

Instalando e atualizando o vRealize Automation

05 de outubro de 2018
vRealize Automation 7.4



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

VMware Brasil

Rua Surubim, 504 4º andar CEP 04571-050
Cidade Monções
São Paulo
SÃO PAULO: 04571-050
Brasil
Tel: +55 11 55097200
Fax: + 55. 11. 5509-7224
www.vmware.com/br

Direitos autorais © 2017–2018 VMware, Inc. Todos os direitos reservados. [Informações sobre direitos autorais e marca registrada.](#)

Conteúdo

| | | |
|----------|--|----------|
| 1 | Instalando ou atualizando o vRealize Automation | 4 |
| | Arquitetura de Referência do vRealize Automation | 4 |
| | Recomendações de implantação inicial e configuração | 4 |
| | Implantação do vRealize Automation | 5 |
| | Considerações de Implantação do vRealize Business for Cloud | 7 |
| | Dimensionamento do vRealize Automation | 8 |
| | Dimensionamento do vRealize Business for Cloud | 11 |
| | Considerações de Configuração de Alta Disponibilidade do vRealize Automation | 11 |
| | Considerações de Alta Disponibilidade do vRealize Business for Cloud | 13 |
| | Especificações de hardware do vRealize Automation e máximos de capacidade | 14 |
| | Requisitos para implantações de pequeno porte do vRealize Automation | 16 |
| | Requisitos para implantações de médio porte do vRealize Automation | 21 |
| | Requisitos para implantações de grande porte do vRealize Automation | 27 |
| | Implantações de Dados em Centros de Multi-Dados do vRealize Automation | 33 |
| | Configuração Segura do vRealize Automation | 34 |
| | Visão geral da linha de base segura do vRealize Automation | 35 |
| | Verificar a integridade da mídia de instalação | 35 |
| | Reforçar infraestrutura de software do sistema da VMware | 36 |
| | Revisar softwares instalados | 37 |
| | Avisos e patches de segurança da VMware | 38 |
| | Configuração Segura | 38 |
| | Configurando a segurança de rede do host | 72 |
| | Auditoria e registro | 88 |
| | Instalando o vRealize Automation | 89 |
| | Visão geral de instalação do vRealize Automation | 89 |
| | Preparando para a instalação do vRealize Automation | 97 |
| | Implantar appliance do vRealize Automation | 113 |
| | Instalando o vRealize Automation com o assistente de instalação | 119 |
| | As interfaces de instalação padrão do vRealize Automation | 146 |
| | Instalação silenciosa do vRealize Automation | 224 |
| | Tarefas pós instalação do vRealize Automation | 231 |
| | Solucionando problemas com uma instalação do vRealize Automation | 249 |
| | Atualizando o vRealize Automation | 277 |
| | Atualizando do vRealize Automation 7.1 ou superior para a versão 7.4 | 280 |
| | Atualizando o vRealize Automation 6.2.5 para o 7.4 | 350 |
| | Migrando para o vRealize Automation 7.4 | 437 |

Instalando ou atualizando o vRealize Automation

1

Você pode instalar o vRealize Automation pela primeira vez ou atualizar seu ambiente atual para a versão mais recente.

Este capítulo inclui os seguintes tópicos:

- [Arquitetura de Referência do vRealize Automation](#)
- [Configuração Segura do vRealize Automation](#)
- [Instalando o vRealize Automation](#)
- [Atualizando o vRealize Automation](#)

Arquitetura de Referência do vRealize Automation

A arquitetura de referência descreve a estrutura e a configuração de implantações típicas do vRealize Automation. Além disso, ela fornece informações sobre alta disponibilidade, dimensionamento e perfis de implantação.

A arquitetura de referência inclui informações sobre os seguintes componentes:

- VMware vRealize Automation
- VMware vRealize Business for Cloud

Para conhecer requisitos de software, instalações e plataformas com suporte, consulte a documentação de cada produto.

Recomendações de implantação inicial e configuração

Implante e configure todos os componentes do VMware vRealize Automation de acordo com as recomendações do VMware.

Mantenha o vRealize Automation, o vRealize Business for Cloud e o vRealize Orchestrator no mesmo fuso horário com os relógios sincronizados.

Instale o vRealize Automation, o vRealize Business for Cloud e o vRealize Orchestrator no mesmo cluster de gerenciamento. Provisione máquinas em um cluster que esteja separado do cluster de gerenciamento, para que a carga de trabalho do usuário e a carga de trabalho do servidor possam ser isoladas.

Implante Agentes de Proxy no mesmo centro de dados que o Endpoint com o qual eles se comunicam. A VMware não recomendada a colocação de Trabalhadores do DEM em centros de dados remotos, a menos que haja um caso de uso expresso baseado em habilidades de fluxo de trabalho que exija isso. Todos os componentes, exceto Agentes de Proxy e Trabalhadores do DEM, devem ser implantados no mesmo centro de dados ou em centros de dados em uma Rede Metropolitana. A latência deve ser inferior a 5 milissegundos e a largura de banda não deve ser inferior a 1 GB/s entre os centros de dados da Rede Metropolitana.

Para obter mais informações, incluindo uma declaração de suporte, consulte o artigo da Base de Dados de Conhecimento da VMware *Instalando o VMware vRealize Automation em uma instância distribuída de vários sites*, disponível em

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2134842.

Implantação do vRealize Automation

Use as recomendações de recursos do VMware como ponto de partida para o planejamento da implantação do vRealize Automation.

Após os testes iniciais e a implantação no ambiente de produção, continue a monitorar o desempenho e alocar recursos adicionais, se necessário, conforme descrito em [Dimensionamento do vRealize Automation](#).

Autenticação

Ao configurar o vRealize Automation, você pode usar o conector padrão do Gerenciamento de Diretórios para autenticação do usuário ou pode especificar um provedor de identidade baseado em SAML pré-existente para oferecer suporte a uma experiência de conexão única.

Se a autenticação de dois fatores for necessária, o vRealize Automation oferecerá suporte à integração com RSA SecurID. Quando esse ponto de integração está configurado, os usuários são solicitados a especificarem a ID de usuário e o código de acesso.

Considerações sobre o balanceador de carga

Use o método do menor tempo de resposta ou de revezamento para balancear o tráfego dos appliances e servidores da Web de infraestrutura do vRealize Automation. Ative a afinidade de sessão ou o recurso de sessão complexa para direcionar solicitações subsequentes de cada sessão exclusiva ao mesmo servidor Web no pool do balanceador de carga.

Você pode usar um balanceador de carga para gerenciar o failover do Serviço de Gerenciador, mas não use um algoritmo de balanceamento de carga, pois apenas um Serviço de Gerenciador está ativo de cada vez. Além disso, não use a afinidade de sessão ao gerenciar o failover com um balanceador de carga.

Use as portas 443 e 8444 ao balancear a carga do appliance do vRealize Automation. Para os Serviços da Web de Infraestrutura e Gerenciador de Infraestrutura, apenas a porta 443 deve ter a carga balanceada.

Embora você possa usar outros balanceadores de carga, o NSX, o hardware F5 BIG-IP e o F5 BIG-IP Virtual Edition são testados e recomendados para uso.

Consulte a documentação do vRealize Automation para obter mais informações sobre como configurar balanceadores de carga.

Implantação de bancos de dados

O vRealize Automation coloca em cluster automaticamente o banco de dados do appliance nas versões 7.0 e mais recentes. Todas as novas implantações das versões 7.0 e mais recentes devem usar o banco de dados do appliance interno. Instâncias do vRealize Automation que estão sendo atualizadas para a versão 7.1 ou superior devem mesclar seus bancos de dados externos no banco de dados do appliance. Veja a documentação do produto vRealize Automation para obter mais informações sobre o processo de upgrade.

Para implantações de produção dos componentes de infraestrutura, use um servidor de banco de dados dedicado para hospedar os bancos de dados do Microsoft SQL Server (MSSQL). O vRealize Automation requer a configuração de máquinas que se comunicam com o servidor de banco de dados para usar o Microsoft Distributed Transaction Coordinator (MSDTC). Por padrão, o MSDTC requer a porta 135 e as portas de 1024 a 65535.

Para obter mais informações sobre como alterar as portas MSDTC padrão, consulte o artigo da base de conhecimento da Microsoft, Configurar Microsoft Distributed coordenador de transações (DTC) funcionem através de um firewall, disponível em https://support.microsoft.com/pt_br/kb/250367.

O host do Serviço de Gerenciador do IaaS deve ser capaz de resolver o nome NETBIOS do host do banco de dados do SQL Server IaaS. Se não for possível resolver o nome NETBIOS, adicione o nome NETBIOS do SQL Server no arquivo `/etc/hosts` da máquina do Serviço de Gerenciador e reinicie o Serviço de Gerenciador.

vRealize Automation tem suporte para grupos do SQL AlwaysON somente com o Microsoft SQL Server 2016. Ao instalar o SQL Server 2016, o banco de dados deve ser criado no modo 100. Caso você use uma versão mais antiga do Microsoft SQL Server, use uma instância do Cluster de Failover com discos compartilhados. Para mais informações sobre configurar grupos do SQL AlwaysOn com o MSDTC, consulte https://msdn.microsoft.com/pt_br/library/ms366279.aspx.

Configuração de coleta de dados

As configurações de coleta de dados padrão fornecem um bom ponto de partida para a maioria das implementações. Após a implantação em produção, continue a monitorar o desempenho da coleta de dados para determinar se você deve fazer ajustes.

Agentes de proxy

Para o desempenho máximo, implante agentes no mesmo centro de dados que o endpoint ao qual eles estão associados. Você pode instalar agentes adicionais para aumentar o rendimento e a simultaneidade do sistema. As implantações distribuídas podem ter vários servidores de agente distribuídos pelo mundo.

Quando agentes são instalados no mesmo centro de dados que o endpoint associado, você pode ver um aumento médio de 200% no desempenho da coleta de dados. O tempo de coleta medido inclui apenas o tempo gasto na transferência de dados entre o agente de proxy e o serviço de gerenciador. O tempo necessário para o serviço de gerenciador processar os dados não está incluído.

Por exemplo, você implanta o produto atualmente em um centro de dados em Palo Alto e possui endpoints do vSphere em Palo Alto, Boston e Londres. Nessa configuração, os agentes de proxy do vSphere são implantados em Palo Alto, Boston e Londres para seus respectivos endpoints. Se, em vez disso, os agentes forem implantados em Palo Alto, você poderá perceber um aumento de 200% no tempo de coleta de dados em Boston e Londres.

Configuração do Distributed Execution Manager

Em geral, localize os DEMs (Distributed Execution Manager) mais próximos possíveis do host do gerenciador de modelos. O Orchestrator do DEM deve ter uma forte conectividade de rede com o gerenciador de modelos em todos os momentos. Por padrão, o instalador coloca DEM Orchestrators lado a lado no Manager Service. Crie duas instâncias do Orchestrator do DEM, uma para failover, e duas instâncias do Trabalhador do DEM no seu centro de dados primário.

Se uma instância do Trabalhador do DEM tiver que executar um fluxo de trabalho específico para uma localização, instale a instância nessa localização.

Atribua competências aos fluxos de trabalho relevantes e DEMs, para que esses fluxos de trabalho sempre sejam executados por DEMs na localização correta. Para obter informações sobre como atribuir competências a fluxos de trabalho e DEMs usando o console de designer do vRealize Automation, consulte a documentação sobre a Extensibilidade do vRealize Automation.

Para obter o melhor desempenho, instale DEMs e agentes em máquinas separadas. Para obter informações adicionais sobre como instalar agentes do vRealize Automation, consulte [Instalando Agentes](#).

vRealize Orchestrator

Use a instância interna do vRealize Orchestrator para todas as novas implementações. Se necessário, implementações legadas podem continuar a utilizar um vRealize Orchestrator externo. Consulte https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2147109 para o procedimento de aumentar a memória alocada à instância interna do vRealize Orchestrator.

Para obter um melhor desempenho do produto, reveja e implemente as diretrizes de configuração descritas no *Guia de Programação do vRealize Orchestrator* antes de importar o conteúdo do vRealize Orchestrator em implantações de produção.

Considerações de Implantação do vRealize Business for Cloud

Implemente o vRealize Business for Cloud, anteriormente conhecido como vRealize Business Standard Edition, em conformidade com as diretrizes da VMware.

Considerações sobre o balanceador de carga

Não há suporte ao balanceamento de carga para conexões de coleta de dados. Para obter mais informações, consulte [Dimensionamento do vRealize Automation](#). No appliance do vRealize Business for Cloud para conexões de clientes de interface de usuário e de API, você pode usar o balanceador de carga do vRealize Automation.

Dimensionamento do vRealize Automation

Considere todos os fatores de dimensionamento aplicáveis ao configurar seu sistema do vRealize Automation.

Usuários

O Appliance do vRealize Automation está configurado para sincronizar menos de 100.000 usuários. Se o seu sistema tiver mais usuários, poderá ser necessário adicionar memória ao Gerenciamento de Diretórios do vRealize Automation. Para mais informações sobre como adicionar memória ao Gerenciamento de Diretórios, consulte [Adicionar Memória ao Gerenciamento de Diretórios](#).

Dimensionamento de provisões simultâneas

Por padrão, o vRealize Automation processa apenas oito provisões simultâneas por endpoint. Para obter informações sobre como aumentar esse limite, consulte [Configurando o provisionamento de máquinas simultâneas](#).

A VMware recomenda que todas as implantações comecem com pelo menos dois Trabalhadores do DEM. Na versão 6.x, cada Trabalhador do DEM podia processar 15 fluxos de trabalho ao mesmo tempo. Esse número aumentou para 30 para o vRealize Automation 7.0 e versões posteriores.

Se as máquinas estiverem sendo personalizadas por meio de Stubs de Fluxo de Trabalho, será necessário ter 1 Trabalhador do DEM para cada 20 máquinas que serão provisionadas simultaneamente. Por exemplo, um sistema com suporte para 100 provisões simultâneas deve ter um mínimo de 5 Trabalhadores do DEM.

Para obter mais informações sobre Trabalhadores do DEM e dimensionamento, consulte [Adaptação e análise de desempenho do Distributed Execution Manager](#)

Dimensionamento de coleta de dados

O tempo de conclusão da coleta de dados depende da capacidade do recurso de processamento, do número de máquinas no recurso de processamento ou endpoint, do sistema atual e da carga da rede, entre outras variáveis. O desempenho é dimensionado a velocidades distintas para diferentes tipos de coletas de dados.

Cada tipo de coleta de dados tem um intervalo padrão que você pode substituir ou modificar. Administradores de infraestrutura podem iniciar a coleta de dados manualmente para endpoints de origem da infraestrutura. Administradores de estrutura podem iniciar a coleta de dados manualmente para recursos de processamento. Os valores a seguir são os intervalos padrão para coleta de dados.

Tabela 1-1. Intervalos Padrão de Coleta de Dados

| Tipo de Coleta de Dados | Intervalo Padrão |
|-------------------------|-------------------------------|
| Inventário | A cada 24 horas (diariamente) |
| Estado | A cada 15 minutos |
| Desempenho | A cada 24 horas (diariamente) |

Adaptação e análise de desempenho

À medida que o número de recursos que coletam dados aumentar, os tempos de conclusão de coleta de dados poderão se tornar maiores que o intervalo entre os intervalos de coletas de dados, particularmente para a coleta de dados de estado. Para determinar se a coleta de dados para um recurso de processamento ou endpoint está sendo concluída em tempo ou está sendo colocada em fila, consulte a página Coleta de Dados. O valor do campo Última Conclusão pode mostrar *Em fila* ou *Em andamento* em vez de exibir um carimbo de data/hora de conclusão da última coleta de dados. Se esse problema ocorrer, você poderá aumentar o intervalo entre coletas de dados para diminuir sua frequência.

Como alternativa, é possível aumentar o limite de coletas de dados simultâneas por agente. Por padrão, o vRealize Automation limita as atividades de coleta de dados simultâneas a duas por agente e enfileira as solicitações que excedem esse limite. Essa limitação permite que atividades de coleta de dados terminem rapidamente sem afetar o desempenho geral. Você pode aumentar o limite para tirar proveito da coleta de dados simultânea, mas deve comparar essa opção em relação a degradação geral do desempenho.

Se você aumentar o limite configurado do vRealize Automation por agente, talvez queira aumentar um ou mais desses intervalos de tempo limite de execução. Para obter mais informações sobre como configurar a simultaneidade de coletas de dados e os intervalos de tempo limite, consulte a documentação de Administração do Sistema do vRealize Automation. A coleta de dados do Serviço de Gerenciador utiliza muitos recursos de CPU. Aumentar o poder de processamento do host do Serviço de Gerenciador pode diminuir o tempo necessário para a coleta de dados geral.

Em particular, a coleta de dados para o Amazon Elastic Compute Cloud (Amazon AWS) pode exigir vários recursos de CPU, especialmente se o seu sistema coletar dados em várias regiões ao mesmo tempo e se esses dados não foram previamente coletados nessas regiões. Esse tipo de coleta de dados pode causar uma degradação geral no desempenho do site. Diminua a frequência da coleta de dados de inventário do Amazon AWS se ela estiver exercendo um efeito perceptível sobre o desempenho.

Dimensionamento de processamento de fluxo de trabalho

O tempo médio de processamento de fluxos de trabalho, do momento em que o Orchestrator do DEM começa a pré-processar o fluxo de trabalho até o momento em que este termina de ser executado, aumenta com o número de fluxos de trabalho simultâneos. O volume de fluxos de trabalho é uma função da quantidade de atividades do vRealize Automation, incluindo solicitações de máquina e algumas atividades de coleta de dados.

Configurar o serviço de gerenciador para volume de dados alto

Se você pretende usar um cluster do VMware vSphere que contém muitos objetos, por exemplo, 3000 ou mais máquinas virtuais, modifique o arquivo de configuração do serviço de gerenciador com valores mais altos. Se você não modificar essa configuração, coletas extensas de dados de inventário poderão falhar.

Modifique o valor padrão das configurações `ProxyAgentServiceBinding` e `maxStringContentLength` no arquivo `ManagerService.exe.config`.

Procedimentos

- 1 Abra o arquivo `ManagerService.exe.config` em um editor de texto.

Normalmente, esse arquivo reside em `C:\Program Files (x86)\VMware\vCAC\Server`.

- 2 Localize as linhas `binding name` e `readerQuotas` no arquivo.

```
<binding name="ProxyAgentServiceBinding" maxReceivedMessageSize="13107200">
  <readerQuotas maxStringContentLength="13107200" />
```

Observação Não confunda essas duas linhas com as linhas semelhantes que contêm a seguinte cadeia de caracteres: `binding name = "ProvisionServiceBinding"`.

- 3 Substitua os valores numéricos atribuídos aos atributos `maxReceivedMessageSize` e `maxStringContentLength` por um valor maior.

O tamanho ideal depende de quantos objetos adicionais você espera que o seu cluster do VMware vSphere contenha no futuro. Por exemplo, você pode aumentar esses números por um fator de 10 para testes.

- 4 Salve suas alterações e feche o arquivo.
- 5 Reinicie o serviço de gerenciador do vRealize Automation.

Adaptação e análise de desempenho do Distributed Execution Manager

Você pode exibir o número total de fluxos de trabalho em andamento ou pendentes a qualquer momento na página Status da Execução Distribuída e pode usar a página Histórico de Fluxos de Trabalho para determinar o tempo necessário para a execução de um determinado fluxo de trabalho.

Se você tiver muitos fluxos de trabalho pendentes, ou se os fluxos de trabalho estiverem demorando mais do que o esperado para serem concluídos, adicione mais instâncias de Trabalhador do DEM (Distributed Execution Manager) para selecionar esses fluxos de trabalho. Cada instância de Trabalhador do DEM pode processar 30 fluxos de trabalho simultâneos. Fluxos de trabalho em excesso são enfileirados para execução.

Você pode ajustar programações de fluxo de trabalho para minimizar o número de fluxos de trabalho que são iniciados simultaneamente. Por exemplo, em vez de programar todos os fluxos de trabalho horários para execução no início da hora, você pode alternar seus tempos de execução para que eles não entrem em competição por recursos do DEM. Para obter mais informações sobre fluxos de trabalho, consulte a documentação sobre Extensibilidade do vRealize Automation.

Alguns fluxos de trabalho, especialmente os personalizados, podem exigir alto consumo de CPU. Se a carga da CPU nas máquinas de Trabalhadores do DEM for alta, considere aumentar a potência de processamento da máquina DEM ou adicionar mais máquinas DEM ao seu ambiente.

Dimensionamento do vRealize Business for Cloud

Configure sua instalação do vRealize Business for Cloud para o dimensionamento de acordo com as diretrizes da VMware.

O vRealize Business for Cloud pode ser dimensionado até 20.000 máquinas virtuais entre dez instâncias do VMware vCenter Server. A primeira sincronização da coleta de dados de inventário demora cerca de três horas para sincronizar 20.000 máquinas virtuais entre três instâncias do VMware vCenter Server. A sincronização de estatísticas do VMware vCenter Server leva aproximadamente uma hora para 20.000 máquinas virtuais. Por padrão, o trabalho de cálculo de custo é executado todos os dias e dura cerca de duas horas para cada execução de 20.000 máquinas virtuais.

Observação No vRealize Business for Cloud 1.0, a configuração padrão do dispositivo virtual pode oferecer suporte a até 20.000 máquinas virtuais. Aumentar os limites do dispositivo virtual para além da sua configuração padrão não aumenta o número de máquinas virtuais com suporte.

Considerações de Configuração de Alta Disponibilidade do vRealize Automation

Se você precisar de robustez máxima para o seu sistema do vRealize Automation, configure-o com alta disponibilidade de acordo com as diretrizes da VMware.

Appliance do vRealize Automation

O Appliance do vRealize Automation tem suporte para alta disponibilidade ativa-ativa para todos os componentes, exceto o banco de dados do appliance. A partir da versão 7.3, o failover do banco de dados é automático quando três nós são implantados e a replicação síncrona está configurada entre dois nós. Quando o Appliance do vRealize Automation detecta uma falha do banco de dados, ele promove um servidor de banco de dados apropriado para ser o mestre. Você pode monitorar e gerenciar o banco de dados do appliance na guia **Configurações do vRA > Banco de Dados** do Console de Gerenciamento de Appliances Virtuais.

Para habilitar a alta disponibilidade desses dispositivos, coloque-os em um balanceador de carga. Para obter mais informações, consulte [Configurar o balanceador de carga](#). A partir da versão 7.0, o banco de dados do dispositivo e o vRealize Orchestrator são automaticamente clusterizados e disponibilizados para uso.

Gerenciamento de Diretórios do vRealize Automation

Cada appliance do vRealize Automation inclui um conector que suporta a autenticação do usuário, embora apenas um conector normalmente seja configurado para executar a sincronização de diretório. Não importa qual conector você escolhe para servir como o conector de sincronização. Para suportar a alta disponibilidade do Gerenciamento de Diretórios, é necessário configurar um segundo conector que corresponde ao seu segundo appliance do vRealize Automation, que se conecta ao seu Provedor de Identidade e aponta para o mesmo Active Directory. Com esta configuração, se um appliance falhar, o outro assume o gerenciamento de autenticação de usuário.

Em um ambiente de alta disponibilidade, todos os nós devem servir o mesmo conjunto de Active Directories, usuários, métodos de autenticação, etc. O método mais direto para alcançar este objetivo é promover o Provedor de Identidade para o cluster, definindo o host do balanceador de carga como o host do Provedor de Identidade. Com esta configuração, todas as solicitações de autenticação são direcionadas para o balanceador de carga, que encaminha a solicitação para qualquer um dos conectores, conforme apropriado.

Para obter mais informações sobre a configuração do Gerenciamento de Diretórios para alta disponibilidade, consulte [Configure Directories Management for High Availability](#).

Servidor da Web de Infraestrutura

Todos os componentes do servidor da Web de infraestrutura oferecem suporte para alta disponibilidade ativa/ativa. Para habilitar a alta disponibilidade para esses componentes, coloque-os em um balanceador de carga.

Serviço de Gerenciador de Infraestrutura

O componente de serviço de gerenciador oferece suporte para alta disponibilidade ativa/passiva. Para habilitar a alta disponibilidade desse componente, coloque dois serviços de gerenciador em um balanceador de carga. No vRealize Automation 7.3 e versões mais recentes, o failover é automático.

Se o serviço de gerenciador ativo falhar, interrompa o serviço Windows se ele ainda não estiver interrompido no balanceador de carga. Habilite o serviço de gerenciador passivo e reinicie o serviço Windows no balanceador de carga. Consulte [Instalar o Active Manager Service](#).

Agentes

Agentes oferecem suporte para alta disponibilidade ativa/ativa. Para obter informações sobre como configurar agentes para alta disponibilidade, consulte a documentação de configuração do vRealize Automation. Verifique o serviço de destino quanto à alta disponibilidade.

Trabalhador do Distributed Execution Manager

Um Distributed Execution Manager (DEM) em execução com a função de Trabalhador oferece suporte à alta disponibilidade ativa/ativa. Se uma instância de Trabalhador do DEM falhar, o Orchestrator do DEM detectará a falha e cancelará os fluxos de trabalho que essa instância estiver executando. Quando a instância de Trabalhador do DEM voltar a ficar online, ela detectará que o Orchestrator do DEM cancelou seus fluxos de trabalho e deixará de executá-los. Para evitar que os fluxos de trabalho sejam canceladas prematuramente, deixe uma instância de Trabalhador do DEM offline por vários minutos antes de cancelar seus fluxos de trabalho.

Orchestrator do Distributed Execution Manager

DEMs em execução na função Orchestrator oferecem suporte à alta disponibilidade ativa/ativa. Quando um Orchestrator do DEM é iniciado, ele procura outro Orchestrator do DEM em execução.

- Se não encontrar instâncias do Orchestrator do DEM em execução, ele começará a ser executado como o Orchestrator do DEM primário.
- Se encontrar outro Orchestrator do DEM em execução, ele monitorará o outro Orchestrator do DEM primário para detectar uma interrupção.
- Se detectar uma interrupção, ele assumirá como instância primária.

Quando a instância primária anterior voltar a ficar online, ela detectará que outro Orchestrator do DEM assumiu sua função como instância primária e realizará um monitoramento em busca de falhas da instância primária do Orchestrator.

Servidor de Banco de Dados MSSQL para Componentes de Infraestrutura

vRealize Automation tem suporte para grupos do SQL AlwaysON somente com o Microsoft SQL Server 2016. Ao instalar o SQL Server 2016, o banco de dados deve ser criado no modo 100. Caso você use uma versão mais antiga do Microsoft SQL Server, use uma instância do Cluster de Failover com discos compartilhados. Para obter mais informações sobre como configurar grupos do SQL AlwaysOn com o MSDTC, consulte o artigo da Microsoft <https://msdn.microsoft.com/en-us/library/ms366279.aspx>.

vRealize Orchestrator

Uma instância interna altamente disponível do vRealize Orchestrator é fornecida como parte do appliance do vRealize Automation.

Considerações de Alta Disponibilidade do vRealize Business for Cloud

Use o recurso do VMware vSphere HA para o dispositivo do vRealize Business for Cloud Edition.

Para configurar o recurso do VMware vSphere HA no host VMware ESXi, consulte a documentação do vCenter Server e do Gerenciamento de Hosts.

Especificações de hardware do vRealize Automation e máximos de capacidade

Instale os componentes apropriados para as suas necessidades de configuração e capacidade em cada perfil de servidor do vRealize Automation no seu ambiente.

| Função de Servidor | Componentes | Especificações de Hardware Necessárias | Especificações de Hardware Recomendadas |
|---|--|---|---|
| Appliance do vRealize Automation | Serviços do vRealize Automation, vRealize Orchestrator, Banco de Dados do Dispositivo do vRealize Automation | CPU: 4 vCPU RAM: 18 GB (Para obter mais informações, consulte Dimensionamento do vRealize Automation.) Disco: 140 GB Rede: 1 GB/s | Igual às especificações de hardware necessárias. |
| Servidor de Infraestrutura para Core | Site, Serviço de Gerenciador, Orchestrator do DEM, Trabalhador do DEM, Agente de Proxy | CPU: 4 vCPU RAM: 8 GB Disco: 40 GB Rede: 1 GB/s | Igual às especificações de hardware necessárias. |
| Servidor da Web de Infraestrutura | Site | CPU: 2 vCPU RAM: 8 GB Disco: 40 GB Rede: 1 GB/s | CPU: 2 vCPU RAM: 8 GB Disco: 40 GB Rede: 1 GB/s |
| Servidor do Gerenciador de Infraestrutura | Serviço de Gerenciador, Orchestrator do DEM | CPU: 2 vCPU RAM: 8 GB Disco: 40 GB Rede: 1 GB/s | CPU: 2 vCPU RAM: 8 GB Disco: 40 GB Rede: 1 GB/s |
| Servidor da Web/Gerenciador de Infraestrutura | Servidor da Web/Gerenciador de Infraestrutura | CPU: 2 vCPU RAM: 8 GB Disco: 40 GB Rede: 1 GB/s | CPU: 2 vCPU RAM: 8 GB Disco: 40 GB Rede: 1 GB/s |
| Servidor de Infraestrutura DEM | (Um ou mais) Trabalhadores do DEM | CPU: 2 vCPU RAM: 8 GB Disco: 40 GB Rede: 1 GB/s por Trabalhador do DEM | CPU: 2 vCPU RAM: 8 GB Disco: 40 GB Rede: 1 GB/s por Trabalhador do DEM |
| Servidor do Agente de Infraestrutura | (Um ou mais) Agente de Proxy | CPU: 2 vCPU RAM: 8 GB Disco: 40 GB Rede: 1 GB/s | CPU: 2 vCPU RAM: 8 GB Disco: 40 GB Rede: 1 GB/s |

| Função de Servidor | Componentes | Especificações de Hardware Necessárias | Especificações de Hardware Recomendadas |
|--|---|--|---|
| Servidor de Banco de Dados MSSQL | Banco de Dados de Infraestrutura | CPU: 2 vCPU RAM: 8 GB Disco: 40 GB Rede: 1 GB/s | CPU: 8 vCPU RAM: 16 GB Disco: 80 GB Rede: 1 GB/s |
| Appliance do vRealize Business for Cloud | Serviços de appliance do vRealize Business for Cloud Servidor do banco de dados do vRealize Business for Cloud | CPU: 2 vCPU RAM: 4 GB Disco: 50 GB Rede: 1 GB/s | Igual às especificações de hardware necessárias |

Máximos de capacidade recomendados para o vRealize Automation

Os seguintes valores de máximos de capacidade de recursos são aplicáveis ao perfil de implantação grande do vRealize Automation.

