedade Dinâmica** e selecione no menu suspenso o valor adequado de **Máscara de Rede**, **Endereço do Gateway** e **Servidores DNS**, respectivamente.

d Clique em **OK** e em **OK** novamente.

e Repita essas etapas para configurar cada chave.

6 Ligue o appliance virtual.

As propriedades são configuradas para usar Pools de IPs.

Próximo passo

Defina as configurações do VMware Identity Manager.

Configurar as definições do VMware Identity Manager

Depois que o OVA do VMware Identity Manager for implantado, use o assistente Instalar para definir senhas e selecionar um banco de dados. Em seguida, configure a conexão com o diretório do Active Directory ou LDAP.

Pré-requisitos

- O appliance virtual do VMware Identity Manager está ligado.
- Se você usar um banco de dados externo, ele está configurado e as informações de conexão dele estão disponíveis. Consulte "Conectando-se ao banco de dados", na página 32 para obter informações.
- Revise Capítulo 4, "Integrando ao seu Diretório Corporativo", na página 43, "Integrando com o Active Directory", na página 45 e "Integrar um diretório LDAP ao serviço", na página 60 para conhecer os requisitos e as limitações.
- Você tem as informações de diretório do Active Directory ou o LDAP.
- Quando um Active Directory de várias florestas está configurado e o grupo Domínio Local contém membros de domínios em diferentes florestas, o usuário DN Bind usado na página Diretório do VMware Identity Manager deve ser adicionado ao grupo Administradores do domínio no qual o grupo Domínio Local reside. Se isso não for feito, esses membros estarão em falta do grupo local de domínio.
- Você tem uma lista de atributos de usuário que deseja usar como filtros, e uma lista dos grupos que deseja adicionar ao VMware Identity Manager.

Procedimentos

1 Acesse a URL do VMware Identity Manager mostrada na tela azul na guia **Console**. Por exemplo, `https://nomedohost.exemplo.com`.

2 Aceite o certificado, se for solicitado a fazê-lo.

3 Na página Iniciar, clique em **Continuar**.

4 Na página Definir Senhas, defina as senhas das seguintes contas de administrador, que são utilizadas para gerenciar o appliance, e clique em **Continuar**.

Conta	
Administrador do appliance	Defina a senha do usuário **admin**. Esse nome de usuário não pode ser alterado. A conta do usuário **admin** é usada para gerenciar as configurações do appliance. **Importante** A senha do usuário **administrador** deve ter pelo menos 6 caracteres.
Raiz do Appliance	Defina a senha do usuário **root**. O usuário **root** tem direitos totais para o appliance.
Usuário Remoto	Defina a senha de **sshuser**, que é usada fazer login remotamente no appliance com uma conexão SSH.

5 Na página Selecionar Banco de Dados, selecione o banco de dados a ser usado.

Consulte "Conectando-se ao banco de dados", na página 32 para obter mais informações.

- Se você estiver usando um banco de dados externo, selecione **Banco de Dados Externo** e insira as informações, o nome de usuário e a senha da conexão do banco de dados externo. Para verificar se o VMware Identity Manager consegue se conectar ao banco de dados, clique em **Testar Conexão**.

  Depois de verificar a conexão, clique em **Continuar**.

- Se você estiver usando o banco de dados interno, clique em **Continuar**.

  Observação Não recomendamos que o banco de dados interno seja usado com implantações de produção.

A conexão com o banco de dados está configurada e ele é inicializado. Quando o processo for concluído, a página **A instalação foi concluída** será exibida.

6 Clique no link **Faça login no console de administração** na página **A instalação foi concluída** para fazer login no console de administração e configurar a conexão do diretório do Active Directory ou LDAP.

7 Faça login no console de administração como o usuário **admin** usando a senha que você definiu.

Você está conectado como um Administrador Local. A página Diretórios é exibida. Antes de adicionar um diretório, certifique-se de revisar Capítulo 4, "Integrando ao seu Diretório Corporativo", na página 43, "Integrando com o Active Directory", na página 45 e "Integrar um diretório LDAP ao serviço", na página 60 para conhecer os requisitos e as limitações.

8 Clique na guia **Gerenciamento de Identidade e Acesso**.

9 Clique em **Instalar > Atributos de Usuário** para selecionar os atributos de usuário a serem sincronizados com o diretório.

Os atributos padrão são listados e você pode selecionar os necessárias. Se um atributo for marcado como necessário, somente os usuários com esse atributo serão sincronizados com o serviço. Você também pode adicionar outros atributos.

Importante Depois que um diretório é criado, você não pode alterar um atributo para que ele seja necessário. Você deve fazer essa seleção agora.

Além disso, esteja ciente de que as definições na página Atributos de Usuário se aplicam a todos os diretórios no serviço. Quando você marca um atributo como necessário, considere o impacto em outros diretórios. Se um atributo for marcado como necessário, os usuários sem esse atributo não serão sincronizados com o serviço.

Importante Se você pretende sincronizar recursos do XenApp para o VMware Identity Manager, torne o **distinguishedName** um atributo obrigatório.

10 Clique em **Salvar**.

11 Clique na guia **Gerenciamento de Identidade e Acesso**.

12 Na página Diretórios, clique em **Adicionar Diretório** e selecione **Adicionar Active Directory sobre LDAP/IWA** ou **Adicionar Diretório LDAP**, dependendo do tipo de diretório que você está integrando.

Você também pode criar um diretório local no serviço. Para obter mais informações sobre o uso de diretórios locais, consulte Capítulo 5, "Usando diretórios locais", na página 65.

13 Para o Active Directory, siga estas etapas.

a Insira um nome para o diretório que você está criando no VMware Identity Manager e selecione o tipo de diretório, **Active Directory sobre LDAP** ou **Active Directory (Autenticação Integrada do Windows)**.

b Forneça as informações de conexão.

Opção	Descrição
Active Directory sobre LDAP	1 No campo **Sincronizar Conector**, selecione o conector que você deseja usar para sincronizar usuários e grupos do Active Directory com o diretório do VMware Identity Manager. Um componente de conector está sempre disponível com o serviço do VMware Identity Manager por padrão. Esse conector é exibido na lista suspensa. Se você instalar vários appliances do VMware Identity Manager para alta disponibilidade, o componente de conector de cada um deles será exibido na lista. 2 No campo **Autenticação**, selecione **Sim** se você desejar usar esse Active Directory para autenticar usuários. Se você desejar usar um provedor de identidade de terceiros para autenticar usuários, clique em **Não**. Depois de configurar a conexão do Active Directory para sincronizar usuários e grupos, acesse a página **Gerenciamento de Identidade e Acesso > Gerenciar > Provedores de Identidade** para adicionar o provedor de identidade de terceiros para autenticação. 3 No campo **Atributo de Pesquisa do Diretório**, selecione o atributo de conta que contém o nome de usuário. 4 Se o Active Directory usar a pesquisa Localização do serviço DNS, faça as seleções a seguir. ■ Na seção **Local do Servidor**, marque a caixa de seleção **Esse diretório suporta localização do serviço DNS**. Será criado um arquivo `domain_krb.properties`, preenchido automaticamente com uma lista de controladores de domínio, quando o diretório for criado. Consulte "Sobre a seleção do controlador de domínio (domain_krb.properties file)", na página 47. ■ Se o Active Directory exigir criptografia STARTTLS, marque a caixa de seleção **Esse diretório requer que todas as conexões usem SSL** na seção **Certificados** e copie e cole o certificado da CA raiz do Active Directory no campo **Certificado SSL**. Verifique se o certificado está no formato PEM e inclui as linhas "BEGIN CERTIFICATE" e "END CERTIFICATE". **Observação** Se o Active Directory exigir STARTTLS e o certificado não for fornecido, você não poderá criar o diretório. 5 Se o Active Directory não usar a pesquisa de Localização do Serviço DNS, faça as seleções a seguir. ■ Na seção **Local do Servidor**, verifique se a caixa de seleção **Esse diretório suporta localização do serviço DNS** está desmarcada e insira o nome do host e o número da porta do servidor do Active Directory. Para configurar o diretório como um catálogo global, consulte a seção Ambiente de vários domínios em única floresta do Active Directory em "Ambientes do Active Directory", na página 45. ■ Se o Active Directory exigir acesso por SSL, marque a caixa de seleção **Esse diretório requer que todas as conexões usem SSL** na seção **Certificados** e copie e cole o certificado da CA raiz do Active Directory no campo **Certificado SSL**. Verifique se o certificado está no formato PEM e inclui as linhas "BEGIN CERTIFICATE" e "END CERTIFICATE".

Opção	Descrição
	Observação Se o Active Directory exigir SSL e o certificado não for fornecido, você não poderá criar o diretório. 6 Na seção **Permitir Alteração de Senha**, selecione **Ativar a Alteração de Senha** se você desejar permitir que os usuários redefinam as próprias senhas na página de login do VMware Identity Manager caso a senha expire ou se o administrador do Active Directory redefinirá a senha do usuário. 7 No campo **DN Base**, insira o DN do qual iniciar as pesquisas de conta. Por exemplo, OU=myUnit,DC=myCorp,DC=com. 8 No campo **DN Bind**, insira a conta que pode pesquisar usuários. Por exemplo, CN=binduser,OU=myUnit,DC=myCorp,DC=com. **Observação** É recomendável usar uma conta de usuário DN Bind com uma senha que não expire. 9 Depois de inserir a Senha do bind, clique em **Testar Conexão** para verificar se o diretório consegue se conectar ao seu Active Directory.
Active Directory (Autenticação Integrada do Windows)	1 No campo **Sincronizar Conector**, selecione o conector que você deseja usar para sincronizar usuários e grupos do Active Directory com o diretório do VMware Identity Manager. Um componente de conector está sempre disponível com o serviço do VMware Identity Manager por padrão. Esse conector é exibido na lista suspensa. Se você instalar vários appliances do VMware Identity Manager para alta disponibilidade, o componente de conector de cada um deles será exibido na lista. 2 No campo **Autenticação**, se você desejar usar esse Active Directory para autenticar usuários, clique em **Sim**. Se você desejar usar um provedor de identidade de terceiros para autenticar usuários, clique em **Não**. Depois de configurar a conexão do Active Directory para sincronizar usuários e grupos, acesse a página **Gerenciamento de Identidade e Acesso > Gerenciar > Provedores de Identidade** para adicionar o provedor de identidade de terceiros para autenticação. 3 No campo **Atributo de Pesquisa do Diretório**, selecione o atributo de conta que contém o nome de usuário. 4 Se o Active Directory exigir criptografia STARTTLS, marque a caixa de seleção **Esse diretório requer que todas as conexões usem STARTTLS** na seção **Certificados** e copie e cole o certificado da CA raiz do Active Directory no campo **Certificado SSL**. Verifique se o certificado está no formato PEM e inclui as linhas “BEGIN CERTIFICATE” e “END CERTIFICATE”. Se o diretório tiver vários domínios, adicione os certificados da CA raiz a todos os domínios, um por vez. **Observação** Se o Active Directory exigir STARTTLS e o certificado não for fornecido, você não poderá criar o diretório. 5 Insira o nome do domínio do Active Directory no qual ingressar. Insira um nome de usuário e uma senha que tenha o direito de ingressar no domínio. Consulte “Permissões necessárias para se ingressar em um domínio”, na página 52 para obter mais informações. 6 Na seção **Permitir Alteração de Senha**, selecione **Ativar a Alteração de Senha** se você desejar permitir que os usuários redefinam as próprias senhas na página de login do VMware Identity Manager caso a senha expire ou se o administrador do Active Directory redefinirá a senha do usuário. 7 No campo **UPN do usuário do bind**, insira o Nome principal do usuário que pode se autenticar no domínio. Por exemplo, nomedeusuario@exemplo.com. **Observação** É recomendável usar uma conta de usuário DN Bind com uma senha que não expire.

Opção	Descrição
	8 Insira a senha do Usuário do DN de associação.

c Clique em **Salvar e Avançar**.

É exibida a página com a lista de domínios.

14 Para diretórios LDAP, siga estas etapas.

a Forneça as informações de conexão.

Opção	Descrição
Nome do diretório	Um nome para o diretório que você está criando no VMware Identity Manager.
Sincronização e Autenticação do Diretório	1 No campo **Sincronizar Conector**, selecione o conector que você deseja usar para sincronizar usuários e grupos a partir de seu diretório LDAP para o diretório do VMware Identity Manager. Um componente de conector está sempre disponível com o serviço do VMware Identity Manager por padrão. Esse conector é exibido na lista suspensa. Se você instalar vários appliances do VMware Identity Manager para alta disponibilidade, o componente de conector de cada um deles será exibido na lista. Você não precisa de um conector separado para um diretório LDAP. Um conector pode ser compatível com vários diretórios, independentemente se eles são diretórios do Active Directory ou LDAP. 2 No campo **Autenticação**, selecione **Sim** se você desejar usar esse diretório LDAP para autenticar usuários. Se você desejar usar um provedor de identidade de terceiros para autenticar usuários, selecione **Não**. Após adicionar a conexão de diretório para sincronizar usuários e grupos, vá para a página **Gerenciamento de Identidade e Acesso > Gerenciar > Provedores de Identidade** para adicionar o provedor de identidade de terceiros para a autenticação. 3 No campo **Atributo de Pesquisa do Diretório**, especifique o atributo de diretório LDAP a ser usado para nomes de usuário. Se o atributo não estiver listado, selecione **Personalizado** e digite o nome do atributo. Por exemplo, **`cn`**.
Localização de Servidor	Insira o número de porta e o host do servidor do Diretório LDAP. Para o host do servidor, você pode especificar o nome de domínio totalmente qualificado ou o endereço IP. Por exemplo, **`meuservidorLDAP.exemplo.com`** ou **`100.00.00.0`**. Se você tiver um cluster de servidores atrás de um balanceador de carga, digite as informações do balanceador de carga.
Configuração LDAP	Especifique os atributos e os filtros de pesquisa LDAP que o VMware Identity Manager pode usar para consultar seu diretório LDAP. Os valores padrão são fornecidos com base no esquema LDAP principal. **Consultas LDAP** ■ **Obter grupos**: o filtro de pesquisa para a obtenção de objetos de grupo. Por exemplo: **`(objectClass=group)`** ■ **Obter usuário de associação**: o filtro de pesquisa para a obtenção do objeto de usuário de associação, quer dizer, o usuário que pode associar-se ao diretório. Por exemplo: **`(objectClass=person)`** ■ **Obter usuário**: o filtro de pesquisa para a obtenção de usuários para sincronização. Por exemplo: **`(&(objectClass=user)(objectCategory=person))`** **Atributos** ■ **Associação**: o atributo usado em seu diretório LDAP para a definição dos membros de um grupo. Por exemplo: **`member`**

Opção	Descrição
	■ **UUID de objeto**: o atributo usado em seu diretório LDAP para a definição do UUID de um usuário ou grupo. Por exemplo: **`entryUUID`** ■ **Nome Distinto**: o atributo usado em seu diretório LDAP para o nome distinto de um usuário ou grupo. Por exemplo: **`entryDN`**
Certificados	Se o seu diretório LDAP requer acesso via SSL, selecione **Esse diretório requer que todas as conexões usem SSL** e copie e cole o certificado SSL da CA raiz do servidor do diretório LDAP. Verifique se o certificado está no formato PEM e inclui as linhas "BEGIN CERTIFICATE" e "END CERTIFICATE".
Associar detalhes do usuário	**DN base**: digite o DN do qual se deseja iniciar as pesquisas. Por exemplo, cn=users,dc=example,dc=com **DN de associação**: digite o nome de usuário a ser usado para vinculação ao diretório LDAP. **Observação** É recomendável usar uma conta de usuário DN Bind com uma senha que não expire. **Senha do DN de associação**: digite a senha para o usuário do DN de associação.

b Para testar a conexão com o servidor do diretório LDAP, clique em **Testar Conexão**.

Se a conexão não for bem-sucedida, verifique as informações que você inseriu e faça as alterações adequadas.

c Clique em **Salvar e Avançar**.

A página que lista o domínio é exibida.

15 Para um diretório LDAP, o domínio é listado e não pode ser modificado.

Para Active Directory sobre LDAP, os domínios são listados e não podem ser modificados.

Para o Active Directory (Autenticação Integrada do Windows), selecione os domínios que devem ser associados com esta conexão do Active Directory.

Observação Se você adicionar um domínio confiante após o diretório ser criado, o serviço não detecta automaticamente o domínio recém confiante. Para habilitar o serviço para detectar o domínio, o conector deve sair e, em seguida, voltar a ingressar no domínio. Quando o conector reingressa no domínio, o domínio de confiança aparece na lista.

Clique em **Avançar**.

16 Verifique se os nomes de atributo do VMware Identity Manager estão mapeados para os atributos corretos do Active Directory ou do LDAP e, se necessário, faça alterações.

Importante Se você estiver integrando um diretório LDAP, deverá especificar um mapeamento para o atributo **domain**.

17 Clique em **Avançar**.

18 Selecione os grupos que você deseja sincronizar do seu diretório do Active Directory ou LDAP para o diretório do VMware Identity Manager.

Opção	Descrição
Especificar os DNs de grupo	Para selecionar grupos, especifique um ou mais DNs de grupo e selecione os grupos sob eles. a Clique em **+** e especifique o DN de grupo. Por exemplo, CN=users,DC=example,DC=company,DC=com. **Importante** Especifique os DNs de grupo que estão sob o DN Base que você digitou. Se um DN de grupo estiver fora do DN Base, os usuários desse DN serão sincronizados, mas não poderão fazer login. b Clique em **Encontrar Grupos**. A coluna **Grupos a Sincronizar** lista o número de grupos encontrados no DN. c Para selecionar todos os grupos no DN, clique em **Selecionar Tudo**; caso contrário, clique em **Selecionar** e selecione os grupos específicos a serem sincronizados. **Observação** Se você tiver vários grupos com o mesmo nome no seu diretório LDAP, especifique nomes exclusivos para eles no VMware Identity Manager. Você pode alterar o nome ao selecionar o grupo. **Observação** Quando você sincroniza um grupo, todos os usuários que não possuem Usuários de Domínio como grupo primário no Active Directory não são sincronizados.
Sincronizar membros reunidos do grupo	A opção **Sincronizar membros reunidos do grupo** é ativada por padrão. Quando essa opção está ativada, todos os usuários que pertencem diretamente ao grupo que você selecionar, bem como todos os usuários que pertencem aos grupos aninhados abaixo dele, serão sincronizados. Observe que os grupos aninhados não são sincronizados; somente os usuários que pertencem aos grupos aninhados são sincronizados. No diretório do VMware Identity Manager, esses usuários serão membros do grupo principal que você selecionou para sincronização. Se a opção **Sincronizar membros reunidos do grupo** estiver desativada, quando você especificar um grupo para a sincronização, todos os usuários que pertencerem diretamente a esse grupo serão sincronizados. Os usuários que pertencem a grupos aninhados abaixo dele não são sincronizados. Desativar essa opção é útil para grandes configurações do Active Directory nas quais passar por uma árvore de grupos exige muitos recursos e tempo. Se você desativá-la, certifique-se de selecionar todos os grupos cujos usuários deseja sincronizar.

19 Clique em **Avançar**.

20 Especifique usuários adicionais para sincronizar, se necessário.

a Clique em **+** e insira os DNs de usuário. Por exemplo, CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com.

Importante Especifique os DNs de usuário que estão sob o DN Base que você digitou. Se um DN de usuário estiver fora do DN Base, os usuários desse DN serão sincronizados, mas não poderão fazer login.

b (Opcional) Para excluir usuários, clique em um filtro para excluir alguns tipos de usuários.

Você seleciona o atributo do usuário a ser usado para filtragem, a regra de consulta e o valor.

21 Clique em **Avançar**.

22 Revise a página para ver quantos usuários e grupos serão sincronizados com o diretório e para exibir a agenda de sincronização.

Para fazer alterações em usuários e grupos, ou na frequência de sincronização, clique nos links **Editar**.

23 Clique em **Sincronizar diretório** para iniciar a sincronização de diretório.

Observação Se ocorrer um erro de rede e o nome do host não puder ser resolvido de forma exclusiva usando o DNS reverso, o processo de configuração será interrompido. Você deverá corrigir os problemas de rede e reiniciar o appliance virtual. Em seguida, poderá continuar o processo de implantação. As novas configurações de rede não estarão disponíveis antes do reinício do appliance virtual.

Próximo passo

Para obter informações sobre como configurar um balanceador de carga ou uma configuração de alta disponibilidade, consulte Capítulo 6, "Configuração avançada do appliance do VMware Identity Manager", na página 73.

Você pode personalizar o catálogo de recursos para os aplicativos da sua organização e permitir o acesso do usuário a esses recursos. Você também pode configurar outros recursos, incluindo o View, o ThinApp e os aplicativos baseados no Citrix. Consulte *Configurando recursos no VMware Identity Manager*.

Definindo as configurações do servidor proxy para o VMware Identity Manager

O appliance virtual do VMware Identity Manager acessa o catálogo de aplicativos em nuvem e outros serviços da Web na Internet. Se a sua configuração de rede fornece acesso à Internet por meio de um proxy HTTP, você deve ajustar suas configurações de proxy no appliance do VMware Identity Manager.

Habilite seu proxy para lidar apenas com o tráfego da Internet. Para garantir que o proxy seja configurado corretamente, defina o parâmetro para o tráfego interno como `no–proxy` no domínio.

Observação Os servidores proxy que exigem autenticação não são suportados.

Procedimentos

1 No cliente vSphere, faça login como o usuário raiz no appliance virtual do VMware Identity Manager.

2 Insira `YaST` na linha de comando para executar o utilitário `YaST`.

3 Selecione **Serviços de Rede** no painel esquerdo e selecione **Proxy**.

4 Insira as URLs do servidor proxy nos campos **URL do Proxy HTTP** e **URL do Proxy HTTPS**.

5 Selecione **Concluir** e saia do utilitário do `YaST`.

6 Reinicie o servidor Tomcat no appliance virtual do VMware Identity Manager para usar as novas configurações de proxy.

```
service horizon–workspace restart
```

O catálogo de aplicativos na nuvem e outros serviços da Web já estão disponíveis no VMware Identity Manager.

Inserir a chave de licença

Depois de implantar o appliance do VMware Identity Manager, insira a sua chave de licença.

Procedimentos

1 Faça login no console de administração do VMware Identity Manager.

2 Selecione a guia **Configurações do Appliance** e clique em **Licença**.

3 Na página Configurações de Licença, insira a chave de licença e clique em **Salvar**.

Gerenciando as definições de configuração do sistema do appliance

3

Após a conclusão da configuração inicial do appliance, você poderá acessar as páginas de administração do appliance para instalar certificados, gerenciar senhas e monitorar as informações do sistema do appliance virtual.

Você também pode atualizar o banco de dados, o FQDN e o syslog, além de fazer download de arquivos de log.

Nome da página	Descrição da definição
Conexão do Banco de Dados	A configuração da conexão do banco de dados, Interno ou Externo, é ativada. Você pode alterar o tipo do banco de dados. Ao selecionar Banco de Dados Externo, insira a URL, o nome de usuário e a senha do banco de dados externo. Para configurar um banco de dados externo, consulte "Conectando-se ao banco de dados", na página 32.
Instalar Certificado	Nessa página você instala um certificado autoassinado ou personalizado para o VMware Identity Manager e, se o VMware Identity Manager estiver configurado com um balanceador de carga, você poderá instalar o certificado raiz do balanceador de carga. A localização do certificado da CA raiz do VMware Identity Manager é mostrada nessa página, bem como na guia **Encerrar o SSL em um Balanceador de Carga**. Consulte "Usando certificados SSL", na página 36.
FQDN do Identity Manager	FQDN do VMware Identity Manager é mostrado nessa página. Você pode modificá-lo. O FQDN do VMware Identity Manager é a URL que os usuários utilizam para acessar o serviço.
Configurar Syslog	Nesta página, você pode ativar um servidor syslog externo. Os logs do VMware Identity Manager são enviados para esse servidor externo. Consulte "Ativar o servidor syslog", na página 39.
Alterar Senha	Nessa página, você pode alterar a senha do usuário administrador do VMware Identity Manager.
Segurança do Sistema	Nessa página, você pode alterar a senha root do appliance do VMware Identity Manager e a senha do usuário ssh usada para fazer login remotamente.
Localizações do Arquivo de Log	Uma lista dos arquivos de log e das respectivas localizações de diretório é exibida nessa página. Você pode empacotar os arquivos de log em um arquivo zip para download. Consulte "Informações de arquivo de log", na página 39.

Você também pode modificar a URL do conector. Consulte "Modificar a URL do conector", na página 39.

Este capítulo inclui os seguintes tópicos:

Alterar as configurações do appliance

Depois de configurar o VMware Identity Manager, você poderá acessar as páginas Configurações do Appliance para atualizar a configuração atual e monitorar as informações do sistema do appliance virtual.

Procedimentos

1 Faça login no console de administração.

2 Selecione a guia **Configurações do Appliance** e clique em **Gerenciar Configuração**.

3 Faça login com a senha do administrador do serviço.

4 No painel esquerdo, selecione a página a ser exibida ou editada.

Próximo passo

Verifique se as configurações ou as atualizações que você realizou estão em vigor.

Conectando-se ao banco de dados

Um banco de dados PostgreSQL interno é embutido no appliance do VMware Identity Manager mas este não é recomendado para uso com implantações de produção. Para usar um banco de dados externo com o VMware Identity Manager, o administrador do seu banco de dados deve preparar um banco de dados e um esquema vazios antes de se conectar ao banco de dados no VMware Identity Manager.