Tabela 1-2. Máximos de capacidade de recursos para o vRealize Automation

| Parâmetro | Valor máximo | |
|--|--|-------|
| Tenant | 100 | |
| Endpoints do vSphere | 20 | |
| Recursos de processamento | 200 | |
| Máquinas gerenciadas | 75.000 | |
| Solicitação Concorrente de Pico | | |
| | constante | 50 |
| | intermitente | 250 |
| Solicitações de pico hora | 400 | |
| Grupos de negócios | 3000 (com 10 usuários exclusivos por grupo de negócios e com nenhum usuário sendo membro de mais de 50 grupos de negócios) | |
| Reservas | 9000 (com 3 reservas por grupo de negócios) | |
| Blueprints | | |
| | Somente CBP | 6000 |
| | CBP + XaaS | 8000 |
| Itens de catálogo | | |
| | entre tenants | 4000 |
| | em um único tenant | 6000 |
| Sincronização de usuários/grupos com 18 GB de memória padrão | | |
| | número de usuários | 95027 |

Tabela 1-2. Máximos de capacidade de recursos para o vRealize Automation (Continuação)

| Parâmetro | Valor máximo |
|---|---|
| número de grupos | 20403 (cada grupo contém 4 usuários incluindo um nível de aninhamento) |
| Usuário/grupo com memória ampliada para 30 GB | |
| número de usuários | 100.000 |
| número de grupos | 750 (cada grupo contém 4.000 usuários e cada usuário está em 30 grupos) |

Requisitos para implantações de pequeno porte do vRealize Automation

Uma implantação de pequeno porte do vRealize Automation compreende sistemas de 10.000 máquinas gerenciadas ou menos e inclui as máquinas virtuais, os balanceadores de carga e as configurações de porta apropriadas. A implantação de pequeno porte serve como ponto de partida para uma implantação do vRealize Automation que permite um dimensionamento com suporte para uma implantação de médio ou grande porte.

Ao implantar o vRealize Automation, use o processo de implantação corporativa para fornecer um site de infraestrutura e um endereço do Manager Service separados.

Suporte

Uma implantação de pequeno porte pode oferecer suporte aos seguintes itens.

- 10.000 máquinas gerenciadas
- 500 itens de catálogo
- 10 provisões de máquinas simultâneas

Requisitos

Uma implantação de pequeno porte deve ser configurada com os componentes apropriados.

- Appliance vRealize Automation: vrava-1.ra.local
- Servidor de Infraestrutura para Core: inf-1.ra.local.
- Servidor de Banco de Dados MSSQL: mssql.ra.local
- Appliance vRealize Business for Cloud: vrb.ra.local

Entradas DNS

| Entrada DNS | Aponta para |
|------------------|------------------|
| vrava.ra.local | vrava-1.ra.local |
| web.ra.local | inf.ra.local |
| manager.ra.local | inf.ra.local |

Certificados

Os nomes de host usados nessa tabela são apenas exemplos.

| Função de Servidor | CN ou SAN |
|---|---|
| Appliance do vRealize Automation | SAN contém vra.va.sqa.local e vra.va-1.sqa.local |
| Servidor de Infraestrutura para Core | SAN contém web.ra.local, managers.ra.local e inf-1.ra.local |
| Servidor do vRealize Business for Cloud | CN = vrb.ra.local |

Portas

Os usuários necessitam acesso a determinadas portas. Todas as portas listadas são portas padrão.

| Função de Servidor | Porta |
|----------------------------------|--|
| Appliance do vRealize Automation | 443, 8444. A porta 8444 é necessária para o Console Remoto da Máquina Virtual. A porta 8283 é necessária para acesso ao Centro de Controle do vRealize Orchestrator. |

Os administradores precisam ter acesso a determinadas portas, além daquelas necessárias para os usuários.

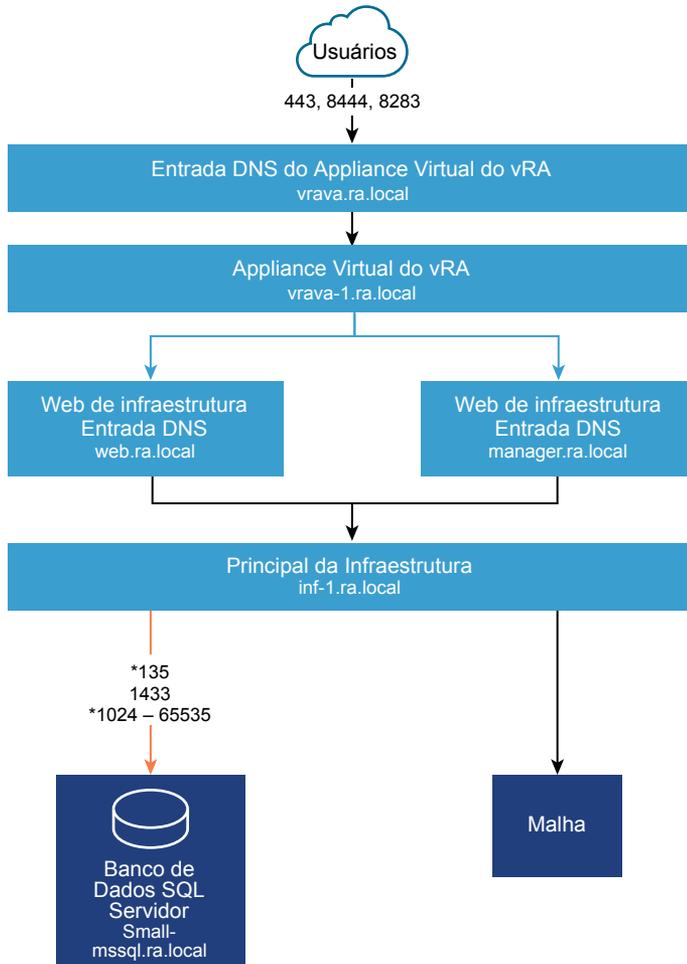
| Função de Servidor | Porta |
|----------------------------------|--|
| Appliance do vRealize Automation | 5480, 8443. A porta 8443 é usada para a configuração avançada do gerenciamento de identidades. VMware Identity Manager para Active Directory: 389, 636, 3268, 3269 VMware Identity Manager to Controlador de Domínio: 88, 464, 135 |
| vRealize Business for Cloud | 5480 |

| Função de Servidor | Portas de Entrada | Portas de Saída do Serviço/Sistema |
|--------------------------------------|--|---|
| Appliance do vRealize Automation | HTTPS: 443 Configuração do Adaptador: 8443 Proxy do Console Remoto: 8444 SSH: 22 Console de Gerenciamento do Appliance Virtual: 5480 | LDAP: 389 LDAPS:636 VMware ESXi: 902 O Infrastructure Core requer acesso à porta 443 do endpoint do vSphere para obter um tíquete para o VMware Remote Console. O appliance vRealize Automation requer acesso à porta 902 do host ESXi para representar o tráfego por proxy para o consumidor. Servidor de Infraestrutura para Core: 443 Autenticação Kerberos: 88 Renovação de senha do objeto de computador: 464 |
| Servidor de Infraestrutura para Core | HTTPS: 443 MSDTC: 135, 1024 - 65535. Para obter informações sobre como restringir esse intervalo, consulte a seção Implantação do Banco de Dados do vRealize Automation . | Appliance virtual do vRealize Automation: 443, 5480 Endpoint do vSphere: 443 O Infrastructure Core requer acesso à porta 443 do endpoint do vSphere para obter um tíquete para o VMware Remote Console. O appliance vRealize Automation requer acesso à porta 902 do host ESXi para representar o tráfego por proxy para o consumidor. MSSQL: 135, 1433, 1024 - 65535 MSDTC: 135, 1024 - 65535. Para obter informações sobre como restringir esse intervalo, consulte a seção Implantação do Banco de Dados do vRealize Automation . |

| Função de Servidor | Portas de Entrada | Portas de Saída do Serviço/Sistema |
|--|--|---|
| Servidor de Banco de Dados MSSQL | MSSQL: 1433 MSDTC: 135, 1024 - 65535. Para obter informações sobre como restringir esse intervalo, consulte a seção Implantação do Banco de Dados do Implantação do vRealize Automation . | Servidor de Infraestrutura para Core: 135, 1024 a 65535. Para obter informações sobre como restringir esse intervalo, consulte a seção Implantação do Banco de Dados do Implantação do vRealize Automation . MSDTC: 135, 1024 - 65535. Para obter informações sobre como restringir esse intervalo, consulte a seção Implantação do Banco de Dados do Implantação do vRealize Automation . |
| Appliance do vRealize Business for Cloud | HTTPS: 443 SSH: 22 Console de Gerenciamento do Appliance Virtual: 5480 | Appliance virtual do vRealize Automation: 443 Infraestrutura para Core: 443 |
| Catálogo Global | | Catálogo Global: 3268, 3269 |

Áreas Ocupadas Mínimas

Figura 1-1. Área ocupada mínima para uma configuração pequena do vRealize Automation



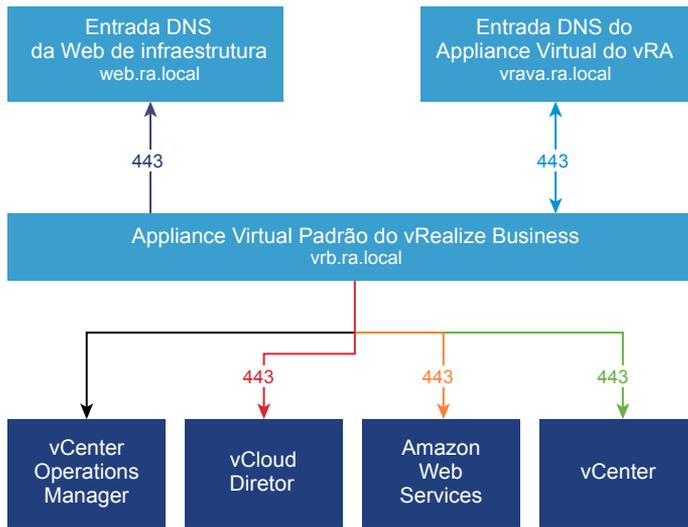
Não Mostrado:
 todos os sistemas de infraestrutura exigem acesso à Porta 5480 de todos os Appliances do vRealize para coleta de logs (Configurações do vRA > Cluster > Coletar Logs no Appliance Virtual:5480) para poderem funcionar.

Para o console remoto da máquina virtual, o Appliance do vRealize requer acesso à Porta 902 do VMware ESXi, enquanto o servidor do núcleo da infraestrutura requer acesso à Porta 443 do endpoint do vSphere.

*Consulte a seção Implantação do Banco de Dados para obter informações sobre como restringir esse intervalo

Além disso, uma comunicação bidirecional é necessária.

Figura 1-2. Área ocupada mínima para uma configuração pequena do vRealize Business for Cloud



Requisitos para implantações de médio porte do vRealize Automation

Uma implantação de médio porte do vRealize Automation compreende sistemas de 30.000 máquinas gerenciadas ou menos e inclui as máquinas virtuais, os balanceadores de carga e as configurações de porta apropriadas.

Suporte

Uma implantação de médio porte pode oferecer suporte aos itens a seguir.

- 30.000 máquinas gerenciadas
- 1.000 itens de catálogo
- 50 provisões de máquinas

Requisitos

Uma implantação de médio porte deve atender aos requisitos de configuração de sistema apropriados.

Appliances virtuais

- Appliance do vRealize Automation 1: vrava-1.ra.local
- Appliance do vRealize Automation 2: vrava-2.ra.local
- Appliance do vRealize Automation 3: vrava-3.ra.local
- Appliance do vRealize Business for Cloud: vrb.ra.local

Máquinas Virtuais do Windows Server

- Servidor da Web/Gerenciador de Infraestrutura 1 (Web ou DEM-O Ativo, Gerenciador Ativo): inf-1.ra.local

- Servidor da Web/Gerenciador de Infraestrutura 2 (Web ou DEM-O Ativo, Gerenciador Passivo): inf-2.ra.local
- Servidor de Infraestrutura DEM 1: dem-1.ra.local
- Servidor de Infraestrutura DEM 2: dem-2.ra.local
- Servidor do Agente de Infraestrutura 1: agent-1.ra.local
- Servidor do Agente de Infraestrutura 2: agent-2.ra.local

Servidores de Banco de Dados

- Instância de Cluster de Failover MSSQL: mssql.ra.local

Balancedores de Carga

- Balanceador de Carga do Appliance do vRealize Automation: med-vrava.ra.local
- Balanceador de Carga da Web de Infraestrutura: med-web.ra.local
- Balanceador de Carga do Serviço de Gerenciador de Infraestrutura: med-manager.ra.local

Certificados

Os nomes de host que são usados nesta tabela são apenas exemplos.

| Função de Servidor | CN ou SAN |
|---|---|
| Appliance do vRealize Automation | SAN contém os seguintes nomes de host: <ul style="list-style-type: none"> ▪ vrava.ra.local ▪ vrava-1.ra.local ▪ vrava-2.ra.local |
| Servidor da Web ou de Gerenciador de Infraestrutura | SAN contém os seguintes nomes de host: <ul style="list-style-type: none"> ▪ web.ra.local ▪ manager.ra.local ▪ inf-1.ra.local ▪ inf-2.ra.local |
| Appliance do vRealize Business for Cloud | CN = vrb.ra.local |

Portas

Os usuários necessitam acesso a determinadas portas. Todas as portas listadas são portas padrão.

| Função de Servidor | Porta |
|---|--|
| Balancedor de Carga do Appliance do vRealize Automation | 443, 8444. A porta 8444 é necessária para o Console Remoto da Máquina Virtual. |

Os administradores precisam ter acesso a determinadas portas, além daquelas necessárias para os usuários.

| Função de Servidor | Porta |
|---|--|
| Appliance do vRealize Automation fVAMI | 5480, 8443. A porta 8443 é para a configuração avançada do gerenciamento de identidades. VMware Identity Manager para Active Directory: 389, 636, 3268, 3269 VMware Identity Manager to Controlador de Domínio: 88, 464, 135 |
| Centro de Controle do vRealize Appliance Orchestrator | 8283 |
| Servidor do vRealize Business for Cloud | 5480 |

A tabela a seguir mostra as comunicações entre aplicativos.

| Função de Servidor | Portas de Entrada | Portas de Saída para Serviço ou Sistema |
|---|---|---|
| Appliance do vRealize Automation | HTTPS: Configuração do Adaptador: 8443 Proxy do Console Remoto: 8444 Postgres: 5432 RabbitMQ: 4369, 25672, 5671, 5672 ElasticSearch: 9300, 40002, 40003 Stomp: 61613 SSH: 22 | LDAP:389 LDAPS: 636 Appliance do vRealize Automation (Todos os outros): 5432, 4369, 25672, 5671, 5672, 9300, 40002, 40003 Balanceador de Carga da Web de Infraestrutura do vRealize Automation: 443 VMware ESXi: 902. A Web ou o Gerenciador de Infraestrutura requer acesso à porta 443 do Endpoint do vSphere para obter um tíquete para o Console Remoto da Máquina Virtual. O Appliance do vRealize Automation requer acesso à porta 902 do host ESXi para representar dados de console por proxy para o usuário. Autenticação Kerberos: 88 Renovação de senha do objeto de computador: 464 |
| Servidor da Web/Gerenciador de Infraestrutura | HTTPS: 443 MSDTC: 135, 1024-65535. Para obter informações sobre como restringir esse intervalo, consulte a seção Implantação do Banco de Dados do vRealize Automation . | Balanceador de Carga do Appliance do vRealize Automation: 443 Balanceador de Carga da Web de Infraestrutura do vRealize Automation: 443 Dispositivo do vRealize Automation (VA): 5480. Endpoint do vSphere: 443. A Web ou o Gerenciador de Infraestrutura requer acesso à porta 443 do Endpoint do vSphere para obter um tíquete para o Console Remoto da Máquina Virtual. O Appliance do vRealize Automation requer acesso à porta 902 do host ESXi para representar dados de console por proxy para o usuário. MSSQL: 135, 1433, 1024 a 65535. Para obter informações sobre como restringir esse intervalo, consulte a seção Implantação do Banco de Dados do vRealize Automation . |

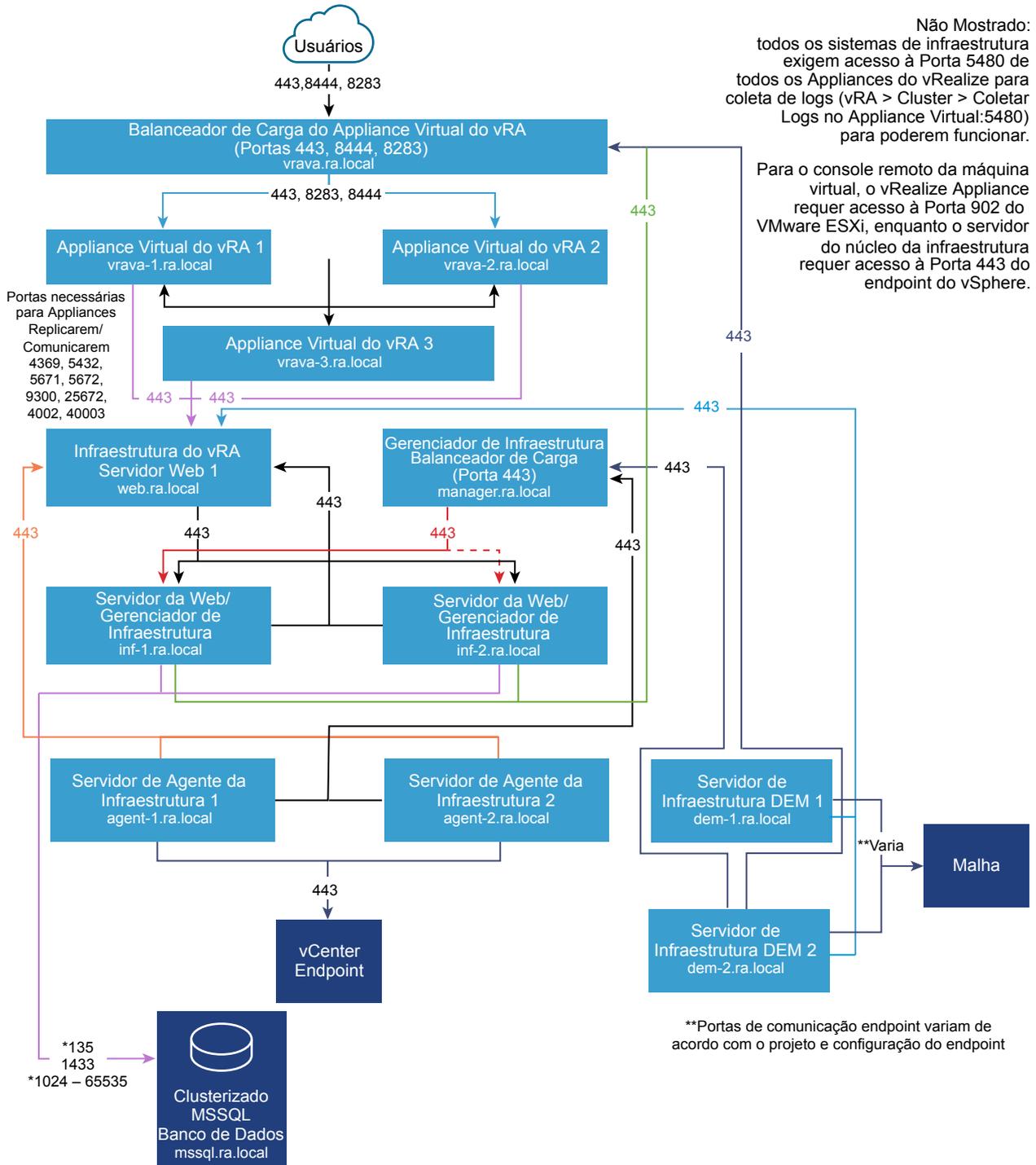
| Função de Servidor | Portas de Entrada | Portas de Saída para Serviço ou Sistema |
|---|--|---|
| Servidor de Infraestrutura DEM | N/D | Balanceador de Carga do Appliance do vRealize Automation: 443 Balanceador de Carga da Web de Infraestrutura do vRealize Automation: 443 Balanceador de Carga do Gerenciador de Infraestrutura do vRealize Automation: 443 Dispositivo do vRealize Automation (VA): 5480. |
| Servidor do Agente de Infraestrutura | N/D | Balanceador de Carga da Web de Infraestrutura do vRealize Automation: 443 Balanceador de Carga do Gerenciador de Infraestrutura do vRealize Automation: 443 Dispositivo do vRealize Automation (VA): 5480. |
| Servidor de Banco de Dados MSSQL | MSSQL: 1433 MSDTC: 135, 1024 - 65535. Para obter informações sobre como restringir esse intervalo, consulte a seção Implantação do Banco de Dados do Implantação do vRealize Automation . | Servidor da Web/Gerenciador de Infraestrutura: 135, 1024 - 65535. Para obter informações sobre como restringir esse intervalo, consulte a seção Implantação do Banco de Dados do Implantação do vRealize Automation . |
| Servidor do vRealize Business for Cloud | HTTPS: 443 SSH: 22 Console de Gerenciamento do Appliance Virtual: 5480 | Balanceador de Carga do Appliance do vRealize Automation: 443 Balanceador de Carga da Web de Infraestrutura do vRealize Automation: 443 |
| Catálogo Global | | Catálogo Global: 3268, 3269 |

Os balanceadores de carga requerem acesso pelas seguintes portas.

| Balanceador de Carga | Portas Balanceadas |
|--|--------------------|
| Balanceador de Carga do Appliance do vRealize Automation | 443, 8444 |
| Balanceador de Carga da Web de Infraestrutura do vRealize Automation | 443 |
| Balanceador de Carga do Serviço de Gerenciador de Infraestrutura vRealize Automation | 443 |

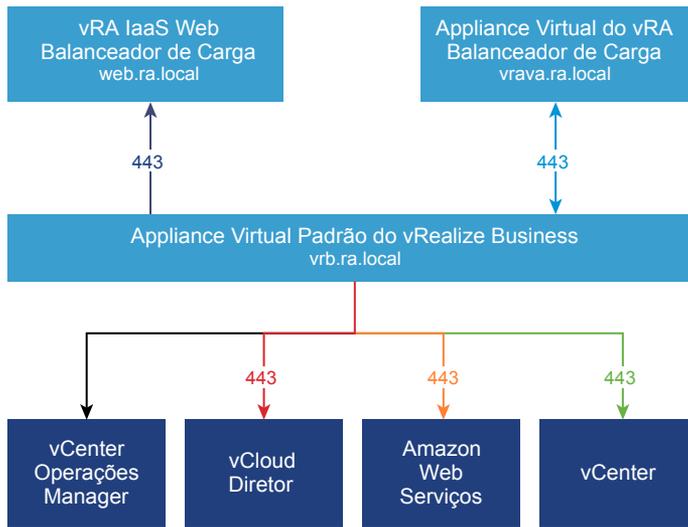
Gráficos

Figura 1-3. Área mínima ocupada para uma configuração média do vRealize Automation



*Consulte a seção Implantação do Banco de Dados para obter informações sobre como restringir esse intervalo
Além disso, uma comunicação bidirecional é necessária.

Figura 1-4. Área mínima ocupada para uma implementação média do vRealize Business for Cloud



Requisitos para implantações de grande porte do vRealize Automation

Uma implantação de grande porte do vRealize Automation compreende sistemas de 50.000 máquinas gerenciadas ou menos e inclui as máquinas virtuais, os balanceadores de carga e as configurações de porta apropriadas.

Suporte

Uma implantação de grande porte pode oferecer suporte aos itens a seguir.

- 50.000 máquinas gerenciadas
- 2500 itens de catálogo
- 100 provisões de máquinas simultâneas

Requisitos

Uma implantação de grande porte deve atender aos requisitos de configuração de sistema apropriados.