Você pode conectar-se à conexão de banco de dados externo ao executar o assistente de Instalação do VMware Identity Manager. Você também pode ir à página Configurações do Appliance > Configuração da VA > Instalação da Conexão do Banco de Dados para configurar a conexão com o banco de dados externo.

Os usuários licenciados podem usar um banco de dados Oracle externo ou um Microsoft SQL Server para criar um ambiente de banco de dados de alta disponibilidade.

Configurar um banco de dados Microsoft SQL

Para usar um banco de dados Microsoft SQL para o VMware Identity Manager, você deve criar um novo banco de dados no Microsoft SQL Server.

Crie um banco de dados chamado **saas** no Microsoft SQL Server e crie um usuário de login chamado **horizon**.

Observação O agrupamento padrão diferencia maiúsculas de minúsculas.

Pré-requisitos

- Uma versão compatível do Microsoft SQL Server instalado como um servidor de banco de dados externo.
- Uma implementação de balanceamento de carga configurada.
- Direitos do administrador para acessar e criar os componentes de banco de dados usando o Microsoft SQL Server Management Studio ou de outro cliente CLI do Microsoft SQL Server.

Procedimentos

1 Faça login na sessão do Microsoft SQL Server Management Studio como sysadmin ou usando uma conta de usuário com privilégios sysadmin.

É exibida a janela do editor.

2 Na barra de ferramentas, clique em **Nova Consulta**.

3 Recorte e cole os comandos a seguir na janela do editor.

Comandos do Microsoft SQL

```
CREATE DATABASE saas
COLLATE Latin1_General_CS_AS;
ALTER DATABASE saas SET READ_COMMITTED_SNAPSHOT ON;
GO
BEGIN
CREATE LOGIN horizon WITH PASSWORD = N'H0rizon!';
END
GO
USE saas;
IF EXISTS (SELECT * FROM sys.database_principals WHERE name = N'horizon')
DROP USER [horizon]
GO
CREATE USER horizon FOR LOGIN horizon
WITH DEFAULT_SCHEMA = saas;
GO
CREATE SCHEMA saas AUTHORIZATION horizon
GRANT ALL ON DATABASE::saas TO horizon;
GO
```

4 Na barra de ferramentas, clique em **!Execute**.

O servidor de banco de dados Microsoft SQL está agora pronto para ser conectado ao banco de dados do VMware Identity Manager

Próximo passo

Configure o banco de dados externo no servidor do VMware Identity Manager. Acesse a página Configurações do Appliance > Configuração da VA > Instalação da Conexão do Banco de Dados do console de administração do VMware Identity Manager. Insira a URL do JDBC como **`jdbc:sqlserver://<hostname-or-DB_VM_IP_ADDR>;DatabaseName=saas`**. Insira o nome de usuário e a senha criados para o banco de dados. Consulte "Configurar o VMware Identity Manager para usar um banco de dados externo", na página 35

Configurar um banco de dados Oracle

Durante a instalação do banco de dados Oracle, você deve especificar determinadas configurações do Oracle para obter um melhor desempenho com o VMware Identity Manager.

Pré-requisitos

O banco de dados Oracle que você criar será chamado `saas`. O VMware Identity Manager exige a identificadores do Oracle entre aspas para o nome de usuário e o esquema. Portanto, você deve usar aspas duplas ao criar o nome de usuário e o esquema `saas` do Oracle.

Procedimentos

1 Especifique as configurações a seguir quando criar um banco de dados Oracle.

   a Selecione a opção de configuração **Bando de Dados para Fins Gerais/Processamento de Transações**.

   b Clique em **Usar Unicode > UTF8**.

   c Use o Conjunto de Caracteres Nacionais.

2 Conecte-se ao banco de dados Oracle após a conclusão da instalação.

3 Conecte-se ao banco de dados Oracle como o usuário sys.

4 Aumente as conexões do processo. Cada máquina virtual de serviço adicional exige um mínimo de 300 conexões de processo para funcionar com o VMware Identity Manager. Por exemplo, se o seu ambiente tiver duas máquinas virtuais de serviço, execute o comando `alter` como o usuário sys ou do sistema.

   a Aumente as conexões de processo usando o comando `alter`.

   ```
   alter system set processes=600 scope=spfile
   ```

   b Reinicie o banco de dados.

5 Crie um gatilho de banco de dados que todos os usuários possam usar.

SQL de amostra para criar um gatilho de banco de dados

```
CREATE OR REPLACE
TRIGGER CASE_INSENSITIVE_ONLOGON
AFTER LOGON ON DATABASE
DECLARE
username VARCHAR2(30);
BEGIN
username:=SYS_CONTEXT('USERENV','SESSION_USER');
IF username = 'saas' THEN
execute immediate 'alter session set NLS_SORT=BINARY_CI';
execute immediate 'alter session set NLS_COMP=LINGUISTIC';
END IF;
EXCEPTION
WHEN OTHERS THEN
NULL;
END;
```

6 Execute os comandos do Oracle para criar um novo esquema de usuário.

SQL de amostra para criar um novo usuário

```
CREATE USER "saas"
IDENTIFIED BY <password>
DEFAULT TABLESPACE USERS
TEMPORARY TABLESPACE TEMP
PROFILE DEFAULT
ACCOUNT UNLOCK;
GRANT RESOURCE TO "saas" ;
GRANT CONNECT TO "saas" ;
ALTER USER "saas" DEFAULT ROLE ALL;
GRANT UNLIMITED TABLESPACE TO "saas";
```

Administrando o banco de dados interno

O banco de dados interno PostgreSQL já vem configurado e pronto para ser usado. Observe que o banco de dados interno não é recomendado para uso com implantações de produção.

Quando o VMware Identity Manager é instalado e ativado, durante o processo de inicialização, é gerada uma senha aleatória para o banco de dados interno. Esta senha é exclusiva para cada implantação e pode ser encontrada no arquivo `/usr/local/horizon/conf/db.pwd`.

Para configurar seu banco de dados interno para alta disponibilidade, veja KB 2094258.

Configurar o VMware Identity Manager para usar um banco de dados externo

Depois de configurar o banco de dados no assistente de Instalação do VMware Identity Manager, você poderá configurar o VMware Identity Manager para usar um banco de dados diferente.

Você deve apontar o VMware Identity Manager para um banco de dados preenchido e inicializado. Por exemplo, você pode usar um banco de dados configurado como o resultado de uma execução bem-sucedida do Assistente de Instalação do VMware Identity Manager, um banco de dados de um backup ou um banco de dados existente de um snapshot recuperado.

Pré-requisitos

- Instale e configure a edição compatível do Microsoft SQL ou do Oracle como o servidor do banco de dados externo. Para obter informações sobre versões específicas compatíveis com o VMware Identity Manager, consulte as Matrizes de interoperabilidade entre produtos VMware em http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Procedimentos

1 No console de administração, clique em **Configurações do Appliance** e selecione **Configuração do VA**.

2 Clique em **Gerenciar Configuração**.

3 Faça login com a senha do administrador do VMware Identity Manager.

4 Na página Instalação da Conexão do Banco de Dados, selecione **Banco de Dados Externo** como o tipo de banco de dados.

5 Insira as informações sobre a conexão do banco de dados.

a Digite a URL do JDBC do servidor de banco de dados.

Microsoft SQL	`jdbc:sqlserver://hostname_or_IP_address;DatabaseName=horizon`
Oracle	`jdbc:oracle:thin:@//hostname_or_IP_address:port/sid`

b Digite o nome do usuário com privilégios de leitura e gravação no banco de dados.

Microsoft SQL	`horizon`
Oracle	“saas”

c Digite a senha do usuário criado quando você configurou o banco de dados.

6 Clique em **Testar Conexão** para verificar e salvar as informações.

Usando certificados SSL

Quando o appliance do VMware Identity Manager é instalado, um certificado do servidor SSL padrão é gerado automaticamente. Você pode usar esse certificado autoassinado para testes gerais de sua implementação. A VMware recomenda gerar e instalar certificados SSL comerciais no seu ambiente de produção.

Uma autoridade de certificação (CA) é uma entidade confiável que garante a identidade do certificado e do respectivo criador. Quando um certificado é assinado por uma CA confiável, os usuários não receberão mais mensagens solicitando a verificação do certificado.

Se você implantar o VMware Identity Manager com o certificado SSL autoassinado, o certificado da CA raiz deverá estar disponível como uma CA confiável para qualquer cliente que acessa o VMware Identity Manager. Os clientes podem incluir máquinas do usuário final, balanceadores de carga, proxies etc. Você pode fazer download da CA raiz em *https://meuconector.domínio.com/horizon_workspace_rootca.pem*.

Você pode instalar um certificado CA assinado na página **Configurações do Appliance > Gerenciar Configuração > Instalar Certificado**. Você também pode adicionar o certificado da CA raiz do balanceador de carga nessa página.

Aplicar Autoridade de Certificação Pública

Quando é instalado o serviço do VMware Identity Manager, é gerado o certificado padrão do servidor SSL. Você pode usar o certificado padrão para fins de teste. Você deve gerar certificados SSL comerciais para o seu ambiente e instalá-los nele.

Observação Se o do VMware Identity Manager apontar para um balanceador de carga, o certificado SSL será aplicado ao balanceador de carga.

Pré-requisitos

Gere uma solicitação de assinatura de certificado (CSR) e obtenha um certificado válido assinado por uma autoridade de certificação. Se a sua organização fornecer certificados SSL assinados por uma autoridade de certificação, você poderá usar esses certificados. O certificado deve estar no formato PEM.

Procedimentos

1 No console de administração, clique em **Configurações do Appliance**.

A configuração VA é selecionada por padrão.

2 Clique em **Gerenciar Configuração**.

3 Na caixa de diálogo exibida, insira a senha do usuário administrador do servidor do VMware Identity Manager.

4 Selecione **Instalar Certificado**.

5 Em Encerrar SSL na guia Appliance do Identity Manager, selecione **Certificado Personalizado**.

6 Na caixa de texto **Cadeia de Certificados SSL**, cole os certificados intermediários, de host e de raiz, nessa ordem.

O certificado SSL somente funcionará se você incluir toda a cadeia de certificados na ordem correta. Para cada certificado, copie tudo que estiver entre as linhas -----INICIAR CERTIFICADO----- e -----FINALIZAR CERTIFICADO----, incluindo-as

Verifique se o certificado inclui o nome do host FQDN.

7 Cole a chave privada na caixa de texto Chave Privada. Copie tudo entre ----INICIAR CHAVE PRIVADA RSA e ---FINALIZAR CHAVE PRIVADA RSA.

8 Clique em **Salvar.**

Exemplo: Exemplos de certificados

Exemplo de cadeia de certificados
-----INICIAR CERTIFICADO-----
jlQvt9WdR9Vpg3WQT5+C3HU17bUOwvhp/r0+ ... ... W53+O05j5xsxzDJfWr1lqBlFF/OkIYCPcyK1
-----FINALIZAR CERTIFICADO-----
-----INICIAR CERTIFICADO-----
WdR9Vpg3WQT5+C3HU17bUOwvhp/rjlQvt90+ ... ... O05j5xsxzDJfWr1lqBlFF/OkIYCPW53+cyK1
-----FINALIZAR CERTIFICADO-----
-----INICIAR CERTIFICADO-----
dR9Vpg3WQTjlQvt9W5+C3HU17bUOwvhp/r0+ ... ... 5j5xsxzDJfWr1lqW53+O0BlFF/OkIYCPcyK1
-----FINALIZAR CERTIFICADO-----

Exemplo de chave privada
-----INICIAR CHAVE PRIVADA RSA-----
jlQvtg3WQT5+C3HU17bU9WdR9VpOwvhp/r0+ ... ... 1lqBlFFW53+O05j5xsxzDJfWr/OkIYCPcyK1
-----FINALIZAR CHAVE PRIVADA RSA-----

Adicionando certificados SSL

Quando você aplicar o certificado, verifique se incluiu toda a cadeia de certificados. O certificado a ser instalado deve estar no formato PEM.

O certificado SSL funcionará somente se você incluir toda a cadeia de certificados. Para cada certificado, copie tudo que estiver entre e incluindo as linhas -----BEGIN CERTIFICATE----- e -----END CERTIFICATE----.

Importante Você deve adicionar a cadeia de certificados na ordem de Certificado SSL, Certificados da CA Intermediária, Certificado da CA Raiz.

Exemplo de cadeia de certificados
-----INICIAR CERTIFICADO-----
SSL Cert - Appliance SSL Cert
-----FINALIZAR CERTIFICADO-----
-----INICIAR CERTIFICADO-----
Intermediate/Issuing CA Cert
-----FINALIZAR CERTIFICADO-----
-----INICIAR CERTIFICADO-----
Root CA Cert
-----FINALIZAR CERTIFICADO-----

Modificar a URL do serviço do VMware Identity Manager

Você pode alterar a URL do serviço do VMware Identity Manager, que é a URL que os usuários usam para acessar o serviço. Por exemplo, você pode alterar a URL para uma URL do balanceador de carga.

Procedimentos

1 Faça login no console de administração do VMware Identity Manager.

2 Clique na guia **Configurações do Appliance** e selecione **Configuração da VA**.

3 Clique em **Gerenciar Configuração** e faça login com a senha do usuário **`administrador`**.

4 Clique em **FQDN do Identity Manager** e insira a nova URL no campo **FQDN do Identity Manager**.

Use o formato **`https://FQDN:porta`**. A especificação de uma porta é opcional. A porta padrão é 443.

Por exemplo, **`https://meuserviço.exemplo.com`**.

5 Clique em **Salvar**.

Próximo passo

Ative a nova interface do usuário do portal.

1 Acesse https://*URLdoVMwareIdentityManager*/admin para acessar o console de administração.

2 No console de administração, clique na seta na guia **Catálogo** e selecione **Configurações**.

3 Selecione **Nova Interface de Usuário do Portal para o Usuário Final** no painel à esquerda e clique em **Habilitar Nova Interface de Usuário do Portal**.

Modificar a URL do conector

Você pode alterar a URL do conector atualizando o nome do host do provedor de identidade no console de administração. Se você estiver usando o conector como o provedor de identidade, a URL do conector será a URL da página de login e será visível para os usuários finais.

Procedimentos

1 Faça login no console de administração do VMware Identity Manager.

2 Clique na guia **Gerenciamento de Identidade e Acesso** e, em seguida, clique na guia **Provedores de Identidade**.

3 Na página Provedores de Identidade, selecione o provedor de identidade a ser atualizado.

4 No campo **Nome do Host IdP**, insira o novo nome do host.

Use o formato ***`nome do host:porta`***. A especificação de uma porta é opcional. A porta padrão é 443.

Por exemplo, **`vidm.exemplo.com`**.

5 Clique em **Salvar**.

Ativar o servidor syslog

Os eventos a nível de aplicativo do serviço podem ser exportados para um servidor syslog externo. Os eventos do sistema operacional não são exportados.

Como a maioria das empresas não têm espaço em disco ilimitado, o appliance virtual não salva o histórico de log completo. Se desejar salvar mais histórico ou criar uma localização centralizada para o seu histórico de log, você poderá configurar um servidor syslog externo.

Se não especificar um servidor syslog durante a configuração inicial, você poderá configurá-lo mais tarde na página **Configurações do Appliance > Configuração da VA > Gerenciar Configuração > Configuração do Syslog**.

Pré-requisitos

Configure um servidor syslog externo. Você pode usar qualquer um dos servidores syslog padrão disponíveis. Vários servidores syslog incluem capacidades avançadas de pesquisa.

Procedimentos

1 Faça login no console de administração.

2 Clique na guia **Configurações do Appliance**, selecione **Configuração da VA** no painel à esquerda e clique em **Gerenciar Configuração**.

3 Selecione **Configurar Syslog** no painel à esquerda.

4 Clique em **Ativar**.

5 Insira o endereço IP ou o FQDN do servidor syslog no qual você deseja armazenar os logs.

6 Clique em **Salvar.**

Uma cópia dos logs é enviada para o servidor syslog.

Informações de arquivo de log

Os arquivos de log do VMware Identity Manager pode ajudar a depurar e solucionar problemas. Os arquivos de log listados abaixo são um ponto de partida comum. Logs adicionais podem ser encontrados no diretório `/opt/vmware/horizon/workspace/logs`.

Tabela 3-1. Arquivos de log

Componente	Localização do arquivo de log	Descrição
Logs do serviço do Identity Manager	`/opt/vmware/horizon/workspace/logs/horizon.log`	Informações sobre a atividade do aplicativo VMware Identity Manager, como direitos, usuários e grupos.
Logs do Configurador	`/opt/vmware/horizon/workspace/logs/configurator.log`	Solicita que o Configurador receba do cliente REST e da interface Web.
Logs do conector	`/opt/vmware/horizon/workspace/logs/connector.log`	Um registro de cada solicitação recebida da interface Web. Cada entrada de log inclui também a URL, o carimbo de data/hora e as exceções da solicitação. Nenhuma ação de sincronização é registrada.
Logs de atualização	`/opt/vmware/var/log/update.log` `/opt/vmware/var/log/vami`	Um registro das mensagens de saída relacionadas a solicitações de atualização durante uma atualização do VMware Identity Manager. Os arquivos no diretório `/opt/vmware/var/log/vami` são úteis para solução de problemas. Você pode encontrar esses arquivos em todas as máquinas virtuais após uma atualização.
Logs do Apache Tomcat	`/opt/vmware/horizon/workspace/logs/catalina.log`	O registros do Apache Tomcat de mensagens que não são registradas em outros arquivos de log.

Coletar informações de log

Durante testes ou solução de problemas, os logs podem oferecer comentários sobre a atividade e o desempenho do appliance virtual, bem como informações sobre qualquer problema que ocorra.

Colete os logs de cada appliance no seu ambiente.

Procedimentos

1 Faça login no console de administração.

2 Selecione a guia **Configurações do Appliance** e clique em **Gerenciar Configuração**.

3 Clique em **Localizações do Arquivo de Log** e em **Preparar pacote de logs**.

As informações são coletadas em um arquivo tar.gz que pode ser baixado.

4 Baixe o pacote preparado.

Próximo passo

Para coletar todos os logs, realize esse procedimento em cada appliance.

Gerenciar as suas senhas do appliance

Quando configurou o appliance virtual, você criou senhas para o usuário administrador, o usuário root e o sshuser. Você pode alterar essas senhas nas páginas Configurações do Appliance.

Certifique-se de criar senhas fortes. As senhas de alta segurança devem ter pelo menos oito caracteres e incluir letras maiúsculas e minúsculas e pelo menos um caractere numérico ou especial.

Procedimentos

1 No console de administração, clique na guia **Configurações do Appliance**.

2 Clique em **Configuração da VA > Gerenciar Configuração**.

3 Para alterar a senha de administrador, selecione **Alterar Senha**. Para alterar as senhas raiz ou sshuser, selecione **Segurança do Sistema**.

Importante A senha do usuário administrador deve ter pelo menos 6 caracteres.

4 Insira a nova senha.

5 Clique em **Salvar**.

Definir as configurações de SMTP

Defina as configurações do servidor SMTP para receber notificações por e-mail do serviço do VMware Identity Manager.

Os e-mails de notificação são enviados para novos usuários criados como usuários locais e quando uma senha é redefinida no serviço do VMware Identity Manager.

Procedimentos

1 Faça login no console de administração.

2 Selecione a guia **Configurações do Appliance** e clique em **SMTP**.

3 Insira o nome do host do servidor SMTP.

Por exemplo: `smtp.example.com`

4 Insira o número da porta do servidor SMTP.

Por exemplo: `25`

5 (Opcional) Insira um nome de usuário e uma senha caso o servidor SMTP exija autenticação.

6 Clique em **Salvar**.

Integrando ao seu Diretório Corporativo

4

Você integra o VMware Identity Manager ao seu diretório corporativo para sincronizar usuários e grupos a partir do seu diretório corporativo para o serviço do VMware Identity Manager.

Os seguintes tipos de diretórios são suportados.

- Active Directory sobre LDAP
- Active Directory, Autenticação integrada do Windows
- Diretório LDAP

Para integrar ao diretório corporativo, execute as seguintes tarefas.

- Especifique os atributos que você deseja que os usuários tenham no serviço do VMware Identity Manager.
- Crie um diretório no serviço do VMware Identity Manager do mesmo tipo que o seu diretório corporativo e especifique os detalhes de conexão.
- Mapeie os atributos do VMware Identity Manager para os atributos usados em seu diretório LDAP ou Active Directory.
- Especifique os usuários e os grupos a serem sincronizados.
- Sincronize os usuários e os grupos.

Depois de integrar o seu diretório corporativo e executar a sincronização inicial, você poderá atualizar a configuração, configurar uma agenda de sincronização para a sincronização regular ou iniciar uma sincronização a qualquer momento.

Este capítulo inclui os seguintes tópicos:

Conceitos importantes relacionados à integração de diretório

Vários conceitos são essenciais para a compreensão de como o serviço do VMware Identity Manager se integra ao seu ambiente Active Directory ou diretório LDAP.

Conector

O conector, um componente de serviço, executa as seguintes funções.

- Sincroniza os dados de usuário e grupo do seu Active Directory ou diretório LDAP com o serviço.
- Ao ser usado como um provedor de identidade, autentica os usuários para o serviço.

  O conector é o provedor de identidade padrão. Você também pode usar provedores de identidade de terceiros que suportam o protocolo SAML 2.0. Use um provedor de identidade de terceiros para um tipo de autenticação com o qual o conector não é compatível ou se o provedor de identidade de terceiros for preferível com base na sua política de segurança empresarial.

  Observação Se você usar provedores de identidade de terceiros, pode configurar o conector para sincronizar dados de usuário e de grupo ou configurar provisionamento de usuários Just-in-Time. Consulte a seção Provisionamento de usuários Just-in-Time em *Administração do VMware Identity Manager* para obter mais informações.

Diretório

O serviço do VMware Identity Manager tem o seu próprio conceito de um diretório, correspondente ao Active Directory ou ao diretório LDAP no seu ambiente. Esse diretório utiliza atributos para definir usuários e grupos. Crie um ou mais diretórios no serviço e, em seguida, sincronize-os com o Active Directory ou o diretório do LDAP. Você pode criar os seguintes tipos de diretório no serviço.

- Active Directory
  - Active Directory via LDAP. Crie este tipo de diretório se você pretende se conectar a um único ambiente de domínio do Active Directory. Para o tipo de diretório Active Directory via LDAP, o conector vincula-se ao Active Directory usando autenticação de vinculação simples.
  - Active Directory, Autenticação integrada do Windows. Crie este tipo de diretório se você pretende se conectar a um ambiente de vários domínios ou florestas do Active Directory. O conector vincula-se ao Active Directory usando a autenticação integrada do Windows.

  O tipo e o número de diretórios que você cria varia de acordo com o ambiente do Active Directory, como domínio único ou vários domínios, e do tipo de confiança usado entre os domínios. Na maioria dos ambientes, você cria um diretório.
- Diretório LDAP

O serviço não tem acesso direto ao Active Directory ou diretório LDAP. Somente o conector tem acesso direto. Portanto, você associa a uma instância do conector cada diretório criado no serviço.

Trabalhador

Quando você associa um diretório a uma instância do conector, o conector cria uma partição para o diretório associado chamado de trabalhador. Uma instância do conector pode ter vários trabalhadores associados a ela. Cada trabalhador atua como um provedor de identidade. Você define e configura os métodos de autenticação por trabalhador.

O conector sincroniza os dados de usuário e de grupo entre o Active Directory ou o diretório LDAP e o serviço usando um ou mais agentes de trabalho.

Importante Você não pode ter dois agentes de trabalho do tipo Active Directory, Autenticação Integrada do Windows na mesma instância do conector.

Considerações de segurança

Para os diretórios corporativos integrados com o serviço do VMware Identity Manager, as configurações de segurança, como regras de complexidade de senha de usuário e políticas de bloqueio de conta, devem ser definidas diretamente no diretório corporativo. O VMware Identity Manager não substitui essas configurações.

Integrando com o Active Directory

Você pode integrar o VMware Identity Manager à implantação do Active Directory para sincronizar usuários e grupos a partir do Active Directory para o VMware Identity Manager.

Consulte também "Conceitos importantes relacionados à integração de diretório", na página 44.

Ambientes do Active Directory

É possível integrar o serviço com um ambiente do Active Directory, que consiste em um único domínio do Active Directory, vários domínios em uma única floresta do Active Directory ou vários domínios em várias florestas do Active Directory.

Ambiente de domínio único do Active Directory

Uma única implantação do Active Directory permite que você sincronize usuários e grupos a partir de um único domínio do Active Directory.

Para este ambiente, ao adicionar um diretório ao serviço, selecione a opção Active Directory sobre LDAP.

Para obter mais informações, consulte:

- "Sobre a seleção do controlador de domínio (domain_krb.properties file)", na página 47
- "Gerenciando atributos de usuário sincronizados a partir do Active Directory", na página 51
- "Permissões necessárias para se ingressar em um domínio", na página 52
- "Configurando a conexão do Active Directory com o serviço", na página 53

Ambiente de vários domínios em única floresta do Active Directory

Uma implantação de vários domínios em uma única floresta do Active Directory permite que você sincronize usuários e grupos de vários domínios do Active Directory em uma única floresta.

É possível configurar o serviço para este ambiente do Active Directory como um único tipo de diretório de Autenticação Integrada do Windows no Active Directory ou, alternativamente, como um tipo de diretório Active Directory sobre LDAP configurado com a opção de catálogo global.

- A opção recomendada é criar um único tipo de diretório de Autenticação Integrada do Windows no Active Directory.

  Ao adicionar um diretório a esse ambiente, selecione a opção Active Directory (Autenticação Integrada do Windows).

  Para obter mais informações, consulte:

  - "Sobre a seleção do controlador de domínio (domain_krb.properties file)", na página 47
  - "Gerenciando atributos de usuário sincronizados a partir do Active Directory", na página 51

- "Permissões necessárias para se ingressar em um domínio", na página 52
- "Configurando a conexão do Active Directory com o serviço", na página 53

- Se a Autenticação Integrada do Windows não funcionar no seu ambiente Active Directory, crie um tipo de diretório Active Directory sobre LDAP e selecione a opção de catálogo global.

  Algumas das limitações da seleção da opção de catálogo global incluem:

  - Os atributos de objeto do Active Directory que são replicados no catálogo global são identificados no esquema do Active Directory como o conjunto de atributos parcial (PAS). Somente esses atributos estão disponíveis para o mapeamento de atributos pelo serviço. Se necessário, edite o esquema para adicionar ou remover atributos armazenados no catálogo global.
  - O catálogo global armazena a associação ao grupo (o atributo do membro) somente dos grupos universais. Somente os grupos universais são sincronizados com o serviço. Se necessário, altere o escopo de um grupo de um domínio local ou global para universal.
  - A conta do DN bind que você define ao configurar um diretório no serviço deve ter permissões para ler o atributo Token-Groups-Global-And-Universal (TGGAU).

  O Active Directory usa as portas 389 e 636 para consultas LDAP padrão. Para as consultas do catálogo global, as portas 3268 e 3269 são usadas.

  Quando você adicionar um diretório para o ambiente do catálogo global, especifique as informações a seguir durante a configuração.

  - Selecione a opção Active Directory sobre LDAP.
  - Desmarque a caixa de seleção da opção **Esse diretório suporta localização do serviço DNS**.
  - Selecione a opção **Este diretório tem um catálogo global**. Quando você seleciona essa opção, o número da porta do servidor é automaticamente alterada para 3268. Além disso, como o DN Base não é necessário durante a configuração da opção de catálogo global, a caixa de texto DN Base não é exibida.
  - Adicione o nome do host servidor do Active Directory.
  - Se o Active Directory exigir acesso por SSL, selecione a opção **Esse diretório requer que todas as conexões usem SSL** e cole o certificado na caixa de texto fornecida. Quando você seleciona essa opção, o número da porta do servidor é automaticamente alterada para 3269.

Ambiente do Active Directory de várias florestas com relações confiáveis

Uma implantação do Active Directory de várias florestas com relações confiáveis permite que você sincronize usuários e grupos de vários domínios do Active Directory entre florestas, onde existe confiança bidirecional entre os domínios.

Ao adicionar um diretório a esse ambiente, selecione a opção Active Directory (Autenticação Integrada do Windows).

Para obter mais informações, consulte:

- "Sobre a seleção do controlador de domínio (domain_krb.properties file)", na página 47
- "Gerenciando atributos de usuário sincronizados a partir do Active Directory", na página 51
- "Permissões necessárias para se ingressar em um domínio", na página 52
- "Configurando a conexão do Active Directory com o serviço", na página 53

Ambiente do Active Directory de várias florestas sem relações confiáveis

Uma implantação do Active Directory de várias florestas sem relações confiáveis permite que você sincronize usuários e grupos de vários domínios do Active Directory entre florestas, sem confiança bidirecional entre os domínios. Neste ambiente, você cria vários diretórios no serviço, um diretório para cada floresta.

O tipo de diretórios que você criar no serviço depende da floresta. Para as florestas com vários domínios, selecione a opção Active Directory (Autenticação Integrada do Windows). Para um floresta com um único domínio, selecione a opção Active Directory sobre LDAP.

Para obter mais informações, consulte:

- "Sobre a seleção do controlador de domínio (domain_krb.properties file)", na página 47
- "Gerenciando atributos de usuário sincronizados a partir do Active Directory", na página 51
- "Permissões necessárias para se ingressar em um domínio", na página 52
- "Configurando a conexão do Active Directory com o serviço", na página 53

Sobre a seleção do controlador de domínio (domain_krb.properties file)

O arquivo `domain_krb.properties` determina quais controladores de domínio são usados para os diretórios com a pesquisa Localização do Serviço DNS (registros SRV) habilitada. Ele contém uma lista de controladores de domínio para cada domínio. O conector cria o arquivo inicialmente e você deve mantê-lo posteriormente. O arquivo substitui a pesquisa Localização do Serviço DNS (SRV).

Os seguintes tipos de diretórios têm a pesquisa Localização do serviço DNS habilitada:

- Active Directory em LDAP com a opção **Esse diretório oferece suporte à Localização do Serviço DNS** selecionada
- Active Directory (autenticação integrada do Windows) sempre com a pesquisa Localização do Serviço DNS habilitada

A primeira vez que você cria um diretório com a pesquisa Localização do Serviço DNS habilitada, um arquivo `domain_krb.properties` é criado automaticamente no diretório `/usr/local/horizon/conf` da máquina virtual e é preenchido automaticamente com controladores de domínio para cada domínio. Para preencher o arquivo, o conector tenta localizar os controladores de domínio que estão no mesmo site que o conector e seleciona dois que são acessíveis e que respondam mais rápido.

Quando você cria diretórios adicionais com a Localização do Serviço DNS habilitada ou adiciona novos domínios em um diretório de autenticação integrada do Windows, os novos domínios e uma lista de controladores de domínio para esses domínios são adicionados ao arquivo.

Você pode substituir a seleção padrão a qualquer momento editando o arquivo `domain_krb.properties`. Como prática recomendada, depois de criar um diretório, exiba o arquivo `domain_krb.properties` e verifique se os controladores de domínio listados são os ideais para a sua configuração. Para uma implantação do Active Directory global com vários controladores de domínio em diferentes localizações geográficas, usar um controlador de domínio que está muito próximo ao conector garante uma comunicação mais rápida com o Active Directory.

Você também deve atualizar o arquivo manualmente para qualquer outra alteração. As seguintes regras aplicam-se.

- O arquivo `domain_krb.properties` é criado na máquina virtual que contém o conector. Em uma implantação típica, sem conectores adicionais implantados, o arquivo é criado na máquina virtual de serviço do VMware Identity Manager. Se você estiver usando um conector adicional para o diretório, o arquivo será criado na máquina virtual do conector. Uma máquina virtual somente pode ter um arquivo `domain_krb.properties`.

- O arquivo é criado e preenchido automaticamente com controladores de domínio para cada domínio na primeira vez que você cria um diretório com a pesquisa Localização do Serviço DNS habilitada.
- Os controladores de domínio para cada domínio são listados em ordem de prioridade. Para se conectar ao Active Directory, o conector tenta usar o primeiro controlador de domínio na lista. Se não for acessível, ele tenta usar o segundo na lista, e assim por diante.
- O arquivo somente é atualizado quando você cria um novo diretório com a pesquisa Localização do Serviço DNS habilitada ou quando adiciona um domínio a um diretório de autenticação integrada do Windows. O novo domínio e uma lista de controladores de domínio para ele são acrescentados ao arquivo.

  Observe que, se uma entrada para um domínio já existe no arquivo, ela não será atualizada. Por exemplo, se você criou um diretório e, em seguida, o excluiu, a entrada de domínio original permanecerá no arquivo e não será atualizada.
- O arquivo não é atualizado automaticamente em nenhum outro cenário. Por exemplo, se você excluir um diretório, a entrada de domínio não será excluída do arquivo.
- Se um controlador de domínio listado no arquivo não estiver acessível, edite o arquivo e remova-o.
- Se você adicionar ou editar uma entrada de domínio manualmente, as alterações não serão substituídas.

Para obter informações sobre a edição do arquivo `domain_krb.properties`, veja "Editando o arquivo domain_krb.properties", na página 49.

Importante O arquivo `/etc/krb5.conf` deve ser consistente com o arquivo `domain_krb.properties`. Sempre que atualizar o arquivo `domain_krb.properties`, atualize também o `krb5.conf`. Consulte "Editando o arquivo domain_krb.properties", na página 49 e Knowledge Base article 2091744 para obter mais informações.

Como os controladores de domínio são selecionados para preencher automaticamente o arquivo domain_krb.properties

Para preencher automaticamente o arquivo `domain_krb.properties`, os controladores de domínio são selecionados primeiramente ao determinar a sub-rede na qual reside o conector (com base no endereço IP e na máscara de rede) e, em seguida, usando a configuração do Active Directory para identificar o site dessa sub-rede, recebendo a lista de controladores de domínio para esse site, filtrando a lista para o domínio apropriado e escolhendo os dois controladores de domínio que respondam mais rapidamente.

Para detectar os controladores de domínio mais próximos, o VMware Identity Manager apresenta os seguintes requisitos.

- A sub-rede do conector deve estar presente na configuração do Active Directory ou uma sub-rede deve ser especificada no arquivo `runtime-config.properties`. Consulte "Substituindo a seleção de sub-rede padrão", na página 49.

  A sub-rede é usada para determinar o site.
- A configuração do Active Directory deve considerar o site.

Se a sub-rede não puder ser determinada ou se a configuração do Active Directory não considerar o site, a pesquisa Localização do Serviço DNS será usada para localizar controladores de domínio e o arquivo será preenchido com alguns controladores de domínio acessíveis. Observe que esses controladores de domínio podem não estar na mesma localização geográfica que o conector, o que pode resultar em atrasos ou tempos limite durante a comunicação com o Active Directory. Nesse caso, edite o arquivo `domain_krb.properties` manualmente e especifique os controladores de domínio corretos a serem usados para cada domínio. Consulte "Editando o arquivo domain_krb.properties", na página 49.

Arquivo de amostra domain_krb.properties

```
example.com=host1.example.com:389,host2.example.com:389
```

Substituindo a seleção de sub-rede padrão

Para preencher automaticamente o arquivo `domain_krb.properties`, o conector tenta localizar os controladores de domínio que estão no mesmo site para que haja o mínimo de latência entre o conector e o Active Directory.

Para localizar o site, o conector determina a sub-rede na qual ele reside, com base no endereço IP e na máscara de rede e, em seguida, usa a configuração do Active Directory para identificar o site para essa sub-rede. Se a sub-rede da máquina virtual não estiver no Active Directory, ou se você desejar substituir a seleção de sub-rede automática, poderá especificar uma sub-rede no arquivo `runtime-config.properties`.

Procedimentos

1 Faça login na máquina virtual do do VMware Identity Manager como o usuário raiz.

Observação Se você estiver usando um conector adicional para o diretório, faça login na máquina virtual do conector.

2 Edite o arquivo `/usr/local/horizon/conf/runtime-config.properties` para adicionar o atributo a seguir.

`siteaware.subnet.override=`*`subnet`*

onde *subnet* é uma sub-rede para o site cujo os controladores de domínio você deseja usar. Por exemplo:

`siteaware.subnet.override=10.100.0.0/20`

3 Salve e feche o arquivo.

4 Reinicie o serviço.

```
service horizon-workspace restart
```

Editando o arquivo domain_krb.properties

O arquivo `/usr/local/horizon/conf/domain_krb.properties` determina quais controladores de domínio são usados para os diretórios com a pesquisa Localização do Serviço DNS habilitada. Você pode editar o arquivo a qualquer momento para modificar a lista de controladores de domínio de um domínio, ou para adicionar ou excluir entradas de domínio. As alterações não serão substituídas.

O arquivo é inicialmente criado e preenchido automaticamente pelo conector. Você precisa atualizá-lo manualmente em cenários como o seguinte:

- Se os controladores de domínio selecionados por padrão não forem os ideais para a sua configuração, edite o arquivo e especifique os controladores de domínio a serem usados.
- Se você excluir um diretório, exclua a entrada de domínio correspondente do arquivo.
- Se algum controlador de domínio no arquivo não for acessível, remova-o do arquivo.

Consulte também "Sobre a seleção do controlador de domínio (domain_krb.properties file)", na página 47.

Procedimentos

1 Faça login na máquina virtual do do VMware Identity Manager como o usuário raiz.

Observação Se você estiver usando um conector adicional para o diretório, faça login na máquina virtual do conector.

2 Altere os diretórios para `/usr/local/horizon/conf`.

3 Edite o arquivo `domain_krb.properties` para adicionar, ou editar, a lista do domínio aos valores de host.

Use o seguinte formato:

domínio`=`*host*`:`*porta*`,`*host2*`:`*porta*`,`*host3*`:`*porta*

Por exemplo:

```
example.com=examplehost1.example.com:389,examplehost2.example.com:389
```

Liste os controladores de domínio em ordem de prioridade. Para se conectar ao Active Directory, o conector tenta usar o primeiro controlador de domínio na lista. Se não for acessível, ele tenta usar o segundo na lista, e assim por diante.

Importante Os nomes de domínio devem estar em letras minúsculas.

4 Altere a propriedade do arquivo `domain_krb.properties` para `horizon` e o grupo para `www` usando o seguinte comando.

```
chown horizon:www /usr/local/horizon/conf/domain_krb.properties
```

5 Reinicie o serviço.

```
service horizon-workspace restart
```

Próximo passo

Depois de editar o arquivo `domain_krb.properties`, edite o arquivo `/etc/krb5.conf`. O arquivo `krb5.conf` deve ser consistente com o arquivo `domain_krb.properties`.

1 Edite o arquivo `/etc/krb5.conf` e atualize a seção `realms` para especificar os mesmos valores de domínio para host que são usados no arquivo `/usr/local/horizon/conf/domain_krb.properties`. Não é necessário especificar o número da porta. Por exemplo, se o seu arquivo `domain_krb.properties` tiver a entrada de domínio `example.com=examplehost.example.com:389`, você atualizaria o arquivo `krb5.conf` para o seguinte.

```
[realms]
GAUTO-QA.COM = {
auth_to_local = RULE:[1:$0\$1](^GAUTO-QA\.COM\\.*)s/^GAUTO-QA\.COM/GAUTO-QA/
auth_to_local = RULE:[1:$0\$1](^GAUTO-QA\.COM\\.*)s/^GAUTO-QA\.COM/GAUTO-QA/
auth_to_local = RULE:[1:$0\$1](^GAUTO2QA\.GAUTO-QA\.COM\\.*)s/^GAUTO2QA\.GAUTO-
QA\.COM/GAUTO2QA/
auth_to_local = RULE:[1:$0\$1](^GLOBEQE\.NET\\.*)s/^GLOBEQE\.NET/GLOBEQE/
auth_to_local = DEFAULT
kdc = examplehost.example.com
}
```

Observação É possível ter várias entradas kdc. No entanto, não é uma exigência uma vez que, na maioria dos casos, há apenas um único valor kdc. Se você optar por definir valores kdc adicionais, cada linha terá uma entrada kdc que definirá um controlador de domínio.

2 Reinicie o serviço do espaço de trabalho.

```
service horizon-workspace restart
```

Consulte também Knowledge Base article 2091744.

Solucionando problemas do domain_krb.properties

Use as seguintes informações para solucionar problemas do arquivo `domain_krb.properties`.

Erro "Erro ao determinar o domínio"

Se o arquivo `domain_krb.properties` já incluir uma entrada para um domínio e você tentar criar um novo diretório de um tipo diferente para o mesmo domínio, ocorrerá o erro "Erro ao determinar o domínio". Você deve editar o arquivo `domain_krb.properties` e remover manualmente a entrada de domínio antes de criar o novo diretório.

Os controladores de domínio são inacessíveis

Depois que uma entrada de domínio é adicionada ao arquivo `domain_krb.properties`, ela não é atualizada automaticamente. Se qualquer controlador de domínio listado no arquivo tornar-se inacessível, edite o arquivo manualmente e remova o controlador de domínio.

Gerenciando atributos de usuário sincronizados a partir do Active Directory

Durante a configuração do diretório de serviços do VMware Identity Manager, você seleciona os filtros e os atributos de usuário do Active Directory para especificar quais usuários sincronizam no diretório do VMware Identity Manager. Você pode mudar o atributos de usuário que sincronizam a partir do console de administração, guia Gerenciamento de Identidade e Acesso, Configuração > Atributos de usuário.

As alterações feitas e guardadas na página Atributos de usuário são adicionadas à página Atributos mapeados no diretório VMware Identity Manager. As alterações de atributo são atualizadas para o diretório com a próxima sincronização para o Active Directory.

A página Atributos de usuário lista os atributos de diretório padrão que podem ser mapeados para os atributos do Active Directory. Você seleciona os atributos necessários e pode adicionar outros atributos do Active Directory que você deseja sincronizar com o diretório. Quando você adicionar atributos, observe que o nome do atributo que você inseriu diferencia letras maiúsculas e minúsculas. Por exemplo, endereço, Endereço e ENDEREÇO são atributos diferentes.

Tabela 4-1. Atributos padrão do Active Directory para sincronização com diretório

Nome do atributo de diretório do VMware Identity Manager	Padrão de mapeamento de atributo do Active Directory
userPrincipalName	userPrincipalName
distinguishedName	distinguishedName
employeeId	employeeID
domain	canonicalName. Adiciona o nome do objeto de domínio totalmente qualificado.
desativado (usuário externo desativado)	userAccountControl. Sinalizada com UF_Account_Disable Quando uma conta é desativada, os usuários não podem fazer login para acessar os aplicativos e recursos. Os recursos a que os usuários tinham o direito não são removidos da conta para que quando a sinalização for removida da conta, os usuários possam fazer login e acessar os recursos autorizados
phone	telephoneNumber
lastName	sn
firstName	givenName
email	mail
userName	sAMAccountName.

Selecionar atributos para sincronizar com o diretório

Quando você configurar o diretório do VMware Identity Manager para sincronizar com o Active Directory, especifique os atributos do usuário que sincronizam com o diretório. Antes de configurar o diretório, você pode especificar na página Atributos de Usuário quais atributos padrão são obrigatórios e adicionar outros atributos que você deseja mapear para atributos do Active Directory.

Quando você configura a página Atributos do usuário antes da criação do diretório, você pode alterar os atributos padrão de obrigatório para não obrigatório, marcar os atributos como obrigatório e adicionar atributos personalizados.

Após a criação do diretório, você pode alterar um atributo obrigatório para não obrigatório e excluir atributos personalizados. Não é possível alterar um atributo para atributo obrigatório.

Quando você adiciona outros atributos para sincronizar com o diretório, depois que o diretório for criado, vá para a página Atributos mapeados do diretório para mapear esses atributos para atributos do Active Directory.

Importante Se você pretende sincronizar recursos do XenApp para o VMware Identity Manager, torne o **distinguishedName** um atributo obrigatório. Você deve especificar isso antes de criar o diretório VMware Identity Manager.

Procedimentos

1 No console de administração, guia Gerenciamento de Identidade e Acesso, clique em **Configuração > Atributos de usuário**.

2 Na seção Atributos padrão, veja a lista de atributos obrigatórios e faça as alterações necessárias para refletir os atributos que devem ser obrigatórios.

3 Na seção Atributos, adicione à lista o nome do atributo do diretório VMware Identity Manager.

4 Clique em **Salvar**.

O status do atributo padrão é atualizado e os atributos que você adicionou são adicionados à lista de atributos mapeados do diretório.

5 Após a criação do diretório, vá até a página **Gerenciar > diretórios** e selecione o diretório.

6 Clique em **Configurações de sincronização > Atributos mapeados**

7 No menu suspenso dos atributos que você adicionou, selecione o atributo do Active Directory para o qual mapear.

8 Clique em **Salvar.**

O diretório será atualizado na próxima vez que o diretório sincronizar com o Active Directory.

Permissões necessárias para se ingressar em um domínio

Talvez você necessite ingressar o conector do VMware Identity Manager em um domínio em alguns casos. Para o Active Directory em diretórios LDAP, você pode ingressar um domínio depois de criar o diretório. Para diretórios do tipo Active Directory (autenticação integrada do Windows), o conector é ingressado no domínio automaticamente quando você cria o diretório. Em ambas as situações, será necessário fornecer suas credenciais.

Para ingressar em um domínio, você precisa de credenciais do Active Directory com o privilégio de "ingressar o computador no domínio do AD". Essa opção é configurada no Active Directory com os seguintes direitos:

- Criar objetos de computador
- Excluir objetos de computador

Ao ingressar em um domínio, cria-se um objeto de computador no local padrão do Active Directory, a menos que você especifique uma UO personalizada.

Caso você não tenha os direitos para ingressar em um domínio, siga esses passos para ingressar nele.

1 Peça ao administrador do Active Directory para criar o objeto de computador no Active Directory em uma localização determinada pela política da sua empresa. Forneça o nome de host do conector. Certifique-se de fornecer o nome de domínio totalmente qualificado, por exemplo, `server.example.com`.

Dica Você pode ver o nome do host na coluna **Nome do Host** na página Conectores no console de administração. Clique em **Gerenciamento de Identidade e Acesso > Configuração > Conectores** para exibir a página Conectores.

2 Após a criação do objeto de computador, ingresse no domínio usando qualquer conta de usuário de domínio no console de administração do VMware Identity Manager.

O comando **Ingressar no Domínio** está disponível na página **Conectores**, acessada clicando em **Gerenciamento de Identidade e Acesso > Configuração > Conectores**.

Opção	Descrição
Domínio	Selecione ou digite o domínio no Active Directory para ingressar nele. Certifique-se de que você digitou o nome do domínio totalmente qualificado. Por exemplo: **server.example.com**
Usuário do domínio	O nome de usuário de um usuário no Active Directory que tenha os direitos para ingressar os sistemas no domínio do Active Directory.
Senha do domínio	A senha do usuário.
Unidade organizacional (UO)	(Opcional) A unidade organizacional (UO) do objeto de computador. Essa opção cria um objeto de computador na UO especificada em vez da UO padrão nos computadores. Por exemplo, **ou=testou,dc=test,dc=example,dc=com**.

Configurando a conexão do Active Directory com o serviço

No console de administração, especifique as informações necessárias para conexão com o seu Active Directory e selecione os usuários e os grupos a serem sincronizados com o diretório do VMware Identity Manager.

As opções de conexão do Active Directory são Active Directory sobre LDAP ou Autenticação Integrada do Windows do Active Directory. Uma conexão do Active Directory sobre LDAP é compatível com a pesquisa de Localização do Serviço DNS. Com a Autenticação Integrada do Windows do Active Directory, você configura o domínio no qual ingressar.

Pré-requisitos

- Selecione quais atributos são necessários e adicione atributos complementares, se necessário, na página Atributos do Usuário. Consulte "Selecionar atributos para sincronizar com o diretório", na página 52.

  Importante Se você pretende sincronizar recursos do XenApp com o VMware Identity Manager, torne **distinguishedName** um atributo obrigatório. Você deve fazer essa seleção antes de criar um diretório, pois os atributos não podem ser alterados para serem necessários depois que um diretório é criado.

- Lista dos grupos e usuários do Active Directory para sincronizar a partir do Active Directory.

- Para o Active Directory sobre LDAP, as informações necessárias incluem o DN Base, o DN Bind e a senha do DN Bind.

  Observação É recomendável usar uma conta de usuário DN Bind com uma senha que não expire.

- Para autenticação integrada do Windows no Active Directory, as informações necessárias incluem a senha e o endereço UPN do usuário de associação do domínio.

  Observação É recomendável usar uma conta de usuário DN Bind com uma senha que não expire.

- Se o Active Directory exigir acesso sobre SSL ou STARTTLS, será necessário o certificado da CA Raiz do controlador de domínio do Active Directory.
- Para autenticação integrada do Windows no Active Directory, quando você tiver várias florestas do Active Directory configuradas e o grupo local de domínio contiver membros de domínios em florestas diferentes, certifique-se de que o usuário de associação seja adicionado ao grupo de administradores do domínio no qual reside o grupo local de domínio. Se isso não for feito, esses membros estarão ausentes do grupo local de domínio.