Appliances virtuais

- Appliance vRealize Automation 1: vrava-1.ra.local
- Appliance vRealize Automation 2: vrava-2.ra.local
- Appliance do vRealize Automation 2: vrava-3.ra.local
- Appliance vRealize Automation: vrb.ra.local

Máquinas Virtuais do Windows Server

- Servidor da Web de Infraestrutura 1: web-1.ra.local

- Servidor da Web de Infraestrutura 2: web-2.ra.local
- Servidor do Gerenciador de Infraestrutura 1: manager-1.ra.local
- Servidor do Gerenciador de Infraestrutura 2: manager-2.ra.local
- Servidor de Infraestrutura DEM 1: dem-1.ra.local
- Servidor de Infraestrutura DEM 2: dem-2.ra.local
- Servidor do Agente de Infraestrutura 1: agent-1.ra.local
- Servidor do Agente de Infraestrutura 2: agent-2.ra.local
- Banco de Dados MSSQL Clusterizado: mssql.ra.local

Balanceadores de Carga

- Balanceador de carga do appliance vRealize Automation: vrava.ra.local
- Balanceador de carga da Web de infraestrutura: web.ra.local
- Balanceador de carga do serviço Infrastructure Manager: manager.ra.local

Certificados

Os nomes de host usados nessa tabela são apenas exemplos.

| Função de Servidor | CN ou SAN |
|--|---|
| Appliance do vRealize Automation | SAN contém os seguintes nomes de host: <ul style="list-style-type: none"> ▪ vrava.ra.local ▪ vrava-1.ra.local ▪ vrava-2.ra.local |
| Servidor do Infrastructure Web | SAN contém os seguintes nomes de host: <ul style="list-style-type: none"> ▪ web.ra.local ▪ web-1.ra.local ▪ web-2.ra.local |
| Servidor do Infrastructure Manager | SAN contém os seguintes nomes de host: <ul style="list-style-type: none"> ▪ manager.ra.local ▪ manager-1.ra.local ▪ manager-2.ra.local |
| Appliance do vRealize Business for Cloud | CN = vrb.ra.local |

Portas

Os usuários necessitam acesso a determinadas portas. Todas as portas listadas são portas padrão.

| Função de Servidor | Porta |
|---|--|
| Balanceador de carga do appliance vRealize Automation | 443, 8444 Porta 88444 é necessário para o VMware Remote Console. |

Os administradores precisam ter acesso a determinadas portas, além daquelas necessárias para os usuários.

| Função de Servidor | Porta |
|---|--|
| Appliance do vRealize Automation | 5480, 8443. A porta 8443 é usada para a configuração avançada do gerenciamento de identidades. VMware Identity Manager para Active Directory: 389, 636, 3268, 3269 VMware Identity Manager to Controlador de Domínio: 88, 464, 135 |
| Servidor do vRealize Business for Cloud | 5480 |

O sistema deve oferecer suporte as comunicações apropriadas entre aplicativos.

| Função de Servidor | Portas de Entrada | Portas de Saída para Serviço ou Sistema |
|----------------------------------|--|--|
| vRealize Automation | | |
| Appliance do vRealize Automation | HTTPS: 443 Configuração do adaptador: 8443 Proxy do console remoto: 8444 Postgres: 5432 Rabbit MQ: 4369, 25672, 5671, 5672 ElasticSearch: 9300, 40002, 40003 Stomp: 61613 SSH: 22 Control-Center: 8283 | LDAP: 389 LDAPS: 636 Appliance vRealize Automation: 5432, 4369, 25672, 5671, 5672, 9300, 40002, 40003. Balanceador de carga da Web de infraestrutura do vRealize Automation: 443 VMware ESXi: 902. O Infrastructure Web requer acesso à porta 443 do endpoint do vSphere para obter um tíquete para o VMware Remote Console. O Appliance do vRealize Automation requer acesso à Porta 902 do host ESXi para representar dados de console por proxy para o usuário. Autenticação Kerberos: 88 Renovação de senha do objeto de computador: 464 |

| Função de Servidor | Portas de Entrada | Portas de Saída para Serviço ou Sistema |
|---|--|---|
| <p>Servidor do Infrastructure Web</p> | <p>HTTPS: 443 MSDTC: 443, 1024-65535. Para obter informações sobre como restringir esse intervalo, consulte a seção Implantação do banco de dados do Implantação do vRealize Automation.</p> | <p>Balanceador de carga do appliance do vRealize Automation: 443 Appliance virtual do appliance vRealize Automation: 5480. Endpoint do vSphere: 443. O Infrastructure Web requer acesso à porta 443 do endpoint do vSphere para obter um tíquete para o VMware Remote Console. O appliance vRealize Automation requer acesso à porta 902 do host ESXi para representar dados de console por proxy para o usuário. MSSQL: 135, 1433, 1024 a 65535. Para obter informações sobre como restringir esse intervalo, consulte a seção Implantação do banco de dados do Implantação do vRealize Automation.</p> |
| <p>Servidor do Infrastructure Manager</p> | <p>HTTPS: 443 MSDTC: 135,1024-65535. Para obter informações sobre como restringir esse intervalo, consulte a seção Implantação do banco de dados do Implantação do vRealize Automation.</p> | <p>Balanceador de carga do appliance do vRealize Automation: 443 Balanceador de Carga da Web de Infraestrutura do vRealize Automation: 443 Appliance vRealize Automation: 443, 5480 MSSQL: 135, 1433, 1024 a 65535. Para obter informações sobre como restringir esse intervalo, consulte a seção Implantação do banco de dados do Implantação do vRealize Automation.</p> |
| <p>Servidor de Infraestrutura DEM</p> | <p>N/D</p> | <p>Balanceador de carga do appliance do vRealize Automation: 443 Balanceador de carga da Web de infraestrutura do vRealize Automation: 443 Balanceador de carga do gerenciador de infraestrutura do vRealize Automation: 443 Balanceador de carga do vRealize Orchestrator: 8281 Appliance do vRealize Automation: 5480.</p> |

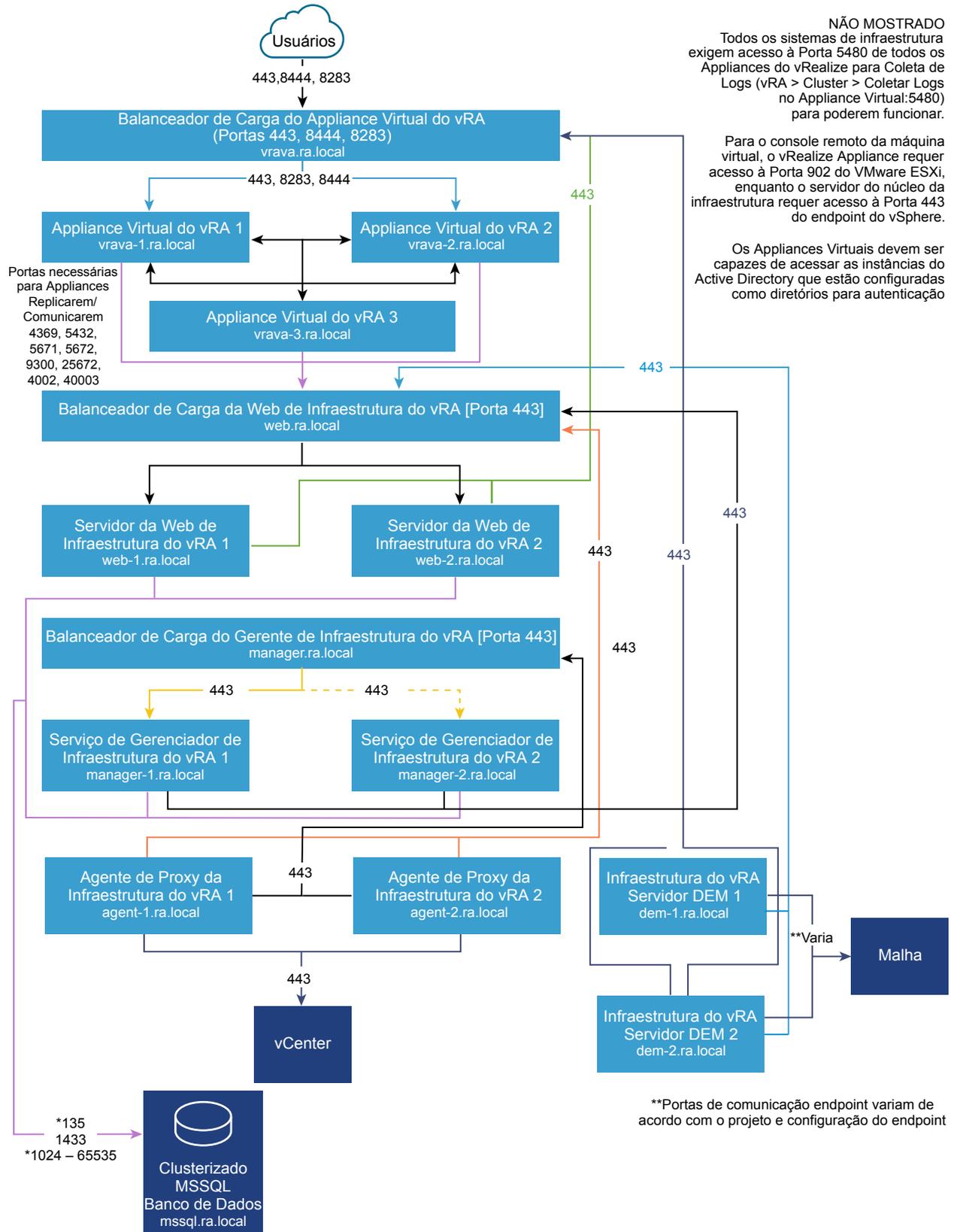
| Função de Servidor | Portas de Entrada | Portas de Saída para Serviço ou Sistema |
|---|---|--|
| Servidor do Agente de Infraestrutura | N/D | Balanceador de carga da Web de infraestrutura do vRealize Automation: 443 Balanceador de carga do gerenciador de infraestrutura do vRealize Automation: 443 Appliance do vRealize Automation: 5480. |
| Servidor de banco de dados MSSQL | MSSQL: 1433 MSDTC: 135, 1024-65535. Para obter informações sobre como restringir esse intervalo, consulte a seção Implantação do banco de dados do Implantação do vRealize Automation . | Servidor do Infrastructure Web: 135, 1024-65535. Para obter informações sobre como restringir esse intervalo, consulte a seção Implantação do banco de dados do Implantação do vRealize Automation . Servidor do Infrastructure Manager: 135, 1024-65535. Para obter informações sobre como restringir esse intervalo, consulte a seção Implantação do banco de dados do Implantação do vRealize Automation . |
| Servidor do vRealize Business for Cloud | HTTPS: 443 SSH: 22 Console de Gerenciamento do Appliance Virtual: 5480 | Balanceador de carga do appliance do vRealize Automation: 443 Balanceador de carga da Web de infraestrutura do vRealize Automation: 443 |
| Catálogo Global | | Catálogo Global: 3268, 3269 |

Os balanceadores de carga requerem acesso pelas seguintes portas.

| Balanceador de Carga | Portas Balanceadas |
|--|---------------------------|
| Balanceador de carga do appliance vRealize Automation | 443, 8444 |
| Balanceador de carga da Web de Infraestrutura do vRealize Automation | 443 |
| Balanceador de carga do servidor do gerenciador do vRealize Automation | 443 |

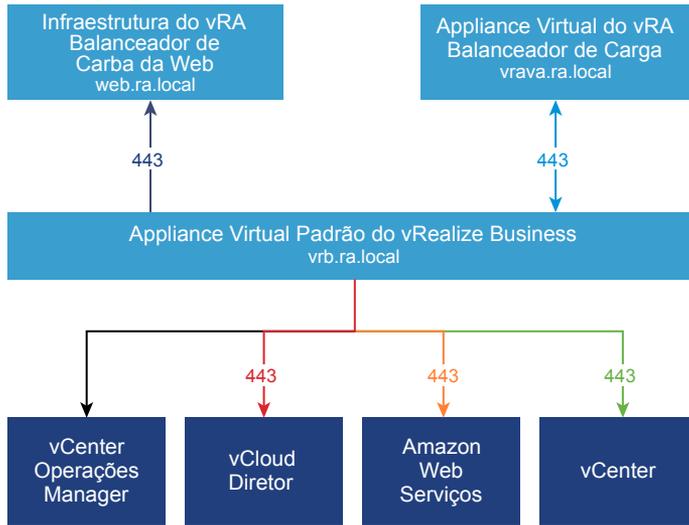
Gráficos

Figura 1-5. Área mínima ocupada para uma configuração extensa do vRealize Automation



*Consulte a seção Implantação do Banco de Dados para obter informações sobre como restringir esse intervalo

Figura 1-6. Área mínima ocupada para uma configuração extensa do vRealize Business for Cloud



Implantações de Dados em Centros de Multi-Dados do vRealize Automation

O vRealize Automation suporta recursos gerenciados em centros de dados remotos.

Para gerenciar o vSphere, os recursos HyperV ou Xen em centros de dados remotos, implantam o agente proxy em uma máquina virtual no centro de dados remoto.

Observação O diagrama abaixo mostra uma implantação do vSphere. Outros endpoints não necessitam de configuração adicional.

Em razão dos fluxos de trabalho de vRealize Orchestrator que irão potencialmente comunicar através de uma WAN, observe as boas práticas conforme orientado no *Guia de Design de Codificação de vRealize Orchestrator*.

Tabela 1-3. Portas necessárias para comunicação WAN.

| Função | Portas de Entrada | Portas de Saída do Serviço/Sistema |
|--|--|---|
| Appliance do vRealize Automation - incluindo vRealize Orchestrator integrado | N/D | Endpoint do vSphere: 443 ESXi Hosts: 903 |
| Balaceador de Carga de infraestrutura do vRealize Automation | Agente Proxy de infraestrutura do vRealize Automation: 443 | N/D |
| Servidor da Web de Infraestrutura do vRealize Automation | N/D | Endpoint do vSphere: 443 |

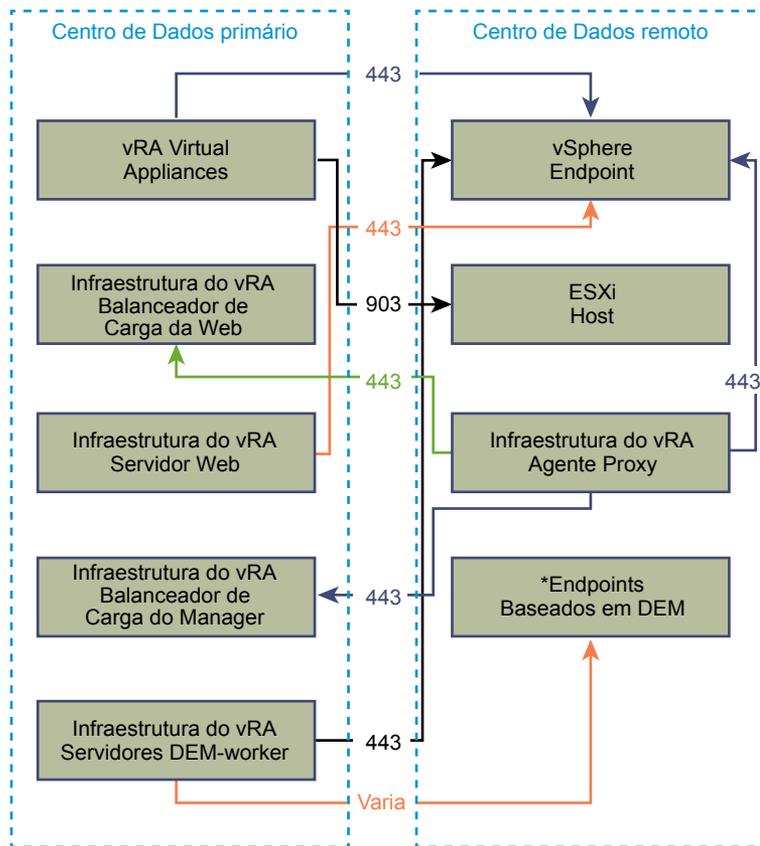
Tabela 1-3. Portas necessárias para comunicação WAN. (Continuação)

| Função | Portas de Entrada | Portas de Saída do Serviço/Sistema |
|---|--|------------------------------------|
| Balancedor de carga do Gerenciador de Infraestrutura do vRealize Automation | Agente Proxy de infraestrutura do vRealize Automation: 443 | N/D |
| Servidores DEM-worker de infraestrutura do vRealize Automation | N/D | Endpoint: **varia |

*Se DEM-workers estão instalados na máquina do Manager Service ou em outro servidor, essas portas devem estar abertas entre esta máquina e o endpoint de destino.

** A porta necessária para comunicar com um endpoint externo varia dependendo do endpoint. Por padrão para o vSphere, é a porta 443.

Figura 1-7. Configuração Multi-Site do vRealize Automation



Configuração Segura do vRealize Automation

A Configuração Segura descreve como verificar, configurar e atualizar o perfil de segurança de uma implantação do vRealize Automation de acordo com as diretrizes da VMware.

A configuração segura aborda os seguintes tópicos:

- Segurança de infraestrutura do software

- Segurança de configuração implantada
- Segurança da rede do host

Visão geral da linha de base segura do vRealize Automation

A VMware oferece recomendações abrangentes para ajudar você a verificar e configurar uma linha de base segura para o seu sistema vRealize Automation.

Use as ferramentas e procedimentos adequados conforme especificado pela VMware para verificar e manter uma configuração de linha de base segura e reforçada para o seu sistema vRealize Automation. Alguns componentes do vRealize Automation são instalados em estado reforçado ou semirreforçado, mas você deve rever e verificar a configuração de cada componente à luz das recomendações de segurança da VMware, políticas de segurança da empresa e ameaças conhecidas.

Postura de segurança do vRealize Automation

A postura de segurança do vRealize Automation presume um ambiente holisticamente seguro baseado nas configurações do sistema e rede, políticas de segurança organizacional e melhores práticas de segurança.

Ao verificar e configurar o reforço de um sistema vRealize Automation, considere cada uma das áreas conforme tratadas pelas recomendações de reforço da VMware.

- Implantação segura
- Configuração Segura
- Segurança da rede

Para garantir que seu sistema esteja reforçado de forma segura, considere as recomendações da VMware e suas políticas de segurança locais, conforme relacionadas a estas áreas conceituais.

Componentes do sistema

Ao considerar o reforço e a configuração segura do seu sistema vRealize Automation, certifique-se de entender todos os componentes e como eles trabalham juntos para garantir a funcionalidade do sistema.

Considere os seguintes componentes ao planejar e implementar um sistema seguro.

- Appliance do vRealize Automation
- Componentes de IaaS

Para se familiarizar com o vRealize Automation e como os componentes operam juntos, consulte [Fundamentos e conceitos](#) no centro de documentação do vRealize Automation da VMware. Para obter informações sobre implantações e arquitetura típicas do vRealize Automation, consulte [Arquitetura de Referência do vRealize Automation](#).

Verificar a integridade da mídia de instalação

Os usuários devem sempre verificar a integridade da mídia de instalação antes de instalar um produto VMware.

Sempre verifique o hash SHA1 após baixar um ISO, pacote off-line ou patch para assegurar a integridade e autenticidade dos arquivos baixados. Caso obtenha a mídia física da VMware e o lacre de segurança estiver rompido, retorne o software para a VMware para substituição.

Após baixar a mídia, use o valor de soma MD5/SHA1 para verificar a integridade do download. Compare a saída do hash MD5/SHA1 com o valor publicado no site da VMware. Os hashes SHA1 ou MD5 devem ser iguais.

Para mais informações sobre a verificação de integridade da mídia de instalação, consulte <http://kb.vmware.com/kb/1537>.

Reforçar infraestrutura de software do sistema da VMware

Como parte do processo de reforço, avalie a infraestrutura de software implantada que dá suporte ao sistema da VMware e verifique se ela atende às diretrizes de reforço da VMware.

Antes de reforçar o sistema da VMware, avalie e resolva falhas de segurança na infraestrutura de software de suporte para criar um ambiente totalmente reforçado e seguro. Elementos de infraestrutura de software para considerar incluem componentes do sistema operacional, software de suporte e software de banco de dados. Resolva preocupações de segurança nestes componentes e em outros de acordo com as recomendações do fabricante e outros protocolos de segurança relevantes.

Reforçar o ambiente do VMware vSphere[®]

Avalie o ambiente do VMware vSphere[®] e verifique se o nível adequado da recomendação de reforço do vSphere está sendo aplicado e mantido.

Para mais informações sobre reforço, consulte <http://www.vmware.com/security/hardening-guides.html>.

Como parte de um ambiente reforçado de forma abrangente, a infraestrutura do VMware vSphere[®] deve atender às diretrizes de segurança estabelecidas pela VMware.

Reforçar o host de Infraestrutura como Serviço

Verifique se a máquina de host Microsoft Windows de Infraestrutura como Serviço está reforçada de acordo com as diretrizes da VMware:

Consulte as recomendações nas diretrizes de reforço e proteção do Microsoft Windows para garantir que o host do Windows Server esteja reforçado corretamente. Deixar de seguir as recomendações de reforço pode resultar em exposição a vulnerabilidades de segurança conhecidas em componentes inseguros nas versões do Windows.

Para verificar se a sua versão é compatível, consulte a [Matriz de Suporte do vRealize Automation](#).

Entre em contato com o seu fornecedor Microsoft para obter a orientação adequada sobre práticas de reforço em produtos Microsoft.

Reforçar o Microsoft SQL Server

Verifique se o banco de dados do Microsoft SQL Server atende às diretrizes de segurança conforme estabelecido pela Microsoft e pela VMware.

Consulte as recomendações definidas nas diretrizes de reforço e proteção do Microsoft SQL Server. Consulte todos os boletins de segurança da Microsoft relacionados à versão instalada do Microsoft SQL Server. Deixar de seguir as recomendações de reforço pode resultar em exposição a vulnerabilidades de segurança conhecidas em componentes inseguros nas versões do Microsoft SQL Server.

Para verificar se a sua versão do Microsoft SQL Server é compatível, consulte a [Matriz de Suporte do vRealize Automation](#).

Entre em contato com o seu fornecedor Microsoft para obter orientação sobre as práticas de reforço dos produtos Microsoft.

Reforçar o Microsoft .NET

Como parte de um ambiente reforçado de forma abrangente, o Microsoft .NET deve atender às diretrizes de segurança estabelecidas pela Microsoft e pela VMware.

Reveja as recomendações definidas nas diretrizes adequadas de reforço e proteção de .NET. Além disso, consulte todos os boletins de segurança da Microsoft relacionados à versão do Microsoft SQL Server que você está utilizando. Deixar de seguir as recomendações de reforço pode resultar em exposição a vulnerabilidades de segurança conhecidas em componentes inseguros do Microsoft.NET.

Para verificar se a sua versão do Microsoft.NET é compatível, consulte a [Matriz de Suporte do vRealize Automation](#).

Entre em contato com o seu fornecedor Microsoft para obter orientação sobre as práticas de reforço dos produtos Microsoft.

Reforçar o Internet Information Services Microsoft (IIS)

Verifique se o Internet Information Services Microsoft (IIS) atendem a todas as diretrizes de segurança da Microsoft e da VMware,

Reveja as recomendações definidas nas diretrizes adequadas de reforço e proteção do Microsoft IIS. Além disso, consulte todos os boletins de segurança da Microsoft relacionados à versão do Microsoft IIS que você está utilizando. Deixar de seguir as recomendações de reforço pode resultar em exposição a vulnerabilidades de segurança conhecidas.

Para verificar se a sua versão é compatível, consulte a [Matriz de Suporte do vRealize Automation](#).

Entre em contato com o seu fornecedor Microsoft para obter orientação sobre as práticas de reforço dos produtos Microsoft.

Revisar softwares instalados

Uma vez que vulnerabilidades em softwares de terceiros ou não utilizados aumentam o risco de acesso não autorizado ao sistema e interrupção da disponibilidade, é importante revisar todos os softwares instalados nas máquinas de host do VMware e avaliar seu uso.

Não instale softwares que não sejam necessários para a operação segura do sistema nas máquinas de host do VMware. Desinstale softwares não utilizados ou externos

Software não compatível instalado no inventário

Avalie sua implantação do VMware e o inventário dos produtos instalados para conferir se nenhum software não compatível externo está instalado.

Para mais informações sobre as políticas de compatibilidade para produtos de terceiros, consulte o artigo de suporte do VMware em <https://www.vmware.com/support/policies/thirdparty.html>.

Verificar softwares de terceiros

A VMware não oferece suporte nem recomenda a instalação de softwares de terceiros que não tenham sido testados e verificados. Softwares de terceiros inseguros, desatualizados ou não autenticados instalados nas máquinas de host do VMware podem colocar o sistema em risco de acesso não autorizado e interrupção da disponibilidade. Caso precise utilizar um software de terceiro não compatíveis, consulte o fornecedor terceiro para os requisitos de configuração segura e atualizações.

Avisos e patches de segurança da VMware

Para manter a máxima segurança em seu sistema, siga os avisos de segurança da VMware e aplique todos os patches relevantes.

A VMware emite avisos de segurança para os produtos. Acompanhe esses avisos para garantir que seu produto esteja protegido contra ameaças conhecidas.

Avale a instalação do vRealize Automation, histórico de patches e atualizações, e confirme se os Avisos de Segurança emitidos pela VMware são seguidos e aplicados.

Para mais informações sobre os avisos de segurança atuais da VMware, consulte <http://www.vmware.com/security/advisories/>.

Configuração Segura

Verifique e atualize as configurações de segurança dos appliances virtuais do vRealize Automation e o componente de Infraestrutura como Serviço conforme apropriado para a configuração do seu sistema. Além disso, verifique e atualize a configuração de outros componentes e aplicações.

Configurar uma instalação do vRealize Automation com segurança envolve tratar a configuração de cada componente individualmente e em seu funcionamento em conjunto. Considere a configuração de todos os componentes do sistema em conjunto para obter uma linha de base razoavelmente segura.

Protegendo o appliance do vRealize Automation

Verifique e atualize as configurações de segurança para o appliance do vRealize Automation conforme necessário para a configuração do sistema.

Defina as configurações de segurança para seus appliances virtuais e seus sistemas operacionais host. Além disso, defina ou verifique a configuração de outros componentes e aplicativos relacionados. Em alguns casos, você precisa verificar as configurações existentes, enquanto em outros casos você deve alterar ou adicionar configurações para obter uma definição apropriada.

Alterar a senha raiz

Você pode alterar a senha raiz do Appliance do vRealize Automation para atender aos requisitos de segurança aplicáveis.

Altere a senha raiz no Appliance do vRealize Automation usando a Virtual Appliance Management Interface. Verifique se a senha raiz atende aos requisitos de complexidade de senha corporativa da organização.

Procedimentos

- 1 Abra a Virtual Appliance Management Interface para o seu Appliance do vRealize Automation.
`https://vRealizeAppliance-url:5480`
- 2 Selecione a guia **Administrador** na Virtual Appliance Management Interface.
- 3 Selecione o submenu **Administrador**.
- 4 Insira a senha existente na caixa de texto **Senha do administrador atual**.
- 5 Insira a nova senha na caixa de texto **Nova senha do administrador**.
- 6 Insira a nova senha na caixa de texto **Redigitar a nova senha do administrador**.
- 7 Clique em **Salvar configurações** para salvar suas alterações.

Verificar hash e complexidade da senha raiz

Verifique se a senha raiz atende aos requisitos de complexidade de senha corporativa da organização.

Validar a complexidade da senha raiz é necessário, já que o usuário raiz ignora a verificação de complexidade de senha do módulo pam_cracklib que é aplicada a contas de usuário.

A senha da conta deve iniciar com \$6\$, que indica um hash sha512. Esse é o hash padrão para todos os appliances reforçados.

Procedimentos

- 1 Para verificar o hash da senha raiz, faça login como raiz e execute o comando `# more /etc/shadow`.

As informações de hash são exibidas.

Figura 1-8. Resultados de hash da senha

```
vcac148-084-111:~ # more /etc/shadow
bin:*:16332:0:60:7:::
daemon:*:16332:0:60:7:::
haldaemon:*:16332:0:60:7:::
mail:*:15870:::60:::
man:*:16332:0:60:7:::
messagebus:*:16332:0:60:7:::
nobody:*:15870:::60:::
ntp:*:16332:0:60:7:::
polkituser:*:16332:0:60:7:::
postfix:*:16332:0:60:7:::
root:$6$PHxGPY5A$ba8KezK4SS44UEHPfAtgs
P/:16346:0:365:7:::
```

- 2 Se a senha raiz não contiver um hash sha512, execute o comando `passwd` para alterá-la.

Todos os appliances reforçados ativam `enforce_for_root` para o módulo `pw_history`, encontrado no arquivo `/etc/pam.d/common-password`. O sistema recorda as últimas cinco senhas por padrão. As senhas antigas são armazenadas para cada usuário no arquivo `/etc/securetty/passwd`.

Verificar histórico de senhas raiz

Verifique se o histórico de senhas é aplicado para a conta raiz.

Todos os appliances reforçados ativam `enforce_for_root` para o módulo `pw_history`, encontrado no arquivo `/etc/pam.d/common-password`. O sistema recorda as últimas cinco senhas por padrão. As senhas antigas são armazenadas para cada usuário no arquivo `/etc/securetty/passwd`.

Procedimentos

- 1 Execute o seguinte comando:

```
cat /etc/pam.d/common-password-vmware.local | grep pam_pwhistory.so
```

- 2 Certifique-se de que o `enforce_for_root` aparece nos resultados retornados.

```
passwd required pam_pwhistory.so enforce_for_root remember=5 retry=3
```

Gerenciar expiração de senha

Configure todas as expirações de senhas de acordo com as políticas de segurança da sua organização.

Por padrão, todas as contas do appliance virtual reforçado do VMware utilizam uma expiração de senha de 60 dias. Na maioria dos appliances reforçados, a conta raiz é definida para uma expiração de senha de 365 dias. Como melhor prática, verifique se a expiração em todas as contas atende aos padrões dos requisitos de segurança e operação.

Se a senha raiz expirar, você não poderá reutilizá-la. Você deve implementar políticas específicas ao local para evitar que as senhas administrativas e raiz expirem.

Procedimentos

- 1 Faça login nas máquinas do appliance virtual como raiz e execute o seguinte comando para verificar a expiração de senha em todas as contas.

```
# cat /etc/shadow
```

A expiração de senha é o quinto campo (os campos são separados por vírgula) do arquivo sombra. A expiração da raiz é definida em dias.

Figura 1-9. Campo de expiração de senha

```
vcac148-084-111:~ # more /etc/shadow
bin:*:16332:0:60:7:::
daemon:*:16332:0:60:7:::
haldaemon:*:16332:0:60:7:::
mail:*:15870::60:::
man:*:16332:0:60:7:::
messagebus:*:16332:0:60:7:::
nobody:*:15870::60:::
ntp:*:16332:0:60:7:::
polkituser:*:16332:0:60:7:::
postfix:*:16332:0:60:7:::
root:$6$PHxGPy5A$ba8KezK4SS44UEHPfAtgsB6iy1nJYbBh
zRbYR1mvJiX.pJpub0AEpP/:16346:0:365:7:::
sshd!:16332:0:60:7:::
```

2 Para modificar a expiração da conta raiz, execute um comando no formato a seguir.

```
# passwd -x 365 root
```

Neste comando, 365 especifica o número de dias até a expiração da senha. Use o mesmo comando para modificar qualquer usuário, substituindo "raiz" pela conta específica e substituindo o número de dias para atender aos padrões de expiração da organização.

Gerenciar Shell Seguro e contas administrativas

Para conexões remotas, todos os appliances reforçados incluem o protocolo Shell seguro (SSH). Use o SSH somente quando necessário e gerencie-o adequadamente para preservar a segurança do sistema.

O SSH é um ambiente interativo de linha de comando compatível com conexões remotas a appliances virtuais do VMware. Por padrão, o acesso do SSH requer credenciais de conta de usuário com alto privilégio. Em geral, as atividades de SSH do usuário raiz dispensam o controle de acesso baseado em função (RBAC) e controles de auditoria dos appliances virtuais.

Como melhor prática, desative o SSH em um ambiente de produção e ative-o somente para resolver problemas que não podem ser resolvidos por outros meios. Deixe-o habilitado somente quando for necessário para uma finalidade específica e em conformidade com as políticas de segurança da sua organização. O SSH está desabilitado por padrão no appliance do vRealize Automation. Dependendo da configuração do vSphere, você pode habilitar ou desabilitar o SSH ao implantar o modelo do Formato Aberto de Virtualização (OVF).

Como teste simples para determinar se o SSH está habilitado em uma máquina, tente abrir uma conexão usando SSH. Se a conexão abrir e solicitar credenciais, isso significa que o SSH está habilitado e disponível para conexões.

Conta de usuário raiz do Shell Seguro

Como appliances do VMware não incluem contas de usuário pré-configuradas, a conta raiz pode usar SSH para fazer login diretamente por padrão. Desative o SSH como raiz assim que possível.

Para atender aos padrões de conformidade de não repúdio, o servidor de SSH em todos os appliances reforçados é pré-configurado com a entrada de roda AllowGroups para restringir o acesso de SSH à roda do grupo secundário. Para separação de obrigações, você pode modificar a entrada de roda AllowGroups no arquivo /etc/ssh/sshd_config para usar outro grupo, como sshd.

O grupo de roda é habilitado com o módulo `pam_wheel` para acesso de superusuário, para que os membros do grupo da roda possam fazer o acesso como superusuário raiz, onde a senha raiz é exigida. A separação de grupos permite que os usuários usem SSH no appliance sem ter acesso de superusuário à raiz. Não remova ou modifique outras entradas no campo `AllowGroups`, que garante a funcionalidade correta do appliance. Após fazer uma alteração, você deve reiniciar o daemon do SSH executando o comando: `# service sshd restart`

Ativar ou desativar Shell Seguro nos appliances do vRealize Automation

Ative o Shell Seguro (SSH) no appliance do vRealize Automation somente para resolução de problemas. Desative o SSH nesses componentes durante a operação de produção normal.

Você pode ativar ou desativar o SSH no appliance do vRealize Automation usando o console de Gerenciamento do Appliance Virtual.

Procedimentos

- 1 Navegue até o Console de Gerenciamento do Appliance Virtual (VAMI) para o seu appliance do vRealize Automation.
: `https://vRealizeAppliance url:5480`
- 2 Clique na guia **Administração**.
- 3 Clique no submenu **Administração**.
- 4 Marque a caixa de seleção **Ativar serviço de SSH** para ativar o SSH ou desmarque-a para desativar o SSH.
- 5 Clique em **Salvar configurações** para salvar suas alterações.

Criar uma conta de administrador local para o Secure Shell

Como prática recomendada de segurança, crie e configure contas administrativas locais para o Secure Shell (SSH) nas suas máquinas host do appliance virtual. Além disso, remova o acesso SSH raiz depois de criar as contas apropriadas.

Crie contas administrativas locais para SSH ou membros do grupo `wheel` secundário, ou ambos. Antes de desativar o acesso raiz direto, teste se os administradores autorizados podem acessar o SSH usando o `AllowGroups` e se eles podem usar o comando `su to root` usando o grupo `wheel`.

Procedimentos

- 1 Faça login no appliance virtual como raiz e execute os seguintes comandos com o nome de usuário apropriado.

```
# useradd -g users <username> -G wheel -m -d /home/nome de usuário  
# passwd username
```

Wheel é o grupo especificado em `AllowGroups` para acesso ssh. Para adicionar vários grupos secundários, use `-G wheel,sshd`.

- 2 Mude para o usuário e forneça uma nova senha para reforçar a verificação de complexidade da senha.

```
# su -username
# username@hostname:~>passwd
```

Se a complexidade da senha for atendida, a senha será atualizada. Se a complexidade da senha não for atendida, a senha voltará para a senha original e será necessário executar novamente o comando de senha.

- 3 Para remover o login direto para SSH, modifique o arquivo `/etc/ssh/sshd_config` substituindo `(#)PermitRootLogin yes` por `PermitRootLogin no`.

Como alternativa, você pode ativar/desativar o SSH na Virtual Appliance Management Interface (VAMI) marcando ou desmarcando a caixa de seleção **Login SSH de administrador ativado** na guia **Administrador**.

Próximo passo

Desative os logins diretos como raiz. Por padrão, os appliances protegidos permitem o login direto para raiz através do console. Depois de criar contas administrativas para não repúdio e testá-las para acesso à roda su-root, desative os logins de raiz diretos editando o arquivo `/etc/security` como root e substituindo a entrada `tty1` por `console`.

- 1 Abra o arquivo `/etc/securetty` em um editor de texto.
- 2 Localize `tty1` e substitua-o por `console`.
- 3 Salve o arquivo e feche-o.

Reforçar a configuração do servidor de Shell Seguro

Quando possível, todos os appliances do VMware possuem uma configuração reforçada por padrão. Os usuários podem verificar se sua configuração está reforçada corretamente examinando as configurações do servidor e serviço do cliente na seção de opções globais do arquivo de configuração.

Procedimentos

- 1 Abra o arquivo de configuração do servidor `/etc/ssh/sshd_config` no appliance do VMware e verifique se as configurações estão corretas.

| Configuração | Status |
|---------------------------------|-------------------------|
| Protocolo do daemon do servidor | Protocolo 2 |
| Cifras CBC | aes256-ctr e aes128-ctr |
| Encaminhamento TCP | AllowTCPForwarding no |
| Portas de gateway do servidor | Gateway Ports no |
| Encaminhamento X11 | X11Forwarding no |

| Configuração | Status |
|---|--|
| Serviço de SSH | Use o campo AllowGroups e especifique um acesso permitido de grupo. Adicione os membros apropriados a esse grupo. |
| Autenticação GSSAPI | GSSAPIAuthentication no, if unused |
| Autenticação Keberos | KeberosAuthentication no, if unused |
| Variáveis locais (opção global AcceptEnv) | Defina como desativado por comentário ou ativado para variáveis LC_* ou LANG |
| Configuração de túnel | PermitTunnel no |
| Sessões de rede | MaxSessions 1 |
| Conexões concorrentes do usuário | Defina como 1 para usuário raiz e qualquer outro usuário. O arquivo /etc/security/limits.conf também precisa ser definido com as mesmas configurações. |
| Verificação de modo restrito | Strict Modes yes |
| Separação de privilégios | UsePrivilegeSeparation yes |
| Autenticação RSA de rhosts | RhostsESAAuthentication no |
| Compressão | Compression delayed or Compression no |
| Código de autenticação da mensagem | MACs hmac-sha1 |
| Restrição ao acesso do usuário | PermitUserEnvironment no |

2 Salve suas alterações e feche o arquivo.

Reforçar a configuração do cliente de Shell Seguro

Como parte do processo de reforço do sistema, verifique o reforço do cliente de SSH examinando o arquivo de configuração do cliente de SSH nas máquinas de host do appliance virtual para garantir que ele está configurado de acordo com as diretrizes da VMware.

Procedimentos

1 Abra o arquivo de configuração do cliente de SSH, /etc/ssh/ssh_config, e verifique se as configurações da seção de opções globais estão corretas.

| Configuração | Status |
|---|--|
| Protocolo do cliente | Protocolo 2 |
| Portas de gateway do cliente | Gateway Ports no |
| Autenticação GSSAPI | GSSAPIAuthentication no |
| Variáveis locais (opção global SendEnv) | Fornecer somente variáveis LC_* ou LANG |
| Cifras CBC | Somente aes256-ctr e aes128-ctr |
| Códigos de autenticação da mensagem | Usados somente na entrada MACs hmac-sha1 |

2 Salve suas alterações e feche o arquivo.

Verificar permissões de arquivo da chave do shell seguro

Para minimizar a possibilidade de ataques maliciosos, mantenha permissões críticas de arquivo de chave de SSH nas máquinas de host do appliance virtual.

Após configurar ou atualizar suas configurações de SSH, sempre verifique se as permissões do arquivo de chave de SSH a seguir não foram alteradas.

- Os arquivos de chave do host público em `/etc/ssh/*key.pub` são de posse do usuário raiz e têm permissões definidas para 0644 (-rw-r--r--).
- Os arquivos de chave do host privado em `/etc/ssh/*key` são de posse do usuário raiz e têm permissões definidas para 0600 (-rw-----).

Verificar permissões de arquivo de chave SSH

Verifique se permissões SSH estão aplicadas a ambos os arquivos de chave pública e particular.

Procedimentos

- 1 Verifique os arquivos de chave pública SSH executando o seguinte comando: `ls -l /etc/ssh/*key.pub`
- 2 Verifique se o proprietário é root, se o proprietário do grupo é root e se os arquivos têm permissões definidas como 0644 (-rw-r--r--).

- 3 Corrija problemas executando os seguintes comandos.

```
chown root /etc/ssh/*key.pub
chgrp root /etc/ssh/*key.pub
chmod 644 /etc/ssh/*key.pub
```

- 4 Verifique os arquivos de chave particular SSH executando o seguinte comando: `ls -l /etc/ssh/*key`

- 5 Corrija problemas executando os seguintes comandos.

```
chown root /etc/ssh/*key
chgrp root /etc/ssh/*key
chmod 644 /etc/ssh/*key
```

Alterar o usuário da Interface de Gerenciamento de Appliances Virtuais

Você pode adicionar e excluir usuários na Interface de Gerenciamento de Appliances Virtuais para criar o nível de segurança apropriado.

A conta de usuário raiz da Interface de Gerenciamento de Appliances Virtuais usa o PAM para autenticação e, portanto, os níveis de corte definidos pelo PAM também se aplicam. Se você não tiver isolado corretamente a Interface de Gerenciamento de Appliances Virtuais, um bloqueio da conta raiz do sistema poderá ocorrer se um invasor tentar forçar o login de forma bruta. Além disso, quando a conta raiz é considerada insuficiente para fornecer não repúdio por mais de uma pessoa na sua organização, você pode optar por alterar o usuário administrador da interface de gerenciamento.

Pré-requisitos

Procedimentos

- 1 Execute o seguinte comando para criar um novo usuário e adicioná-lo ao grupo da Interface de Gerenciamento de Appliances Virtuais.

```
useradd -G vami,root user
```

- 2 Crie uma senha para o usuário.

```
passwd user
```

- 3 (Opcional) Execute o seguinte comando para desativar o acesso raiz na Interface de Gerenciamento de Appliances Virtuais.

```
usermod -R vami root
```

Observação A ação de desativar o acesso raiz à Interface de Gerenciamento de Appliances Virtuais também desativa a capacidade de atualizar a senha do administrador, ou raiz, na guia Administração.

Definir autenticação do bootloader

Para oferecer um nível adequado de segurança, configure a autenticação do bootloader nos appliances virtuais do VMware.

Se o bootloader do sistema não exigir autenticação, os usuários com acesso ao console do sistema poderão alterar as configurações de inicialização do sistema, ou inicializar o sistema em modo de usuário único ou manutenção, o que pode resultar em negação do serviço ou em acesso não autorizado ao sistema. Como a autenticação do bootloader não é definida por padrão nos appliances virtuais do VMware, você deverá criar uma senha GRUB para configurá-la.

Procedimentos

- 1 Verifique se existe uma senha de inicialização localizando a linha `password --md5 <password-hash>` no arquivo `/boot/grub/menu.lst` nos appliances virtuais.

- 2 Se não existir nenhuma senha, execute o comando `# /usr/sbin/grub-md5-crypt` no appliance virtual.

Uma senha MD5 será gerada e o comando fornecerá a saída de hash md5.

- 3 Anexe a senha ao arquivo `menu.lst` executando o comando `# password --md5 <hash from grub-md5-crypt>`.

Configurar o NTP

Para o fornecimento de horário crítico, desative a sincronização de data/hora do host e use o Network Time Protocol (NTP) no appliance do vRealize Automation.

O daemon NTP no appliance do vRealize Automation fornece serviços de hora sincronizados. O NTP está desativado por padrão; portanto, é necessário configurá-lo manualmente. Se possível, use o NTP em ambientes de produção para rastrear ações de usuários e detectar possíveis ataques e intrusões maliciosos por meio de auditoria e registro de manutenção precisos. Para obter informações sobre avisos de segurança do NTP, consulte o site do NTP.

O arquivo de configuração do NTP está localizado na pasta `/etc/` em cada appliance. Você pode ativar o serviço NTP para o appliance do vRealize Automation e adicionar servidores de horário na guia **Administrador** da Virtual Appliance Management Interface.

Procedimentos

- 1 Abra o arquivo de configuração `/etc/ntp.conf` na máquina host do appliance virtual usando um editor de texto.
- 2 Defina a propriedade do arquivo como **root:root**.
- 3 Defina as permissões para **0640**.
- 4 Para reduzir o risco de um ataque de amplificação de negação de serviço no NTP, abra o arquivo `/etc/ntp.conf` e verifique se as linhas de restrição aparecem no arquivo.

```
restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery
restrict 127.0.0.1
restrict -6 ::1
```

- 5 Salve as alterações e feche os arquivos.

Configurando o TLS para dados do appliance do vRealize Automation em trânsito

Certifique-se de que a implantação do seu vRealize Automation usa protocolos TLS fortes para proteger canais de transmissão para componentes do appliance do vRealize Automation.

Para considerações de desempenho, o TLS não está habilitado para conexões localhost entre alguns application services. Em locais onde a defesa em profundidade é preocupante, habilite o TLS em todas as comunicações localhost.

Importante Se você estiver finalizando o TLS no balanceador de carga, desative protocolos inseguros, como SSLv2, SSLv3 e TLS 1.0 em todos os balanceadores de carga.

Ativar TLS na configuração do localhost

Por padrão, algumas comunicações do localhost não usam TLS. Você pode ativar o TLS em todas as conexões do localhost para oferecer maior segurança.

Procedimentos

- 1 Conectar ao Appliance do vRealize Automation usando SSH.

2 Defina as permissões para o keystore vcac executando os seguintes comandos.

```
usermod -A vco,coredump,pivotal vco
chown vcac.pivotal /etc/vcac/vcac.keystore
chmod 640 /etc/vcac/vcac.keystore
```

3 Atualize a configuração de HAProxy.

a Abra o arquivo de configuração HAProxy localizado em /etc/haproxy/conf.d e escolha o serviço 20-vcac.cfg.

b Localize as linhas contendo a seguinte cadeia de caracteres:

```
server local 127.0.0.1...
```

e adicione o seguinte ao final dessas linhas: `ssl verify none`

Esta seção contém outras linhas semelhantes às linhas abaixo.

| | |
|--------------------|---------------------|
| backend-horizon | backend-vro |
| backend-vra | backend-artifactory |
| backend-vra-health | |

c Altere a porta de backend-horizon de 8080 para 8443.

4 Obtenha a senha de keystorePass.

a Localize a propriedade `certificate.store.password` no arquivo `/etc/vcac/security.properties`.

Por exemplo, `certificate.store.password=s2enc~iom0GXATG+RB8ff7Wdm4Bg==`

b Desencrpte o valor usando o seguinte comando:

```
vcac-config prop-util -d --p VALUE
```

Por exemplo, `vcac-config prop-util -d --p s2enc~iom0GXATG+RB8ff7Wdm4Bg==`

5 Configure o serviço vRealize Automation

a Abra o arquivo `/etc/vcac/server.xml`.

b Adicione o seguinte atributo à tag `Connector`, substituindo `certificate.store.password` pelo valor da senha do repositório de certificados encontrado em `etc/vcac/security.properties`.

```
scheme="https" secure="true" SSLEnabled="true" sslProtocol="TLS"
keystoreFile="/etc/vcac/vcac.keystore" keyAlias="apache"
keystorePass="certificate.store.password"
```

6 Configure o serviço vRealize Orchestrator.

- a Abra o arquivo `/etc/vco/app-server.xml`
- b Adicione o seguinte atributo à tag `Connector`, substituindo `certificate.store.password` pelo valor da senha do repositório de certificados encontrado em `etc/vcac/security.properties`.

```
scheme="https" secure="true" SSLEnabled="true" sslProtocol="TLS"  
keystoreFile="/etc/vcac/vcac.keystore" keyAlias="apache"  
keystorePass="certificate.store.password"
```

7 Reinicie o vRealize Orchestrator, vRealize Automation e serviços de haproxy.

```
service vcac-server restart  
service vco-server restart  
service haproxy restart
```

Observação Se o `vco-server` não reiniciar, reinicialize o computador `host`.

8 Configure a Interface de Gerenciamento do Appliance Virtual.

- a Abra o arquivo `/opt/vmware/share/htdocs/service/café-services/services.py`.
- b Altere a linha `conn = httpLib.HTTP()` para `conn = httpLib.HTTPS()` para aumentar a segurança.

Ativar conformidade com o Padrão Federal de Processamento de Informações (FIPS) 140-2

O appliance do vRealize Automation agora utiliza a versão do OpenSSL certificada conforme o Padrão Federal de Processamento de Informações (FIPS) 140-2 para dados em trânsito sobre TLS em todo o tráfego de entrada e saída da rede.

Você pode ativar ou desativar o modo FIPS na interface de gerenciamento do appliance do vRealize Automation. Você também pode configurar o FIPS a partir da linha de comando ao acessar como raiz, usando os seguintes comandos:

```
vcac-vami fips enable  
vcac-vami fips disable  
vcac-vami fips status
```

Quando o FIPS está ativado, o tráfego de rede de entrada e saída do Appliance do vRealize Automation na porta 443 usa a criptografia em conformidade com FIPS 140–2. Independentemente da configuração de FIPS, o vRealize Automation usa AES–256 para proteger os dados seguros armazenados no appliance do vRealize Automation.

Observação Atualmente, o vRealize Automation só pode ativar parcialmente a conformidade com FIPS, porque alguns componentes internos não usam ainda os módulos criptográficos certificados. Em casos onde módulos certificados ainda não tenham sido implantados, a criptografia baseada em AES–256 é usada em todos os algoritmos criptográficos.

Observação O procedimento a seguir vai reinicializar a máquina física quando você alterar a configuração.

Procedimentos

- 1 Faça login como raiz na interface de gerenciamento do appliance do vRealize Automation.
`https:// vrealize-automation-appliance-FQDN:5480`
- 2 Selecione **Configurações do vRA > Configurações do Host**.
- 3 Clique no botão sob o cabeçalho **Ações** no canto superior direito para ativar ou desativar o FIPS.
- 4 Clique em **Sim** para reiniciar o appliance do vRealize Automation

Verifique se o SSLv3, o TLS 1.0 e o TLS 1.1 estão desativados

Como parte do processo de reforço, certifique-se de que o Appliance do vRealize Automation implantado utilize canais seguros de transmissão.

Observação Não é possível executar a operação Ingressar no cluster após desativar o TLS 1.0/1.1 e ativar o TLS 1.2

Pré-requisitos

Conclua a [Ativar TLS na configuração do localhost](#).

Procedimentos

- 1 Verifique se o SSLv3, o TLS 1.0 e o TLS 1.1 estão desativados nos manipuladores https de HAProxy no Appliance do vRealize Automation.

| Reveja este arquivo | Certifique-se de que o seguinte está presente | Na linha apropriada como mostrado |
|---------------------------------------|---|---|
| /etc/haproxy/conf.d/20-vcac.cfg | no-sslv3 no-tlsv10 no-tls11 force-tls12 | bind 0.0.0.0:443 ssl crt /etc/apache2/server.pem ciphers !aNULL:!eNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH no-sslv3 no-tlsv10 no-tlsv11 |
| /etc/haproxy/conf.d/30-vro-config.cfg | no-sslv3 no-tlsv10 no-tls11 force-tls12 | bind :::8283 v4v6 ssl crt /opt/vmware/etc/lighttpd/server.pem ciphers !aNULL:!eNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH no-sslv3 no-tlsv10 no-tlsv11 |

- 2 Reinicie o serviço.

```
service haproxy restart
```

- 3 Abra o arquivo /opt/vmware/etc/lighttpd/lighttpd.conf e verifique se as entradas desativadas corretas aparecem.

Observação Não há uma diretiva para desativar o TLS 1.0 ou TLS 1.1 no Lighttpd. A restrição sobre o uso do TLS 1.0 e TLS 1.1 pode ser parcialmente atenuada ao forçar o OpenSSL a não usar conjuntos de cifras do TLS 1.0 e TLS 1.1.

```
ssl.use-ssl2 = "disable"  
ssl.use-ssl3 = "disable"
```

- 4 Verifique se o SSLv3, o TLS 1.0 e o TLS 1.1 estão desativados para o Proxy do Console no Appliance do vRealize Automation.
 - a Edite o arquivo /etc/vcac/security.properties adicionando ou modificando a seguinte linha:

```
consoleproxy.ssl.server.protocols = TLSv1.2
```

- b Reinicie o servidor executando o seguinte comando:

```
service vcac-server restart
```

- 5 Verifique se o SSLv3, o TLS 1.0 e o TLS 1.1 estão desativados para o serviço vCO.
 - a Localize a tag <Connector> no arquivo /etc/vco/app-server/server.xml e adicione o seguinte atributo:

```
sslEnabledProtocols = "TLSv1.2"
```

- b Reinicie o serviço vCO executando o seguinte comando.

```
service vco-server restart
```

- 6 Verifique se o SSLv3, o TLS 1.0 e o TLS 1.1 estão desativados para o serviço do vRealize Automation .
 - a Adicione os seguintes atributos à tag <Connector> no arquivo /etc/vcac/server.xml

```
sslEnabledProtocols = "TLSv1.2"
```

- b Reinicie o serviço vRealize Automation executando o seguinte comando:

```
service vcac-server restart
```

- 7 Verifique se o SSLv3, o TLS 1.0 e o TLS 1.1 estão desativados para o RabbitMQ.

Abra o arquivo /etc/rabbitmq/rabbitmq.config e verifique se {versions, ['tlsv1.2', 'tlsv1.1']} está presente nas seções ssl e ssl_options.

```
[
  {ssl, [
    {versions, ['tlsv1.2', 'tlsv1.1']},
    {ciphers, ["AES256-SHA", "AES128-SHA"]}
  ]},
  {rabbit, [
    {tcp_listeners, [{"127.0.0.1", 5672}]},
    {frame_max, 262144},
    {ssl_listeners, [5671]},
    {ssl_options, [
      {cacertfile, "/etc/rabbitmq/certs/ca/cacert.pem"},
      {certfile, "/etc/rabbitmq/certs/server/cert.pem"},
      {keyfile, "/etc/rabbitmq/certs/server/key.pem"},
      {versions, ['tlsv1.2', 'tlsv1.1']},
      {ciphers, ["AES256-SHA", "AES128-SHA"]},
      {verify, verify_peer},
      {fail_if_no_peer_cert, false}
    ]},
    {mnesia_table_loading_timeout, 600000},
    {cluster_partition_handling, autoheal},
    {heartbeat, 600}
  ]},
  {kernel, [{net_ticktime, 120}]}
].
```

- 8 Reinicie o servidor RabbitMQ.

```
# service rabbitmq-server restart
```

- 9 Verifique se o SSLv3, o TLS 1.0 e o TLS 1.1 estão desativados para o serviço de vIDM.

Abra o arquivo `opt/vmware/horizon/workspace/conf/server.xml` para cada instância do conector contendo `SSLEnabled="true"` e certifique-se de que a linha a seguir esteja presente.

```
sslEnabledProtocols="TLSv1.2"
```

Configurando pacotes de codificação de TLS para componentes do vRealize Automation

Para obter segurança máxima, você deve configurar componentes do vRealize Automation para usar codificação forte.

A codificação de criptografia negociada entre o servidor e o navegador determina a força de criptografia que é usada em uma sessão TLS.

Para garantir que apenas codificações fortes sejam selecionadas, desative as codificações fracas nos componentes do vRealize Automation. Configure o servidor para permitir somente codificações fortes e usar tamanhos de chave suficientemente grandes. Além disso, configure todas as codificações em uma ordem adequada.

Desative pacotes de codificação que não ofereçam autenticação, como pacotes de codificação NULL, aNULL ou eNULL. Além disso, desative a troca de chaves Diffie-Hellman anônima (ADH), a codificação de nível de exportação (EXP, codificação contendo DES), os tamanhos de chave menores de 128 bits para criptografar tráfego de carga, o uso do MD5 como mecanismo de hashing para tráfego de carga, os pacotes de codificação IDEA e os pacotes de codificação RC4. Certifique-se também de que os pacotes de codificação que usam a troca de chaves Diffie-Hellman (DHE) estejam desativados.

Desativar cifras fracas no HA Proxy

Compare as cifras do serviço de HA Proxy do appliance do vRealize Automation com a lista de cifras aceitáveis e desative todas aquelas consideradas fracas.

Desative pacotes de codificação que não ofereçam autenticação, como pacotes de codificação NULL, aNULL ou eNULL. Além disso, desative a troca de chaves Diffie-Hellman anônima (ADH), a codificação de nível de exportação (EXP, codificação contendo DES), os tamanhos de chave menores de 128 bits para criptografar tráfego de carga, o uso do MD5 como mecanismo de hashing para tráfego de carga, os pacotes de codificação IDEA e os pacotes de codificação RC4.

Procedimentos

- 1 Consulte a entrada de cifras no arquivo `/etc/haproxy/conf.d/20-vcac.cfg` da diretiva vinculante e desative todas as que são consideradas fracas.

```
bind 0.0.0.0:443 ssl crt /etc/apache2/server.pem ciphers !aNULL:!eNULL:kECDH
+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH no-ssl3 no-
tlsv10 no-tlsv11
```

- 2 Consulte a entrada de cifras no arquivo `/etc/haproxy/conf.d/30-vro-config.cfg` da diretiva vinculante e desative todas as que são consideradas fracas.

```
bind :::8283 v4v6 ssl crt /opt/vmware/etc/lighttpd/server.pem ciphers !aNULL:!
eNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH
no-ssl3 no-tlsv10 no-tlsv11
```

Desativar as cifras fracas no serviço de proxy do console do appliance do Appliance do vRealize Automation

Compare as cifras do serviço de proxy do console do appliance do vRealize Automation com a lista de cifras aceitáveis e desative todas aquelas consideradas fracas.

Desative pacotes de codificação que não ofereçam autenticação, como pacotes de codificação NULL, aNULL ou eNULL. Além disso, desative a troca de chaves Diffie-Hellman anônima (ADH), a codificação de nível de exportação (EXP, codificação contendo DES), os tamanhos de chave menores de 128 bits para criptografar tráfego de carga, o uso do MD5 como mecanismo de hashing para tráfego de carga, os pacotes de codificação IDEA e os pacotes de codificação RC4.

Procedimentos

- 1 Abra o arquivo `/etc/vcac/security.properties` em um editor de texto.
- 2 Adicione uma linha ao arquivo para desativar os conjuntos de cifras indesejados.

Use uma variação da seguinte linha:

```
consoleproxy.ssl.ciphers.disallowed=cipher_suite_1, cipher_suite_2,etc
```

Por exemplo, para desativar os conjuntos de codificações AES 128 e AES 256, adicione a seguinte linha:

```
consoleproxy.ssl.ciphers.disallowed=TLS_DH_DSS_WITH_AES_128_CBC_SHA,  
TLS_DH_DSS_WITH_AES_256_CBC_SHA, TLS_DH_RSA_WITH_AES_256_CBC_SHA,  
TLS_DHE_DSS_WITH_AES_128_CBC_SHA, TLS_DHE_DSS_WITH_AES_256_CBC_SHA,  
TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA
```

- 3 Reinicie o servidor usando o comando a seguir.

```
service vcac-server restart
```

Desativar cifras fracas no serviço vCO do Appliance do vRealize Automation

Compare as cifras do serviço vCO do Appliance do vRealize Automation com a lista de cifras aceitáveis e desative todas aquelas consideradas fracas.

Desative pacotes de codificação que não ofereçam autenticação, como pacotes de codificação NULL, aNULL ou eNULL. Além disso, desative a troca de chaves Diffie-Hellman anônima (ADH), a codificação de nível de exportação (EXP, codificação contendo DES), os tamanhos de chave menores de 128 bits para criptografar tráfego de carga, o uso do MD5 como mecanismo de hashing para tráfego de carga, os pacotes de codificação IDEA e os pacotes de codificação RC4.

Procedimentos

- 1 Localize a tag `<Connector>` no arquivo `/etc/vco/app/server/server.xml`.

2 Edite ou adicione o atributo de cifra para usar os conjuntos de cifras desejados.

Consulte o exemplo a seguir:

```
ciphers="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
```

Desativar cifras fracas no serviço RabbitMQ do Appliance do vRealize Automation

Compare as cifras do serviço RabbitMQ do Appliance do vRealize Automation com a lista de cifras aceitáveis e desative todas aquelas consideradas fracas.

Desative pacotes de codificação que não ofereçam autenticação, como pacotes de codificação NULL, aNULL ou eNULL. Além disso, desative a troca de chaves Diffie-Hellman anônima (ADH), a codificação de nível de exportação (EXP, codificação contendo DES), os tamanhos de chave menores de 128 bits para criptografar tráfego de carga, o uso do MD5 como mecanismo de hashing para tráfego de carga, os pacotes de codificação IDEA e os pacotes de codificação RC4.

Procedimentos

- 1 Avalie os conjuntos de cifras compatíveis. executando o comando `# /usr/sbin/rabbitmqctl eval 'ssl:cipher_suites()'`.