Procedimentos

1 No console de administração, clique na guia **Gerenciamento de Identidade e Acesso**.

2 Na página Diretórios, clique em **Adicionar Diretório**.

3 Insira um nome para esse diretório do VMware Identity Manager.

4 Selecione o tipo de Active Directory no seu ambiente e configurar as informações de conexão.

Opção	Descrição
Active Directory sobre LDAP	a No campo **Sincronizar Conector**, selecione o conector a ser usado para sincronização com o Active Directory. b No campo **Autenticação**, se esse Active Directory for usado para autenticar usuários, clique em **Sim**. Se um provedor de identidade de terceiros for usado para autenticar usuários, clique em **Não**. Depois de configurar a conexão do Active Directory para sincronizar usuários e grupos, acesse a página Gerenciamento de Identidade e Acesso > Gerenciar > Provedores de Identidade para adicionar o provedor de identidade de terceiros para autenticação. c No campo **Atributo de Pesquisa do Diretório**, selecione o atributo de conta que contém o nome de usuário. d Se o Active Directory usar a pesquisa Localização do serviço DNS, faça as seleções a seguir. ■ Na seção **Local do Servidor**, marque a caixa de seleção **Esse diretório suporta localização do serviço DNS**. Será criado um arquivo `domain_krb.properties`, preenchido automaticamente com uma lista de controladores de domínio, quando o diretório for criado. Consulte "Sobre a seleção do controlador de domínio (domain_krb.properties file)", na página 47. ■ Se o Active Directory exigir criptografia STARTTLS, marque a caixa de seleção **Esse diretório requer que todas as conexões usem SSL** na seção **Certificados** e copie e cole o certificado da CA raiz do Active Directory no campo **Certificado SSL**. Verifique se o certificado está no formato PEM e inclui as linhas "BEGIN CERTIFICATE" e "END CERTIFICATE". **Observação** Se o Active Directory exigir STARTTLS e o certificado não for fornecido, você não poderá criar o diretório. e Se o Active Directory não usar a pesquisa de Localização do Serviço DNS, faça as seleções a seguir. ■ Na seção **Local do Servidor**, verifique se a caixa de seleção **Esse diretório suporta localização do serviço DNS** está desmarcada e insira o nome do host e o número da porta do servidor do Active Directory. Para configurar o diretório como um catálogo global, consulte a seção Ambiente de vários domínios em única floresta do Active Directory em "Ambientes do Active Directory", na página 45. ■ Se o Active Directory exigir acesso por SSL, marque a caixa de seleção **Esse diretório requer que todas as conexões usem SSL** na seção **Certificados** e copie e cole o certificado da CA raiz do Active Directory no campo **Certificado SSL**. Verifique se o certificado está no formato PEM e inclui as linhas "BEGIN CERTIFICATE" e "END CERTIFICATE". **Observação** Se o Active Directory exigir SSL e o certificado não for fornecido, você não poderá criar o diretório. f No campo **DN Base**, insira o DN do qual iniciar as pesquisas de conta. Por exemplo, OU=myUnit,DC=myCorp,DC=com. g No campo **DN Bind**, insira a conta que pode pesquisar usuários. Por exemplo, CN=binduser,OU=myUnit,DC=myCorp,DC=com. **Observação** É recomendável usar uma conta de usuário DN Bind com uma senha que não expire. h Depois de inserir a Senha do bind, clique em **Testar Conexão** para verificar se o diretório consegue se conectar ao seu Active Directory.
Active Directory (Autenticação Integrada do Windows)	a No campo **Sincronizar Conector**, selecione o conector a ser usado para sincronização com o Active Directory.

Opção	Descrição
	b No campo **Autenticação**, se esse Active Directory for usado para autenticar usuários, clique em **Sim**. Se um provedor de identidade de terceiros for usado para autenticar usuários, clique em **Não**. Depois de configurar a conexão do Active Directory para sincronizar usuários e grupos, acesse a página Gerenciamento de Identidade e Acesso > Gerenciar > Provedores de Identidade para adicionar o provedor de identidade de terceiros para autenticação. c No campo **Atributo de Pesquisa do Diretório**, selecione o atributo de conta que contém o nome de usuário. d Se o Active Directory exigir criptografia STARTTLS, marque a caixa de seleção **Esse diretório requer que todas as conexões usem STARTTLS** na seção **Certificados** e copie e cole o certificado da CA raiz do Active Directory no campo **Certificado SSL**. Verifique se o certificado está no formato PEM e inclui as linhas "BEGIN CERTIFICATE" e "END CERTIFICATE". Se o diretório tiver vários domínios, adicione os certificados da CA raiz a todos os domínios, um por vez. **Observação** Se o Active Directory exigir STARTTLS e o certificado não for fornecido, você não poderá criar o diretório. e Insira o nome do domínio do Active Directory no qual ingressar. Insira um nome de usuário e uma senha que tenha o direito de ingressar no domínio. Consulte "Permissões necessárias para se ingressar em um domínio", na página 52 para obter mais informações. f No campo UPN do Usuário do Bind, insira o Nome Principal do Usuário que pode se autenticar no domínio. Por exemplo, nomedeusuario@exemplo.com. **Observação** É recomendável usar uma conta de usuário DN Bind com uma senha que não expire. g Insira a senha do Usuário de Associação.

5 Clique em **Salvar e Avançar**.

É exibida a página com a lista de domínios.

6 Para o Active Directory sobre LDAP, os domínios são listados com uma marca de seleção.

Para o Active Directory (Autenticação Integrada do Windows), selecione os domínios que devem ser associados com esta conexão do Active Directory.

Observação Se você adicionar um domínio confiante após o diretório ser criado, o serviço não detecta automaticamente o domínio recém confiante. Para habilitar o serviço para detectar o domínio, o conector deve sair e, em seguida, voltar a ingressar no domínio. Quando o conector reingressa no domínio, o domínio de confiança aparece na lista.

Clique em **Avançar**.

7 Verifique se os nomes de atributos do diretório do VMware Identity Manager estão mapeados para os atributos corretos do Active Directory, faça alterações, se necessário, e clique em **Avançar**.

8 Selecione os grupos que você deseja sincronizar do Active Directory para o diretório do VMware Identity Manager.

Opção	Descrição
Especificar os DNs de grupo	Para selecionar grupos, especifique um ou mais DNs de grupo e selecione os grupos sob eles. a Clique em **+** e especifique o DN de grupo. Por exemplo, CN=users,DC=example,DC=company,DC=com. **Importante** Especifique os DNs de grupo que estão sob o DN Base que você digitou. Se um DN de grupo estiver fora do DN Base, os usuários desse DN serão sincronizados, mas não poderão fazer login. b Clique em **Encontrar Grupos**. A coluna **Grupos a Sincronizar** lista o número de grupos encontrados no DN. c Para selecionar todos os grupos no DN, clique em **Selecionar Tudo**; caso contrário, clique em **Selecionar** e selecione os grupos específicos a serem sincronizados. **Observação** Quando você sincroniza um grupo, todos os usuários que não possuem Usuários de Domínio como grupo primário no Active Directory não são sincronizados.
Sincronizar membros reunidos do grupo	A opção **Sincronizar membros reunidos do grupo** é ativada por padrão. Quando essa opção está ativada, todos os usuários que pertencem diretamente ao grupo que você selecionar, bem como todos os usuários que pertencem aos grupos aninhados abaixo dele, serão sincronizados. Observe que os grupos aninhados não são sincronizados; somente os usuários que pertencem aos grupos aninhados são sincronizados. No diretório do VMware Identity Manager, esses usuários serão membros do grupo principal que você selecionou para sincronização. Se a opção **Sincronizar membros reunidos do grupo** estiver desativada, quando você especificar um grupo para a sincronização, todos os usuários que pertencerem diretamente a esse grupo serão sincronizados. Os usuários que pertencem a grupos aninhados abaixo dele não são sincronizados. Desativar essa opção é útil para grandes configurações do Active Directory nas quais passar por uma árvore de grupos exige muitos recursos e tempo. Se você desativá-la, certifique-se de selecionar todos os grupos cujos usuários deseja sincronizar.

9 Clique em **Avançar**.

10 Especifique usuários adicionais para sincronizar, se necessário.

a Clique em **+** e insira os DNs de usuário. Por exemplo, CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com.

Importante Especifique os DNs de usuário que estão sob o DN Base que você digitou. Se um DN de usuário estiver fora do DN Base, os usuários desse DN serão sincronizados, mas não poderão fazer login.

b (Opcional) Para excluir usuários, clique em um filtro para excluir alguns tipos de usuários.

Você seleciona o atributo do usuário a ser usado para filtragem, a regra de consulta e o valor.

11 Clique em **Avançar**.

12 Revise a página para ver quantos usuários e grupos estão sendo sincronizados com o diretório e para exibir a agenda de sincronização.

Para fazer alterações em usuários e grupos, ou na frequência de sincronização, clique nos links **Editar**.

13 Clique em **Sincronizar Diretório** para iniciar a sincronização com o diretório.

A conexão com o Active Directory é estabelecida, e os usuários e os grupos são sincronizados a partir do Active Directory para o diretório do VMware Identity Manager. O usuário DN Bind tem uma função de administrador no VMware Identity Manager por padrão.

Próximo passo

- Se você tiver criado um diretório compatível com a Localização do Serviço DNS, um arquivo `domain_krb.properties` terá sido criado e preenchido automaticamente com uma lista dos controladores de domínio. Exiba o arquivo para verificar ou editar a lista dos controladores de domínio. Consulte "Sobre a seleção do controlador de domínio (domain_krb.properties file)", na página 47.
- Configure os métodos de autenticação. Depois de sincronizar usuários e grupos para o diretório, se o conector também é usado para autenticação, você pode configurar métodos de autenticação adicionais no conector. Se um terceiro é o provedor de identidade de autenticação, configure esse provedor de identidade no conector.
- Reveja a política de acesso padrão. A política de acesso padrão é configurada para permitir que todos os appliances em todos os intervalos de rede acessem o navegador da Web com um tempo limite de sessão definido para oito horas, ou acessem um aplicativo cliente com um tempo limite de sessão de 2160 horas (90 dias). É possível alterar a política de acesso padrão e quando adicionar aplicativos da Web para o catálogo, você pode criar novos.
- Aplique a marca personalizada para o console de administração, as páginas do portal do usuário e a tela de login.

Habilitando os usuários a alterar senhas do Active Directory

Você pode fornecer aos usuários a capacidade de alterar as senhas do Active Directory a partir do portal ou do aplicativo do Workspace ONE sempre que eles desejarem. Você poderá permitir que os usuários alterem as próprias senhas do Active Directory na página de login do VMware Identity Manager se a senha tiver expirado ou se o administrador do Active Directory tiver redefinido a senha, forçando o usuário a alterá-la no próximo login.

Você pode ativar essa opção por diretório selecionando a opção **Permitir alteração de senha** na página Configuração do diretório.

Os usuários podem alterar suas senhas quando estiverem conectados ao portal do Workspace ONE clicando no nome no canto superior direito, selecionando **Conta** no menu suspenso e clicando no link **Alterar Senha**. No aplicativo do Workspace ONE, os usuários podem alterar suas senhas clicando no ícone do menu da barra tripla e selecionando **Senha**.

As senhas expiradas ou as redefinidas pelo administrador no Active directory podem ser alteradas a partir da página de login. Quando um usuário tenta fazer login com uma senha expirada, ele recebe uma solicitação para redefinir a senha. O usuário deve inserir a senha antiga, bem como a nova senha.

Os requisitos da nova senha são determinados pela política de senha do Active Directory. O número de tentativas permitidas também depende da política de senha do Active Directory.

As seguintes limitações aplicam-se.

- Caso você use appliances virtuais com conectores autônomos adicionais, observe que a opção **Permitir Alteração de Senha** estará disponível apenas para a versão 2016.11.1 do conector e posteriores.
- Quando um diretório for adicionado ao VMware Identity Manager como um Catálogo Global, a opção **Permitir Alteração de Senha** não estará disponível. Os diretórios podem ser adicionados como Active Directory sobre LDAP ou Autenticação Integrada do Windows, usando as portas 389 ou 636.
- A senha de um usuário DN Bind não pode ser redefinida no VMware Identity Manager, mesmo que expire ou que o administrador do Active Directory a redefina.

Observação É recomendável usar uma conta de usuário DN Bind com uma senha que não expire.

- As senhas dos usuários cujos nomes de login consistem em caracteres de vários bytes (caracteres diferentes de ASCII) não podem ser redefinidas no VMware Identity Manager.

Pré-requisitos

- A porta 464 deve ser aberta do VMware Identity Manager para os controladores do domínio.

Procedimentos

1 No console de administração, clique na guia **Gerenciamento de Identidade e Acesso**.

2 Na guia **Diretórios**, clique no diretório.

3 Na seção **Permitir alteração de senha**, selecione **Ativar a Alteração de Senha**.

4 Insira a senha do DN Bind na seção **Detalhes do Usuário do Bind** e clique em **Salvar**.

Integrando a diretórios LDAP

Você pode integrar o seu diretório LDAP corporativo ao VMware Identity Manager para sincronizar usuários e grupos do diretório LDAP com o serviço do VMware Identity Manager.

Consulte também "Conceitos importantes relacionados à integração de diretório", na página 44.

Limitações da Integração de Diretório LDAP

As seguintes limitações aplicam-se atualmente ao recurso de integração de diretório LDAP.

- Você só pode integrar um ambiente de diretório LDAP de domínio único.

  Para integrar vários domínios a partir de um diretório LDAP, você precisa criar diretórios adicionais do VMware Identity Manager, um para cada domínio.

- Os seguintes métodos de autenticação não são suportados para diretórios do VMware Identity Manager do tipo diretório LDAP.
  - autenticação Kerberos
  - Autenticação RSA adaptativa
  - ADFS como um provedor de identidade de terceiros
  - SecurID
  - Autenticação Radius com o servidor de código de acesso SMS e Vasco
- Você não pode ingressar em um domínio LDAP.
- A integração a recursos publicados Citrix ou View não é suportada para diretórios do VMware Identity Manager do tipo diretório LDAP.
- Os nomes de usuário não devem conter espaços. Se um nome de usuário contiver um espaço, o usuário é sincronizado, mas os direitos não estarão disponíveis para o usuário.
- Se você planeja adicionar tanto o Active Directory quanto o diretório LDAP, certifique-se de não marcar nenhum atributo obrigatório na página Atributos de Usuário, exceto userName, que pode ser marcado como obrigatório. As configurações na página Atributos de Usuário aplicam-se a todos os diretórios no serviço. Se um atributo for marcado como obrigatório, os usuários sem esse atributo não serão sincronizados com o serviço do VMware Identity Manager.
- Se você tiver vários grupos com o mesmo nome no seu diretório LDAP, especifique nomes exclusivos para eles no serviço do VMware Identity Manager. Você pode especificar os nomes ao selecionar os grupos a serem sincronizados.
- A opção para permitir que os usuários redefinam senhas expiradas não está disponível.

- O arquivo `domain_krb.properties` não é suportado.

Integrar um diretório LDAP ao serviço

Você pode integrar o seu diretório LDAP corporativo ao VMware Identity Manager para sincronizar usuários e grupos do diretório LDAP com o serviço do VMware Identity Manager.

Para integrar seu diretório LDAP, você cria um diretório correspondente do VMware Identity Manager e sincroniza usuários e grupos a partir do diretório LDAP para o diretório do VMware Identity Manager. Você pode configurar uma agenda de sincronização regular para atualizações subsequentes.

Você também pode selecionar os atributos LDAP que deseja sincronizar para os usuários e os mapear para atributos do VMware Identity Manager.

Sua configuração do diretório LDAP pode estar baseada em esquemas padrão ou você pode ter criado esquemas personalizados. Você também pode ter definido atributos personalizados. Para o VMware Identity Manager poder consultar seu diretório LDAP e obter objetos de usuário ou de grupo, você precisa fornecer os nomes de atributos e os filtros de pesquisa LDAP aplicáveis ao seu diretório LDAP.

Especificamente, você precisa fornecer as seguintes informações.

- Filtros de pesquisa LDAP para a obtenção de grupos, usuários e o usuário de associação
- Nomes de atributo LDAP para associação ao grupo, o UUID e o nome distinto

Certas limitações aplicam-se ao recurso de integração de diretório LDAP. Consulte "Limitações da Integração de Diretório LDAP", na página 59.

Pré-requisitos

- Caso você use appliances virtuais adicionais com conectores externos, observe que a capacidade de integrar diretórios LDAP está disponível apenas com a versão 2016.6.1 do conector e posteriores.
- Verifique os atributos na página **Gerenciamento de Identidade e Acesso > Configuração > Atributos do Usuário** e adicione os atributos adicionais que você deseja sincronizar. Você mapeará depois esses atributos do VMware Identity Manager para os atributos de diretório LDAP ao criar o diretório. Esses atributos são sincronizados para os usuários no diretório.

  Observação Quando você fizer alterações nos atributos do usuário, considere o efeito dessas alterações sobre outros diretórios no serviço. Se você planeja adicionar tanto o Active Directory quanto o diretório LDAP, certifique-se de não marcar nenhum atributo obrigatório, exceto **userName**, que pode ser marcado como obrigatório. As configurações na página Atributos de Usuário aplicam-se a todos os diretórios no serviço. Se um atributo for marcado como obrigatório, os usuários sem esse atributo não serão sincronizados com o serviço do VMware Identity Manager.
- Uma conta de usuário de DN de associação. É recomendável usar uma conta de usuário DN Bind com uma senha que não expire.
- No seu diretório LDAP, o UUID de usuários e grupos deve estar em formato de texto simples.
- No seu diretório LDAP, deve existir um atributo de domínio para todos os usuários e grupos.

  Você mapeia esse atributo para o atributo VMware Identity Manager **domain** quando criar o diretório do VMware Identity Manager.
- Os nomes de usuário não devem conter espaços. Se um nome de usuário contiver um espaço, o usuário é sincronizado, mas os direitos não estarão disponíveis para o usuário.
- Se você usar a autenticação de certificado, os usuários deverão ter valores para os atributos de endereço de e-mail e userPrincipalName.

Procedimentos

1 No console de administração, clique na guia **Gerenciamento de Identidade e Acesso**.

2 Na página Diretórios, clique em **Adicionar diretório** e selecione **Adicionar Diretório LDAP**.

3 Insira as informações necessárias na página Adicionar Diretório LDAP.

Opção	Descrição
Nome do diretório	Um nome para o diretório do VMware Identity Manager.
Sincronização e Autenticação do Diretório	a No campo **Sincronizar Conector**, selecione o conector que você deseja usar para sincronizar usuários e grupos a partir de seu diretório LDAP para o diretório do VMware Identity Manager. Um componente de conector está sempre disponível com o serviço do VMware Identity Manager por padrão. Esse conector é exibido na lista suspensa. Se você instalar vários appliances do VMware Identity Manager para alta disponibilidade, o componente de conector de cada um deles será exibido na lista. Você não precisa de um conector separado para um diretório LDAP. Um conector pode ser compatível com vários diretórios, independentemente se eles são diretórios do Active Directory ou LDAP. Para os cenários em que você precisa de conectores adicionais, consulte "Instalando appliances do conector" no *Guia de Instalação do VMware Identity Manager*. b No campo **Autenticação**, se você quiser usar este diretório LDAP para autenticar usuários, selecione **Sim**. Se você desejar usar um provedor de identidade de terceiros para autenticar usuários, selecione **Não**. Após adicionar a conexão de diretório para sincronizar usuários e grupos, vá para a página **Gerenciamento de Identidade e Acesso > Gerenciar > Provedores de Identidade** para adicionar o provedor de identidade de terceiros para a autenticação. c No campo **Atributo de Pesquisa do Diretório**, especifique o atributo de diretório LDAP a ser usado para nomes de usuário. Se o atributo não estiver listado, selecione **Personalizado** e digite o nome do atributo. Por exemplo, **`cn`**.
Localização de Servidor	Insira o número de porta e o host do servidor do Diretório LDAP. Para o host do servidor, você pode especificar o nome de domínio totalmente qualificado ou o endereço IP. Por exemplo, **`meuservidorLDAP.exemplo.com`** ou **`100.00.00.0`**. Se você tiver um cluster de servidores atrás de um balanceador de carga, digite as informações do balanceador de carga.

Opção	Descrição
Configuração LDAP	Especifique os atributos e os filtros de pesquisa LDAP que o VMware Identity Manager pode usar para consultar seu diretório LDAP. Os valores padrão são fornecidos com base no esquema LDAP principal. **Consultas LDAP** ■ **Obter grupos**: o filtro de pesquisa para a obtenção de objetos de grupo. Por exemplo: **`(objectClass=group)`** ■ **Obter usuário de associação**: o filtro de pesquisa para a obtenção do objeto de usuário de associação, quer dizer, o usuário que pode associar-se ao diretório. Por exemplo: **`(objectClass=person)`** ■ **Obter usuário**: o filtro de pesquisa para a obtenção de usuários para sincronização. Por exemplo:**`(&(objectClass=user)(objectCategory=person))`** **Atributos** ■ **Associação**: o atributo usado em seu diretório LDAP para a definição dos membros de um grupo. Por exemplo: **`member`** ■ **UUID de objeto**: o atributo usado em seu diretório LDAP para a definição do UUID de um usuário ou grupo. Por exemplo: **`entryUUID`** ■ **Nome Distinto**: o atributo usado em seu diretório LDAP para o nome distinto de um usuário ou grupo. Por exemplo: **`entryDN`**
Certificados	Se o seu diretório LDAP requer acesso via SSL, selecione **Esse diretório requer que todas as conexões usem SSL** e copie e cole o certificado SSL da CA raiz do servidor do diretório LDAP. Verifique se o certificado está no formato PEM e inclui as linhas "BEGIN CERTIFICATE" e "END CERTIFICATE".
Associar detalhes do usuário	**DN base**: digite o DN do qual se deseja iniciar as pesquisas. Por exemplo, cn=users,dc=example,dc=com **DN de associação**: digite o nome de usuário a ser usado para vinculação ao diretório LDAP. **Observação** É recomendável usar uma conta de usuário DN Bind com uma senha que não expire. **Senha do DN de associação**: digite a senha para o usuário do DN de associação.

4 Para testar a conexão com o servidor do diretório LDAP, clique em **Testar Conexão**.

Se a conexão não for bem-sucedida, verifique as informações que você inseriu e faça as alterações adequadas.

5 Clique em **Salvar e Avançar**.

6 Na página Domínios, verifique se o domínio correto está listado e clique em **Avançar**.

7 Na página Atributos Mapeados, verifique se os atributos do VMware Identity Manager estão mapeados para os atributos LDAP corretos.

Importante Você deve especificar um mapeamento para o atributo **domain**.

Você pode adicionar atributos à lista na página Atributos de Usuário.

8 Clique em **Avançar**.

9 Na página de grupos, clique em **+** para selecionar os grupos que você deseja sincronizar a partir do diretório LDAP para o diretório do VMware Identity Manager.

Se você tiver vários grupos com o mesmo nome no seu diretório LDAP, especifique nomes exclusivos para eles na página de grupos.

A opção **Sincronizar usuários do grupo aninhado** é habilitada por padrão. Quando essa opção está ativada, todos os usuários que pertencem diretamente ao grupo que você selecionar, bem como todos os usuários que pertencem aos grupos aninhados abaixo dele, serão sincronizados. Observe que os grupos aninhados não são sincronizados; somente os usuários que pertencem aos grupos aninhados são sincronizados. No diretório do VMware Identity Manager, esses usuários serão exibidos como membros do grupo de nível superior que você selecionou para sincronização. Com efeito, a hierarquia sob um grupo selecionado é simplificada e os usuários de todos os níveis aparecem no VMware Identity Manager como membros do grupo selecionado.

Se essa opção estiver desativada, quando você especificar um grupo para sincronização, todos os usuários que pertencem diretamente a esse grupo serão sincronizados. Os usuários que pertencem a grupos aninhados abaixo dele não são sincronizados. A desativação dessa opção é útil para grandes configurações de diretório em que percorrer uma árvore de grupo exige muitos recursos e muito tempo. Se você desativá-la, certifique-se de selecionar todos os grupos cujos usuários deseja sincronizar.

10 Clique em **Avançar**.

11 Clique em **+** para adicionar mais usuários. Por exemplo, digite `CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com`.

Para excluir usuários, clique em um filtro para excluir alguns tipos de usuários. Você seleciona o atributo do usuário a ser usado para filtragem, a regra de consulta e o valor.

Clique em **Avançar**.

12 Analise a página para ver quantos usuários e grupos serão sincronizados com o diretório e ver a agenda de sincronização padrão.

Para fazer alterações em usuários e grupos, ou na frequência de sincronização, clique nos links **Editar**.

13 Clique em **Sincronizar diretório** para iniciar a sincronização de diretório.

A conexão com o diretório LDAP é estabelecida e os usuários e grupos são sincronizados a partir do diretório LDAP para o diretório do VMware Identity Manager. O usuário DN Bind tem uma função de administrador no VMware Identity Manager por padrão.

Adicionando um diretório depois de configurar o failover e a redundância

Se você adicionar um novo diretório ao serviço do VMware Identity Manager depois de já ter implantado um cluster para alta disponibilidade, e desejar tornar o novo diretório parte da configuração de alta disponibilidade, você precisará adicionar o diretório a todos os appliances no seu cluster.

Você pode fazer isso adicionando o componente de conector de cada uma das instâncias de serviço ao novo diretório.

Procedimentos

1 Faça login no console de administração do VMware Identity Manager.

2 Selecione a guia **Gerenciamento de Identidade e Acesso** e, em seguida, selecione a guia **Provedores de Identidade**.

3 Na página Provedores de Identidade, localize o provedor de identidade do novo diretório e clique no nome do provedor de identidade.

4 No campo **Nome do Host IdP**, insira o FQDN do balanceador de carga se ele ainda não estiver definido como o FQDN do balanceador de carga correto.

5 No campo **Conectores**, selecione o conector a ser adicionado.

6 Insira a senha e clique em **Salvar**.

7 Na página Provedores de Identidade, clique no nome do provedor de identidade novamente e verifique se o campo **Nome do Host IdP** exibe o nome do host correto. O campo **Nome do Host IdP** deve exibir o FQDN do balanceador de carga. Se o nome estiver incorreto, insira o FQDN do balanceador de carga e clique em **Salvar**.

8 Repita as etapas anteriores para adicionar todos os conectores listados no campo **Conectores**.

Observação Depois de adicionar todos os conectores, verifique o nome do host IdP e modifique-o, se necessário, conforme descrito na etapa 7.

O diretório agora está associado a todos os conectores na sua implantação.

Usando diretórios locais 5

Um diretório local é um dos tipos de diretórios que você pode criar no serviço do VMware Identity Manager. Um diretório local permite provisionar usuários locais e fornecer acesso a aplicativos específicos, sem precisar adicioná-los ao diretório da empresa. Um diretório local não está conectado a um diretório corporativo, e os usuários e grupos não são sincronizados de um diretório corporativo. Em vez disso, você cria usuários locais diretamente no diretório local.

Um diretório local padrão, denominado Diretório do Sistema, está disponível no serviço. Você também pode criar vários diretórios locais novos.

Diretório do Sistema

O Diretório do Sistema é um diretório local que é criado automaticamente no serviço quando ele é configurado pela primeira vez. Este diretório tem o Domínio do sistema do domínio. Não é possível alterar o nome ou o domínio do Diretório do Sistema ou adicionar novos domínios a ele. Também não é possível excluir o Diretório do Sistema ou o Domínio do Sistema.

O usuário administrador local que é criado quando você configura pela primeira vez o appliance do VMware Identity Manager é criado no Domínio do Sistema do Diretório do Sistema.

Você pode adicionar outros usuários ao Diretório do Sistema. O Diretório do Sistema é normalmente usado para configurar alguns usuários administradores locais para gerenciar o serviço. Para provisionar usuários finais e administradores adicionais e qualificá-los para os aplicativos, é recomendável criar um novo diretório local.

Diretórios Locais

Você pode criar vários diretórios locais. Cada diretório local pode ter um ou mais domínios. Ao criar um usuário local, você especifica o diretório e o domínio para o usuário.

Você também pode selecionar atributos para todos os usuários em um diretório local. Os atributos do usuário como userName, lastName e firstName são especificados em nível global no serviço do VMware Identity Manager. Uma lista padrão de atributos está disponível, e você pode adicionar atributos personalizados. Os atributos globais do usuário se aplicam a todos os diretórios no serviço, incluindo os diretórios locais. No nível do diretório local, você pode selecionar quais atributos são necessários para o diretório. Isso permite que você tenha um conjunto personalizado de atributos para diferentes diretórios locais. Os atributos userName, lastName, firstName e email são sempre obrigatórios para diretórios locais.

Observação A capacidade de personalizar atributos de usuário no nível de diretório está disponível somente para diretórios locais, e não para diretórios do Active Directory ou LDAP.

A criação de diretórios locais é útil em cenários como os seguintes.

- Você pode criar um diretório local para um tipo específico de usuário que não faz parte do diretório corporativo. Por exemplo, você pode criar um diretório local para parceiros, que geralmente não fazem parte do diretório corporativo, e fornecer acesso somente aos aplicativos específicos de que precisam.
- Você pode criar vários diretórios locais se desejar atributos de usuário ou métodos de autenticação diferentes para diferentes conjuntos de usuários. Por exemplo, você pode criar um diretório local para distribuidores que possua atributos de usuário, como região e tamanho de mercado, e outro diretório local para fornecedores que possua atributos de usuário, como um tipo de fornecedor e de categoria de produto.

Provedor de Identidade para Diretório do Sistema e Diretórios Locais

Por padrão, o Diretório do Sistema está associado a um provedor de identidade chamado Provedor de Identidade do Sistema. O método Senha (Diretório na Nuvem) está habilitado por padrão nesse provedor de identidade e aplica-se à política default_access_policy_set para o intervalo de rede TODOS OS INTERVALOS e o tipo de dispositivo do navegador da Web. Você pode configurar métodos de autenticação adicionais e definir políticas de autenticação.

Quando você cria um novo diretório local, ele não está associado a nenhum provedor de identidade. Depois de criar o diretório, crie um novo provedor de identidade do tipo Incorporado e associe o diretório a ele. Habilite o método de autenticação Senha (Diretório na Nuvem) no provedor de identidade. Vários diretórios locais podem ser associados ao mesmo provedor de identidade.

O conector do VMware Identity Manager não é necessário para o Diretório do Sistema ou para os diretórios locais que você cria.

Para obter mais informações, consulte "Configurando a autenticação de usuário no VMware Identity Manager" na *Administração do VMware Identity Manager*.

Gerenciamento de senhas para usuários do diretório local

Por padrão, todos os usuários de diretórios locais têm a capacidade de alterar sua senha no aplicativo ou no portal do Workspace ONE. Você pode definir uma política de senha para os usuários locais. Também pode redefinir senhas de usuários locais conforme necessário.

Os usuários podem alterar suas senhas quando estiverem conectados ao portal do Workspace ONE clicando no nome no canto superior direito, selecionando **Conta** no menu suspenso e clicando no link **Alterar Senha**. No aplicativo do Workspace ONE, os usuários podem alterar suas senhas clicando no ícone do menu da barra tripla e selecionando **Senha**.

Para obter informações sobre como definir políticas de senha e redefinir senhas de usuários locais, consulte "Gerenciando usuários e grupos" na *Administração do VMware Identity Manager*.

Este capítulo inclui os seguintes tópicos:

Criando um diretório local

Para criar um diretório local, especifique os atributos de usuário para o diretório, crie o diretório e identifique-o com um provedor de identidade.

1 Definir atributos do usuário no nível global na página 67

Antes de criar um diretório local, examine os atributos globais do usuário na página Atributos do Usuário e adicione atributos personalizados, se necessário.

2 Criar um diretório local na página 68

Após revisar e estabelecer os atributos globais do usuário, crie o diretório local.

3 Associar o diretório local a um provedor de identidade na página 70

Associe o diretório local a um provedor de identidade para que os usuários no diretório possam ser autenticados. Crie um novo provedor de identidade do tipo Incorporado e ative o método de autenticação Senha (Diretório Local) nele.

Definir atributos do usuário no nível global

Antes de criar um diretório local, examine os atributos globais do usuário na página Atributos do Usuário e adicione atributos personalizados, se necessário.

Os atributos do usuário, como firstName, lastName, email e domain, fazem parte do perfil de um usuário. No serviço do VMware Identity Manager, os atributos do usuário são definidos no nível global e se aplicam a todos os diretórios no serviço, incluindo diretórios locais. No nível de diretório local, você pode substituir se um atributo é obrigatório ou opcional para usuários nesse diretório local, mas não é possível adicionar atributos personalizados. Se um atributo for obrigatório, você deve fornecer um valor para ele ao criar um usuário.

As palavras a seguir não podem ser usadas quando você cria atributos personalizados.

Tabela 5-1. As palavras não podem ser usadas como Nomes de atributo de personalização.

ativo	endereços	costCenter
departamento	displayName	divisão
e-mails	employeeNumber	direitos
externalId	grupos	id
ims	localidade	gerente
meta	nome	nickName
organização	senha	phoneNumber
fotos	preferredLanguage	profileUrl
funções	fuso horário	título
userName	userType	x509Certificate

Observação A capacidade de substituir os atributos de usuário ao nível do diretório aplica-se apenas aos diretórios locais, não ao Active Directory nem aos diretórios do LDAP.

Procedimentos

1 No console de administração, clique na guia **Gerenciamento de Identidade e Acesso**.

2 Clique na guia **Configuração** e, em seguida, clique na guia **Atributos do Usuário**.

3 Revise a lista de atributos do usuário e adicione atributos adicionais, se necessário.

Observação Embora esta página permita que você selecione quais atributos são obrigatórios, é recomendável que você faça a seleção para diretórios locais no nível de diretório local. Se um atributo estiver marcado como obrigatório nesta página, ele se aplica a todos os diretórios no serviço, incluindo os diretórios do Active Directory ou LDAP.

4 Clique em **Salvar**.

Próximo passo

Crie um diretório local.

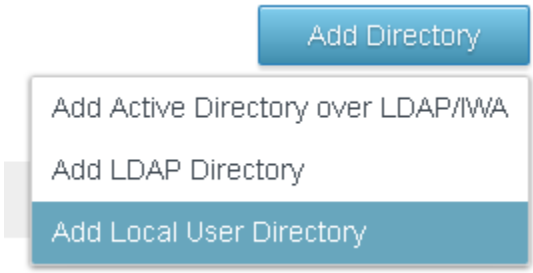
Criar um diretório local

Após revisar e estabelecer os atributos globais do usuário, crie o diretório local.

Procedimentos

1 No console de administração, clique na guia **Gerenciamento de Identidade e Acesso**; em seguida, clique na guia **Diretórios**.

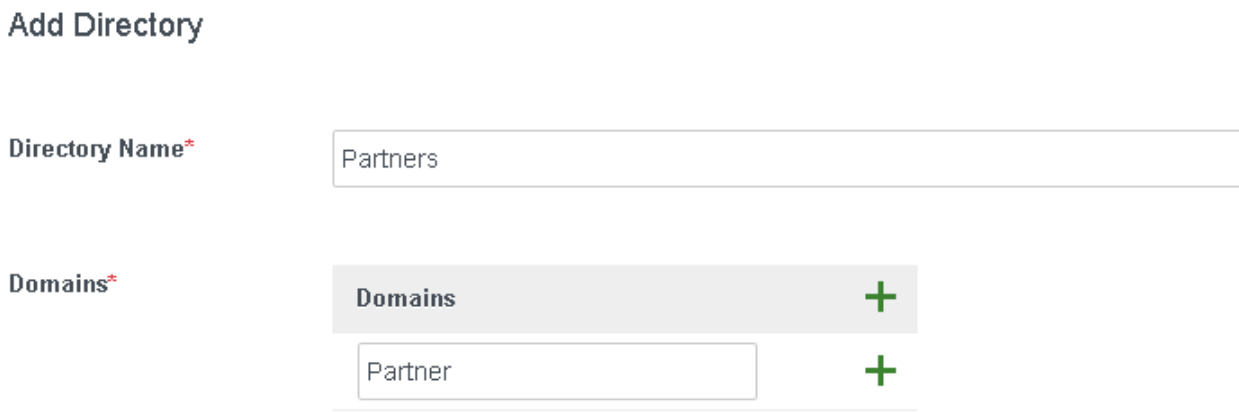
2 Clique em **Adicionar diretório** e selecione **Adicionar diretório de usuário local** a partir do menu suspenso.



3 Na página Adicionar diretório, digite o nome de um diretório e especifique ao menos o nome de um domínio.

O nome de domínio deve ser exclusivo em todos os diretórios do serviço.

Por exemplo:



4 Clique em **Salvar**.

5 Na página Diretórios, clique no novo diretório.

6 Clique na guia **Atributos do Usuário**.

Todos os atributos que constam na página Gerenciamento de Identidade e Acesso > Configuração > Atributos do usuário estão listados no diretório local. Os atributos nessa página marcados como obrigatórios são listados como obrigatórios também na página do diretório local.

7 Personalizar os atributos para o diretório local.

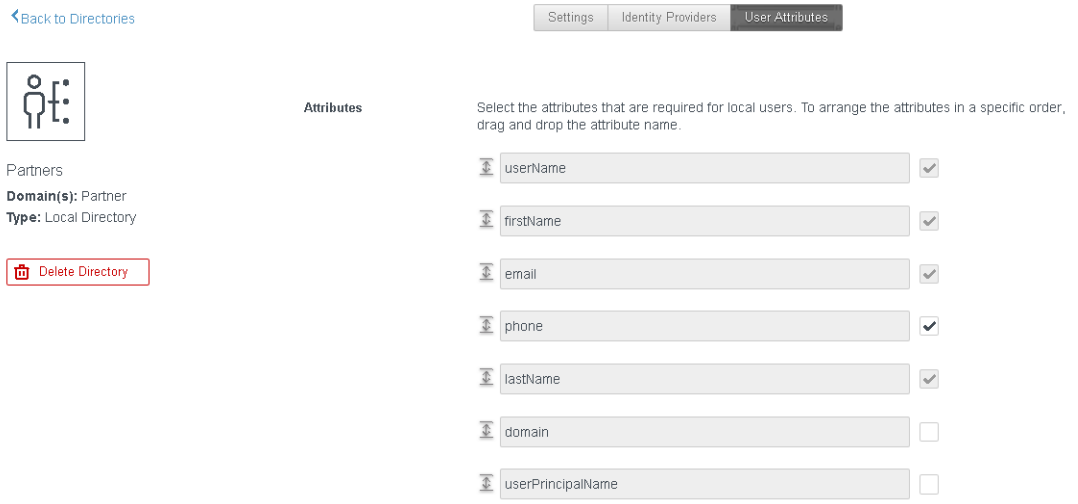
Você pode especificar quais atributos são obrigatórios e quais atributos são opcionais. Você também pode alterar a ordem na qual os atributos aparecem.

Importante Os atributos userName, firstName, lastName e email são sempre obrigatórios para diretórios locais.

- Para tornar um atributo obrigatório, marque a caixa de seleção adjacente ao nome do atributo.
- Para tornar um atributo obrigatório, desmarque a caixa de seleção adjacente ao nome do atributo.
- Para alterar a ordem dos atributos, clique e arraste o atributo para a nova posição.

Caso um atributo seja obrigatório, ao criar um usuário você deve especificar um valor para o atributo.

Por exemplo:



8 Clique em **Salvar**.

Próximo passo

Associe o diretório local ao provedor de identidade que você deseja usar para autenticar usuários no diretório.

Associar o diretório local a um provedor de identidade

Associe o diretório local a um provedor de identidade para que os usuários no diretório possam ser autenticados. Crie um novo provedor de identidade do tipo Incorporado e ative o método de autenticação Senha (Diretório Local) nele.

Observação Não use o provedor de identidade Integrado. Não é recomendável habilitar o método de autenticação Senha (Diretório local) no provedor de identidade Integrado.

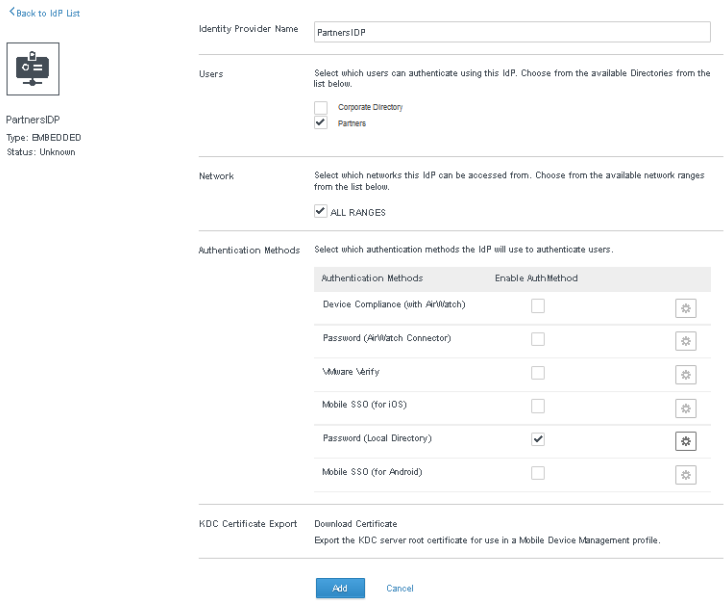
Procedimentos

1 Na guia **Gerenciamento de Identidade e Acesso**, clique na guia **Provedores de Identidade**.

2 Clique em **Adicionar Provedor de Identidade** e selecione **Criar IDP Integrado**.

3 Insira as seguintes informações.

Opção	Descrição
Nome do provedor de identidade	Digite um nome para o provedor de identidade.
Usuários	Selecione o diretório local criado.
Rede	Selecione as redes das quais esse provedor de identidade pode ser acessado.
Métodos de autenticação	Selecione Senha (Diretório Local).
Exportação de Certificado KDC	Você não precisa baixar o certificado, a menos que esteja configurando o SSO móvel para dispositivos iOS gerenciados pelo AirWatch.



4 Clique em **Adicionar**.

O provedor de identidade é criado e associado ao diretório local. Mais tarde, você pode configurar outros métodos de autenticação no provedor de identidade. Para obter mais informações sobre autenticação, consulte "Configurando a autenticação de usuário no VMware Identity Manager" na *Administração do VMware Identity Manager*.

Você pode usar o mesmo provedor de identidade para vários diretórios locais.

Próximo passo

Crie usuários e grupos locais. Você cria usuários e grupos locais na guia **Usuários e Grupos** no console de administração. Consulte "Gerenciando usuários e grupos" na *Administração do VMware Identity Manager* para obter mais informações.

Alterando as configurações do diretório local

Depois de criar um diretório local, você poderá modificar suas configurações a qualquer momento.

Você pode alterar as seguintes configurações.

- Altere o nome do diretório.
- Adicione, exclua ou renomeie domínios.
  - Os nomes de domínio devem ser exclusivos em todos os diretórios no serviço.
  - Ao alterar um nome de domínio, os usuários que estavam associados ao domínio antigo serão associados ao novo domínio.
  - O diretório deve ter pelo menos um domínio.
  - Não é possível adicionar um domínio ao Diretório do Sistema ou excluir o Domínio do Sistema.
- Adicione novos atributos do usuário ou torne um atributo existente obrigatório ou opcional.
  - Se o diretório local ainda não tiver nenhum usuário, você poderá adicionar novos atributos como opcionais ou obrigatórios e alterar os atributos existentes para obrigatórios ou opcionais.
  - Se você já criou usuários no diretório local, é possível adicionar novos atributos apenas como atributos opcionais e alterar os atributos existentes de obrigatórios para opcionais. Não é possível tornar um atributo opcional obrigatório após a criação dos usuários.

- Os atributos userName, firstName, lastName e email são sempre obrigatórios para diretórios locais.
- Como os atributos do usuário são definidos a nível global no serviço do VMware Identity Manager, todos os novos atributos que você adicionar aparecerão em todos os diretórios do serviço.

- Altere a ordem na qual os atributos aparecem.

Procedimentos

1 Clique na guia **Gerenciamento de Identidade e Acesso**.

2 Na página Diretórios, clique no diretório que você deseja editar.

3 Edite as configurações do diretório local.

Opção	Ação
Alterar o nome do diretório	a Na guia **Configurações**, edite o nome do diretório. b Clique em **Salvar**.
Adicionar, excluir ou renomear um domínio	a Na guia **Configurações**, edite a lista **Domínios** b Para adicionar um domínio, clique no ícone de mais verde. c Para excluir um domínio, clique no ícone de exclusão vermelho. d Para renomear um domínio, edite o nome de domínio na caixa de texto.
Adicionar atributos do usuário ao diretório	a Clique na guia **Gerenciamento de Identidade e Acesso** e, em seguida, clique em **Instalar**. b Clique na guia **Atributos do Usuário**. c Adicione atributos na lista **Adicionar outros atributos a usar** e clique em **Salvar**.
Tornar um atributo obrigatório ou opcional para o diretório	a Na guia **Gerenciamento de Identidade e Acesso**, clique na guia **Diretórios**. b Clique no nome do diretório local e na guia **Atributos do Usuário**. c Marque a caixa de seleção ao lado de um atributo para torná-lo um atributo obrigatório ou desmarque a caixa de seleção para torná-lo um atributo opcional. d Clique em **Salvar**.
Alterar a ordem dos atributos	a Na guia **Gerenciamento de Identidade e Acesso**, clique na guia **Diretórios**. b Clique no nome do diretório local e na guia **Atributos do Usuário**. c Clique e arraste os atributos para a nova posição. d Clique em **Salvar**.

Excluindo um diretório local

Você pode excluir um diretório local criado no serviço do VMware Identity Manager. Você não pode excluir o Diretório do Sistema, que é criado por padrão ao configurar o serviço pela primeira vez.

Cuidado Ao excluir um diretório, todos os usuários no diretório também são excluídos do serviço.

Procedimentos

1 Clique na guia **Gerenciamento de Identidade e Acesso** e, em seguida, clique na guia **Diretórios**.

2 Clique no diretório que deseja excluir.

3 Na página Diretórios, clique em **Excluir Diretório**.

Configuração avançada do appliance do VMware Identity Manager 6

Depois de concluir a instalação básica do appliance virtual do VMware Identity Manager, talvez seja necessário concluir outras tarefas de configuração, como ativar o acesso externo ao VMware Identity Manager e configurar a redundância.

O diagrama de arquitetura do VMware Identity Manager demonstra como você pode implantar o ambiente VMware Identity Manager. Consulte Capítulo 1, "Preparando a instalação do VMware Identity Manager", na página 9 para conhecer uma implantação típica.

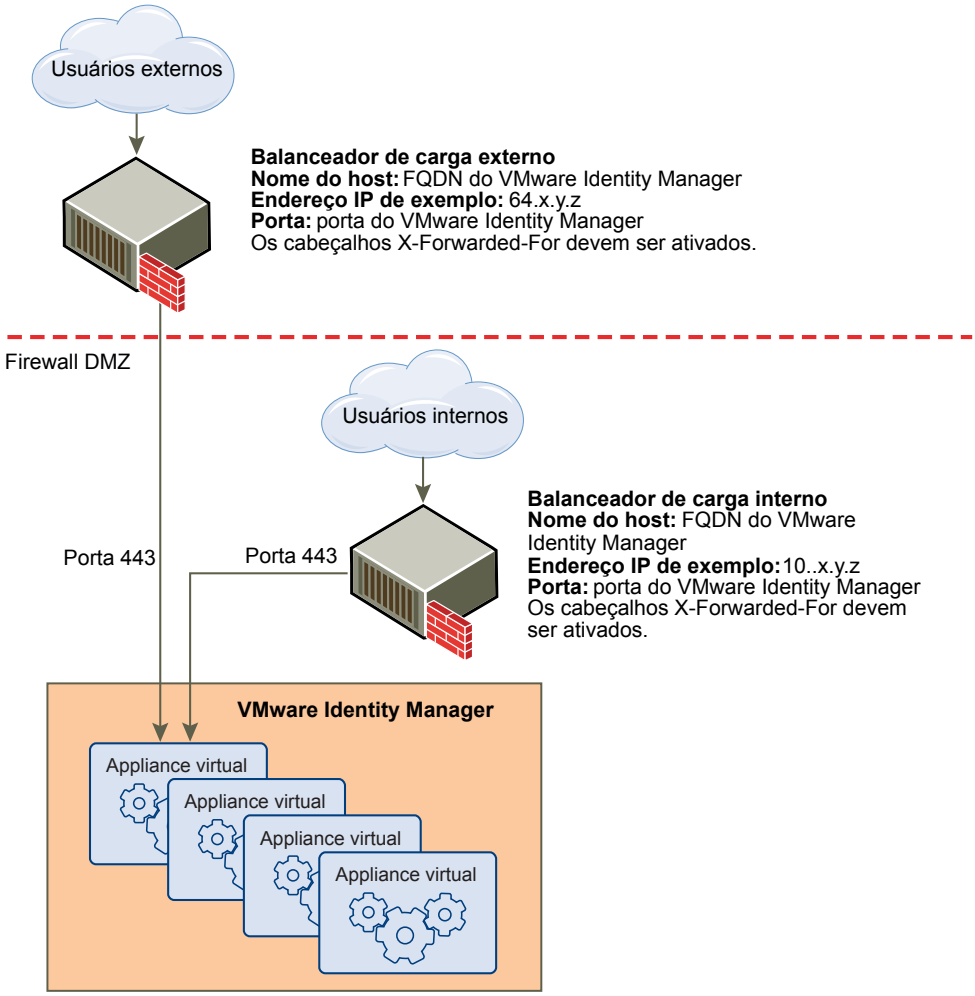
Este capítulo inclui os seguintes tópicos:

Usando um balanceador de carga ou proxy reverso para habilitar o acesso externo ao VMware Identity Manager

Durante a implantação, o appliance virtual do VMware Identity Manager é instalado na rede interna. Se você desejar fornecer acesso ao serviço aos usuários que se conectam de redes externas, deverá instalar um balanceador de carga ou um proxy reverso, como o Apache, o nginx, o F5 etc, no DMZ.

Se você não usar um balanceador de carga ou um proxy reverso, não poderá expandir o número de appliances do VMware Identity Manager depois. Talvez seja necessário adicionar mais dispositivos para fornecer redundância e balanceamento de carga. O diagrama a seguir mostra a arquitetura de implantação básica que você pode usar para ativar o acesso externo.

Figura 6-1. Proxy do balanceador de carga externo com máquina virtual



Especificar o FQDN do VMware Identity Manager durante a implantação

Durante a implantação da máquina virtual do VMware Identity Manager , insira o FQDN e o número da porta do VMware Identity Manager . Esses valores devem apontar para o nome do host que você deseja que os usuários finais acessem.

A máquina virtual do VMware Identity Manager é sempre executada na porta 443. Você pode usar um número da porta diferente para o balanceador de carga. Se você usar um número da porta diferente, deverá especificá-lo durante a implantação.

Definições do balanceador de carga a serem configuradas

As definições do balanceador de carga a serem configuradas incluem ativar cabeçalhos X-Forwarded-For, definir corretamente o tempo limite do balanceador de carga e ativar sessões fixas. Além disso, a confiança SSL deve ser configurada entre o appliance virtual do VMware Identity Manager e o balanceador de carga.

- Cabeçalhos X-Forwarded-For

  Você deve ativar os cabeçalhos X-Forwarded-For no seu balanceador de carga. Isso determina o método de autenticação. Consulte a documentação fornecida pelo fornecedor do seu balanceador de carga para obter mais informações.

- Tempo limite do balanceador de carga

Para que o VMware Identity Manager funcione corretamente, talvez você precise aumentar o padrão do tempo limite de solicitação do balanceador de carga. O valor é definido em minutos. Se a configuração de tempo limite for muito baixa, talvez você veja este erro: “Erro 502: o serviço está indisponível no momento”.

- Ativar sessões fixas

  Você deverá ativar a configuração de sessão fixa no balanceador de carga se sua implantação tiver vários appliances do VMware Identity Manager. Em seguida, o balanceador de carga associará a sessão de um usuário a uma instância específica.