As cifras retornadas no exemplo a seguir representam somente as cifras compatíveis. O servidor do RabbitMQ não usa ou anuncia estas cifras exceto se configurado para tal no arquivo `rabbitmq.config`.

```
["ECDHE-ECDSA-AES256-GCM-SHA384", "ECDHE-RSA-AES256-GCM-SHA384",
 "ECDHE-ECDSA-AES256-SHA384", "ECDHE-RSA-AES256-SHA384",
 "ECDH-ECDSA-AES256-GCM-SHA384", "ECDH-RSA-AES256-GCM-SHA384",
 "ECDH-ECDSA-AES256-SHA384", "ECDH-RSA-AES256-SHA384",
 "DHE-RSA-AES256-GCM-SHA384", "DHE-DSS-AES256-GCM-SHA384",
 "DHE-RSA-AES256-SHA256", "DHE-DSS-AES256-SHA256", "AES256-GCM-SHA384",
 "AES256-SHA256", "ECDHE-ECDSA-AES128-GCM-SHA256",
 "ECDHE-RSA-AES128-GCM-SHA256", "ECDHE-ECDSA-AES128-SHA256",
 "ECDHE-RSA-AES128-SHA256", "ECDH-ECDSA-AES128-GCM-SHA256",
 "ECDH-RSA-AES128-GCM-SHA256", "ECDH-ECDSA-AES128-SHA256",
 "ECDH-RSA-AES128-SHA256", "DHE-RSA-AES128-GCM-SHA256",
 "DHE-DSS-AES128-GCM-SHA256", "DHE-RSA-AES128-SHA256", "DHE-DSS-AES128-SHA256",
 "AES128-GCM-SHA256", "AES128-SHA256", "ECDHE-ECDSA-AES256-SHA",
 "ECDHE-RSA-AES256-SHA", "DHE-RSA-AES256-SHA", "DHE-DSS-AES256-SHA",
 "ECDH-ECDSA-AES256-SHA", "ECDH-RSA-AES256-SHA", "AES256-SHA",
 "ECDHE-ECDSA-DES-CBC3-SHA", "ECDHE-RSA-DES-CBC3-SHA", "EDH-RSA-DES-CBC3-SHA",
 "EDH-DSS-DES-CBC3-SHA", "ECDH-ECDSA-DES-CBC3-SHA", "ECDH-RSA-DES-CBC3-SHA",
 "DES-CBC3-SHA", "ECDHE-ECDSA-AES128-SHA", "ECDHE-RSA-AES128-SHA",
 "DHE-RSA-AES128-SHA", "DHE-DSS-AES128-SHA", "ECDH-ECDSA-AES128-SHA",
 "ECDH-RSA-AES128-SHA", "AES128-SHA"]
```

- 2 Selecione as cifras compatíveis que atendem aos requisitos de segurança da sua organização.

Por exemplo, para permitir somente ECDHE–ECDSA–AES128–GCM–SHA256 & ECDHE–ECDSA–AES256–GCM–SHA384, abra o arquivo `/etc/rabbitmq/rabbitmq.config` e adicione a seguinte linha a `ssl` e `ssl_options`.

```
{ciphers, ["ECDHE–ECDSA–AES128–GCM–SHA256", "ECDHE–ECDSA–AES256–GCM–SHA384"]}
```

- 3 Reinicie o servidor do RabbitMQ usando o seguinte comando.

```
service rabbitmq-server restart
```

Verificar a segurança de dados em repouso

Verificar a segurança dos usuários do banco de dados e contas usadas com o vRealize Automation.

Usuário postgres

A conta de usuário Linux postgres está vinculada à função de conta de superusuário do banco de dados postgres e, por padrão, é uma conta bloqueada. Esta é a configuração mais segura para este usuário, pois só é acessível a partir da conta do usuário raiz. Não desbloqueie esta conta de usuário.

Funções de conta do usuário do banco de dados

As funções padrão de conta do usuário postgres não devem ser utilizadas além da funcionalidade da aplicação. Para compatibilidade com atividades não padrão de revisão ou relatórios do banco de dados, uma conta adicional deve ser criada e a senha protegida adequadamente.

Execute o seguinte script na linha de comando:

```
vcac-vami add-db-user newUsername newPassword
```

Isso vai adicionar um novo usuário e uma senha fornecida pelo usuário.

Observação Esse script deve ser executado contra um banco de dados postgres mestre nos casos onde a configuração de postgres mestre-escravo HA está configurada.

Configurar autenticação do cliente PostgreSQL

Certifique-se de que a autenticação de confiança local não esteja configurada no banco de dados PostgreSQL do appliance do vRealize Automation. Essa configuração permite que qualquer usuário local, incluindo o superusuário do banco de dados, conecte-se como qualquer usuário do PostgreSQL sem uma senha.

Observação A conta de superusuário do Postgres deve permanecer como confiança local.

O método de autenticação md5 é recomendado porque ele envia senhas criptografadas.

As configurações de autenticação do cliente estão localizadas no arquivo `/storage/db/pgdata/pg_hba.conf`.

```
# TYPE DATABASE USER ADDRESS METHOD

# "local" is for Unix domain socket connections only
local all postgres trust
# IPv4 local connections:
#host all all 127.0.0.1/32 md5
hostssl all all 127.0.0.1/32 md5
# IPv6 local connections:
#host all all ::1/128 md5
hostssl all all ::1/128 md5

# Allow remote connections for VCAC user.
#host vcac vcac 0.0.0.0/0 md5
hostssl vcac vcac 0.0.0.0/0 md5
hostssl vcac vcac ::0/0 md5
# Allow remote connections for VCAC replication user.
#host vcac vcac_replication 0.0.0.0/0 md5
hostssl vcac vcac_replication 0.0.0.0/0 md5
hostssl vcac vcac_replication ::0/0 md5
# Allow replication connections by a user with the replication privilege.
#host replication vcac_replication 0.0.0.0/0 md5
hostssl replication vcac_replication 0.0.0.0/0 md5
hostssl replication vcac_replication ::0/0 md5
```

Caso você edite o arquivo `pg_hba.conf`, deverá reiniciar o servidor do Postgres executando os seguintes comandos antes que as alterações possam ser efetivadas.

```
# cd /opt/vmware/vpostgres/9.2/bin
# su postgres
# ./pg_ctl restart -D /storage/db/pgdata/ -m fast
```

Configurar recursos de aplicação do vRealize Automation

Revisar recursos de aplicação do vRealize Automation e restringir permissões de arquivo.

Procedimentos

- 1 Execute o seguinte comando para verificar se os arquivos com conjunto de bits SUID e GUID estão bem-definidos.

```
find / -path /proc -prune -o -type f -perm +6000 -ls
```

A seguinte lista deverá aparecer.

```
2197357 24 -rwsr-xr-x 1 polkituser root 23176 Mar 31 2015 /usr/lib/PolicyKit/polkit-
set-default-helper
2197354 16 -rwxr-sr-x 1 root polkituser 14856 Mar 31 2015 /usr/lib/PolicyKit/polkit-
read-auth-helper
2197353 12 -rwsr-x--- 1 root polkituser 10744 Mar 31 2015 /usr/lib/PolicyKit/polkit-
grant-helper-pam
2197352 20 -rwxr-sr-x 1 root polkituser 19208 Mar 31 2015 /usr/lib/PolicyKit/polkit-
```

```

grant-helper
2197351 20 -rwxr-sr-x 1 root polkituser 19008 Mar 31 2015 /usr/lib/PolicyKit/polkit-
explicit-grant-helper
2197356 24 -rwxr-sr-x 1 root polkituser 23160 Mar 31 2015 /usr/lib/PolicyKit/polkit-
revoke-helper
2188203 460 -rws--x--x 1 root root 465364 Apr 21 22:38 /usr/lib64/ssh/ssh-keysign
2138858 12 -rwxr-sr-x 1 root tty 10680 May 10 2010 /usr/sbin/utempter
2142482 144 -rwsr-xr-x 1 root root 142890 Sep 15 2015 /usr/bin/passwd
2142477 164 -rwsr-xr-x 1 root shadow 161782 Sep 15 2015 /usr/bin/chage
2142467 156 -rwsr-xr-x 1 root shadow 152850 Sep 15 2015 /usr/bin/chfn
1458298 364 -rwsr-xr-x 1 root root 365787 Jul 22 2015 /usr/bin/sudo
2142481 64 -rwsr-xr-x 1 root root 57776 Sep 15 2015 /usr/bin/newgrp
1458249 40 -rwsr-x--- 1 root trusted 40432 Mar 18 2015 /usr/bin/crontab
2142478 148 -rwsr-xr-x 1 root shadow 146459 Sep 15 2015 /usr/bin/chsh
2142480 156 -rwsr-xr-x 1 root shadow 152387 Sep 15 2015 /usr/bin/gpasswd
2142479 48 -rwsr-xr-x 1 root shadow 46967 Sep 15 2015 /usr/bin/expiry
311484 48 -rwsr-x--- 1 root messagebus 47912 Sep 16 2014 /lib64/dbus-1/dbus-daemon-
launch-helper
876574 36 -rwsr-xr-x 1 root shadow 35688 Apr 10 2014 /sbin/unix_chkpwd
876648 12 -rwsr-xr-x 1 root shadow 10736 Dec 16 2011 /sbin/unix2_chkpwd
49308 68 -rwsr-xr-x 1 root root 63376 May 27 2015 /opt/likewise/bin/ksu
1130552 40 -rwsr-xr-x 1 root root 40016 Apr 16 2015 /bin/su
1130511 40 -rwsr-xr-x 1 root root 40048 Apr 15 2011 /bin/ping
1130600 100 -rwsr-xr-x 1 root root 94808 Mar 11 2015 /bin/mount
1130601 72 -rwsr-xr-x 1 root root 69240 Mar 11 2015 /bin/umount
1130512 36 -rwsr-xr-x 1 root root 35792 Apr 15 2011 /bin/ping6
2012 /lib64/dbus-1/dbus-daemon-launch-helper

```

- 2 Execute o seguinte comando para verificar se todos os arquivos no appliance virtual têm um proprietário.

```
find / -path /proc -prune -o -nouser -o -nogroup
```

- 3 Reveja as permissões para todos os arquivos ao appliance virtual para verificar se nenhum deles é gravável globalmente executando o comando a seguir.

```
find / -name ".*" -type f -perm -a+w | xargs ls -ldb
```

- 4 Execute o seguinte comando para verificar se somente o usuário vcac tem posse dos arquivos corretos.

```
find / -name "proc" -prune -o -user vcac -print | egrep -v -e "*/vcac/*" | egrep -v -e "*/vmware-vcac/*"
```

Se nenhum resultado aparecer, isso significa que todos os arquivos corretos são de posse apenas do usuário vcac.

- 5 Verifique se os arquivos a seguir são graváveis somente pelo usuário vcac.

```

/etc/vcac/vcac/security.properties
/etc/vcac/vcac/solution-users.properties
/etc/vcac/vcac/sso-admin.properties
/etc/vcac/vcac/vcac.keystore

```

```
/etc/vcac/vcac/vcac.properties
```

Além disso, verifique os arquivos a seguir e seus subdiretórios

```
/var/log/vcac/*
```

```
/var/lib/vcac/*
```

```
/var/cache/vcac/*
```

- 6 Verifique se somente o usuário vcac ou raiz pode ler os arquivos corretos nos diretórios a seguir e seus subdiretórios.

```
/etc/vcac/*
```

```
/var/log/vcac/*
```

```
/var/lib/vcac/*
```

```
/var/cache/vcac/*
```

- 7 Verifique se os arquivos corretos são de posse somente do usuário vco ou raiz, conforme mostrado nos diretórios a seguir e seus subdiretórios.

```
/etc/vco/*
```

```
/var/log/vco/*
```

```
/var/lib/vco/*
```

```
/var/cache/vco/*
```

- 8 Verifique se os arquivos corretos são graváveis somente pelo usuário vco ou raiz, conforme mostrado nos diretórios a seguir e seus subdiretórios.

```
/etc/vco/*
```

```
/var/log/vco/*
```

```
/var/lib/vco/*
```

```
/var/cache/vco/*
```

- 9 Verifique se os arquivos corretos são legíveis somente pelo usuário vco ou raiz, conforme mostrado nos diretórios a seguir e seus subdiretórios.

```
/etc/vco/*
```

```
/var/log/vco/*
```

```
/var/lib/vco/*
```

```
/var/cache/vco/*
```

Personalizando a configuração do proxy do console

Você pode personalizar a configuração do console remoto para o vRealize Automation facilitar a solução de problemas e as práticas organizacionais.

Ao instalar, configurar ou manter o vRealize Automation, você pode alterar algumas configurações para ativar a solução de problemas e a depuração da sua instalação. Catalogue e faça auditoria de cada uma das alterações que você faz para garantir que os componentes aplicáveis estejam devidamente protegidos, de acordo com o uso necessário. Não continue a produção se você não tiver certeza de que as alterações de configuração estejam protegidas corretamente.

Personalizar a expiração do tíquete do VMware Remote Console

Você pode personalizar o período de validade para os tíquetes do console remoto usados no estabelecimento de conexões no VMware Remote Console.

Quando um usuário faz conexões no VMware Remote Console, o sistema cria e retorna uma credencial única que estabelece uma conexão específica a uma máquina virtual. Você pode definir a expiração do tíquete por um período de tempo especificado em minutos.

Procedimentos

- 1 Abra o arquivo `/etc/vcac/security.properties` em um editor de texto.
- 2 Adicione uma linha ao arquivo do formulário `consoleproxy.ticket.validitySec=30`.
Nesta linha, o valor numérico especifica o número de minutos antes de o tíquete expirar.
- 3 Salve o arquivo e feche-o.
- 4 Reinicie o servidor `vcac` usando o comando `/etc/init.d/vcac-server restart`.

O valor de expiração do tíquete é redefinido para o período de tempo especificado em minutos.

Personalizar a porta do servidor proxy do console

Você pode personalizar a porta na qual o proxy do console do VMware Remote Console escuta as mensagens.

Procedimentos

- 1 Abra o arquivo `/etc/vcac/security.properties` em um editor de texto.
- 2 Adicione uma linha ao arquivo do formulário `consoleproxy.service.port=8445`.
O valor numérico especifica o número da porta de serviço do proxy do console, neste caso 8445.
- 3 Salve o arquivo e feche-o.
- 4 Reinicie o servidor `vcac` usando o comando `/etc/init.d/vcac-server restart`.

A porta de serviço do proxy é alterada para o número de porta especificado.

Configurar o cabeçalho de resposta do X-XSS-Protection

Adicione o cabeçalho de resposta do X-XSS-Protection ao arquivo de configuração `haproxy`.

Procedimentos

- 1 Abra `/etc/haproxy/conf.d/20-vcac.cfg` para edição.

- 2 Adicione as seguintes linhas em uma seção front-end:

```
rspdel X-XSS-Protection:\ 1;\ mode=block
      rspadd X-XSS-Protection:\ 1;\ mode=block
```

- 3 Recarregue a configuração do HAProxy usando o seguinte comando.

```
/etc/init.d/haproxy reload
```

Configurar o cabeçalho de resposta do HTTP Strict Transport Security

Adicione o cabeçalho de resposta do HTTP Strict Transport (HSTS) à configuração do HAProxy.

Procedimentos

- 1 Abra `/etc/haproxy/conf.d/20-vcac.cfg` para edição.
- 2 Adicione as seguintes linhas em uma seção front-end:

```
rspdel Strict-Transport-Security:\ max-age=31536000
      rspadd Strict-Transport-Security:\ max-age=31536000
```

- 3 Recarregue a configuração do HAProxy usando o seguinte comando.

```
/etc/init.d/haproxy reload
```

Configurar o cabeçalho de resposta do X-Frame-Options

O cabeçalho de resposta do X-Frame-Options pode aparecer duas vezes em alguns casos.

O cabeçalho de resposta do X-Frame-Options pode aparecer duas vezes porque o serviço vIDM adiciona esse cabeçalho ao back-end, bem como ao HAProxy. Você pode impedir que ele apareça duas vezes com uma configuração apropriada.

Procedimentos

- 1 Abra `/etc/haproxy/conf.d/20-vcac.cfg` para edição.
- 2 Localize a seguinte linha na seção front-end:

```
rspadd X-Frame-Options:\ SAMEORIGIN
```
- 3 Adicione as seguintes linhas antes da linha localizada na etapa anterior:

```
rspdel X-Frame-Options:\ SAMEORIGIN
```
- 4 Recarregue a configuração do HAProxy usando o seguinte comando.

```
/etc/init.d/haproxy reload
```

Configurar cabeçalhos de resposta do servidor

Como melhor prática de segurança, configure o sistema do vRealize Automation para limitar as informações disponíveis para invasores em potencial.

Até onde possível, minimize a quantidade de informações que o sistema compartilha sobre sua identidade e versão. Hackers e agentes maliciosos podem usar essas informações para criar ataques direcionados contra o seu servidor web ou versão.

Configurar o cabeçalho de resposta do servidor Lighttpd

Como uma prática recomendada, crie um cabeçalho de servidor em branco para o servidor lighttpd do appliance do vRealize Automation.

Procedimentos

- 1 Abra o arquivo `/opt/vmware/etc/lighttpd/lighttpd.conf` em um editor de texto.
- 2 Adicione `server.tag = " "` ao arquivo.
- 3 Salve suas alterações e feche o arquivo.
- 4 Reinicie o servidor lighttpd executando o comando `# /opt/vmware/etc/init.d/vami-lighttpd restart`.

Configurar o cabeçalho de resposta do TCServer para o appliance do vRealize Automation

Como uma prática recomendada, crie um cabeçalho de servidor em branco personalizado para o cabeçalho de resposta do TCServer usado com o appliance do vRealize Automation para limitar a possibilidade de um invasor mal-intencionado obter informações valiosas.

Procedimentos

- 1 Abra o arquivo `/etc/vco/app-server/server.xml` em um editor de texto.
- 2 Em cada elemento do `<Connector>`, adicione `server=" "`.
Por exemplo: `<Connector protocol="HTTP/1.1" server="" />`
- 3 Salve suas alterações e feche o arquivo.
- 4 Reinicie o servidor usando o comando a seguir.
`service vco-server restart`

Configurar o cabeçalho de resposta do servidor Internet Information Services

Como uma prática recomendada, crie um cabeçalho de servidor em branco personalizado para o servidor Internet Information Services (IIS) usado com o Identity Appliance para limitar a possibilidade de invasores maliciosos obterem informações valiosas.

Procedimentos

- 1 Abra o arquivo `C:\Windows\System32\inetsrv\urlscan\UrlScan.ini` em um editor de texto.
- 2 Procure por `RemoveServerHeader=0` e altere para `RemoveServerHeader=1`.
- 3 Salve suas alterações e feche o arquivo.
- 4 Reinicie o servidor executando o comando `iisreset`.

Próximo passo

Desative o cabeçalho IIS X-Powered By removendo cabeçalhos de resposta HTTP da lista no Console do Gerenciador do IIS.

- 1 Abra o console do Gerenciador do IIS.
- 2 Abra o cabeçalho de resposta HTTP e remova-o da lista.
- 3 Reinicie o servidor executando o comando `iisreset`.

Tempo limite de sessão do Appliance do vRealize Automation

Ajuste a configuração de tempo limite de sessão no Appliance do vRealize Automation de acordo com a política de segurança da sua empresa.

O tempo limite de sessão padrão do Appliance do vRealize Automation para inatividade do usuário é de 30 minutos. Para ajustar o valor do tempo limite de acordo com a política de segurança da sua organização, edite o arquivo `web.xml` na máquina de host do Appliance do vRealize Automation.

Procedimentos

- 1 Abra o arquivo `/usr/lib/vcac/server/webapps/vcac/WEB-INF/web.xml` em um editor de texto.
- 2 Localize `session-config` e ajuste o valor `session-timeout`. Consulte o código de exemplo a seguir.

```
<!-- 30 minutes session expiration time -->
<session-config>
  <session-timeout>30</session-timeout>
  <tracking-mode>COOKIE</tracking-mode>
  <cookie-config>
    <path>/</path>
  </cookie-config>
</session-config>
```

- 3 Reinicie o servidor executando o comando a seguir.

```
service vcac-server restart
```

Gerenciar softwares não essenciais

Para minimizar os riscos de segurança, remova ou configure os softwares não essenciais nas máquinas de host do vRealize Automation.

Configure todos os softwares não removidos de acordo com as recomendações do fabricante e melhores práticas de segurança para minimizar o potencial de criar brechas de segurança.

Proteger o manipulador de armazenamento em massa USB

Proteja o manipulador de armazenamento em massa USB para evitar seu uso, como o manipulador de dispositivo USB com as máquinas de host do appliance virtual do VMware. Invasores em potencial podem explorar este manipulador para comprometer o seu sistema.

Procedimentos

- 1 Abra o arquivo `/etc/modprobe.conf.local` em um editor de texto.

- 2 Certifique-se de que a linha `install usb-storage /bin/true` aparece no arquivo.
- 3 Salve o arquivo e feche-o.

Proteger o Manipulador do Protocolo de Bluetooth

Proteja o Manipulador do Protocolo de Bluetooth nas máquinas de host do appliance virtual para evitar que invasores em potencial o explorem.

Vincular o protocolo de Bluetooth à pilha da rede é desnecessário e pode aumentar a superfície de ataque do host.

Procedimentos

- 1 Abra o arquivo `/etc/modprobe.conf.local` em um editor de texto.
- 2 Certifique-se de que a seguinte linha aparece no arquivo.

```
install bluetooth /bin/true
```
- 3 Salve o arquivo e feche-o.

Proteger o Protocolo de Transmissão de Controle de Fluxo

Evite que o Protocolo de Transmissão de Controle de Fluxo (SCTP) carregue no sistema por padrão. Invasores em potencial podem explorar esse protocolo para comprometer seu sistema.

Configure o sistema para impedir que o módulo do Protocolo de Transmissão de Controle de Fluxo (SCTP) carregue exceto se for absolutamente necessário. O SCTP é um protocolo de camada de transporte com padrão IETF não utilizado. Vincular este protocolo à pilha da rede aumenta a superfície de ataque do host. Processos locais não privilegiados podem fazer com que o kernel carregue dinamicamente um manipulador de protocolo abrindo um soquete usando o protocolo.

Procedimentos

- 1 Abra o arquivo `/etc/modprobe.conf.local` em um editor de texto.
- 2 Certifique-se de que a seguinte linha aparece no arquivo.

```
install sctp /bin/true
```
- 3 Salve o arquivo e feche-o.

Proteger o Protocolo de Controle de Congestionamento de Datagramas

Como parte das atividades de reforço do sistema, evite que o Protocolo de Controle de Congestionamento de Datagramas (DCCP) carregue em suas máquinas de host do appliance virtual por padrão. Invasores em potencial podem explorar esse protocolo para comprometer seu sistema.

Evite carregar o módulo do Protocolo de Controle de Congestionamento de Datagramas (DCCP), exceto se for absolutamente necessário. O DCCP é um protocolo proposto para a camada de transporte, que não é usado. Vincular este protocolo à pilha da rede aumenta a superfície de ataque do host. Os processos locais não privilegiados podem fazer com que o kernel carregue dinamicamente um manipulador de protocolo usando o protocolo para abrir um soquete.

Procedimentos

- 1 Abra o arquivo `/etc/modprobe.conf.local` em um editor de texto.
- 2 Certifique-se de que as linhas do DCCP aparecem no arquivo.

```
install dccp/bin/true
install dccp_ipv4/bin/true
install dccp_ipv6/bin/true
```

- 3 Salve o arquivo e feche-o.

Proteger ponte de rede

Evite que o módulo de ponte de rede carregue no sistema por padrão. Invasores em potencial podem explorá-lo para comprometer seu sistema.

Configure o sistema para evitar o carregamento da ponte de rede, exceto se for absolutamente necessária. Invasores em potencial podem explorá-la para contornar o particionamento e segurança da rede.

Procedimentos

- 1 Execute o seguinte comando em todas as máquinas de host do appliance virtual do VMware.

```
# rmmod bridge
```

- 2 Abra o arquivo `/etc/modprobe.conf.local` em um editor de texto.
- 3 Certifique-se de que a seguinte linha aparece no arquivo.

```
install bridge /bin/false
```

- 4 Salve o arquivo e feche-o.

Proteger Protocolo de Soquetes Confiáveis de Datagramas

Como parte das atividades de reforço do sistema, evite que o Protocolo de Soquetes Confiáveis de Datagramas (RDS) carregue em suas máquinas de host do appliance virtual por padrão. Invasores em potencial podem explorar esse protocolo para comprometer seu sistema.

Vincular o Protocolo de Soquetes Confiáveis de Datagramas (RDS) à pilha da rede aumenta a superfície de ataque do host. Os processos locais não privilegiados podem fazer com que o sistema carregue dinamicamente um manipulador de protocolo usando o protocolo para abrir um soquete.

Procedimentos

- 1 Abra o arquivo `/etc/modprobe.conf.local` em um editor de texto.
- 2 Certifique-se de que a linha `install rds /bin/true` aparece no arquivo.
- 3 Salve o arquivo e feche-o.

Proteger protocolo de comunicações transparentes interprocessos

Como parte das atividades de reforço do sistema, evite que o Protocolo de Comunicações Transparentes Interprocessos (TIPC) carregue em suas máquinas de host do appliance virtual por padrão. Invasores em potencial podem explorar esse protocolo para comprometer seu sistema.

Vincular o Protocolo de Comunicações Transparentes Interprocessos (TIPC) à pilha da rede aumenta a superfície de ataque do host. Os processos locais não privilegiados podem fazer com que o kernel carregue dinamicamente um manipulador de protocolo usando o protocolo para abrir um soquete.

Procedimentos

- 1 Abra o arquivo `/etc/modprobe.conf.local` em um editor de texto.
- 2 Certifique-se de que a linha `install tipc /bin/true` aparece no arquivo.
- 3 Salve o arquivo e feche-o.

Proteger o Protocolo de Troca de Pacotes Inter-Rede

Evite que o Protocolo de Troca de Pacotes Inter-Rede (IPX) carregue no sistema por padrão. Invasores em potencial podem explorar esse protocolo para comprometer seu sistema.

Evite carregar o módulo do Protocolo de Troca de Pacotes Inter-Rede (IPX) exceto se for absolutamente necessário. O protocolo IPX é um protocolo obsoleto de camada de rede. Vincular este protocolo à pilha da rede aumenta a superfície de ataque do host. Os processos locais não privilegiados podem fazer com que o sistema carregue dinamicamente um manipulador de protocolo usando o protocolo para abrir um soquete.

Procedimentos

- 1 Abra o arquivo `/etc/modprobe.conf.local` em um editor de texto.
- 2 Certifique-se de que a seguinte linha aparece no arquivo.

```
install ipx /bin/true
```
- 3 Salve o arquivo e feche-o.

Proteger protocolo Appletalk

Evite que o Protocolo Appletalk carregue no sistema por padrão. Invasores em potencial podem explorar esse protocolo para comprometer seu sistema.

Evite carregar o módulo do Protocolo Appletalk exceto se for absolutamente necessário. Vincular este protocolo à pilha da rede aumenta a superfície de ataque do host. Os processos locais não privilegiados podem fazer com que o sistema carregue dinamicamente um manipulador de protocolo usando o protocolo para abrir um soquete.

Procedimentos

- 1 Abra o arquivo `/etc/modprobe.conf.local` em um editor de texto.
- 2 Certifique-se de que a seguinte linha aparece no arquivo.

```
install appletalk /bin/true
```

- 3 Salve o arquivo e feche-o.

Proteger protocolo DECnet

Evite que o Protocolo DECnet carregue no sistema por padrão. Invasores em potencial podem explorar esse protocolo para comprometer seu sistema.

Evite carregar o módulo do Protocolo DECnet exceto se for absolutamente necessário. Vincular este protocolo à pilha da rede aumenta a superfície de ataque do host. Os processos locais não privilegiados podem fazer com que o sistema carregue dinamicamente um manipulador de protocolo usando o protocolo para abrir um soquete.

Procedimentos

- 1 Abra o arquivo `/etc/modprobe.conf.local` do Protocolo DECnet em um editor de texto.
- 2 Certifique-se de que a seguinte linha aparece no arquivo.

```
install decnet /bin/true
```

- 3 Salve o arquivo e feche-o.

Proteger módulo de Firewire

Evite que o módulo de Firewire carregue no sistema por padrão. Invasores em potencial podem explorar esse protocolo para comprometer seu sistema.

Evite carregar o módulo do Firewire exceto se for absolutamente necessário.

Procedimentos

- 1 Abra o arquivo `/etc/modprobe.conf.local` em um editor de texto.
- 2 Certifique-se de que a seguinte linha aparece no arquivo.

```
install ieee1394 /bin/true
```

- 3 Salve o arquivo e feche-o.

Proteger o componente de Infraestrutura como Serviço

Ao reforçar o sistema, proteja o componente de Infraestrutura como Serviço (IaaS) do vRealize Automation e sua máquina de host para evitar que potenciais invasores os explorem.

Você deve ajustar as configurações de segurança do componente de Infraestrutura como Serviço (IaaS) do vRealize Automation e o host onde ele reside. Você deve ajustar ou verificar a configuração de outros componentes e aplicações relacionados. Em alguns casos, você pode verificar as configurações existentes; em outros, você deve alterar ou adicionar configurações para uma configuração adequada.

Desativar serviço de tempo do Windows

Como melhor prática de segurança, use servidores de tempo autorizados em vez de sincronização de tempo com o host em um ambiente de produção do vRealize Automation.

Em um ambiente de produção, desative a sincronização de tempo do host e use servidores de tempo autorizados como suporte a um monitoramento preciso das ações do usuário, e à identificação de possíveis ataques maliciosos e invasão através de auditoria e logs.