Aplicar o certificado raiz do VMware Identity Manager ao balanceador de carga

Quando o appliance virtual do VMware Identity Manager é configurado com um balanceador de carga, você deve estabelecer a confiança SSL entre o balanceador de carga e o VMware Identity Manager. O certificado raiz do VMware Identity Manager deve ser copiado para o balanceador de carga.

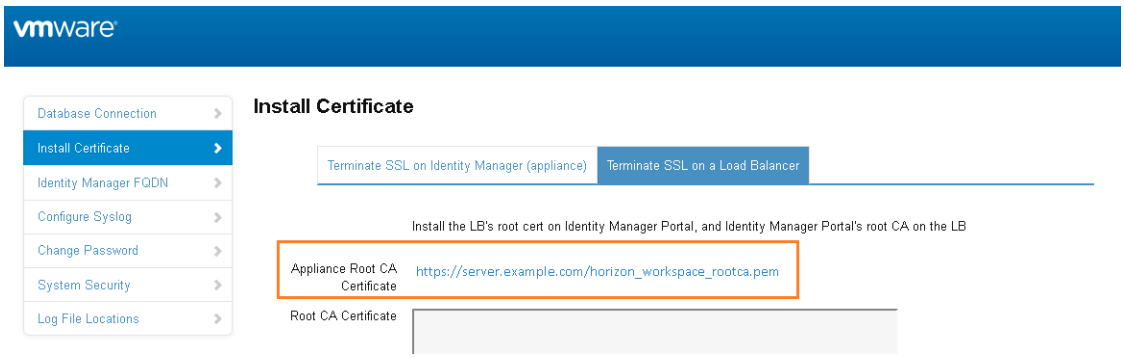
O certificado do VMware Identity Manager pode ser baixado no console de administração, na página **Configurações do Appliance > Configuração da VA > Gerenciar Configuração**.

Se o FQDN do VMware Identity Manager apontar para um balanceador de carga, o certificado SSL poderá ser aplicado somente ao balanceador de carga.

Como o balanceador de carga se comunica com o appliance virtual do VMware Identity Manager , você deve copiar o certificado da CA raiz do VMware Identity Manager para o balanceador de carga como um certificado raiz confiável.

Procedimentos

1. No console de administração, selecione a guia **Configurações do Appliance** e selecione **Configuração da VA**.
2. Clique em **Gerenciar Configuração**.
3. Selecione **Instalar Certificado**.
4. Selecione a guia **Encerrar o SSL em um Balanceador de Carga** e, no campo **Certificado da CA Raiz do Appliance**, clique no link `https://nome do host/horizon_workspace_rootca.pem`.



5. Copie tudo entre e incluindo as linhas -----BEGIN CERTIFICATE----- e -----END CERTIFICATE----, e cole o certificado raiz na localização correta em cada balanceador de carga. Consulte a documentação fornecida pelo fornecedor do seu balanceador de carga.

Próximo passo

Copie e cole o certificado raiz do balanceador de carga no appliance do VMware Identity Managerconector.

Aplicar o certificado raiz do balanceador de carga ao VMware Identity Manager

Quando o appliance virtual do VMware Identity Manager é configurado com um balanceador de carga, você deve estabelecer a confiança entre o balanceador de carga e o VMware Identity Manager. Além de copiar o certificado raiz do VMware Identity Manager para o balanceador de carga, você deverá copiar o certificado raiz do balanceador de carga para o VMware Identity Manager.

Procedimentos

1 Obtenha o certificado raiz do balanceador de carga.

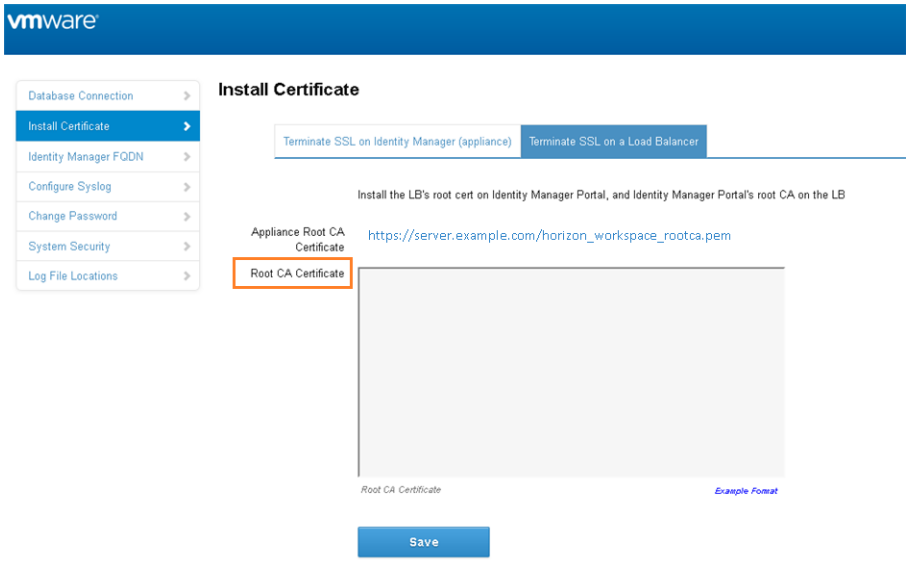
2 No console de administração do VMware Identity Manager, selecione a guia **Configurações do Appliance** e selecione **Configuração da VA**.

3 Clique em **Gerenciar Configuração**.

4 Faça login com a senha do usuário administrador.

5 Na página **Instalar Certificado**, selecione a guia **Encerrar o SSL em um Balanceador de Carga**.

6 Cole o texto do certificado do balanceador de carga no campo **Certificado da CA Raiz**.



7 Clique em **Salvar**.

Definindo as configurações do servidor proxy para o VMware Identity Manager

O appliance virtual do VMware Identity Manager acessa o catálogo de aplicativos em nuvem e outros serviços da Web na Internet. Se a sua configuração de rede fornece acesso à Internet por meio de um proxy HTTP, você deve ajustar suas configurações de proxy no appliance do VMware Identity Manager.

Habilite seu proxy para lidar apenas com o tráfego da Internet. Para garantir que o proxy seja configurado corretamente, defina o parâmetro para o tráfego interno como `no-proxy` no domínio.

Observação Os servidores proxy que exigem autenticação não são suportados.

Procedimentos

1 No cliente vSphere, faça login como o usuário raiz no appliance virtual do VMware Identity Manager.

2 Insira `YaST` na linha de comando para executar o utilitário `YaST`.

3 Selecione **Serviços de Rede** no painel esquerdo e selecione **Proxy**.

4 Insira as URLs do servidor proxy nos campos **URL do Proxy HTTP** e **URL do Proxy HTTPS**.

5 Selecione **Concluir** e saia do utilitário do `YaST`.

6 Reinicie o servidor Tomcat no appliance virtual do VMware Identity Manager para usar as novas configurações de proxy.

```
service horizon-workspace restart
```

O catálogo de aplicativos na nuvem e outros serviços da Web já estão disponíveis no VMware Identity Manager.

Configurando failover e redundância em um único centro de dados

Para obter failover e redundância, você pode adicionar vários appliances virtuais do VMware Identity Manager a um cluster. Se um dos appliances virtuais for encerrado por qualquer motivo, o VMware Identity Manager continuará disponível.

Primeiro, você instala e configura um appliance virtual do VMware Identity Manager; em seguida, você o clona. Clonar o appliance virtual cria uma duplicata do appliance com a mesma configuração do original. Você pode personalizar o appliance virtual clonado para alterar o nome, as configurações de rede e outras propriedades, conforme necessário.

Antes de clonar o appliance virtual do VMware Identity Manager, você deve configurá-lo atrás de um balanceador de carga e alterar o respectivo nome de domínio totalmente qualificado (FQDN) para corresponder ao FQDN do balanceador de carga. Além disso, conclua a configuração do diretório no serviço do VMware Identity Manager antes de clonar o appliance.

Após a clonagem, atribua ao appliance virtual clonado um novo endereço IP antes de ligá-lo. O endereço IP do appliance virtual clonado deve seguir as mesmas diretrizes do endereço IP do appliance virtual original. O endereço IP deve ser resolvido para um nome do host válido usando DNS progressivo e reverso.

Todos os nós no cluster do VMware Identity Manager são cópias idênticas e quase sem monitoração de estado um do outro. A sincronização com o Active Directory e os recursos configurados, como View ou ThinApp, é desativada nas máquinas virtuais clonadas.

1 Número recomendado de nós no cluster do VMware Identity Manager na página 78

   É recomendável configurar um cluster do VMware Identity Manager com três nós.

2 Alterar o FQDN do VMware Identity Manager para o FQDN do balanceador de carga na página 78

   Antes de clonar o appliance virtual do VMware Identity Manager, você deve alterar o respectivo nome de domínio totalmente qualificado (FQDN) para corresponder ao FQDN do balanceador de carga.

3 Clonar o appliance virtual na página 79

4 Atribuir um novo endereço IP a um appliance virtual clonado na página 80

   Você deve atribuir um novo endereço IP a cada appliance virtual clonado antes de ligá-lo. O endereço IP deve poder ser resolvido no DNS. Se o endereço não estiver no DNS reverso, você também deverá atribuir o nome do host.

5 Ativando a sincronização de diretório em outra instância do em caso de falha na página 82

6 Removendo um nó de um cluster na página 83

   Se um nó no cluster do VMware Identity Manager não estiver funcionando corretamente e você não conseguir recuperá-lo, poderá removê-lo do cluster com o comando Remover Nó. O comando remove as entradas do nó do banco de dados do VMware Identity Manager.

Número recomendado de nós no cluster do VMware Identity Manager

É recomendável configurar um cluster do VMware Identity Manager com três nós.

O appliance do VMware Identity Manager inclui o ElasticSearch, um mecanismo de pesquisa e análise. O Elasticsearch tem uma limitação conhecida com clusters de dois nós. Para obter uma descrição da limitação "cérebro dividido" do ElasticSearch, consulte a documentação do Elasticsearch. Observe que você não precisa configurar nenhuma definição do ElasticSearch.

Um cluster do VMware Identity Manager com dois nós fornece a capacidade de failover com algumas limitações relacionadas ao ElasticSearch. Se um dos nós for encerrado, as seguintes limitações serão aplicadas até que o nó seja reativado:

- O painel não exibe dados.
- A maioria dos relatórios não estão disponíveis.
- As informações de log de sincronização não são exibidas para os diretórios.
- O campo de pesquisa no canto superior direito do console de administração não retorna nenhum resultado.
- O preenchimento automático não está disponível para campos de texto.

Não há perda de dados durante o período durante o qual o nó está inativo. Os dados de log de evento de auditoria e sincronização são armazenados e serão exibidos quando o nó é restaurado.

Alterar o FQDN do VMware Identity Manager para o FQDN do balanceador de carga

Antes de clonar o appliance virtual do VMware Identity Manager, você deve alterar o respectivo nome de domínio totalmente qualificado (FQDN) para corresponder ao FQDN do balanceador de carga.

Pré-requisitos

- O appliance do VMware Identity Manager é adicionado a um balanceador de carga.
- Você aplicou o certificado da CA raiz do balanceador de carga ao VMware Identity Manager.

Procedimentos

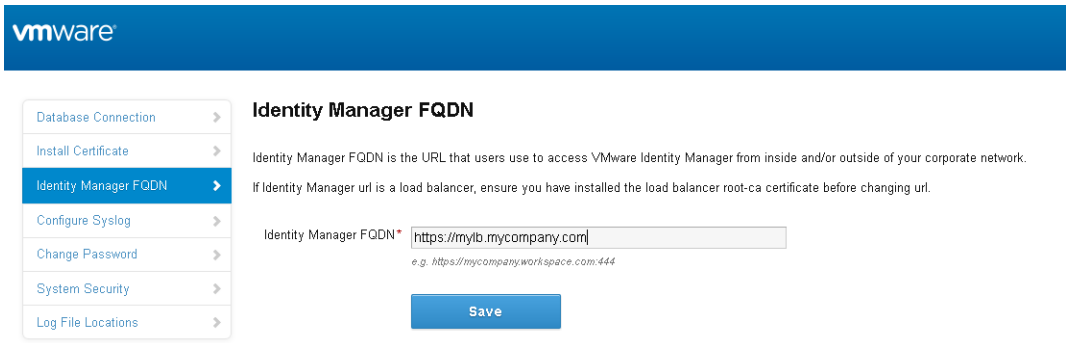
1. Faça login no console de administração do VMware Identity Manager.
2. Selecione a guia **Configurações do Appliance**.
3. Na página Configuração do Appliance Virtual, clique em **Gerenciar Configuração**.
4. Insira sua senha do administrador para fazer login.
5. Clique em **Configuração do Identity Manager**.
6. No campo **FQDN do Identity Manager**, altere a parte do nome do host da URL do nome do host do VMware Identity Manager para o nome do host do balanceador de carga.

   Por exemplo, se o nome do host do VMware Identity Manager for `meuserviço` e seu nome do host do balanceador de carga for `meubc`, você alteraria a URL

   `https://myservice.mycompany.com`

   para o seguinte:

   `https://meubc.minhaempresa.com`



7 Clique em **Salvar**.

- O FQDN do serviço é alterado para o FQDN do balanceador de carga.
- A URL do Provedor de Identidade é alterada para a URL do balanceador de carga.

Próximo passo

Clone o appliance virtual.

Clonar o appliance virtual

Clone o appliance virtual do VMware Identity Manager para criar vários appliances virtuais do mesmo tipo para distribuir o tráfego e eliminar o tempo de inatividade potencial.

Usar vários appliances virtuais do VMware Identity Manager melhora a disponibilidade, balanceia a carga das solicitações ao serviço e diminui os tempos de resposta para o usuário final.

Pré-requisitos

- O appliance virtual do VMware Identity Manager deve ser configurado atrás de um balanceador de carga. Verifique se a porta do balanceador de carga é 443. Não utilize 8443, pois esse número de porta é a porta administrativa e é exclusivo de cada appliance virtual.
- Um banco de dados externo é configurado conforme descrito em "Conectando-se ao banco de dados", na página 32.
- Certifique-se de ter concluído a configuração do diretório em VMware Identity Manager.
- Faça login no console do appliance virtual como raiz e exclua o arquivo `/etc/udev/rules.d/70-persistent-net.rules`, se ele existir. Se você não excluir esse arquivo antes da clonagem, a rede não estará configurada corretamente no appliance virtual clonado.

Procedimentos

1 Faça login no vSphere Client ou no vSphere Web Client e navegue até o appliance virtual do VMware Identity Manager.

2 Clique com o botão direito do mouse no appliance virtual e selecione **Clonar**.

3 Insira o nome do appliance virtual clonado e clique em **Avançar**.

O nome deve ser exclusivo na pasta da VM.

4 Selecione o host ou o cluster no qual executar o aplicativo virtual clonado e clique em **Avançar**.

5 Selecione o pool de recursos no qual executar o aplicativo virtual e clique em **Avançar**.

6 Para o formato de disco virtual, selecione **Mesmo formato da origem**.

7 Selecione a localização do repositório de dados na qual você deseja armazenar os arquivos do appliance virtual e clique em **Avançar**.

8 Selecione **Não personalizar** como a opção do sistema operacional guest.

9 Revise as opções e clique em **Concluir**.

O appliance virtual clonado é implantado. Você não pode usar ou editar o appliance virtual até que a clonagem seja concluída.

Próximo passo

Atribua um endereço IP ao appliance virtual clonado antes de ligá-lo e adicioná-lo ao balanceador de carga.

Atribuir um novo endereço IP a um appliance virtual clonado

Você deve atribuir um novo endereço IP a cada appliance virtual clonado antes de ligá-lo. O endereço IP deve poder ser resolvido no DNS. Se o endereço não estiver no DNS reverso, você também deverá atribuir o nome do host.

Procedimentos

1 No vSphere Client ou no vSphere Web Client, selecione o appliance virtual clonado.

2 Na guia **Resumo**, em **Comandos**, clique em **Editar Configurações**.

3 Selecione **Opções** e, na lista **Opções do vApp**, selecione **Propriedades**.

4 Altere o endereço IP no campo **Endereço IP**.

5 Se o endereço IP não estiver no DNS reverso, adicione o nome do host na caixa de texto **Nome do Host**.

6 Clique em **OK.**

7 Ligue o appliance clonado e aguarde até que a tela de login azul seja exibida na guia **Console**.

Importante Antes de ligar o appliance clonado, verifique se o appliance original está totalmente ligado.

Próximo passo

- Aguarde alguns minutos até que o cluster do Elasticsearch seja criado antes da adição do appliance virtual clonado ao balanceador de carga.

  O Elasticsearch, um mecanismo de pesquisa e análise, está incorporado no appliance virtual.

  a Faça login no appliance virtual clonado.

  b Verifique o cluster Elasticsearch:

  ```
  curl –XGET 'http://localhost:9200/_cluster/health?pretty=true'
  ```

  Verifique se o resultado corresponde ao número de nós.

- Adicione o appliance virtual clonado ao balanceador de carga e configure o balanceador de carga para distribuir o tráfego. Consulte a documentação do fornecedor do balanceador de carga para obter informações.

- Se você tiver ingressado em um domínio na instância original do serviço, precisará ingressar no domínio nas instâncias do serviço clonado.

  a Faça login no console de administração do VMware Identity Manager.

  b Selecione a guia **Gerenciamento de identidade e acesso** e clique em **Instalar**.

  O componente de conector de cada uma das instâncias do serviço clonado é listado na página Conectores.

  c Para cada conector na lista, clique em **Ingressar no Domínio** e especifique as informações do domínio.

Para obter mais informações sobre o Active Directory, consulte "Integrando com o Active Directory", na página 45.

- Para diretórios do tipo Autenticação Integrada do Windows (IWA), faça o seguinte:

  a Para as instâncias do serviço clonado, ingresse no domínio no qual o diretório IWA na instância original do serviço ingressou.

    1 Faça login no console de administração do VMware Identity Manager.

    2 Selecione a guia **Gerenciamento de identidade e acesso** e clique em **Instalar**.

      O componente de conector de cada uma das instâncias do serviço clonado é listado na página Conectores.

    3 Para cada conector na lista, clique em **Ingressar no Domínio** e especifique as informações do domínio.

  b Salve a configuração do diretório IWA.

    1 Selecione a guia **Gerenciamento de Identidade e Acesso**.

    2 Na página Diretórios, clique no link do diretório IWA.

    3 Clique em **Salvar** para salvar a configuração do diretório.

- Se você atualizou manualmente o arquivo `/etc/krb5.conf` na instância de serviço original, por exemplo, para resolver a falha ou a lentidão da sincronização do View, você deve atualizar o arquivo na instância clonada depois que ela for associada ao domínio. Em todas as instâncias de serviço clonadas, execute as seguintes tarefas.

  a Edite o arquivo `/etc/krb5.conf` e atualize a seção `realms` para especificar os mesmos valores de domínio para host que são usados no arquivo `/usr/local/horizon/conf/domain_krb.properties`. Não é necessário especificar o número da porta. Por exemplo, se o seu arquivo `domain_krb.properties` tiver a entrada de domínio `example.com=examplehost.example.com:389`, você atualizaria o arquivo `krb5.conf` para o seguinte.

```
[realms]
GAUTO-QA.COM = {
auth_to_local = RULE:[1:$0\$1](^GAUTO-QA\.COM\\.*)s/^GAUTO-QA\.COM/GAUTO-QA/
auth_to_local = RULE:[1:$0\$1](^GAUTO-QA\.COM\\.*)s/^GAUTO-QA\.COM/GAUTO-QA/
auth_to_local = RULE:[1:$0\$1](^GAUTO2QA\.GAUTO-QA\.COM\\.*)s/^GAUTO2QA\.GAUTO-
QA\.COM/GAUTO2QA/
auth_to_local = RULE:[1:$0\$1](^GLOBEQE\.NET\\.*)s/^GLOBEQE\.NET/GLOBEQE/
auth_to_local = DEFAULT
kdc = examplehost.example.com
}
```

  Observação É possível ter várias entradas kdc. No entanto, não é uma exigência uma vez que, na maioria dos casos, há apenas um único valor kdc. Se você optar por definir valores kdc adicionais, cada linha terá uma entrada kdc que definirá um controlador de domínio.

  b Reinicie o serviço do espaço de trabalho.

```
service horizon-workspace restart
```

Observação Consulte também Knowledge Base article 2091744.

- Ative os métodos de autenticação configurados para o conector em cada uma das instâncias clonadas. Consulte o *Guia de administração do VMware Identity Manager* para obter informações.

O appliance virtual do serviço do VMware Identity Manager é agora altamente disponível. O tráfego é distribuído para os appliances virtuais no seu cluster com base na configuração do balanceador de carga. A autenticação no serviço é altamente disponível. Para o recurso de sincronização de diretório do serviço, no entanto, em caso de uma falha da instância do serviço, você precisará ativar manualmente a sincronização do diretório em uma instância do serviço clonado. A sincronização de diretório é manipulada pelo componente de conector do serviço e pode ser ativada somente em um conector por vez. Consulte "Ativando a sincronização de diretório em outra instância do em caso de falha", na página 82.

Ativando a sincronização de diretório em outra instância do em caso de falha

Em caso de uma falha da instância do serviço, a autenticação é manipulada automaticamente por uma instância clonada, conforme configurado no balanceador de carga. No entanto, para a sincronização de diretório, você precisa modificar as configurações de diretório no serviço do VMware Identity Manager para usar uma instância clonada. A sincronização de diretório é manipulada pelo componente de conector do serviço e pode ser ativada somente em um conector por vez.

Procedimentos

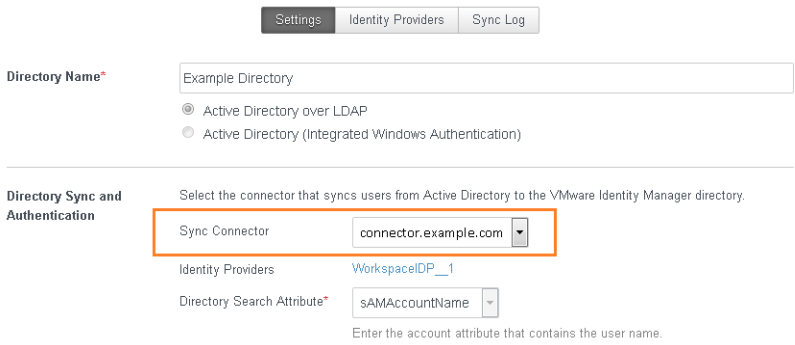
1 Faça login no console de administração do VMware Identity Manager.

2 Clique na guia **Gerenciamento de Identidade e Acesso** e, em seguida, clique em **Diretórios**.

3 Clique no diretório que era associado à instância original do serviço.

Você pode exibir essas informações na página **Instalar > Conectores**. A página lista o componente do conector de cada um dos appliances virtuais do serviço no seu cluster.

4 Na seção **Sincronização e Autenticação do Diretório** da página do diretório, no campo **Sincronizar Conector**, selecione um dos outros conectores.



5 No campo **Senha do DN do Bind**, insira a senha da conta de associação do Active Directory.

6 Clique em **Salvar**.

Removendo um nó de um cluster

Se um nó no cluster do VMware Identity Manager não estiver funcionando corretamente e você não conseguir recuperá-lo, poderá removê-lo do cluster com o comando Remover Nó. O comando remove as entradas do nó do banco de dados do VMware Identity Manager.

Você pode verificar a integridade dos nós no cluster exibindo seus status no Painel de Diagnóstico do Sistema. Uma mensagem `O nó atual está em um estado incorreto` indica que o nó não está funcionando corretamente.

Importante Use o comando Remover Nó com moderação. Use-o somente se um nó estiver em um estado irrecuperável e tiver de ser removido completamente da implantação do VMware Identity Manager.

Observação Você não pode usar o comando Remover Nó para remover o último nó em um cluster.

Desassociar o componente do conector dos domínios, das configurações de sincronização de diretório e do provedor de identidade integrado

Antes de poder remover um nó de um cluster do VMware Identity Manager, você deve garantir que o componente do conector do nó não esteja vinculado a qualquer domínio, não esteja sendo usado como um conector de sincronização e não esteja associado ao provedor de identidade integrado.

Pré-requisitos

Você deve efetuar logon como administrador de tenant, ou seja, um administrador local no serviço do VMware Identity Manager. Um administrador de domínio sincronizado a partir do diretório corporativo não possui as permissões necessárias.

Procedimentos

1 Faça login no console de administração.

2 Clique na guia **Gerenciamento de Identidade e Acesso** e, em seguida, clique em **Instalar**.

A página Conectores é exibida.

3 Se o componente do conector do nó estiver associado ao domínio, saia do domínio.

a Na página Conectores, localize o componente do conector do nó que você deseja remover.

O componente do conector tem o mesmo nome que o nó.

b Se a coluna **Ações Disponíveis** mostrar o botão **Sair do Domínio**, clique no botão para sair do domínio.

4 Se o componente do conector do nó estiver sendo usado como o conector de sincronização para qualquer diretório, altere a configuração do conector de sincronização do diretório para usar outro conector.

a Na coluna **Diretório Associado** na página Conectores, visualize os diretórios aos quais o componente do conector está associado.

b Clique no link de um diretório.

c Na seção **Sincronização e Autenticação de diretório** da página do diretório, verifique o valor da opção **Conector de Sincronização**.

d Se o componente do conector estiver sendo usado como o conector de sincronização, selecione outro conector para a opção **Conector de Sincronização** e clique em **Salvar**.

e Repita essas etapas para todos os diretórios aos quais o componente do conector está associado.