Configurando o TLS para dados da Infraestrutura como Serviço em trânsito

Certifique-se de que a implantação do seu vRealize Automation use protocolos TLS fortes para proteger canais de transmissão para componentes da Infraestrutura como Serviço.

Secure Sockets Layer (SSL) e o mais recentemente desenvolvido Transport Layer Security (TLS) são protocolos criptográficos que ajudam a garantir a segurança do sistema durante as comunicações de rede entre os diferentes componentes do sistema. Como o SSL é um padrão mais antigo, muitos de seus implementos não fornecem mais segurança adequada contra possíveis ataques. Foram identificadas vulnerabilidades graves com protocolos SSL anteriores, incluindo o SSLv2 e o SSLv3. Esses protocolos não são mais considerados seguros.

Dependendo das políticas de segurança da sua organização, você também poderá desativar o TLS 1.0.

Observação Ao finalizar o TLS no balanceador de carga, desative também protocolos fracos, como o SSLv2, o SSLv3 e o TLS 1.0, se necessário.

Desativar o SSLV3 no Internet Information Services

Como melhor prática de segurança, desative o SSLv3 no Internet Information Services (IIS) na máquina do servidor de host de Infraestrutura como Serviço (IaaS).

Procedimentos

- 1 Execute o editor de registro do Windows como administrador.
- 2 Navegue até
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\ na janela de registro.
- 3 Clique com o botão direito em **Protocolos** e selecione **Novo > Chave**
- 4 Insira **SSL 3.0**.
- 5 Na árvore de navegação, clique com o botão direito na chave recém-criada de **SSL 3.0**, e no menu pop-up selecione **Novo > Chave** e insira **Client**.
- 6 Na árvore de navegação, clique com o botão direito na chave recém-criada de **SSL 3.0**, e no menu pop-up selecione **Novo > Chave** e insira **Server**.
- 7 Na árvore de navegação, em **SSL 3.0**, clique com o botão direito em **Cliente**, e selecione **Novo > Valor DWORD (32-bit)** e insira **DisabledByDefault**.
- 8 Na árvore de navegação, em **SSL 3.0**, selecione **Cliente**, e no painel à direita, clique duas vezes em **DisabledByDefault** e insira **1**.
- 9 Na árvore de navegação, em **SSL 3.0**, clique com o botão direito em **Servidor**, e selecione **Novo > Valor DWORD (32-bit)** e insira **Enabled**.

10 Na árvore de navegação, em SSL 3.0, selecione **Servidor**, e no painel à direita, clique duas vezes no **DWORD** habilitado e insira **0**.

11 Reinicie o Windows Server.

Desativar o TLS 1.0 para IaaS

Para oferecer máxima segurança, configure o IaaS para utilizar pooling e desative o TLS 1.0.

Para obter mais informações, consulte o artigo da base de dados de conhecimento Microsoft em <https://support.microsoft.com/en-us/kb/245030>.

Procedimentos

1 Configure o IaaS para usar pooling em vez de soquetes web.

- a Atualize o arquivo de configuração dos Serviços de Gerenciador C:\Program Files (x86)\VMware\VCAC\Server\ManagerService.exe.config adicionando os seguintes valores na seção <appSettings>

```
<add key="Extensibility.Client.RetrievalMethod" value="Polling"/>
<add key="Extensibility.Client.PollingInterval" value="2000"/>
<add key="Extensibility.Client.PollingMaxEvents" value="128"/>
```

- b Reinicie o Serviço de Gerenciador (VMware vCloud Automation Center Service).

2 Verifique se o TLS 1.0 está desativado no servidor IaaS.

- a Execute o editor de registro como administrador.
- b Na janela de registro, navegue até
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\
1\
- c Clique com o botão direito em Protocolos, selecione **Novo > Chave** e insira **TLS 1.0**.
- d Na árvore de navegação, clique com o botão direito na chave recém-criada do TLS 1.0, e no menu pop-up selecione **Novo > Chave** e insira **Client**.
- e Na árvore de navegação, clique com o botão direito na chave recém-criada do TLS 1.0, e no menu pop-up selecione **Novo > Chave** e insira **Server**.
- f Na árvore de navegação, em TLS 1.0, clique com o botão direito em **Cliente**, clique em **Novo > Valor DWORD (32-bit)** e insira **DisabledByDefault**.
- g Na árvore de navegação, em TLS 1.0, selecione **Cliente**, e no painel à direita, clique duas vezes em **DisabledByDefault** DWORD e insira **1**.
- h Na árvore de navegação, em TLS 1.0, clique com o botão direito em **Servidor**, e selecione **Novo > Valor DWORD (32-bit)** e insira **Enabled**.
- i Na árvore de navegação, em TLS 1.0, selecione **Servidor**, e no painel à direita, clique duas vezes em **Enabled** DWORD e insira **0**.
- j Reinicie o Windows Server.

Configurando pacotes de codificação TLS

Para obter segurança máxima, você deve configurar componentes do vRealize Automation para usar codificação forte. A codificação de criptografia negociada entre o servidor e o navegador determina a força de criptografia que é usada em uma sessão TLS. Para garantir que apenas codificações fortes sejam selecionadas, desative as codificações fracas nos componentes do vRealize Automation. Configure o servidor para permitir somente codificações fortes e usar tamanhos de chave suficientemente grandes. Além disso, configure todas as codificações em uma ordem adequada.

Pacotes de codificação que não são aceitáveis

Desative pacotes de codificação que não ofereçam autenticação, como pacotes de codificação NULL, aNULL ou eNULL. Além disso, desative a troca de chaves Diffie-Hellman anônima (ADH), a codificação de nível de exportação (EXP, codificação contendo DES), os tamanhos de chave menores de 128 bits para criptografar tráfego de carga, o uso do MD5 como mecanismo de hashing para tráfego de carga, os pacotes de codificação IDEA e os pacotes de codificação RC4. Certifique-se também de que os pacotes de codificação que usam a troca de chaves Diffie-Hellman (DHE) estejam desativados.

Verificar segurança do servidor do host

Como melhor prática de segurança, verifique a configuração de segurança das máquinas do servidor do host da Infraestrutura como Serviço (IaaS).

A Microsoft oferece diversas ferramentas para ajudar você a verificar a segurança das máquinas do servidor do host. Entre em contato com o seu fornecedor Microsoft para obter orientação sobre o uso mais adequado dessas ferramentas.

Verificar a linha de base segura do servidor do host

Execute o Analisador de Segurança de Linha de Base Microsoft (MBSA) para confirmar rapidamente se o servidor possui as atualizações e hot fixes mais recentes. Você pode usar o MBSA para instalar patches de segurança ausentes da Microsoft e manter o servidor atualizado em relação às recomendações de segurança da Microsoft.

Baixe a versão mais recente da ferramenta do MBSA no site da Microsoft.

Verificar configuração de segurança do servidor do host

Use o kit de ferramentas do Assistente de Configuração de Segurança (SCW) e o Gerente de Conformidade de Segurança Microsoft (SCM) para verificar se o servidor do host está configurado de forma segura.

Execute o SCW a partir das ferramentas administrativas do servidor Windows. Essa ferramenta pode identificar as funções do servidor e os recursos instalados, incluindo rede, firewalls do Windows e configurações de registro. Compare o relatório com a orientação mais recente sobre reforço do SCM relevante para o seu servidor Windows. Com base nos resultados, é possível ajustar as configurações de segurança para cada recurso como serviços de rede, configurações de conta e firewalls do Windows, e aplicar as configurações ao seu servidor.

Encontre mais informações sobre a ferramenta do SCW no site do Microsoft TechNet.

Proteger recursos da aplicação

Como melhor prática de segurança, certifique-se de que todos os arquivos relevantes de Infraestrutura como Serviço tenha permissões adequadas.

Compare os arquivos de Infraestrutura como Serviço com a sua instalação de Infraestrutura como Serviço. Na maioria dos casos, subpastas e arquivos de cada pasta devem ter as mesmas configurações da pasta.

| Diretório ou arquivo | Grupo ou usuários | Controle total | Modificar | Ler e executar | Ler | Escrever |
|--|-------------------|----------------|-----------|----------------|-----|----------|
| VMware\vCAC\Agents \<agent_name> \logs | SISTEMA | X | X | X | X | X |
| | Administrador | X | X | X | X | X |
| | Administradores | X | X | X | X | X |
| VMware\vCAC\Agents\<agent_name> \temp | SISTEMA | X | X | X | X | X |
| | Administrador | X | X | X | X | X |
| | Administradores | X | X | X | X | X |
| VMware\vCAC\Agents\ | SISTEMA | X | X | X | X | X |
| | Administradores | X | X | X | X | X |
| | Usuários | | | X | X | |
| VMware\vCAC\Distributed Execution Manager\ | SISTEMA | X | X | X | X | X |
| | Administradores | X | X | X | X | X |
| | Usuários | | | X | X | |
| VMware\vCAC\Distributed Execution Manager\DEM\Logs | SISTEMA | X | X | X | X | X |
| | Administrador | X | X | X | X | X |
| | Administradores | X | X | X | X | X |
| VMware\vCAC\Distributed Execution Manager\DEO\Logs | SISTEMA | X | X | X | X | X |
| | Administrador | X | X | X | X | X |
| | Administradores | X | X | X | X | X |
| VMware\vCAC\Management Agent\ | SISTEMA | X | X | X | X | X |
| | Administradores | X | X | X | X | X |
| | Usuários | | | X | X | |
| VMware\vCAC\Server\ | SISTEMA | X | X | X | X | X |
| | Administradores | X | X | X | X | X |
| | Usuários | | | X | X | |
| VMware\vCAC\Web API | SISTEMA | X | X | X | X | X |
| | Administradores | X | X | X | X | X |
| | Usuários | | | X | X | |

Proteger a máquina host de Infraestrutura como Serviço

Como uma prática recomendada de segurança, revise as configurações básicas na sua máquina host de Infraestrutura como Serviço (IaaS) para garantir que ela esteja em conformidade com as diretrizes de segurança.

Proteja várias contas, aplicativos, portas e serviços na máquina host de Infraestrutura como Serviço (IaaS).

Verificar configurações de conta de usuário do servidor

Verifique se existem configurações e contas de usuário local e de domínio desnecessárias. Restrinja qualquer conta de usuário que não esteja relacionada às funções do aplicativo com aquelas necessárias para administração, manutenção e solução de problemas. Restrinja o acesso remoto das contas de usuário do domínio ao mínimo necessário para manter o servidor. Controle rigorosamente e faça auditoria dessas contas.

Excluir aplicativos desnecessários

Exclua todos os aplicativos desnecessários dos servidores host. Aplicativos desnecessários aumentam o risco de exposição por causa de suas vulnerabilidades desconhecidas ou não corrigidas.

Desativar portas e serviços desnecessários

Examine o firewall do servidor host para obter a lista de portas abertas. Bloqueie todas as portas que não são necessárias para o componente IaaS ou para a operação crítica do sistema. Consulte o [Configurar portas e protocolos](#). Faça auditoria dos serviços em execução no seu servidor host e desative os que não são necessários.

Configurando a segurança de rede do host

Para fornecer proteção máxima contra ameaças de segurança conhecidas, configure a interface de rede e as configurações de comunicação em todas as máquinas host do VMware.

Como parte de um plano de segurança abrangente, defina as configurações de segurança da interface de rede para os appliances virtuais da VMware e para os componentes da Infraestrutura como Serviço de acordo com as diretrizes de segurança estabelecidas.

Definindo as configurações de rede para appliances da VMware

Para garantir que as suas máquinas host do appliance virtual da VMware ofereçam suporte a apenas comunicações seguras e essenciais, revise e edite as configurações de comunicação de rede.

Examine a configuração do protocolo de rede IP das suas máquinas host da VMware e defina as configurações de rede de acordo com as diretrizes de segurança. Desative todos os protocolos de comunicação não essenciais.

Prevenir controle do usuário de interfaces de rede

Como melhor prática de segurança, permita que os usuários utilizem somente os privilégios do sistema que precisam para realizar seu trabalho nas máquinas de host do appliance do VMware.

Permitir contas de usuário com privilégios para manipular as interfaces de rede pode resultar em evasão dos mecanismos de segurança da rede ou negação de serviço. Restrinja a capacidade de alterar as configurações de interface da rede a usuários privilegiados.

Procedimentos

- 1 Execute o seguinte comando em cada máquina de host do appliance do VMware.

```
# grep -i '^USERCONTROL=' /etc/sysconfig/network/ifcfg*
```

- 2 Certifique-se de que todas as interfaces estejam definidas para N0.

Definir tamanho da fila de backlog de TCP

Para oferecer certo nível de defesa contra ataques maliciosos, configure um tamanho de fila de backlog de TCP padrão nas máquinas de host do appliance do VMware.

Defina os tamanhos da fila de backlog de TCP conforme um tamanho padrão adequado para oferecer mitigação de ataques de negação de serviço de TCP. A configuração padrão recomendada é 1280.

Procedimentos

- 1 Execute o seguinte comando em cada máquina de host do appliance do VMware.

```
# cat /proc/sys/net/ipv4/tcp_max_syn_backlog
```

- 2 Abra o arquivo `/etc/sysctl.conf` em um editor de texto.

- 3 Defina o tamanho da fila de backlog de TCP padrão adicionando a seguinte entrada ao arquivo.

```
net.ipv4.tcp_max_syn_backlog=1280
```

- 4 Salve suas alterações e feche o arquivo.

Negar ecos ICMPv4 para endereço de difusão

Como uma prática recomendada de segurança, verifique se as suas máquinas host do appliance da VMware ignoram solicitações de eco de endereço de difusão ICMP.

As respostas para ecos de Internet Control Message Protocol (ICMP) de difusão fornecem um vetor de ataque para ataques de amplificação e podem facilitar o mapeamento de rede por agentes maliciosos. Configurar as suas máquinas host do appliance para ignorar os ecos ICMPv4 fornece proteção contra esses ataques.

Procedimentos

- 1 Execute o comando `# cat /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts` nas máquinas host do appliance virtual da VMware para confirmar se elas negam solicitações de eco de endereço de difusão IPv4.

Se as máquinas host estiverem configuradas para negar redirecionamentos IPv4, este comando retornará um valor de 0 para `/proc/sys/net/ipv4/icmp_echo_ignore_broadcasts`.

- 2 Para configurar uma máquina host do appliance virtual para negar solicitações de eco de endereços de difusão ICMPv4, abra o arquivo `/etc/sysctl.conf` nas máquinas host Windows em um editor de texto.

- 3 Localize a entrada que lê `net.ipv4.icmp_echo_ignore_broadcasts=0` . Se o valor para esta entrada não estiver definido como zero ou se a entrada não existir, adicione-a ou atualize a entrada existente em conformidade.
- 4 Salve as alterações e feche o arquivo.

Desativar IPv4 Proxy ARP

Verifique se o IPv4 Proxy ARP está desativado caso não seja necessário nas máquinas de host do appliance do VMware para impedir o compartilhamento não autorizado de informações.

O IPv4 Proxy ARP permite que um sistema envie respostas para solicitações de ARP em uma interface em nome de hosts conectados a outra interface. Desative se ele não for necessário para impedir o vazamento de informações de endereçamento entre os segmentos de rede anexos.

Procedimentos

- 1 Execute o comando `# grep [01] /proc/sys/net/ipv4/conf/*/proxy_arp | egrep "default|all"` nas máquinas de host do appliance virtual do VMware para verificar se o IPv4 Proxy ARP está desativado.

Se o IPv4 Proxy ARP estiver desativado nas máquinas de host, esse comando retornará o valor 0.

```
/proc/sys/net/ipv4/conf/all/proxy_arp:0  
/proc/sys/net/ipv4/conf/default/proxy_arp:0
```

Se as máquinas de host estiverem configuradas corretamente, nenhuma ação adicional será necessária.

- 2 Caso você precise configurar o IPv4 Proxy ARP nas máquinas de host, abra o arquivo `/etc/sysctl.conf` em um editor de texto.
- 3 Verifique as seguintes entradas.

```
net.ipv4.conf.default.proxy_arp=0  
net.ipv4.conf.all.proxy_arp=0
```

Se as entradas não existirem ou se os seus valores não estiverem definidos como zero, adicione as entradas ou atualize as entradas existentes em conformidade.

- 4 Salve todas as alterações feitas e feche o arquivo.

Negar mensagens de redirecionamento IPv4 ICMP

Como prática recomendada de segurança, verifique se as suas máquinas de host do appliance virtual da VMware negam mensagens de redirecionamento IPv4 ICMP.

Os roteadores usam mensagens de redirecionamento ICMP para informar aos hosts que existe uma rota mais direta para um destino. Uma mensagem de redirecionamento ICMP maliciosa pode facilitar um ataque a intermediários. Essas mensagens modificam a tabela de rotas do host e não são autenticadas. Certifique-se de que o sistema esteja configurado para ignorá-las se não forem necessárias.

Procedimentos

- 1 Execute o comando `# grep [01] /proc/sys/net/ipv4/conf/*/accept_redirects | egrep "default|all"` nas máquinas host do appliance da VMware para confirmar se elas negam as mensagens de redirecionamento IPv4.

Se as máquinas host estiverem configuradas para negar redirecionamentos IPv4, este comando retornará o seguinte:

```
/proc/sys/net/ipv4/conf/all/accept_reidrects:0
/proc/sys/net/ipv4/conf/default/accept_redirects:0
```

- 2 Se você precisa configurar uma máquina host do appliance virtual para negar as mensagens de redirecionamento ICMPv4, abra o arquivo `/etc/sysctl.conf` em um editor de texto.
- 3 Verifique os valores das linhas que começam com `net.ipv4.conf`.

Se os valores para as entradas a seguir não forem definidos como zero ou se as entradas não existirem, adicione-as ao arquivo ou atualize as entradas existentes corretamente.

```
net.ipv4.conf.all.accept_redirects=0
net.ipv4.conf.default.accept_redirects=0
```

- 4 Salve as alterações feitas e feche o arquivo.

Negar mensagens de ICMP Redirect para IPv6

Como melhor prática de segurança, verifique se as máquinas de host do appliance virtual do VMware negam as mensagens de ICMP Redirect para IPv6.

Os roteadores usam mensagens de redirecionamento ICMP para informar aos hosts que existe uma rota mais direta para um destino. Uma mensagem de redirecionamento ICMP maliciosa pode facilitar um ataque a intermediários. Essas mensagens modificam a tabela de rotas do host e não são autenticadas. Certifique-se de que seu sistema esteja configurado para ignorá-las caso não sejam necessárias.

Procedimentos

- 1 Execute o comando `# grep [01] /proc/sys/net/ipv6/conf/*/accept_redirects | egrep "default|all"` nas máquinas de host do appliance virtual do VMware para confirmar se eles negam mensagens Redirect para IPv6.

Se as máquinas de host estiverem configuradas para negar Redirect de IPv6, esse comando retornará o seguinte:

```
/proc/sys/net/ipv6/conf/all/accept_redirects:0
/proc/sys/net/ipv6/conf/default/accept_redirects:0
```

- 2 Para configurar uma máquina de host do appliance virtual para negar mensagens Redirect para IPv4, abra o arquivo `/etc/sysctl.conf` em um editor de texto.

- 3 Verifique os valores das linhas que começam com `net.ipv6.conf`.

Se os valores das seguintes entradas não estiverem definidos como zero, ou se as entradas não existirem, adicione-as ao arquivo ou atualize as entradas existentes conforme necessário.

```
net.ipv6.conf.all.accept_redirects=0
net.ipv6.conf.default.accept_redirects=0
```

- 4 Salve as alterações e feche o arquivo.

Log dos pacotes Martian de IPv4

Como melhor prática de segurança, verifique se as máquinas de host do appliance virtual do VMware fazem o log dos pacotes Martian de IPv4.

Os pacotes Martian contêm endereços que o sistema reconhece como inválidos. Configure as máquinas de host para fazer o log dessas mensagens de modo que você possa identificar falhas de configuração ou ataques em andamento.

Procedimentos

- 1 Execute o comando `# grep [01] /proc/sys/net/ipv4/conf/*/log_martians|grep "default|all"` nas máquinas de host do appliance do VMware para verificar se eles fazem o log de pacotes Martian de IPv4.

Se as máquinas virtuais estiverem configuradas para fazer o log de pacotes Martian, elas retornarão o seguinte:

```
/proc/sys/net/ipv4/conf/all/log_martians:1
/proc/sys/net/ipv4/default/log_martians:1
```

Se as máquinas host estiverem configuradas corretamente, nenhuma ação adicional será necessária.

- 2 Caso precise configurar um appliance virtual para fazer o log de pacotes Martian de IPv4, abra o arquivo `/etc/sysctl.conf` em um editor de texto.
- 3 Confira os valores das linhas iniciadas por `net.ipv4.conf`.

Se o valor das seguintes entradas não estiverem definidos como 1, ou se as entradas não existirem, adicione-as ao arquivo ou atualize as entradas existentes conforme necessário.

```
net.ipv4.conf.all.log_martians=1
net.ipv4.conf.default.log_martians=1
```

- 4 Salve suas alterações e feche o arquivo.

Usar filtragem por caminho inverso IPv4

Como prática recomendada de segurança, verifique se as suas máquinas host do appliance virtual da VMware usam filtragem por caminho inverso IPv4.

A filtragem por caminho inverso protege contra endereços de origem falsos, fazendo com que o sistema descarte pacotes com endereços de origem que não têm rota ou com uma rota que não aponta para a interface de origem. Configure suas máquinas host para usar filtragem por caminho inverso sempre que possível. Em alguns casos, dependendo da função do sistema, a filtragem por caminho inverso pode fazer com que o sistema descarte o tráfego legítimo. Se você encontrar esses problemas, poderá precisar usar um modo mais permissivo ou desativar a filtragem por caminho inverso.

Procedimentos

- 1 Execute o comando `# grep [01] /proc/sys/net/ipv4/conf/*/rp_filter | egrep "default|all"` nas máquinas host do appliance virtual da VMware para verificar se elas usam filtragem por caminho inverso IPv4.

Se as máquinas virtuais usarem filtragem por caminho inverso IPv4, este comando retornará o seguinte:

```
/proc/sys/net/ipv4/conf/all/rp_filter:1
/proc/sys/net/ipv4/conf/default/re_filter:1
```

Se suas máquinas virtuais estiverem configuradas corretamente, nenhuma ação adicional será necessária.

- 2 Se você precisar configurar a filtragem por caminho inverso IPv4 nas máquinas host, abra o arquivo `/etc/sysctl.conf` em um editor de texto.
- 3 Verifique os valores das linhas que começam com `net.ipv4.conf`.

Se os valores para as entradas a seguir não forem definidos como 1 ou se eles não existirem, adicione-os ao arquivo ou atualize as entradas existentes em conformidade.

```
net.ipv4.conf.all.rp_filter=1
net.ipv4.conf.default.rp_filter=1
```

- 4 Salve as alterações e feche o arquivo.

Negar o encaminhamento IPv4

Verifique se as suas máquinas host do appliance da VMware negam o encaminhamento IPv4.

Se o sistema estiver configurado para encaminhamento IP e não for um roteador designado, os invasores poderão usá-lo para ignorar a segurança da rede, fornecendo um caminho para comunicação não filtrada por dispositivos de rede. Configure suas máquinas host do appliance virtual para negar o encaminhamento IPv4 para evitar esse risco.

Procedimentos

- 1 Execute o comando `# cat /proc/sys/net/ipv4/ip_forward` nas máquinas host do appliance da VMware para confirmar se elas negam o encaminhamento IPv4.

Se as máquinas host estiverem configuradas para negar o encaminhamento IPv4, esse comando retornará um valor de 0 para `/proc/sys/net/ipv4/ip_forward`. Se as máquinas virtuais estiverem configuradas corretamente, nenhuma ação adicional será necessária.

- 2 Para configurar uma máquina host do appliance virtual para negar o encaminhamento ICMPv4, abra o arquivo `/etc/sysctl.conf` em um editor de texto.
- 3 Localize a entrada que lê `net.ipv4.ip_forward=0`. Se o valor para esta entrada não estiver definido no momento como zero ou se a entrada não existir, adicione-a ou atualize a entrada existente em conformidade.
- 4 Salve todas as alterações e feche o arquivo.

Negar o encaminhamento IPv6

Como uma prática recomendada de segurança, verifique se os seus sistemas host do appliance da VMware negam o encaminhamento IPv6.

Se o sistema estiver configurado para encaminhamento IP e não for um roteador designado, os invasores poderão usá-lo para ignorar a segurança da rede, fornecendo um caminho para comunicação não filtrada por dispositivos de rede. Configure suas máquinas host do appliance virtual para negar o encaminhamento IPv6 para evitar esse risco.

Procedimentos

- 1 Execute o comando `# grep [01] /proc/sys/net/ipv6/conf/*/forwarding|egrep "default|all"` nas máquinas host do appliance da VMware para verificar se elas negam o encaminhamento IPv6.

Se as máquinas host estiverem configuradas para negar o encaminhamento IPv6, esse comando retornará o seguinte:

```
/proc/sys/net/ipv6/conf/all/forwarding:0
/proc/sys/net/ipv6/conf/default/forwarding:0
```

Se as máquinas host estiverem configuradas corretamente, nenhuma ação adicional será necessária.

- 2 Se você precisar configurar uma máquina host para negar o encaminhamento IPv6, abra o arquivo `/etc/sysctl.conf` em um editor de texto.
- 3 Verifique os valores das linhas que começam com `net.ipv6.conf`.

Se os valores para as entradas a seguir não estiverem definidos como zero ou se as entradas não existirem, adicione-as ou atualize as entradas existentes corretamente.

```
net.ipv6.conf.all.accept_redirects=0
net.ipv6.conf.default.accept_redirects=0
```

- 4 Salve todas as alterações feitas e feche o arquivo.

Usar Syncookies IPv4 TCP

Verifique se suas máquinas de host do appliance do VMware usam Syncookies IPv4 TCP.

Um ataque de TCP SYN Flood pode causar uma negação de serviço ao preencher a tabela de conexão TCP do sistema com conexões no estado SYN_RCVD. Os Syncookies impedem o rastreamento de uma conexão até o recebimento de um ACK subsequente, verificando que o iniciador está tentando uma conexão válida e não é uma fonte de flood. Esta técnica não opera de forma totalmente em conformidade com os padrões, mas só é ativada durante uma condição de flood, e possibilita a defesa do sistema sem interromper o atendimento a solicitações válidas.

Procedimentos

- 1 Execute o comando `# cat /proc/sys/net/ipv4/tcp_syncookies` nas máquinas de host do appliance do VMware para verificar se eles usam Syncookies IPv4 TCP.

Se as máquinas de host estiverem configuradas para negar encaminhamento IPv4, esse comando retornará o valor 1 para `/proc/sys/net/ipv4/tcp_syncookies`. Se as máquinas virtuais estiverem configuradas corretamente, nenhuma ação adicional será necessária.

- 2 Caso precise configurar um appliance virtual para utilizar os Syncookies IPv4 TCP, abra o arquivo `/etc/sysctl.conf` em um editor de texto.

- 3 Localize a entrada que lê `net.ipv4.tcp_syncookies=1`.

Se o valor desta entrada não estiver definido como 1 ou se a entrada não existir, adicione a entrada ou atualize a entrada existente conforme necessário.

- 4 Salve todas alterações feitas e feche o arquivo.

Negar anúncios do roteador IPv6

Verifique se as máquinas host da VMware negam a aceitação de anúncios do roteador e redirecionamentos ICMP, a menos que sejam necessários para a operação do sistema.

O IPv6 permite que os sistemas configurem seus dispositivos de rede automaticamente usando informações da rede. Do ponto de vista de segurança, a configuração manual de informações de configuração importantes é preferível para aceitá-la da rede de maneira não autenticada.

Procedimentos

- 1 Execute o comando `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra | egrep "default|all"` nas máquinas host do appliance da VMware para verificar se elas negam os anúncios do roteador.

Se as máquinas host estiverem configuradas para negar os anúncios do roteador IPv6, esse comando retornará valores de 0:

```
/proc/sys/net/ipv6/conf/all/accept_ra:0
/proc/sys/net/ipv6/conf/default/accept_ra:0
```

Se as máquinas host estiverem configuradas corretamente, nenhuma ação adicional será necessária.

- 2 Se você precisar configurar uma máquina host para negar anúncios do roteador IPv6, abra o arquivo `/etc/sysctl.conf` em um editor de texto.

3 Verifique as seguintes entradas.

```
net.ipv6.conf.all.accept_ra=0
net.ipv6.conf.default.accept_ra=0
```

Se essas entradas não existirem ou se os seus valores não estiverem definidos como zero, adicione as entradas ou atualize as entradas existentes em conformidade.

4 Salve todas alterações feitas e feche o arquivo.

Negar solicitações de roteador IPv6

Como uma prática recomendada de segurança, verifique se as suas máquinas host do appliance da VMware negam solicitações de roteador IPv6, a menos que sejam necessárias para operação do sistema.

A configuração de solicitações de roteador determina quantas solicitações de roteador são enviadas ao criar a interface. Se os endereços forem atribuídos estaticamente, não haverá necessidade de enviar solicitações.

Procedimentos

- 1 Execute o comando `# grep [01] /proc/sys/net/ipv6/conf/*/router_solicitations | egrep "default|all"` nas máquinas host do appliance da VMware para verificar se elas negam as solicitações do roteador IPv6.