5 Se o componente do conector estiver associado ao provedor de identidade integrado, remova-o do provedor de identidade.

   a Na página Conectores, na coluna **Provedor de Identidade**, visualize os provedores de identidade aos quais o componente do conector está associado.

   b Se o provedor de identidade integrado estiver listado, clique no link.

   c Na página do provedor de identidade, na seção **Conectores**, clique no ícone de exclusão ao lado do conector.

Próximo passo

Remova o nó do cluster.

Remover o nó do cluster

Depois de desassociar o componente do conector do nó dos domínios, as configurações de sincronização de diretório e o fornecedor de identidade integrado, você poderá remover o nó do cluster.

Observação Você não pode usar o comando Remover para remover o último nó em um cluster.

Pré-requisitos

- Para remover um nó, você deve efetuar logon como administrador de tenant, ou seja, um administrador local no serviço do VMware Identity Manager. Um administrador de domínio sincronizado a partir do diretório corporativo não possui as permissões necessárias.
- Você desassociou o componente de conector do nó dos domínios, as configurações de sincronização de diretório e o provedor de identidade integrado, se necessário. Consulte "Desassociar o componente do conector dos domínios, das configurações de sincronização de diretório e do provedor de identidade integrado", na página 83.

Procedimentos

1 Encerre a máquina virtual do nó.

   a Faça logon na instância do vCenter Server.

   b Clique com o botão direito do mouse na máquina virtual do nó e selecione **Ligar > Desligar**.

2 Remova o nó do balanceador de carga.

3 No console de administração do VMware Identity Manager, remova o nó.

   a Faça logon no console de administração do VMware Identity Manager como administrador local.

   b Clique na seta para baixo na guia **Painel** e selecione **Painel de Diagnóstico do Sistema**.

   c Localize o nó que você deseja remover.

   O nó exibe o seguinte status:

   ```
   O nó atual está em um estado incorreto. Deseja removê-lo?
   ```

   d Clique no link **Remover** que é exibido ao lado da mensagem.

O nó é removido do cluster. As entradas para o nó são removidas do banco de dados do VMware Identity Manager. O nó também é removido dos clusters incorporados Elasticsearch e Ehcache.

Próximo passo

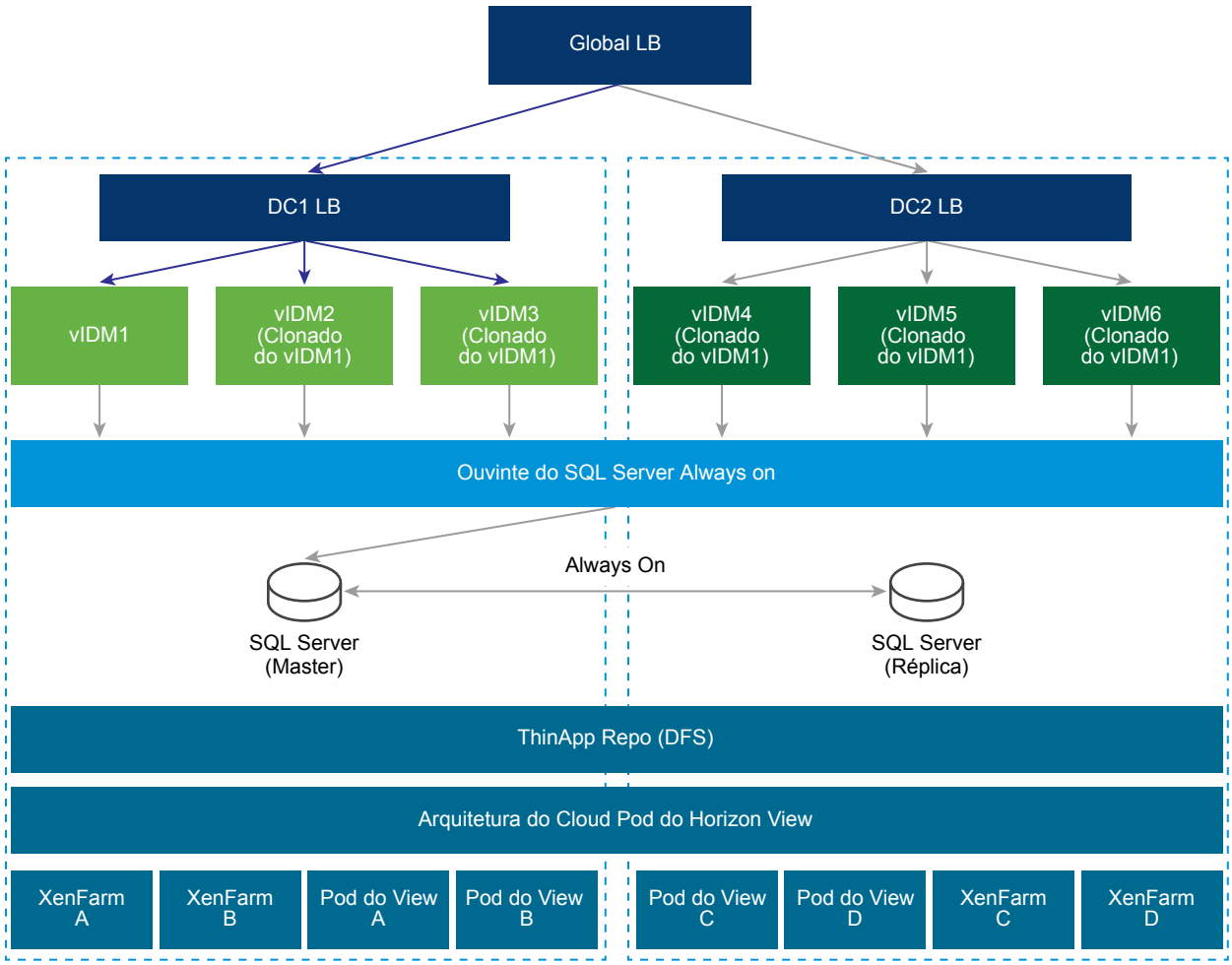
Aguarde de 5 a 15 minutos para que os clusters incorporados Elasticsearch e Ehcache se estabilizem antes de usar qualquer outro comando.

Implantando o VMware Identity Manager em um centro de dados secundário para failover e redundância.

Para fornecer funcionalidades se o centro de dados principal do VMware Identity Manager ficar indisponível, o VMware Identity Manager precisará ser implantado em um centro de dados secundário.

Usando um centro de dados secundário, os usuários finais podem fazer login e usar os aplicativos sem nenhum tempo de inatividade. Um centro de dados secundário também permite que os administradores tenham a capacidade de atualizar o VMware Identity Manager para a próxima versão sem nenhum tempo de inatividade. Consulte "Atualizando o VMware Identity Manager sem paralisação", na página 95.

Mostramos aqui uma implantação típica usando um centro de dados secundário.



Siga essas orientações para uma implantação de vários centros de dados.

- Implantação de cluster: Você precisa implantar um conjunto de três ou mais appliances virtuais do VMware Identity Manager como cluster em um centro de dados e outro conjunto de três ou mais appliances virtuais como outro cluster no centro de dados secundário. Consulte "Configurando um centro de dados secundário", na página 87 para obter mais informações.
- Banco de dados: o VMware Identity Manager usa o banco de dados para armazenar os dados. Para a implantação de vários centros de dados, a replicação do banco de dados entre os dois centros de dados é crucial. Consulte a documentação de seu banco de dados a respeito de como definir um banco de dados em vários centros de dados. Por exemplo, com o SQL Server, recomendamos o uso da

implantação Always On. Para obter mais informações, consulte Visão geral doa grupos de disponibilidade do Always On (SQL Server) no site da Microsoft. VMware Identity Manager as funcionalidades esperam muito pouca latência entre o banco de dados e o appliance do VMware Identity Manager. Portanto, a expectativa é a de que os os appliances de um centro de dados conectem-se a um banco de dados no mesmo centro de dados.

- Não ativo-ativo: o VMware Identity Manager não suporta uma implantação ativo-ativo em que os usuários possam receber serviço de ambos os centros de dados simultaneamente. O centro de dados secundário é do tipo espera quente e pode ser usado para fornecer a continuidade dos negócios para os usuários finais. Os appliances do VMware Identity Manager no centro de dados secundário estão em modo somente leitura. Assim, após um failover nesse centro de dados, a maioria das operações dos administradores, como adicionar usuários ou aplicativos, ou autorizar usuários, não funcionará.
- Failback para um principal: Na maior parte dos casos de falha, você poderá executar failback para o centro de dados principal já que o centro de dados voltou ao normal. Consulte "Failback para centro de dados principal", na página 94 para obter informações.
- Promover um secundário a principal: No caso de uma falha estendida no centro de dados, o centro de dados secundário pode ser promovido a principal. Consulte "Promovendo um centro de dados secundário a principal", na página 94 para obter informações.
- Nome de domínio totalmente qualificado: O nome de domínio totalmente qualificado para acessar o VMware Identity Manager deve ser o mesmo em todos os centros de dados.
- Auditorias: VMware Identity Manager usa o Elasticsearch incorporado ao appliance do VMware Identity Manager para auditorias, relatórios e logs de sincronização de diretório. Os clusters separados do Elasticsearch têm de ser criados em cada centro de dados. Consulte "Configurando um centro de dados secundário", na página 87 para obter mais informações.
- Active Directory: o VMware Identity Manager pode conectar-se ao Active Directory usando a API LDAP ou a Autenticação integrada do Windows. Em ambos os métodos, o VMware Identity Manager pode aproveitar os registros do Active Directory para encontrar o controlador de domínio adequado em cada centro de dados.
- Aplicativos do Windows: o VMware Identity Manager suporta acessar os aplicativos do Windows usando o ThinApp e os aplicativos e desktops do Windows por meio do Horizon View ou das tecnologias Citrix. Em geral, é importante fornecer esses recursos a partir de um centro de dados que esteja mais próximo do usuário, também denominado Geo-Affinity. Observe o seguinte a respeito dos recursos do Windows:
  - ThinApps - o VMware Identity Manager suporta o Windows Distributed File Systems (Sistemas de arquivos distribuídos no Windows) como um repositório do ThinApp. Use a documentação do Windows Distributed File Systems (Sistemas de arquivos distribuídos no Windows) para definir políticas adequadas relacionadas especificamente ao local.
  - O Horizon View (com a Arquitetura do Cloud Pod) - o VMware Identity Manager suporta a Arquitetura do Cloud Pod do Horizon. A Arquitetura do Cloud Pod do Horizon oferece o Geo-Affinity usando direitos globais. Consulte "Integrando as implantações da Arquitetura do Cloud Pod" no *Definindo recursos no VMware Identity Manager* para obter mais informações. Não há nenhuma alteração adicional obrigatória para a implantação do VMware Identity Manager em vários centros de dados.
  - O Horizon View (sem a Arquitetura do Cloud Pod) - caso a Arquitetura do Cloud Pod do Horizon não esteja habilitada em seu ambiente, você não poderá habilitar o Geo-Affinity. Após um failover, você poderá mudar manualmente o VMware Identity Manager para inicializar os recursos do Horizon View a partir dos pods do View configurados no centro de dados secundário. Consulte "Configurar ordem de failover do Horizon View e dos recursos baseados em Citrix", na página 91 para obter mais informações.

- Recursos Citrix - Assim como acontece com o Horizon View (sem a Arquitetura do Cloud Pod), você não poderá habilitar o Geo-Affinity para os recursos Citrix. Após um failover, você poderá mudar manualmente o VMware Identity Manager para inicializar os recursos Citrix a partir dos pods do XenFarms configurados no centro de dados secundário. Consulte "Configurar ordem de failover do Horizon View e dos recursos baseados em Citrix", na página 91 para obter mais informações.

Configurando um centro de dados secundário

O centro de dados secundário normalmente é gerenciado por um vCenter Server diferente. Quando você configura o centro de dados secundário, pode configurar e implementar as opções a seguir com base nos seus requisitos.

- Os appliances do VMware Identity Manager no centro de dados secundário de um arquivo OVA importado do centro de dados principal
- Balanceador de carga do centro de dados secundário
- Recursos e direitos duplicados do Horizon View e dos baseados em Citrix
- Configuração do banco de dados
- Balanceador de carga ou entrada DNS nos centros de dados primário e secundário para failover

Modificar o centro de dados principal para replicação

Antes de configurar o centro de dados secundário, configure o centro de dados principal para a replicação de Elasticsearch e Ehcache nos clusters.

Elasticsearch e Ehcache são incorporados no appliance virtual do VMware Identity Manager. O Elasticsearch é um mecanismo de pesquisa e de análise usado para auditorias, relatórios e logs de sincronização de diretório. O Ehcache fornece funcionalidades de cache.

Configure essas alterações em todos os nós do cluster do centro de dados principal.

Pré-requisitos

Você definiu um cluster VMware Identity Manager no centro de dados principal.

Procedimentos

1 Configure o Elasticsearch para replicação.

Faça essas alterações em todos os nós do cluster do centro de dados principal.

a Desabilite o trabalho cron para o Elasticsearch.

1 Edite o arquivo `/etc/cron.d/hznelasticsearchsync`:

```
vi /etc/cron.d/hznelasticsearchsync
```

2 Assinale a seguinte linha como comentário:

```
#*/1 * * * * root /usr/local/horizon/scripts/elasticsearchnodes.hzn
```

b Adicione os endereços IP de todos os nós do cluster do centro de dados principal.

1 Edite o arquivo `/etc/sysconfig/elasticsearch`:

```
vi /etc/sysconfig/elasticsearch
```

2 Adicione os endereços IP de todos os nós do cluster:

```
ES_UNICAST_HOSTS=endereçoIP1,endereçoIP2,endereçoIP3
```

c Adicione o balanceador de carga FQDN do cluster do centro de dados secundário no arquivo `/usr/local/horizon/conf/runtime-config.properties`.

1 Edite o arquivo `/usr/local/horizon/conf/runtime-config.properties`.

```
vi /usr/local/horizon/conf/runtime-config.properties
```

2 Adicione esta linha ao arquivo:

```
analytics.replication.peers=LB_FQDN_do_segundo_cluster
```

2 Configure o Ehcache para replicação.

Faça essas alterações em todos os nós do cluster do centro de dados principal.

a `vi /usr/local/horizon/conf/runtime-config.properties`

b Adicione o FQDN de todos os nós do cluster. Não adicione o FQDN para o nó que você estiver editando. Separe os FQDNs com dois pontos.

```
ehcache.replication.rmi.servers=nó2FQDN:nó3FQDN
```

Por exemplo:

```
ehcache.replication.rmi.servers=server2.example.com:server3.example.com
```

3 Reinicie o serviço do VMware Identity Manager em todos os nós.

```
service horizon-workspace restart
```

4 Verifique se o cluster está configurado adequadamente.

Execute esses comandos em todos os nós do primeiro cluster.

a Verifique a integridade do Elasticsearch.

```
curl 'http://localhost:9200/_cluster/health?pretty'
```

O comando deve retornar um resultado semelhante ao seguinte.

```
        {
  "cluster_name" : "horizon",
  "status" : "green",
  "timed_out" : false,
  "number_of_nodes" : 3,
  "number_of_data_nodes" : 3,
```

```
  "active_primary_shards" : 20,
  "active_shards" : 40,
  "relocating_shards" : 0,
  "initializing_shards" : 0,
  "unassigned_shards" : 0,
  "delayed_unassigned_shards" : 0,
  "number_of_pending_tasks" : 0,
  "number_of_in_flight_fetch" : 0
}
```

Caso haja problemas, consulte "Solucionando problemas no Elasticsearch", na página 106.

b Verifique se o arquivo `/opt/vmware/horizon/workspace/logs/ horizon.log` contém esta linha.

```
Added ehcache replication peer: //node3.example.com:40002
```

O nome do host deve ser o mesmo dos outros nós do cluster.

Próximo passo

Crie um cluster no centro de dados secundário. Crie os nós exportando o arquivo OVA do primeiro appliance virtual do VMware Identity Manager a partir do cluster do centro de dados principal e usando-o para implantar os novos appliances no centro de dados secundário.

Criar appliances virtuais do VMware Identity Manager no centro de dados secundário

Para configurar um cluster do VMware Identity Manager no centro de dados secundário, exporte o arquivo OVA do appliance original do VMware Identity Manager no centro de dados primário e use-o para implantar appliances no centro de dados secundário.

Pré-requisitos

- O arquivo OVA do VMware Identity Manager que foi exportado do appliance original do VMware Identity Manager no centro de dados primário
- Endereços IP e registros DNS para centro de dados secundário

Procedimentos

1 No centro de dados primário, exporte o arquivo OVA do appliance original do VMware Identity Manager.

Consulte a documentação do vSphere para obter informações.

2 No centro de dados secundário, implante o arquivo OVA do VMware Identity Manager que foi exportado para criar os novos nós.

Consulte a documentação do vSphere para obter informações. Consulte também "Instalar o arquivo OVA do VMware Identity Manager", na página 19.

3 Depois que os appliances do VMware Identity Manager forem ligados, atualize a configuração de cada appliance.

Os appliances do VMware Identity Manager no centro de dados secundário são cópias idênticas do appliance original do VMware Identity Manager no centro de dados primário. A sincronização com o Active Directory e com os recursos configurados no centro de dados primário é desativada.

Próximo passo

Acesse as páginas do console de administração e configure o seguinte:

- Habilite a opção Ingressar no Domínio, conforme configurado no appliance original do VMware Identity Manager no centro de dados primário.

- Na página Adaptadores de Autenticação, adicione os métodos de autenticação que estão configurados no centro de dados primário.
- Na página Método de Autenticação de Diretório, ative a autenticação do Windows se ela estiver configurada no centro de dados primário.

Acesse a página Instalar Certificado do configurações do appliance para adicionar certificados assinados pela autoridade de certificação, duplicando os certificados nos appliances do VMware Identity Manager no centro de dados primário. Consulte "Usando certificados SSL", na página 36.

Configurar os nós no centro de dados secundário

Depois que você tiver criado os nós no centro de dados secundário usando o arquivo OVA exportado do centro de dados primário, configure os nós.

Siga esses passos para cada um dos nós contidos no centro de dados secundário.

Procedimentos

- Atualizar as tabelas de IP.
  a. No arquivo `/usr/local/horizon/scripts/updateiptables.hzn` , atualize os endereços IP de todos os nós contidos no centro de dados secundário.
     1. `vi /usr/local/horizon/scripts/updateiptables.hzn`
     2. Encontre e substitua a linha `ALL_IPS`. Especifique o endereço IP delimitado por um espaço.

        `ALL_IPS="Nó1_endereçoIP Nó2_endereçoIP Nó3_endereçoIP"`
     3. Abra as portas executando este script.

        `/usr/local/horizon/scripts/updateiptables.hzn`
  b. Configure os nós para a replicação do Elasticsearch e do Ehcache e verifique se eles estão configurados corretamente.

     Veja as instruções em "Modificar o centro de dados principal para replicação", na página 87 e aplique-as aos nós no centro de dados secundário.

     Observe que os trabalhos cron já estão desabilitados.

Editar o arquivo runtime-config.properties no centro de dados secundário

Caso você esteja usando um banco de dados que não seja a implantação SQL Server Always On, você deverá editar os arquivos `runtime-config.properties` para os appliances do VMware Identity Manager no centro de dados secundário para alterar a URL JDBC de modo que ela aponte para o banco de dados no centros de dados secundário e configure o appliance para acesso somente leitura. Caso você esteja usando uma implantação SQL Server Always On, essa etapa não é obrigatória.

Faça essas alterações em cada appliance do VMware Identity Manager no centro de dados secundário.

Procedimentos

1. Usando um cliente ssh, faça login no appliance do VMware Identity Manager como o usuário root.
2. Abra o arquivo `runtime-config.properties` em `/usr/local/horizon/conf/runtime-config.properties`.
3. Altere a URL do JDBC para apontar para o banco de dados do centro de dados secundário.

   Consulte "Configurar o VMware Identity Manager para usar um banco de dados externo", na página 35.
4. Configure o appliance do VMware Identity Manager para ter acesso somente leitura.

   Adicione a linha `read.only.service=true`.

5 Reinicie o servidor Tomcat no appliance.

```
service horizon-workspace restart
```

Configurar ordem de failover do Horizon View e dos recursos baseados em Citrix

Para o Horizon View e recursos baseados em Citrix, você deve configurar a ordem de failover dos recursos nos centros de dados primário e secundário para disponibilizar os recursos adequados a partir de qualquer centro de dados.

Use o comando hznAdminTool para criar uma tabela de banco de dados com a ordem de failover dos recursos na sua organização por instância de serviço. A ordem de failover configurada é seguida quando um recurso é inicializado. Execute o `hznAdminTool failoverConfiguration` em ambos os centros de dados para configurar a ordem de failover.

Pré-requisitos

Quando o VMware Identity Manager é implantado em vários centros de dados, os mesmos recursos também são configurados em cada centro de dados. Cada pool de aplicativos ou desktops nos Pods do View ou XenFarms baseados em Citrix é considerado um recurso diferente no catálogo do VMware Identity Manager. Para evitar a duplicação do recurso no catálogo, verifique se você ativou a opção **Não sincronizar aplicativos duplicados** nas páginas Pools do View ou Aplicativos Publicados - Citrix na página console de administração.

Procedimentos

1 Usando um cliente ssh, faça login no appliance do VMware Identity Manager como o usuário root.

2 Para ver uma lista das instâncias do servidor, digite `hznAdminTool serviceInstances`.

A lista das instâncias de serviço com o número de ID atribuído é exibida, como neste exemplo.

```
{"id":103,"hostName":"ws4.domain.com","ipaddress":"10.142.28.92"}{"id":
154,"hostName":"ws3.domain.com","ipaddress":"10.142.28.91"}{"id":
1,"hostName":"ws1.domain.com","ipaddress":"10.143.104.176"}{"id":
52,"hostName":"ws2.domain.com","ipaddress":"10.143.104.177"}
```

3 Para cada instância de serviço na sua organização, configure a ordem de failover dos recursos do View e baseados em Citrix.

Digite o `hznAdminTool failoverConfiguration –configType <configType> –configuration <configuration> –serviceInstanceId <serviceInstanceId> [–orgId <orgId>]`.

Opção	Descrição
-configType	Digite o tipo de recurso a ser configurado para failover. Os valores são `VIEW` ou `XENAPP`.
-configuration	Digite a ordem de failover. Para o tipo de configuração VIEW configType, digite uma lista separada de nomes de host do View Connector Server listados na página Pools do View no console de administração. Para XENAPP configType, digite uma lista de nomes do XenFarm separados por vírgula.
-serviceInstanceId	Digite o ID da instância de serviço para a qual a configuração é definida. O ID pode ser encontrado na lista exibida na Etapa 2, `"id":`
-orgId	(Opcional). Se for deixada em branco, a configuração será definida para a organização padrão.

Por exemplo, `hznAdminTool failoverConfiguration –configType VIEW –configuration pod1vcs1.domain.com,pod2vcs1.hs.trcint.com –orgId 1 –serviceInstanceId 1`.

Quando você digitar esse comando para as instâncias do VMware Identity Manager no centro de dados secundário, inverta a ordem dos Servidores de Conexão do View. Nesse exemplo, o comando seria `hznAdminTool failoverConfiguration –configType VIEW –configuration pod2vcs1.hs.trcint.com, pod1vcs1.domain.com –orgId 1 –serviceInstanceId 103`

A tabela de banco de dados dos recursos de failover é configurada para cada centro de dados.

Próximo passo

Para ver a configuração de failover existente para cada um dos recursos do View e baseados em Citrix, execute `hznAdminTool failoverConfigurationList –configType <configtype> –<orgId)`.

O valor de <configtype> é VIEW ou XENAPP. Este é um exemplo de saída de `hznAdminTool failoverConfiguraitonList` com configType VIEW.

```
{"idOrganization":1,"serviceInstanceId":
52,"configType":"VIEW","configuration":"pod1vcs1.domain.com,pod2vcs1.domain.com"}
{"idOrganization":1,"serviceInstanceId":
103,"configType":"VIEW","configuration":"pod2vcs1.domain.com,pod1vcs1.domain.com"}
{"idOrganization":1,"serviceInstanceId":
154,"configType":"VIEW","configuration":"pod2vcs1.domain.com,pod1vcs1.domain.com"}
```

Configurar um banco de dados para failover

No VMware Identity Manager, a replicação de banco de dados é configurada para que os dados sejam consistentes entre os servidores de banco de dados no centro de dados primário e no centro de dados secundário.

Você deve configurar seu banco de dados externo para alta disponibilidade. Configure uma arquitetura de banco de dados mestre e escravo, na qual o escravo é uma réplica exata do mestre.

Consulte a documentação de seu banco de dados externo para obter mais informações.

Caso você esteja usando um SQL Server Always On, use o nome do host ou o endereço IP do ouvinte do SQL Server ao configurar o banco de dados em cada appliance do VMware Identity Manager. Por exemplo:

`jdbc:sqlserver://<listener_hostname>;DatabaseName=saas`

Failover para o centro de dados secundário

Quando ocorre uma falha no centro de dados principal, você pode ressincronizar com o centro de dados secundário. Para ressincronizar, modifique o balanceador de carga global ou o registro de DNS para apontar para o balanceador de carga do centro de dados principal.

Dependendo da configuração de seu banco de dados, os appliances do VMware Identity Manager localizados no centro de dados secundário estarão apenas em modo leitura ou em modo leitura-gravação. Para todos os bancos de dados, com exceção do SQL Server Always On, os appliances do VMware Identity Manager estão em modo leitura-gravação. Portanto, a maior parte das operações de administrador, como adicionar usuários ou aplicativos, ou autorizar usuários, não estão disponíveis.