Se as máquinas host estiverem configuradas para negar anúncios do roteador IPv6, esse comando retornará o seguinte:

```
/proc/sys/net/ipv6/conf/all/router_solicitations:0
/proc/sys/net/ipv6/conf/default/router_solicitations:0
```

Se as máquinas host estiverem configuradas corretamente, nenhuma ação adicional será necessária.

- 2 Se você precisar configurar máquinas host para negar solicitações de roteador IPv6, abra o arquivo `/etc/sysctl.conf` em um editor de texto.
- 3 Verifique as seguintes entradas.

```
net.ipv6.conf.all.router_solicitations=0
net.ipv6.conf.default.router_solicitations=0
```

Se as entradas não existirem ou se os seus valores não estiverem definidos como zero, adicione as entradas ou atualize as entradas existentes em conformidade.

- 4 Salve todas as alterações e feche o arquivo.

Negar a preferência de roteador IPv6 em solicitações de roteador

Verifique se as suas máquinas host do appliance da VMware negam solicitações de roteador IPv6, a menos que sejam necessárias para operação do sistema.

A preferência de roteador na configuração de solicitações determina as preferências de roteador. Se os endereços forem atribuídos estaticamente, não haverá necessidade de receber qualquer preferência de roteador para solicitações.

Procedimentos

- 1 Execute o comando `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_rtr_pref | egrep "default|all"` nas máquinas host do appliance da VMware para verificar se elas negam as solicitações do roteador IPv6.

Se as máquinas host estiverem configuradas para negar anúncios do roteador IPv6, esse comando retornará o seguinte:

```
/proc/sys/net/ipv6/conf/all/accept_ra_rtr_pref:0
/proc/sys/net/ipv6/conf/default/accept_ra_rtr_pref:0
```

Se as máquinas host estiverem configuradas corretamente, nenhuma ação adicional será necessária.

- 2 Se você precisar configurar máquinas host para negar solicitações de roteador IPv6, abra o arquivo `/etc/sysctl.conf` em um editor de texto.
- 3 Verifique as seguintes entradas.

```
net.ipv6.conf.all.accept_ra_rtr_pref=0
net.ipv6.conf.default.accept_ra_rtr_pref=0
```

Se as entradas não existirem ou se os seus valores não estiverem definidos como zero, adicione as entradas ou atualize as entradas existentes em conformidade.

- 4 Salve todas alterações feitas e feche o arquivo.

Negar o prefixo do roteador IPv6

Verifique se as suas máquinas host do appliance da VMware negam informações de prefixo do roteador IPv6, a menos que sejam necessárias para operação do sistema.

A configuração `accept_ra_pinfo` controla se o sistema aceita informações de prefixo do roteador. Se os endereços forem atribuídos estaticamente, não haverá necessidade de receber qualquer informação de prefixo do roteador.

Procedimentos

- 1 Execute o comando `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_pinfo | egrep "default|all"` nas máquinas host do appliance da VMware para verificar se elas negam as informações de prefixo do roteador IPv6.

Se as máquinas host estiverem configuradas para negar anúncios do roteador IPv6, esse comando retornará o seguinte.

```
/proc/sys/net/ipv6/conf/all/accept_ra_pinfo:0
/proc/sys/net/ipv6/conf/default/accept_ra_pinfo:0
```

Se as máquinas host estiverem configuradas corretamente, nenhuma ação adicional será necessária.

- 2 Se você precisar configurar máquinas host para negar informações de prefixo do roteador IPv6, abra o arquivo `/etc/sysctl.conf` em um editor de texto.
- 3 Verifique as seguintes entradas.

```
net.ipv6.conf.all.accept_ra_pinfo=0
net.ipv6.conf.default.accept_ra_pinfo=0
```

Se as entradas não existirem ou se os seus valores não estiverem definidos como zero, adicione as entradas ou atualize as entradas existentes em conformidade.

- 4 Salve todas as alterações e feche o arquivo.

Negar configurações de limite de saltos do anúncio do roteador IPv6

Verifique se as suas máquinas host do appliance da VMware negam configurações de limite de saltos do roteador IPv6, a menos que sejam necessárias.

A configuração `accept_ra_defrtr` controla se o sistema aceitará as configurações de Limite de salto de um anúncio do roteador. Configurar-la como zero evita que um roteador altere seu limite de saltos IPv6 padrão para pacotes de saída.

Procedimentos

- 1 Execute o comando `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_defrtr | egrep "default|all"` nas máquinas host do appliance da VMware para verificar se elas negam as configurações de limite de saltos do roteador IPv6.

Se as máquinas host estiverem configuradas para negar as configurações de limite de saltos do roteador IPv6, este comando retornará valores de 0.

```
/proc/sys/net/ipv6/conf/all/accept_ra_defrtr:0
/proc/sys/net/ipv6/conf/default/accept_ra_defrtr:0
```

Se as máquinas host estiverem configuradas corretamente, nenhuma ação adicional será necessária.

- 2 Se você precisar configurar uma máquina host para negar configurações de limite de saltos do roteador IPv6, abra o arquivo `/etc/sysctl.conf` em um editor de texto.
- 3 Verifique as seguintes entradas.

```
net.ipv6.conf.all.autoconf=0
net.ipv6.conf.default.autoconf=0
```

Se as entradas não existirem ou se os seus valores não estiverem definidos como zero, adicione as entradas ou atualize as entradas existentes em conformidade.

- 4 Salve todas as alterações feitas e feche o arquivo.

Negar configurações do autoconf de anúncio do roteador IPv6

Verifique se as suas máquinas host do appliance da VMware negam configurações do autoconf do roteador IPv6, a menos que sejam necessárias.

A configuração autoconf controla se os anúncios do roteador podem fazer com que o sistema atribua um endereço de unicast global a uma interface.

Procedimentos

- 1 Execute o comando `# grep [01] /proc/sys/net/ipv6/conf/*/autoconf | egrep "default|all"` nas máquinas host do appliance da VMware para verificar se elas negam as configurações do autoconf do roteador IPv6.

Se as máquinas host estiverem configuradas para negar as configurações de autoconf do roteador IPv6, esse comando retornará valores de 0.

```
/proc/sys/net/ipv6/conf/all/autoconf:0  
/proc/sys/net/ipv6/conf/default/autoconf:0
```

Se as máquinas host estiverem configuradas corretamente, nenhuma ação adicional será necessária.

- 2 Se você precisar configurar máquinas host para negar configurações do autoconf do roteador IPv6, abra o arquivo `/etc/sysctl.conf` em um editor de texto.
- 3 Verifique as seguintes entradas.

```
net.ipv6.conf.all.autoconf=0  
net.ipv6.conf.default.autoconf=0
```

Se as entradas não existirem ou se os seus valores não estiverem definidos como zero, adicione as entradas ou atualize as entradas existentes em conformidade.

- 4 Salve todas alterações feitas e feche o arquivo.

Negar solicitações de vizinhança IPv6

Verifique se as suas máquinas host do appliance da VMware negam solicitações de vizinhança IPv6, a menos que sejam necessárias.

A configuração `dad_transmits` determina quantas solicitações de vizinhança são enviadas por endereço (global e link-local) ao criar uma interface para garantir que o endereço desejado seja exclusivo na rede.

Procedimentos

- 1 Execute o comando `# grep [01] /proc/sys/net/ipv6/conf/*/dad_transmits | egrep "default|all"` nas máquinas host do appliance da VMware para confirmar se elas negam as solicitações de vizinhança IPv6.

Se as máquinas host estiverem configuradas para negar as solicitações de vizinhança IPv6, esse comando retornará valores de 0.

```
/proc/sys/net/ipv6/conf/all/dad_transmits:0
/proc/sys/net/ipv6/conf/default/dad_transmits:0
```

Se as máquinas host estiverem configuradas corretamente, nenhuma ação adicional será necessária.

- 2 Se você precisar configurar máquinas host para negar solicitações de vizinhança IPv6, abra o arquivo `/etc/sysctl.conf` em um editor de texto.
- 3 Verifique as seguintes entradas.

```
net.ipv6.conf.all.dad_transmits=0
net.ipv6.conf.default.dad_transmits=0
```

Se as entradas não existirem ou se os seus valores não estiverem definidos como zero, adicione as entradas ou atualize as entradas existentes em conformidade.

- 4 Salve todas alterações feitas e feche o arquivo.

Restringir número máximo de endereços IPv6

Verifique se as máquinas de host do appliance do VMware restringem o número máximo de endereços IPv6 conforme o mínimo necessário para a operação do sistema.

A configuração de número máximo de endereços determina quantos endereços IPv6 unicast globais estão disponíveis para cada interface. O padrão é 16, mas você deve definir o número exato de endereços globais estaticamente configurados exigidos pelo seu sistema.

Procedimentos

- 1 Execute o comando `# grep [1] /proc/sys/net/ipv6/conf/*/max_addresses | egrep "default|all"` nas máquinas de host do appliance do VMware para verificar se eles restringem o número máximo de endereços IPv6 corretamente.

Se as máquinas de host estiverem configuradas para restringir o número máximo de endereços IPv6, esse comando retornará o valor 1.

```
/proc/sys/net/ipv6/conf/all/max_addresses:1
/proc/sys/net/ipv6/conf/default/max_addresses:1
```

Se as máquinas host estiverem configuradas corretamente, nenhuma ação adicional será necessária.

- 2 Caso você precise configurar o número máximo de endereços IPv6 nas máquinas de host, abra o arquivo `/etc/sysctl.conf` em um editor de texto.
- 3 Verifique as seguintes entradas.

```
net.ipv6.conf.all.max_addresses=1
net.ipv6.conf.default.max_addresses=1
```

Se as entradas não existirem ou se os seus valores não estiverem definidos como 1, adicione as entradas ou atualize as entradas existentes conforme necessário.

- 4 Salve todas alterações feitas e feche o arquivo.

Definindo as configurações de rede para o host da Infraestrutura como Serviço

Como prática recomendada de segurança, defina as configurações de comunicação de rede na sua máquina host do componente de Infraestrutura como Serviço (IaaS) da VMware de acordo com os requisitos e diretrizes da VMware.

Defina a configuração de rede da máquina host de Infraestrutura como um Serviço (IaaS) para oferecer suporte a funções completas do vRealize Automation com a segurança apropriada.

Consulte [Proteger o componente de Infraestrutura como Serviço](#).

Configurar portas e protocolos

Como melhor prática de segurança, configure portas e protocolos para todos os appliances e componentes do vRealize Automation de acordo com as diretrizes da VMware.

Configure as portas de entrada e saída para os componentes do vRealize Automation conforme exigido para os componentes críticos do sistema operarem em produção. Desative todas as portas e protocolos desnecessários. Consulte [Arquitetura de Referência do vRealize Automation](#).

Portas de usuário necessárias

Como melhor prática de segurança, configure as portas de usuário do vRealize Automation conforme as diretrizes da VMware.

Exponha as portas necessárias apenas por meio de uma rede segura.

| SERVIDOR | PORTAS |
|----------------------------------|-----------|
| Appliance do vRealize Automation | 443, 8443 |

Portas necessárias do administrador

Como uma prática recomendada de segurança, configure as portas do administrador do vRealize Automation de acordo com as diretrizes da VMware.

Exponha as portas necessárias apenas por meio de uma rede segura.

| SERVIDOR | PORTAS |
|---|--------|
| Servidor do vRealize Application Services | 5480 |

Portas do appliance do vRealize Automation

Como melhor prática de segurança, configure as portas de entrada e saída para o Appliance do vRealize Automation de acordo com as diretrizes da VMware.

Portas de entrada

Configure o número mínimo de portas de entrada necessárias para o Appliance do vRealize Automation. Configure portas opcionais se necessário para a configuração do seu sistema.

Tabela 1-4. Número mínimo de portas de entrada necessárias

| PORTA | PROTOCOLO | COMENTÁRIOS |
|------------|-----------|---|
| 443 | TCP | Acesso ao console do vRealize Automation e às chamadas de API. |
| 8443 | TCP | Proxy do console (VMRC). |
| 5480 | TCP | Acesso ao console de gerenciamento Web do appliance virtual |
| 5488, 5489 | TCP | Interna. Usado pelo Appliance do vRealize Automation para atualizações. |
| 5672 | TCP | Mensagens do RabbitMQ. Observação Ao clusterizar instâncias do Appliance do vRealize Automation, pode ser necessário configurar as portas abertas 4369 e 25672. |
| 40002 | TCP | Necessária para o serviço vIDM. Isto é colocado no firewall para todo tráfego externo, exceto o tráfego de outros nós do Appliance do vRealize Automation quando adicionados em configuração de HA. |

Se necessário, configure as portas de entrada opcionais.

Tabela 1-5. Portas de entrada opcionais

| PORTA | PROTOCOLO | COMENTÁRIOS |
|-------|-----------|---|
| 22 | TCP | SSH (opcional) Em um ambiente de produção, desative a escuta do serviço de SSH na porta 22, e feche a porta 22. |
| 80 | TCP | Redireciona para 443 (opcional). |

Portas de saída

Configure as portas de saída necessárias.

Tabela 1-6. Número mínimo de portas de saída necessárias

| PORTA | PROTOCOLO | COMENTÁRIOS |
|--------|-----------|---|
| 25,587 | TCP, UDP | SMTP para o envio de e-mails de notificação de saída. |
| 53 | TCP, UDP | DNS. |

Tabela 1-6. Número mínimo de portas de saída necessárias (Continuação)

| PORTA | PROTOCOLO | COMENTÁRIOS |
|------------------|-----------|---|
| 67, 68, 546, 547 | TCP, UDP | DHCP. |
| 110, 995 | TCP, UDP | POP para receber e-mails de notificação de entrada. |
| 143, 993 | TCP, UDP | IMAP para receber e-mails de notificação de entrada. |
| 443 | TCP | Manager Service de Infraestrutura como Serviço sobre HTTPS. |

Se necessário, configure as portas de saída opcionais.

Tabela 1-7. Portas de saída opcionais

| PORTA | PROTOCOLO | COMENTÁRIOS |
|-------|-----------|---|
| 80 | TCP | Para obter as atualizações de software (opcional). Você pode baixar e aplicar atualizações separadamente. |
| 123 | TCP, UDP | Para conexão direta com o NTP em vez de usar o tempo do host (Opcional). |

Portas de Infraestrutura como Serviço

Como melhor prática de segurança, configure as portas de entrada e saída para os componentes de Infraestrutura como Serviço (IaaS) em conformidade com as diretrizes da VMware.

Portas de entrada

Configure o número mínimo de portas de entrada necessárias para os componentes de IaaS.

Tabela 1-8. Número mínimo de portas de entrada necessárias

| COMPONENTE | PORTA | PROTOCOLO | COMENTÁRIOS |
|-----------------|-------|-----------|--|
| Manager Service | 443 | TCP | Comunicação com os componentes de IaaS e do appliance do vRealize Automation sobre HTTPS. Todos os hosts de virtualização gerenciados por agentes de proxy também devem ter a porta TCP 443 aberta para o tráfego de entrada |

Portas de saída

Configure o número mínimo de portas de saída necessárias para os componentes de IaaS.

Tabela 1-9. Número mínimo de portas de saída necessárias

| COMPONENTE | PORTA | PROTOCOL O | COMENTÁRIOS |
|--------------------------------|-------|------------|---|
| Tudo | 53 | TCP, UDP | DNS. |
| Tudo | | TCP, UDP | DHCP. |
| Manager Service | 443 | TCP | Comunicação com o appliance do vRealize Automation sobre HTTPS. |
| Site | 443 | TCP | Comunicação com o Manager Service sobre HTTPS. |
| Distributed Execution Managers | 443 | TCP | Comunicação com o Manager Service sobre HTTPS. |

Tabela 1-9. Número mínimo de portas de saída necessárias (Continuação)

| COMPONENTE | PORTA | PROTOCOL O | COMENTÁRIOS |
|-----------------------|-------|------------|--|
| Agentes de proxy | 443 | TCP | Comunicação com o Manager Service e os hosts de virtualização sobre HTTPS. |
| Agente guest | 443 | TCP | Comunicação com o Manager Service sobre HTTPS. |
| Manager Service, Site | 1433 | TCP | MSSQL. |

Se necessário, configure as portas de saída opcionais.

Tabela 1-10. Portas de saída opcionais

| COMPONENTE | PORTA | PROTOCOLO | COMENTÁRIOS |
|------------|-------|-----------|-------------------|
| Tudo | 123 | TCP, UDP | O NTP é opcional. |

Auditoria e registro

Como uma prática recomendada de segurança, configure a auditoria e o registro no seu sistema do vRealize Automation de acordo com as recomendações da VMware.

O registro remoto em um host de registro central fornece um armazenamento seguro para arquivos de registro. Ao reunir arquivos de registro em um host central, você pode monitorar o ambiente com uma única ferramenta. Além disso, você pode executar a análise agregada e procurar provas de ameaças, como ataques coordenados em várias entidades dentro da infraestrutura. Fazer o registro em um servidor de registro seguro e centralizado pode ajudar a evitar a violação do registro e também fornece um registro de auditoria de longo prazo.

Garantir que o servidor de registro remoto é seguro

Muitas vezes, depois que os invasores violam a segurança da sua máquina host, eles tentam procurar e manipular arquivos de registro para apagar seus rastros e manter controle sem serem descobertos. Proteger adequadamente o servidor de registro remoto ajuda a desencorajar a adulteração do registro.

Usar um servidor NTP autorizado

Certifique-se de que todas as máquinas host usem a mesma fonte de tempo relativa, incluindo o deslocamento de localização relevante, e de que você possa correlacionar a fonte de tempo relativa com um padrão de tempo acordado, como o Tempo Universal Coordenado (UTC). Uma abordagem disciplinada das fontes de tempo permite que você rastreie e correlacione rapidamente as ações de um intruso ao revisar os arquivos de registro relevantes. Configurações de hora incorretas podem dificultar a inspeção e a correlação de arquivos de registro para detectar ataques e podem tornar a auditoria imprecisa.

Use pelo menos três servidores NTP de fontes de tempo externas ou configure alguns servidores NTP locais em uma rede confiável que, por sua vez, obtenha seu tempo de pelo menos três fontes de tempo externas.

Instalando o vRealize Automation

Siga as instruções fornecidas para instalar uma nova instância do vRealize Automation.

Visão geral de instalação do vRealize Automation

Você pode instalar o vRealize Automation para suportar ambientes mínimos de prova do conceito, ou em diferentes tamanhos de configurações empresariais distribuídas, capazes de lidar com cargas de trabalho de produção. A instalação pode ser interativa ou silenciosa.

Após a instalação, você começa usando o vRealize Automation ao personalizar os tenants de instalação e configuração, o que fornece aos usuários acesso para provisionamento de autoatendimento e gerenciamento do ciclo de vida dos serviços de nuvem.

Sobre a instalação do vRealize Automation

Você pode instalar o vRealize Automation de diferentes formas, com diferentes níveis de interatividade.

Para instalar, você implementa um appliance do vRealize Automation e depois executa a instalação em si usando uma das opções a seguir:

- Um Assistente de Instalação consolidado, baseado em navegador
- Configuração de appliance baseado em navegador separada, e instalações separadas do Windows para componentes do servidor do IaaS
- Um instalador silencioso baseado em linha de comando que aceita entrada de um arquivo de propriedades de resposta
- Um API REST de instalação que aceita entrada formatada para JSON

Você também pode instalar o vRealize Automation usando o vRealize Suite Lifecycle Manager. Consulte a [documentação do vRealize Suite](#).

Novidade nesta instalação do vRealize Automation

Se você instalou versões anteriores do vRealize Automation, esteja ciente das alterações na instalação desta versão antes de começar.

- Esta versão simplifica o appliance do vRealize Automation renomeando o processo. Consulte [Alterar o nome de host do appliance do vRealize Automation](#).
- Nesta versão, o appliance do vRealize Automation usa o TLS 1.2 por padrão. A interface de administração inclui uma opção para ativar temporariamente o TLS 1.0 e 1.1, o que é necessário para atualizar os agentes existentes para essa versão.
- A interface de administração do appliance do vRealize Automation agora inclui uma página para a instalação e o gerenciamento de patches. Consulte [Gerenciamento de patches de acesso](#).
- Esta versão descreve como alterar a porta do proxy padrão para o VMware Remote Console. Consulte [Alterar a porta de proxy do VMware Remote Console](#).

- Esta versão corrige alguns links de ajuda desfeitos no assistente de instalação.

Componentes de instalação do vRealize Automation

Uma instalação típica do vRealize Automation consiste em um appliance do vRealize Automation e em um ou mais servidores Windows que, juntos, fornecem o vRealize Automation Infrastructure as a Service (IaaS).

O appliance do vRealize Automation

O appliance do vRealize Automation é um appliance virtual Linux pré-configurado. O appliance do vRealize Automation é entregue como um arquivo de virtualização aberto que você implementa em uma infraestrutura virtualizada existente, como o vSphere.

O appliance do vRealize Automation realiza diversas funções importantes do vRealize Automation.

- O appliance contém o servidor que hospeda o portal do produto vRealize Automation, onde os usuários fazem login para acessar o provisionamento de autoatendimento e gerenciamento dos serviços de nuvem.
- O appliance gerencia o single sign-on (SSO) para autorização e autenticação do usuário.
- O appliance hospeda uma interface de gerenciamento para as configurações do appliance do vRealize Automation.
- O appliance inclui um banco de dados PostgreSQL pré-configurado usado para operações internas do appliance do vRealize Automation.

Em implementações grandes com appliances redundantes, os bancos de dados de appliances secundários servem como réplicas para oferecer alta disponibilidade.

- O appliance inclui uma instância pré-configurada do vRealize Orchestrator. O vRealize Automation usa fluxos de trabalho e ações do vRealize Orchestrator para estender suas capacidades.

A instância incorporada do vRealize Orchestrator agora é recomendada. Em implementações mais antigas ou em casos especiais, os usuários podem conectar o vRealize Automation a um vRealize Orchestrator externo em vez disso.

- O appliance contém o instalador baixável do Agente de Gerenciamento. Todos os servidores Windows que compõem seu vRealize Automation IaaS devem ter o Agente de Gerenciamento instalado.

O Agente de gerenciamento registra os servidores Windows do IaaS no appliance do vRealize Automation, automatiza a instalação e o gerenciamento de componentes do IaaS e coleta informações de telemetria e suporte.

Infraestrutura como Serviço

vRealize Automation IaaS consiste de um ou mais servidores Windows que trabalham juntos para modelar e provisionar sistemas em infraestruturas híbridas privadas, públicas ou de nuvem.

Você instala componentes de vRealize Automation IaaS em um ou mais servidores Windows virtuais ou físicos. Após a instalação, as operações do IaaS aparecem sob a guia Infraestrutura na interface do produto.

IaaS consiste dos componentes a seguir, que podem ser instalados juntos ou separadamente, dependendo do tamanho da implementação.

Servidor Web

O servidor Web IaaS oferece administração de infraestrutura e autoração de serviço à interface do produto vRealize Automation. O componente do servidor Web comunica-se com o Serviço de Gerenciamento, que fornece atualizações do Distributed Execution Manager (DEM), banco de dados SQL Server e agentes.

Model Manager

vRealize Automation usa modelos para facilitar a integração com sistemas e bancos de dados externos. Os modelos implementam a lógica de negócios usada pelo DEM.

O Model Manager fornece serviços e utilitários para persistência, controle de versões, proteção e distribuição de elementos de modelo. O Model Manager está hospedado em um dos servidores Web IaaS e se comunica com os DEMs, com o banco de dados SQL Server e com o site da interface do produto.

Manager Service

O Manager Service é um serviço do Windows que coordena a comunicação entre DEMs de IaaS, o banco de dados SQL Server, agentes e o SMTP. Além disso, o Manager Service comunica-se com o servidor Web por meio do Model Manager e deve ser executado em uma conta de domínio com privilégios de administrador em todos os servidores Windows de IaaS.

A menos que você ative o failover automático do Manager Service, o IaaS exige que apenas uma máquina Windows execute ativamente o Manager Service de cada vez. Para backup ou alta disponibilidade, você pode implantar máquinas adicionais do Manager Service, mas a abordagem de failover manual requer que as máquinas de backup tenham o serviço interrompido e configurado para iniciar manualmente.

Para obter mais informações, consulte [Sobre o failover automático do Serviço de Gerenciador](#).

Banco de Dados SQL Server

O IaaS usa um banco de dados do Microsoft SQL Server para manter informações sobre as máquinas que ele gerencia, mais seus próprios elementos e políticas. A maioria dos usuários permite que o vRealize Automation crie o banco de dados durante a instalação. Como alternativa, você pode criar o banco de dados separadamente, de acordo com suas políticas de site.

Distributed Execution Manager

O componente do DEM de IaaS executa a lógica de negócios de modelos personalizados, interagindo com o banco de dados SQL Server do IaaS, e com bancos de dados e sistemas externos. Uma abordagem comum é instalar DEMs no servidor Windows do IaaS que hospeda o Manager Service ativo, mas isto não é necessário.

Cada instância do DEM age como Worker ou Orchestrator. As funções podem ser instaladas nos mesmos servidores ou em servidores diferentes.

DEM Worker—Um DEM Worker possui uma função: executar fluxos de trabalho. Múltiplos DEM Workers aumentam a capacidade e podem ser instalados nos mesmos servidores ou em servidores diferentes.

DEM Orchestrator—Um DEM Orchestrator realiza as seguintes funções de supervisão.

- Monitora os DEM Workers. Se um Worker parar de funcionar ou perder sua conexão com o Model Manager, o DEM Orchestrator moverá os fluxos de trabalho para outro DEM Worker.
- Agenda fluxos de trabalho criando instâncias de fluxo de trabalho no horário agendado.
- Assegura que somente uma instância de um fluxo de trabalho agendado esteja em execução em um determinado momento.
- Pré-processa fluxos de trabalho antes que sejam executados. O pré-processamento inclui a verificação das pré-condições para os fluxos de trabalho e a criação do histórico de execução do fluxo de trabalho.

O DEM Orchestrator ativo precisa de uma boa conexão de rede com o host do Model Manager. Em implantações grandes com vários orquestradores DEM em servidores separados, os orquestradores secundários servem como backups. Os orquestradores DEM secundários monitoram o orquestrador DEM ativo e fornecem redundância e failover quando ocorre um problema com o orquestrador DEM ativo. Para este tipo de configuração de failover, considere instalar o DEM Orchestrator ativo com o host do Manager Service ativo, e os DEM Orchestrators secundários com os hosts do Manager Service em espera.

Agentes

O vRealize Automation IaaS usa agentes para a integração com sistemas externos e para o gerenciamento de informações entre os componentes do vRealize Automation.

Uma abordagem comum é instalar os agentes do vRealize Automation no servidor Windows do IaaS que hospeda o Manager Service ativo, mas isto não é necessário. Múltiplos agentes aumentam a capacidade e podem ser instalados nos mesmos servidores ou em servidores diferentes.

Agentes de proxy de virtualização

O vRealize Automation cria e gerencia máquinas virtuais em hosts de virtualização. Os agentes de proxy de virtualização enviam comandos e coletam dados dos hosts do vSphere ESX Server, XenServer e Hyper-V, e das máquinas virtuais provisionadas neles.

Um agente de proxy de virtualização possui as seguintes características.

- Normalmente, exige privilégios de administrador na plataforma de virtualização que gerencia.

- Comunica-se com o Manager Service do IaaS.
- É instalado separadamente e tem seu próprio arquivo de configuração

A maioria das implementações do vRealize Automation instala o agente de proxy vSphere. Você pode instalar outros agentes de proxy conforme os recursos de virtualização em uso no seu site.

Agentes de Integração do Desktop Virtual

Os agentes PowerShell de VDI (infraestrutura de desktop virtual) permitem que o vRealize Automation faça integração a sistemas externos de desktop virtual. Os agentes de VDI exigem privilégios de administrador nos sistemas externos.

Você pode registrar máquinas virtuais provisionadas pelo vRealize Automation com o XenDesktop em um Citrix Desktop Delivery Controller (DDC), que permite que o usuário acesse a interface Web do XenDesktop no vRealize Automation.

Agentes de Integração do Provisionamento Externo

Os agentes PowerShell de EPI (integração de provisionamento externo) permitem que o vRealize Automation integre sistemas externos ao processo de provisionamento de máquinas.

Por exemplo, a integração ao Citrix Provisioning Server permite o provisionamento de máquinas por meio de streaming de disco sob demanda, e um agente de EPI permite que você execute scripts do Visual Basic como etapas extras durante o processo de provisionamento.

Os agentes de EPI exigem privilégios de administrador nos sistemas externos com os quais eles interagem.

Agente de instrumentação de gerenciamento do Windows

O agente de instrumentação de gerenciamento do Windows (WMI) do vRealize Automation aprimora sua capacidade de monitorar e controlar as informações do sistema e permite que você gerencie servidores Windows remotos a partir de uma localização remota. O agente de WMI também possibilita a coleta de dados dos servidores Windows que o vRealize Automation gerencia.