Caso você esteja usando uma implantação SQL Server Always On, os appliances do VMware Identity Manager localizados no centro de dados estarão em modo leitura-gravação.

Usando um registro DNS para controlar qual centro de dados está ativo

Se você usar um registro Sistema de Nomes de Domínio (DNS) para direcionar o tráfego de usuários rota nos seus centros de dados, o registro DNS deverá apontar para um balanceador de carga no centro de dados primário em situações normais de funcionamento.

Se o centro de dados primário se tornar indisponível, o registro DNS deverá ser atualizado para apontar para o balanceador de carga no centro de dados secundário.

Quando o centro de dados primário se tornar disponível novamente, o registro DNS deverá ser atualizado para apontar para o balanceador de carga no centro de dados primário.

Definindo a vida útil no registro DNS

A definição de vida útil (TTL) determina quanto tempo deve decorrer antes que as informações relacionadas a DNS sejam atualizadas no cache. Para um failover perfeito de desktops e aplicativos do View, certifique-se de que a vida útil (TTL) nos registros DNS seja curta. Se a configuração TTL for definida como um período muito longo, talvez os usuários não consigam acessar os respectivos desktops e aplicativos do View imediatamente após o failover. Para ativar a atualização rápida do DNS, defina o TTL do DNS como 30 segundos.

Atividades do VMware Identity Manager não disponíveis no modo somente leitura

Usar o VMware Identity Manager no modo somente leitura é projetado para alta disponibilidade para permitir que os usuários finais acessem os recursos no respectivo portal Meus Aplicativos. Algumas atividades no console de administração do VMware Identity Manager e em outras páginas de serviços de administração podem não estar disponíveis no modo somente leitura. Abaixo está uma lista parcial das atividades comuns que não estão disponíveis.

Quando o VMware Identity Manager está em execução no modo somente leitura, as atividades relacionadas a alterações no Active Directory ou no banco de dados não podem ser realizadas e a sincronização com o banco de dados do VMware Identity Manager não funciona.

As funções administrativas que exigem a gravação no banco de dados não estão disponíveis durante esse tempo. Você deve esperar até que o VMware Identity Manager retorne para o modo de leitura e gravação.

Modo somente leitura do console de administração do VMware Identity Manager

A seguir estão algumas das limitações do console de administração no modo somente leitura.

- Adicionar, excluir e editar usuários e grupos na guia **Usuários e grupos**
- Adicionar, excluir e editar aplicativos na guia **Catálogo**
- Adicionar, excluir e editar direitos de aplicativo
- Alterar informações de identidade visual
- Sincronização de Diretório para adicionar, editar e excluir usuários e grupos
- Editar informações sobre recursos, incluindo recursos do View, do XenApp e de outros
- Editar a página Métodos de Autenticação

Observação Os componentes de conector dos appliances do VMware Identity Manager no centro de dados secundário são exibidos no console de administração. Certifique-se de não selecionar um conector no centro de dados secundário como o conector de sincronização.

Modo apenas leitura das páginas de configuração do Virtual Appliance

A seguir estão algumas das limitações nas páginas Configuração do appliance no modo somente leitura

- Testar a configuração da conexão do banco de dados
- Alterar a senha do administrador na página Alterar senha

Modo somente leitura do Portal de aplicativos do usuário final

Quando o VMware Identity Manager está no modo somente leitura, os usuários podem entrar no respectivo portal do VMware Identity Manager e acessar os recursos. As funcionalidades a seguir no portal do usuário final não estão disponíveis no modo somente leitura.

- Marcar ou desmarcar um recurso como Favorito

- Adicione recursos que constam na página Catálogo ou remova os recursos constantes na página Inicializador
- Altere a senha atribuída a eles a partir da página do portal de aplicativos

Modo somente leitura do cliente Windows do VMware Identity Manager

Quando o VMware Identity Manager está no modo somente leitura, os usuários não podem configurar novos clientes Windows. Os clientes Windows existentes continuam a funcionar.

Failback para centro de dados principal

Na maioria dos cenários, você poderá ressincronizar com o centro de dados principal uma vez que esse centro de dados está funcionando novamente.

Procedimentos

1 Modifique o balanceador de carga global ou o registro de DNS para apontar para o balanceador de carga do centro de dados principal.

Consulte "Usando um registro DNS para controlar qual centro de dados está ativo", na página 92.

2 Limpe o cache no centro de dados secundário.

Você pode usar as REST APIs para limpar o cache.

CAMINHO: /SAAS/jersey/manager/api/removeAllCaches

Método: POST

Funções permitidas: apenas OPERADOR

Promovendo um centro de dados secundário a principal

No caso de uma falha estendida no centro de dados, o centro de dados secundário pode ser promovido a principal.

Para uma implantação do SQL Server Always On, não é necessário fazer nenhuma alteração. Para outras configurações relativas ao banco de dados, é preciso editar o arquivo `runtime-config.properties` nos appliances do VMware Identity Manager no centro de dados secundário para configurar os appliances para o modo somente leitura.

Faça essas alterações em cada appliance do VMware Identity Manager no centro de dados secundário.

Procedimentos

1 Usando um cliente ssh, faça login no appliance do VMware Identity Manager como o usuário root.

2 Abra o arquivo `/usr/local/horizon/conf/runtime-config.properties`.

3 Altere a linha `read.only.service=true` para `read.only.service=false`.

4 Salve o arquivo `runtime-config.properties`.

5 Reinicie o servidor Tomcat no appliance.

```
service horizon-workspace restart
```

Atualizando o VMware Identity Manager sem paralisação

Com uma implantação de centro de dados múltiplo, você pode atualizar o VMware Identity Manager para a próxima versão sem nenhum tempo de inatividade. Use esta sugestão de fluxo de trabalho para implementar atualizações.

Consulte o diagrama em "Implantando o VMware Identity Manager em um centro de dados secundário para failover e redundância.", na página 85 ao seguir estas etapas.

Procedimentos

1 Mude o roteamento do Global LB para enviar as solicitações ao DC2 LB.

2 Interrompa a replicação do banco de dados.

3 Atualize o appliance virtual vIDM1; em seguida, atualize o appliance virtual vIDM2; só então atualize o appliance virtual vIDM3.

4 Atualizações de teste usando o DC1-LB.

5 Assim que estiver satisfeito, mude para o Global LB de modo que ele faça as solicitações de roteamento para o DC1 LB.

6 Atualize o appliance virtual vIDM4; em seguida, atualize o appliance virtual vIDM5; só então atualize o appliance virtual vIDM6.

7 Atualizações de teste usando o DC2-LB.

8 Inicie a replicação do banco de dados.

Instalando appliances do conector adicionais

7

O conector é uma parte do serviço do VMware Identity Manager. Quando você instala um appliance virtual do VMware Identity Manager, um componente de conector é sempre incluído por padrão.

O conector executa as funções a seguir.

- Sincroniza os dados de usuário e grupo entre o seu diretório empresarial e o diretório correspondente criado no serviço.
- Quando usado como um provedor de identidade, autentica os usuários no serviço.

  O conector é o provedor de identidade padrão.

Como um conector já está disponível como parte do serviço, você não precisa instalar um conector adicional em implantações típicas.

Em alguns cenários, no entanto, um conector adicional pode ser necessário. Por exemplo:

- Se você tiver vários diretórios do tipo Active Directory (Autenticação Integrada do Windows), precisará de um conector separado para cada um.

  A instância do conector pode ser associada a vários diretórios. Uma partição chamada agente de trabalho é criada no conector para cada diretório. No entanto, você não pode ter dois agentes de trabalho do tipo Autenticação Integrada do Windows na mesma instância do conector.
- Se você desejar gerenciar o acesso dos usuários com base em se eles fizeram login de um local interno ou externo.
- Se você desejar usar a autenticação baseada em certificados, mas o balanceador de carga estiver configurado para encerrar o SSL no balanceador de carga. A autenticação de certificado exige a passagem SSL no balanceador de carga.

Para instalar um conector adicional, realize as tarefas a seguir.

- Faça download do pacote OVA do conector.
- Gere um token de ativação no serviço.
- Implante o appliance virtual do conector.
- Defina as configurações do conector.

Qualquer conector adicional que você implantar será exibido na interface do usuário do serviço.

Este capítulo inclui os seguintes tópicos:

Gerar código de ativação do conector

Antes de implantar o appliance virtual do conector, gere um código de ativação para o novo conector no serviço do VMware Identity Manager. O código de ativação do conector é usado para estabelecer a comunicação entre o serviço e o conector.

Procedimentos

1 Faça login no console de administração do VMware Identity Manager.

2 Clique na guia **Gerenciamento de Identidade e Acesso**.

3 Clique em **Instalar**.

4 Na página Conectores, clique em **Adicionar Conector**.

5 Insira um nome para a nova instância do conector.

6 Clique em **Gerar Código de Ativação**.

O código de ativação é exibido no campo **Código de Ativação do Conector**.

7 Copie e salve o código de ativação do conector.

Você usará o código de ativação ao executar o Assistente de Configuração do Conector.

Próximo passo

Instale o appliance virtual do conector.

Implantar o arquivo OVA do Conector

Faça download do arquivo OVA do conector e implante-o usando o VMware vSphere Client ou o vSphere Web Client.

Pré-requisitos

- Identifique os registros DNS e o nome do host para ser usado na implantação do OVA do conector.
- Se estiver usando o vSphere Web Client, use os navegadores Firefox ou Chrome. Não use o Internet Explorer para implantar o arquivo OVA.
- Faça download do arquivo OVA do conector.

Procedimentos

1 No vSphere Client ou no vSphere Web Client, selecione **Arquivo > Implantar Modelo OVF**.

2 Nas páginas Implantar Modelo OVF, insira as informações específicas para a implantação do conector.

Página	Descrição
Origem	Navegue até a localização do pacote OVA ou insira uma URL específica.
Detalhes do modelo OVA	Verifique se você selecionou a versão correta.
Licença	Leia o contrato de licença de usuário final e clique em **Aceitar**.
Nome e localização	Insira um nome para o appliance virtual. O nome deve ser exclusivo na pasta de inventário e pode conter até 80 caracteres. Os nomes diferenciam maiúsculas de minúsculas. Insira uma localização para o appliance virtual.
Host/Cluster	Selecione o host ou cluster para executar o modelo implantado.
Pool de recursos	Selecione o pool de recursos.
Armazenamento	Selecione a localização para armazenar os arquivos da máquina virtual.

Página	Descrição
Formato do disco	Selecione o formato do disco para os arquivos. Para ambientes de produção, selecione um formato de **Provisionamento Estático**. Use o formato de **Provisionamento Dinâmico** para avaliação e teste.
Mapeamento de rede	Mapeie as redes no seu ambiente para as redes no modelo OVF.
Propriedades	a No campo **Configuração de fuso horário**, selecione o fuso horário correto. b A caixa de seleção Programa de Aperfeiçoamento da Experiência do Cliente é selecionada por padrão. A VMware coleta dados anônimos sobre sua implantação para melhorar a resposta da VMware às necessidades do usuário. Desmarque a caixa de seleção se você não desejar que os dados sejam coletados. c Na caixa de texto Nome do Host, insira o nome do host a ser usado. Se estiver em branco, o DNS reverso será usado para procurar o nome do host. d Para configurar o endereço IP estático do conector, insira o endereço para cada uma das seguintes opções: gateway padrão, DNS, Endereço IP e máscara de rede. **Importante** Se qualquer um dos quatro campos de endereço, incluindo o nome do host, forem deixados em branco, o DHCP será usado. Para configurar o DHCP, deixe os campos de endereço em branco.
Pronto para ser concluído	Revise as seleções e clique em **Finalizar**.

Dependendo da velocidade da rede, a implantação pode levar vários minutos. Você pode exibir o progresso na caixa de diálogo de progresso.

3 Quando a implantação estiver concluída, selecione o appliance do , clique com o botão direito do mouse e selecione **Potência > Ativar**.

O appliance do é inicializado. Você pode ir até a guia **Console** para ver os detalhes. Após a conclusão da inicialização do appliance virtual, a tela do console exibe a versão do e as URLs para se fazer login no assistente de instalação do a fim de concluir a instalação.

Próximo passo

Use o Assistente de instalação para adicionar o código de ativação e as senhas administrativas.

Configurar as definições do Conector

Depois que o OVA do conector for distribuído e instalado, execute o Assistente de Instalação para ativar o appliance e configurar as senhas de administrador.

Pré-requisitos

- Você tem o código de ativação do novo conector. Consulte "Gerar código de ativação do conector", na página 98.
- Verifique se o appliance conector está ligado e você conhece a URL do conector.
- Colete uma lista de senhas a serem usadas pelo administrador do conector, pela conta raiz e pela conta sshuser.

Procedimentos

1 Para executar o assistente de configuração, insira a URL do conector que foi exibida na guia Console após a implantação do OVA.

2 Na página de boas-vindas, clique em **Continuar**.

3 Crie senhas de alta segurança para as seguintes contas de administrador do appliance virtual do conector.

As senhas de alta segurança devem ter pelo menos oito caracteres e incluir letras maiúsculas e minúsculas e pelo menos um caractere numérico ou especial.

Opção	Descrição
Administrador do appliance	Crie a senha do administrador do appliance. O nome do usuário é **admin** e não pode ser alterado. Use esta conta e senha para fazer login nos serviços do conector para gerenciar certificados, senhas do appliance e configurações do Syslog. **Importante** A senha do usuário **administrador** deve ter pelo menos 6 caracteres.
Conta raiz	Uma senha raiz padrão da VMware foi usada para instalar o appliance do conector. Criar uma nova senha raiz.
Conta de usuário SSH	Crie a senha a ser usada para o acesso remoto ao appliance do conector.

4 Clique em **Continuar**.

5 Na página Ativar Conector, cole o código de ativação e clique em **Continuar**.

O código de ativação é verificado e a comunicação entre o serviço e a instância do conector é estabelecida.

A configuração do conector é concluída.

Próximo passo

No serviço, configure o ambiente com base em suas necessidades. Por exemplo, se você adicionou um conector adicional porque deseja sincronizar dois diretórios de autenticação integrada do Windows, crie o diretório e associe-o ao novo conector.

Configure certificados SSL para o conector. Consulte "Usando certificados SSL", na página 36.

Usando o KDC integrado

8

Para a autenticação SSO móvel para iOS em dispositivos iOS gerenciados pelo AirWatch, você pode usar o KDC integrado. Você inicializa manualmente o Centro de Distribuição de Chave (KDC) no appliance antes de habilitar o método de autenticação a partir do console de administração.

Observação Quando você integrar o VMware Identity Manager ao AirWatch em um ambiente do Windows, use o serviço hospedado na nuvem do KDC do VMware Identity Manager, não o KDC integrado. O uso do KDC na nuvem requer a seleção do nome de território apropriado na página do adaptador de autenticação do iOS a partir do console de administração. Veja o Guia de Administração do VMware Identity Manager.

Antes de inicializar o KDC no VMware Identity Manager, determine o nome do território para o servidor do KDC; se os subdomínios estão na sua implantação e se deseja usar o certificado do servidor do KDC padrão ou não.

Território

O território é o nome de uma entidade administrativa que mantém os dados de autenticação. É importante selecionar um nome descritivo para o território de autenticação Kerberos. O nome do território deve ser parte de um domínio DNS que a empresa pode configurar.

O nome do território e o nome de domínio totalmente qualificado (FQDN) que são usados para acessar o serviço do VMware Identity Manager são independentes. Sua empresa deve controlar os domínios DNS do nome do território e do FQDN. A convenção é fazer com que o nome do território seja o mesmo que o seu nome de domínio, inserido em letras maiúsculas. Às vezes o nome do território e de domínio são diferentes. Por exemplo, um nome de território é *EXEMPLO.NET*, e *idm.exemplo.com* é o FQDN do VMware Identity Manager. Nesse caso, você pode definir as entradas DNS de ambos os domínios *exemplo.net* e *exemplo.com*.

O nome do território é usado por um cliente Kerberos para gerar nomes DNS. Por exemplo, quando o nome é exemplo.com, o nome relacionado do Kerberos para entrar em contato com o KDC por TCP é *_kerberos._tcp.EXEMPLO.COM*.

Usando subdomínios

O serviço do VMware Identity Manager instalado em um ambiente local pode usar o subdomínio do FQDN do VMware Identity Manager. Caso seu site do VMware Identity Manager acesse vários domínios DNS, configure os domínios como local1.exemplo.com; local2.exemplo.com; local3.exemplo.com. O do valor subdomínio nesse caso é exemplo.com, digitado em letras minúsculas. Para configurar um subdomínio no seu ambiente, trabalhe com a sua equipe de suporte ao serviço.

Usando certificados de servidor KDC

Quando o KDC é inicializado, por padrão, um certificado de servidor KDC e um certificado raiz autoassinado são gerados. O certificado é usado para emitir o certificado de servidor KDC. Esse certificado raiz é incluído no perfil do dispositivo de modo a que o dispositivo possa confiar no KDC.

Você pode gerar manualmente o certificado do servidor KDC usando um certificado raiz ou intermediário da empresa. Entre em contato com sua equipe de suporte ao serviço para obter mais detalhes sobre esse recurso.

Baixe o certificado raiz do servidor do KDC no console de administração do VMware Identity Manager a ser usado na configuração do AirWatch do perfil de gerenciamento de dispositivos iOS.

Este capítulo inclui os seguintes tópicos:

Inicializar o centro de distribuição de chaves no appliance

Antes de poder utilizar o SSO Móvel para método de autenticação iOS, você deve inicializar o Centro de Distribuição de Chaves (KDC) no appliance do VMware Identity Manager.

Para inicializar o KDC, atribua o seu nome do host do Identity Manager aos territórios Kerberos. O nome de domínio é inserido em letras maiúsculas. Se você estiver configurando vários territórios Kerberos, para ajudar a identificar o domínio, use nomes descritivos que terminam com o seu nome de domínio do Identity Manager. Por exemplo, VENDAS.MEU-IDENTITYMANAGER.EXEMPLO.COM. Se você configurar subdomínios, digite o nome do subdomínio em letras minúsculas.

Pré-requisitos

O VMware Identity Manager está instalado e configurado.

Nome do território identificado. Consulte Capítulo 8, "Usando o KDC integrado", na página 101.

Procedimentos

1 Entre usando SSH no appliance do VMware Identity Manager como o usuário root.

2 Inicialize o KDC. Insira `/etc/init.d/vmware-kdc init --realm {REALM.COM} --subdomain {sva-name.subdomain}`.

  Por exemplo, `/etc/init.d/vmware-kdc init --realm MY-IDM.EXAMPLE.COM --subdomain my-idm.example.com`

  Se você estiver usando um balanceador de carga com vários appliances do Identity Manager, utilize o nome do balanceador de carga em ambos os casos.

3 Reinicie o serviço do VMWare Identity Manager. Insira `service horizon-workspace restart`.

4 Inicie o serviço do KDC. Insira `service vmware-kdc restart`.

Próximo passo

Crie entradas DNS públicas. Os registros DNS devem ser provisionados para permitir que os clientes localizem o KDC. Consulte "Criando várias entradas de DNS público para o KDC com o Kerberos integrado", na página 103.

Criando várias entradas de DNS público para o KDC com o Kerberos integrado

Depois de inicializar o KDC no VMware Identity Manager, você deverá criar registros DNS públicos para permitir que os clientes Kerberos localizem o KDC quando o recurso de autenticação Kerberos integrado estiver ativado.

O nome do território do KDC é usado como parte do nome DNS para as entradas do appliance do VMware Identity Manager que são usadas para descobrir o serviço do KDC. Um registro DNS de SRV é necessário para cada site do VMware Identity Manager e duas entradas de endereço A.

Observação O valor de entrada AAAA é um endereço IPv6 que codifica um endereço IPv4. Se o KDC não for endereçável via IPv6, e um endereço IPv4 for utilizado, talvez a entrada AAAA precise ser especificada em notação IPv6 estrita como `::ffff:175c:e147` no servidor DNS. Você pode usar uma ferramenta de conversão de IPv4 em IPv6, como alguma disponível em Neustar.UltraTools, para converter o IPv4 para a notação de endereço IPv6.

Exemplo: Entradas de registro DNS para KDC

Neste exemplo de registro DNS, o território é `EXAMPLE.COM`; o nome de domínio totalmente qualificado do VMware Identity Manager é `idm.example.com` e o endereço IP do VMware Identity Manager é `1.2.3.4`.

```
idm.example.com.               1800 IN  AAAA         ::ffff:1.2.3.4

idm.example.com.               1800 IN  A            1.2.3.4

_kerberos._tcp.EXAMPLE.COM           IN  SRV  10  0   88 idm.example.com.

_kerberos._udp.EXAMPLE.COM           IN  SRV  10  0   88 idm.example.com.
```

Solucionando problemas de instalação e configuração 9

Os tópicos de solução de problemas descrevem soluções para problemas potenciais que você pode encontrar ao instalar e configurar o VMware Identity Manager.

Este capítulo inclui os seguintes tópicos:

Usuários não conseguem inicializar aplicativos ou método de autenticação incorreto aplicado em ambientes com carga balanceada

Os usuários não conseguem inicializar aplicativos no portal Workspace ONE ou o método de autenticação incorreto é aplicado em um ambiente com carga balanceada.

Problema

Em um ambiente de carga balanceada, podem ocorrer os seguintes problemas:

- Os usuários não conseguem inicializar aplicativos no portal Workspace ONE depois de fazerem login.
- O método de autenticação incorreto é apresentado aos usuários para configurar a autenticação.

Causa

Esses problemas podem ocorrer se as políticas de acesso forem determinadas incorretamente. O endereço IP do cliente determina qual política de acesso é aplicada durante o login e durante a inicialização do aplicativo. Em um ambiente de carga balanceada, o VMware Identity Manager usa o cabeçalho X-Forwarded-For para determinar o endereço IP do cliente. Em alguns casos, pode ocorrer um erro.

Solução

Configure a propriedade do `service.numberOfLoadBalancers` no arquivo `runtime-config.properties` em cada nó no seu VMware Identity Manager cluster. A propriedade especifica o número de balanceadores de carga à frente das instâncias do VMware Identity Manager.

Observação A configuração desta propriedade é opcional.

1 Faça login no appliance do VMware Identity Manager.

2 Edite o arquivo `/usr/local/horizon/conf/runtime-config.properties` e adicione a propriedade a seguir.

```
service.numberOfLoadBalancers numberOfLBs
```

onde *numberOfLBs* é o número de balanceadores de carga que estão à frente das instâncias do VMware Identity Manager.

3 Reinicie o appliance do espaço de trabalho.

```
service horizon-workspace restart
```

O grupo não exibe nenhum membro após a sincronização de diretório

A sincronização do diretório é concluída com sucesso mas nenhum usuário é exibido nos grupos sincronizados.

Problema

Após a sincronização de diretório, quer de modo automático ou manual com base na agenda de sincronização, o processo de sincronização é concluído com sucesso mas nenhum usuário é exibido nos grupos sincronizados.

Causa

Esse problema ocorre quando você tem dois ou mais nós em um cluster e há uma diferença de tempo de mais de 5 segundos entre os nós.

Solução

1 Certifique-se de que não há nenhuma diferença de tempo entre os nós. use o mesmo servidor NTP para todos os nós do cluster para sincronizar o tempo.

2 Reinicie o serviço em todos os nós.

```
service horizon-workspace restart
```

3 (Opcional) No console de administração, exclua o grupo, adicione-o novamente às configurações de sincronização e sincronize o diretório novamente.

Solucionando problemas no Elasticsearch

Use essas informações para solucionar problemas com o Elasticsearch em um ambiente de cluster. Elasticsearch, um mecanismo de pesquisa e análise usado para auditoria, relatórios e logs de sincronização de diretório, é incorporado ao appliance virtual do VMware Identity Manager.

Solucionando problemas no Elasticsearch

Você pode verificar a integridade do Elasticsearch usando o seguinte comando no appliance do VMware Identity Manager.

```
curl 'http://localhost:9200/_cluster/health?pretty'
```

O comando deve retornar um resultado semelhante ao seguinte.

```
        {
  "cluster_name" : "horizon",
  "status" : "green",
  "timed_out" : false,
  "number_of_nodes" : 3,
  "number_of_data_nodes" : 3,
  "active_primary_shards" : 20,
  "active_shards" : 40,
  "relocating_shards" : 0,
  "initializing_shards" : 0,
```

```
  "unassigned_shards" : 0,
  "delayed_unassigned_shards" : 0,
  "number_of_pending_tasks" : 0,
  "number_of_in_flight_fetch" : 0
}
```

Caso o Elasticsearch não inicie corretamente ou o status esteja vermelho, siga estes passos para solucionar o problema.

1 Certifique-se de que a porta 9300 esteja aberta.

   a Atualize os detalhes do nó adicionando os endereços IP de todos os nós no cluster no arquivo `/usr/local/horizon/scripts/updateiptables.hzn`

   ```
   ALL_IPS="node1IPadd node2IPadd node3IPadd"
   ```

   b execute o seguinte script em todos os nós do cluster.

   ```
   /usr/local/horizon/scripts/updateiptables.hzn
   ```

2 Reinicie o Elasticsearch em todos os nós do cluster.

   ```
   service elasticsearch restart
   ```

3 Verifique os logs para obter mais detalhes.

   ```
   cd /opt/vmware/elasticsearch/logs
   ```

   ```
   tail –f horizon.log
   ```

Índice