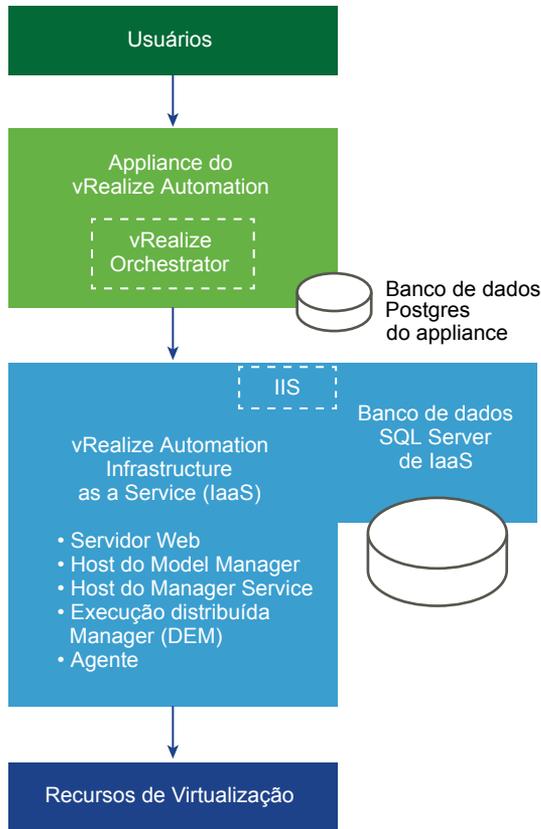
Tipo de implantação

Você pode instalar o vRealize Automation como uma implementação mínima para prova de conceito ou trabalho de desenvolvimento, ou em uma configuração distribuída adequada para cargas de trabalho de produção médias a grandes.

Implementações mínimas do vRealize Automation

Implementações mínimas incluem um appliance do vRealize Automation e um servidor Windows que hospeda os componentes do IaaS. Em uma implementação mínima, o banco de dados SQL Server do vRealize Automation pode estar no mesmo servidor Windows do IaaS com os componentes do IaaS, ou em um servidor Windows separado.

Figura 1-10. Implementação mínima do vRealize Automation



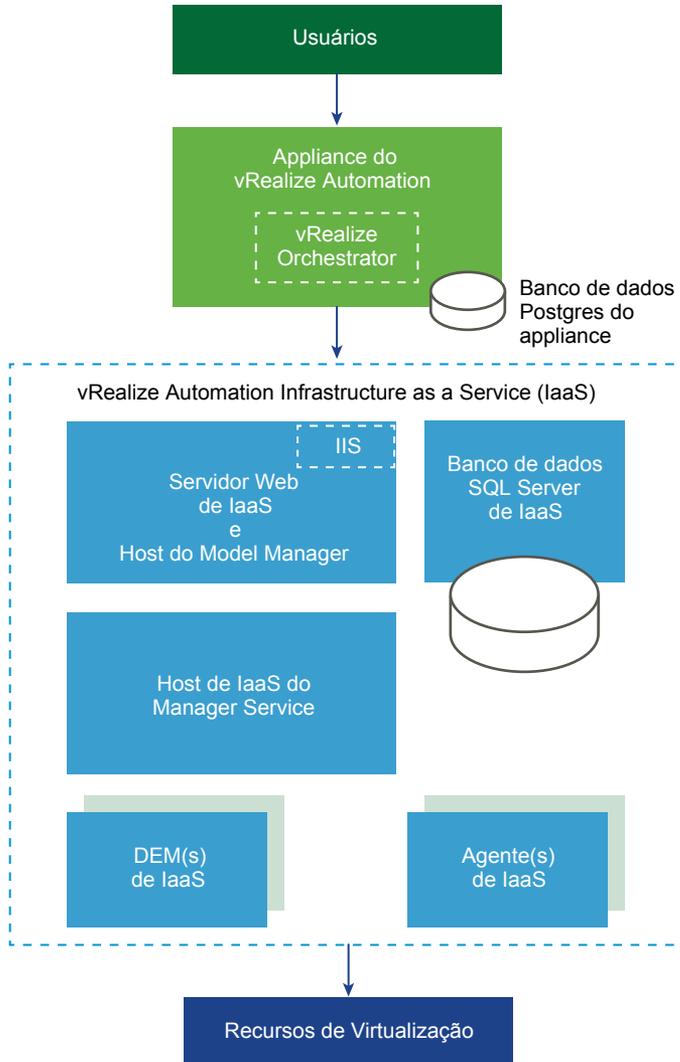
Não é possível converter uma implantação mínima em uma implantação corporativa. Para expandir uma implantação, comece com uma pequena implantação corporativa e adicione componentes a ela. Não é possível iniciar com uma implantação mínima.

Observação A documentação do vRealize Automation inclui um cenário de implementação mínima completa, de exemplo, que conduz você através da instalação e ensina como começar a usar o produto para prova do conceito. Consulte *Instalar e configurar o vRealize Automation para o cenário de Rainpole*.

Implementações distribuídas do vRealize Automation

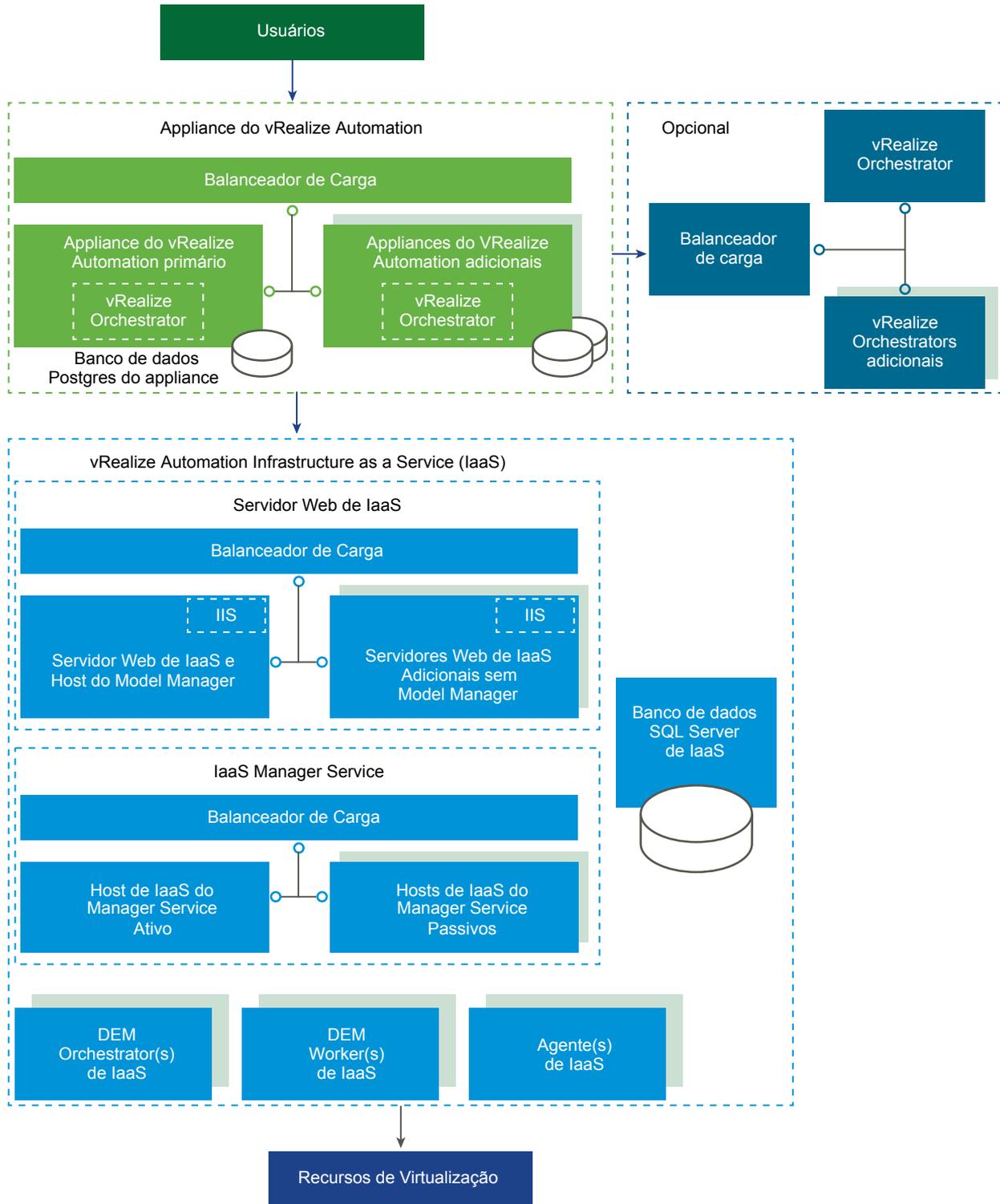
Implementações corporativas distribuídas podem ser de diferentes tamanhos. Uma implementação distribuída básica pode melhorar o vRealize Automation ao hospedar componentes do IaaS em servidores Windows diferentes, como mostrado na figura a seguir.

Figura 1-11. Implementação distribuída do vRealize Automation



Muitas implementações de produção vão além, com appliances redundantes, servidores redundantes e balanceamento de carga para ainda mais capacidade. Implementações distribuídas grandes fornecem melhor dimensionamento, alta disponibilidade e recuperação de desastres. Observe que a instância incorporada do vRealize Orchestrator agora é recomendada, mas você poderá ver o vRealize Automation conectado a um vRealize Orchestrator externo em implementações mais antigas.

Figura 1-12. Implementação do vRealize Automation grande, distribuída e com balanceamento de carga



Para mais informações sobre dimensionamento e alta disponibilidade, consulte o guia *Arquitetura de Referência do vRealize Automation*.

Escolhendo o método de instalação

O Assistente de Instalação consolidado do vRealize Automation é sua ferramenta primária para novas instalações do vRealize Automation. Alternativamente, você pode desejar executar os processos de instalação manuais separados ou uma instalação silenciosa.

- O Assistente de Instalação oferece uma forma simples e rápida de instalar desde implementações mínimas a implementações corporativas distribuídas com ou sem balanceadores de carga. A maioria dos usuários executa o Assistente de Instalação.
- Se você desejar expandir um implantação do vRealize Automation ou se o Assistente de Instalação parou por qualquer motivo, será necessário utilizar as etapas de instalação manual. Após começar uma instalação manual, você não poderá voltar e executar o Assistente de Instalação.
- Dependendo das necessidades de seu local, pode ser necessário também utilizar uma instalação silenciosa, com linha de comando ou baseada na API.

Preparando para a instalação do vRealize Automation

Você instala o vRealize Automation em uma infraestrutura de virtualização existente. Antes de começar uma instalação, é necessário satisfazer certos requisitos ambientais e de sistema.

Preparo geral

Há diversas considerações aplicáveis a toda a implantação que devem ser observadas antes de instalar o vRealize Automation.

Para mais informações sobre requisitos de ambiente de alto nível, incluindo sistema operacional e versões do navegador compatíveis, consulte a [Matriz de Suporte do vRealize Automation](#).

Navegadores Web do usuário

Não há suporte para várias janelas e guias do navegador. O vRealize Automation oferece suporte a uma sessão por usuário.

Os VMware Remote Consoles provisionados no vSphere oferecem suporte apenas a um subconjunto de navegadores aos quais o vRealize Automation também oferece suporte.

Software de terceiros

Todos os softwares de terceiros devem ter os patches mais recentes do fornecedor. Softwares de terceiros incluem o Microsoft Windows e o SQL Server.

Sincronização de hora

Todos os appliances do vRealize Automation e servidores Windows de IaaS devem sincronizar à mesma fonte de horário. Você só pode usar uma das fontes a seguir. Não misture as fontes de horário.

- O host do appliance do vRealize Automation
- Um servidor externo de NTP

Para usar o host do appliance do vRealize Automation, você deve executar o NTP no host ESXi. Para obter mais informações sobre pontualidade, consulte [Artigo da Base de Conhecimento da VMware 1318](#).

Você seleciona a fonte de horário na página de Pré-Requisitos de Instalação do Assistente de Instalação.

Contas e senhas

É possível que você tenha que criar ou planejar configurações para diversas contas e senhas de usuários antes de instalar o vRealize Automation.

Conta de serviço de IaaS

O IaaS instala diversos serviços Windows que devem ser executados sob uma única conta de usuário.

- A conta deve ser um usuário do domínio.
- A conta não precisa ser um administrador do domínio, mas deve ter permissão de administrador local, antes da instalação, em todos os servidores Windows de IaaS.
- A senha da conta não pode conter um caractere de aspas duplas ("").
- O instalador do Agente de Gerenciamento para servidores Windows de IaaS solicita suas credenciais de conta.
- A conta deve ter permissão para **Fazer login como serviço**, o que permite que o Manager Service inicie e gere arquivos de log.
- A conta também deve ter permissão dbo no banco de dados de IaaS.

Se você utilizar o instalador para criar o banco de dados, adicione o login da conta ao SQL Server antes da instalação. O instalador concede a permissão dbo após criar o banco de dados.

- Se você utilizar o instalador para criar o banco de dados, no SQL, adicione a função sysadmin à conta antes da instalação.

A função sysadmin não será necessária se você optar por utilizar um banco de dados vazio preexistente.

Identidade do pool da aplicação do IIS

A conta que você utiliza como a identidade do pool da aplicação do IIS para o serviço Web do Model Manager deve ter a permissão para **Fazer login como trabalho em lote**.

Credenciais do banco de dados de IaaS

Você pode permitir que o instalador do vRealize Automation crie o banco de dados, ou você pode criá-lo separadamente usando o SQL Server. Quando o instalador do vRealize Automation criar o banco de dados, os requisitos a seguir serão aplicáveis.

- Para o instalador do vRealize Automation, se você selecionar Autenticação do Windows, a conta que executa o Agente de Gerenciamento no servidor Web primário de IaaS deverá ter a função sysadmin no SQL para criar e alterar o tamanho do banco de dados.

- Para o instalador do vRealize Automation, mesmo se você não selecionar Autenticação do Windows, a conta que executa o Agente de Gerenciamento no servidor Web primário de IaaS deverá ter a função sysadmin no SQL porque as credenciais são usadas em tempo de execução.
- Se você criar o banco de dados separadamente, o usuário Windows ou credenciais de usuário SQL que você fornecer só precisarão de permissão dbowner no banco de dados.

Código de acesso de segurança do banco de dados de IaaS

O código de acesso de segurança do banco de dados gera uma chave criptográfica que protege os dados no banco de dados SQL de IaaS. Você especifica o código de acesso na página do Host de IaaS do Assistente de Instalação.

- Planeje utilizar o mesmo código de acesso de segurança do banco de dados em toda a instalação, para que cada componente tenha a mesma chave criptográfica.
- Anote o código de acesso, porque você precisará dele para restaurar o banco de dados se houver uma falha ou para adicionar componentes após a instalação inicial.
- O código de acesso de segurança do banco de dados não pode conter um caractere de aspas duplas (""). O código de acesso é aceito quando você o cria, mas faz com que a instalação falhe.

Endpoints do vSphere

Se você planeja provisionar a um endpoint do vSphere, você precisará de um domínio ou conta local com permissão suficiente para realizar operações no destino. A conta também precisa ter o nível adequado de permissão configurado no vRealize Orchestrator.

Senha do administrador do vRealize Automation

Após a instalação, a senha do administrador do vRealize Automation é utilizada para fazer login no tenant padrão. Você especifica a senha do administrador na página de Single Sign-On do Assistente de Instalação.

A senha de administrador do vRealize Automation não pode conter um caractere de igual (=). A senha será aceita durante a criação, mas resultará em erros posteriormente quando você executar operações como salvar endpoints.

Nomes de host e endereços IP

O vRealize Automation requer que você nomeie os hosts na sua instalação de acordo com certos requisitos.

- Todas as máquinas do vRealize Automation na sua instalação devem ser capazes de resolver umas às outras pelo nome de domínio totalmente qualificado (FQDN).

Ao realizar a instalação, sempre insira o FQDN completo quando for identificar ou selecionar uma máquina do vRealize Automation. Não insira o endereço IP ou nomes curtos da máquina.

- Além do requisito de FQDN, máquinas Windows que hospedam o serviço Web do Model Manager, o Manager Service e o banco de dados Microsoft SQL Server devem ser capazes de resolverem umas às outras com base no nome WINS (Serviço de Cadastramento na Internet do Windows).

Configure seu Sistema de Nomes de Domínio (DNS) para resolver todos os nomes de host WINS curtos.

- Planeje o domínio e o nome da máquina com antecedência para que os nomes de máquina do vRealize Automation comecem com letras (a-z, A-Z), letras ou dígitos (0-9) e tenham somente letras, dígitos ou hifens (-) no meio da nomeação da máquina. O caractere de sublinhado (_) não deve aparecer no nome do host ou em qualquer parte do FQDN.

Para obter mais informações sobre nomes permitidos, reveja as especificações de nome de host na Internet Engineering Task Force. Consulte www.ietf.org.

- Em geral, você deve esperar manter os nomes de hosts e FQDNs que você planejou para sistemas vRealize Automation. Alterar o nome de um host nem sempre é possível. Quando a alteração for possível, pode ser um procedimento complicado.
- Uma prática recomendada é reservar e usar endereços IP estáticos para todos os appliances do vRealize Automation e servidores Windows do IaaS. O vRealize Automation oferece suporte para DHCP, mas endereços IP estáticos são recomendados para implementações a longo prazo, como ambientes de produção.
 - Você aplica um endereço IP ao appliance do vRealize Automation durante a implantação do OVF ou OVA.
 - Para os servidores Windows IaaS, você segue o processo habitual do sistema operacional. Defina o endereço IP antes de instalar o IaaS do vRealize Automation.

Latência e largura de banda

O vRealize Automation suporta vários sites, instalação distribuída, mas o volume e a velocidade de transmissão de dados devem atender aos pré-requisitos mínimos.

O vRealize Automation precisa de um ambiente de 5 ms ou uma latência da rede mais baixa e uma largura de banda de 1 GB ou mais alta, entre os componentes a seguir.

- Appliance do vRealize Automation
- Servidor Web do IaaS
- Host do Model Manager do IaaS
- Host do Manager Service do IaaS
- Banco de dados SQL Server do IaaS
- DEM Orchestrator do IaaS

O seguinte componente pode funcionar em um site de latência superior, mas a prática não é recomendada.

- DEM Worker do IaaS

Você pode instalar o seguinte componente no site do endpoint com o qual ele se comunica.

- Agente de Proxy do IaaS

Appliance do vRealize Automation

A maioria dos requisitos do appliance do vRealize Automation são pré-configurados no OVF ou OVA que você implanta. Os mesmos requisitos se aplicam aos appliances independentes, mestre ou réplica do vRealize Automation.

O hardware mínimo da máquina virtual no qual você pode implantar é a Versão 7 ou o ESX/ESXi 4.x ou mais recente. Consulte [Artigo da Base de Conhecimento da VMware 2007240](#). Devido à demanda de recursos de hardware, não implante o VMware Workstation.

Após a implantação, você pode utilizar o vSphere para ajustar as configurações de hardware do appliance do vRealize Automation para satisfazer aos requisitos do Active Directory. Consulte a tabela a seguir.

Tabela 1-11. Requisitos de hardware do appliance do vRealize Automation para o Active Directory

| Appliance do vRealize Automation para Active Directories pequenos | Appliance do vRealize Automation para Active Directories grandes |
|---|---|
| <ul style="list-style-type: none"> ▪ 4 CPUs ▪ 18 GB de memória ▪ 60 GB de armazenamento de disco | <ul style="list-style-type: none"> ▪ 4 CPUs ▪ 22 GB de memória ▪ 60 GB de armazenamento de disco |

Um Active Directory pequeno tem até 25.000 usuários na unidade organizacional (UO) a serem sincronizados na configuração de Armazenamento de ID. Um Active Directory grande tem mais de 25.000 usuários na UO.

Portas do appliance do vRealize Automation

As portas no appliance do vRealize Automation, normalmente, são pré-configuradas no OVF ou OVA que você implanta.

As seguintes portas são usadas pelo appliance vRealize Automation.

Tabela 1-12. Portas de entrada

| Porta | Protocolo | Comentários |
|-------------------------|--------------------|--|
| 22 | TCP | Opcional. Acesso para sessões SSH. |
| 80 | TCP | Opcional. Redireciona para 443. |
| 88 | TCP (UDP opcional) | Autenticação Cloud KDC Kerberos de dispositivos móveis externos. |
| 443 | TCP | Acesso ao console do vRealize Automation e às chamadas de API. Acesso para máquinas para baixar o agente guest e o agente de bootstrap do software. Acesso ao balanceador de carga, navegador. |
| 4369, 5671, 5672, 25672 | TCP | Mensagens do RabbitMQ. |

Tabela 1-12. Portas de entrada (Continuação)

| Porta | Protocolo | Comentários |
|------------------------|-----------|--|
| 5480 | TCP | Acesso à interface de gerenciamento do appliance virtual. Usado pelo Agente de Gerenciamento. |
| 5488, 5489 | TCP | Usado internamente pelo appliance do vRealize Automation para atualizações. |
| 8230, 8280, 8281, 8283 | TCP | Instância interna do vRealize Orchestrator. |
| 8443 | TCP | Acesso ao navegador. Porta de administrador do Identity Manager sobre HTTPS. |
| 8444 | TCP | Comunicação do proxy do console para conexões do vSphere VMware Remote Console. |
| 9300–9400 | TCP | Acesso às auditorias do Identity Manager. |
| 54328 | UDP | |

Tabela 1-13. Portas de saída

| Porta | Protocolo | Comentários |
|----------------------|-----------|---|
| 25, 587 | TCP, UDP | SMTP para o envio de e-mail de notificação de saída. |
| 53 | TCP, UDP | Servidor DNS. |
| 67, 68, 546, 547 | TCP, UDP | DHCP. |
| 80 | TCP | Opcional. Para obter as atualizações de software. O download das atualizações pode ser realizado e aplicado separadamente. |
| 88, 464, 135 | TCP, UDP | Controlador de domínio. |
| 110, 995 | TCP, UDP | POP para receber e-mail de notificação de entrada. |
| 143, 993 | TCP, UDP | IMAP para receber e-mail de notificação de entrada. |
| 123 | TCP, UDP | Opcional. Para conexão direta com o NTP em vez de usar o tempo do host. |
| 389 | TCP | Acesso ao Servidor de Conexão do View |
| 389, 636, 3268, 3269 | TCP | Active Directory. Portas padrão mostradas, mas são configuráveis. |
| 443 | TCP | Comunicação por HTTPS com o IaaS Manager Service e hosts de endpoint de infraestrutura. Comunicação com o serviço de software do vRealize Automation sobre HTTPS. Acesso ao servidor de atualização do Identity Manager. Acesso ao Servidor de Conexão do View |
| 445 | TCP | Acesso ao repositório do ThinApp para o Identity Manager. |
| 902 | TCP | Operações de cópia de arquivo de rede do ESXi e conexões do VMware Remote Console. |
| 5050 | TCP | Opcional. Para comunicação com o vRealize Business for Cloud. |
| 5432 | TCP, UDP | Opcional. Para comunicação com outro banco de dados do appliance PostgreSQL. |
| 5500 | TCP | Sistema RSA SecurID. Porta padrão mostrada, mas é configurável. |
| 8281 | TCP | Opcional. Para comunicação com uma instância externa do vRealize Orchestrator. |

Tabela 1-13. Portas de saída (Continuação)

| Porta | Protocolo | Comentários |
|-----------|-----------|---|
| 9300–9400 | TCP | Acesso às auditorias do Identity Manager. |
| 54328 | UDP | |

Outras portas podem ser exigidas pelos plug-ins do vRealize Orchestrator específicos que comunicam-se com sistemas externos. Consulte a documentação do plug-in do vRealize Orchestrator.

Servidores Windows do IaaS

Todos os servidores Windows que hospedam componentes IaaS devem satisfazer determinados requisitos. Satisfaça os requisitos antes de executar o Assistente de Instalação do vRealize Automation ou o instalador padrão baseado em Windows.

- Coloque todos os servidores Windows do IaaS no mesmo domínio. Não use Grupos de trabalho.
- Cada servidor precisa do seguinte hardware mínimo.
 - 2 CPUs
 - 8 GB de memória
 - 40 GB de armazenamento de disco

Um servidor que hospeda o banco de dados SQL em conjunto com componentes do IaaS pode precisar de hardware adicional.

- Devido à demanda de recursos de hardware, não implante o VMware Workstation.
- Instale o Microsoft .NET Framework 3.5.
- Instale o Microsoft .NET Framework 4.5.2 ou posterior.

Uma cópia do .NET está disponível em qualquer appliance do vRealize Automation:

<https://vrealize-automation-appliance-fqdn:5480/installer/>

Se você usa o Internet Explorer para fazer o download, verifique se a Configuração de Segurança Reforçada está desativada. Navegue para `res://iesetup.dll/SoftAdmin.htm` no servidor Windows.

- Instale o Microsoft PowerShell 2.0, 3.0 ou 4.0, com base em sua versão do Windows.

Observe que algumas atualizações ou migrações do vRealize Automation podem exigir uma versão mais antiga ou mais recente do PowerShell, além daquela que está em execução no momento.
- Se você instalar mais de um componente do IaaS no mesmo servidor Windows, planeje instalá-los na mesma pasta de instalação. Não use caminhos diferentes.
- Os servidores do IaaS usam TLS para autenticação, que é ativada por padrão em alguns servidores Windows.

Alguns sites desative o TLS por motivos de segurança, mas você deve deixar pelo menos um protocolo TLS habilitado. Esta versão do vRealize Automation é compatível com o TLS 1.2.

- Ative o serviço de Coordenador de Transações Distribuídas (DTC). O IaaS usa o DTC para transações e ações de banco de dados, como a criação de fluxos de trabalho.

Observação Se você clonar uma máquina para criar um servidor Windows do IaaS, instale o DTC no clone após a clonagem. Se você clonar uma máquina que já tem o DTC, seu identificador exclusivo será copiado no clone, fazendo com que a comunicação falhe. Consulte [Erro na comunicação do serviço de gerenciador](#).

Ative também o DTC no servidor que hospeda o banco de dados SQL, se ele for separado do IaaS. Para obter mais informações sobre a habilitação do DTC, consulte [Artigo da Base de Conhecimento da VMware 2038943](#).

- Verifique se o serviço de Login secundário está sendo executado. Se desejar, é possível interromper o serviço após a conclusão da instalação.

Portas do Servidor Windows de IaaS

Portas nos servidores Windows de IaaS devem ser configuradas antes da instalação do vRealize Automation.

Portas abertas entre todos os servidores Windows de IaaS de acordo com as tabelas a seguir. Incluir o servidor que hospeda o banco de dados SQL, se for separado de IaaS. Como alternativa, se as políticas do site permitirem, você poderá desativar os firewalls entre os servidores Windows do IaaS e o SQL Server.

Tabela 1-14. Portas de entrada

| Porta | Protocolo | Componente | Comentários |
|-------|-----------|---|---|
| 443 | TCP | Manager Service | Comunicação com os componentes de IaaS e do appliance do vRealize Automation sobre HTTPS |
| 443 | TCP | Appliance do vRealize Automation | Comunicação com os componentes de IaaS e do appliance do vRealize Automation sobre HTTPS |
| 443 | TCP | Hosts de endpoint de infraestrutura | Comunicação com os componentes de IaaS e do appliance do vRealize Automation sobre HTTPS. Em geral, 443 é a porta de comunicação padrão para hosts de endpoint de infraestrutura de nuvem e virtuais, mas consulte a documentação fornecida pelos seus hosts de infraestrutura para obter uma lista completa de portas padrão e necessárias |
| 443 | TCP | Agente guest Agente de bootstrap de software | Comunicação com o Manager Service sobre HTTPS |
| 443 | TCP | DEM Worker | Comunicação com o NSX Manager |
| 1433 | TCP | Instância do SQL Server | MSSQL |

Tabela 1-15. Portas de saída

| Porta | Protocolo | Componente | Comentários |
|------------------|-----------|---|---|
| 53 | TCP, UDP | Tudo | DNS |
| 67, 68, 546, 547 | TCP, UDP | Tudo | DHCP |
| 123 | TCP, UDP | Tudo | Opcional. NTP |
| 443 | TCP | Manager Service | Comunicação com o appliance do vRealize Automation sobre HTTPS |
| 443 | TCP | Distributed Execution Managers | Comunicação com o Manager Service sobre HTTPS |
| 443 | TCP | Agentes de proxy | Comunicação por HTTPS com o Manager Service e hosts de endpoint de infraestrutura |
| 443 | TCP | Agente de gerenciamento | Comunicação com o appliance do vRealize Automation |
| 443 | TCP | Agente guest Agente de bootstrap de software | Comunicação com o Manager Service sobre HTTPS |
| 1433 | TCP | Manager Service Website | MSSQL |
| 5480 | TCP | Tudo | Comunicação com o appliance do vRealize Automation. |

Além disso, uma vez que você habilita DTC entre todos os servidores, o DTC requer a porta 135 sobre TCP e uma porta aleatória entre 1024 e 65535. Observe que o Verificador de Pré-Requisitos valida se o DTC está em execução e se as portas necessárias estão abertas.

Servidor Web de IaaS

Um servidor Windows que hospeda o componente Web deve atender a requisitos adicionais, além daqueles para todos os servidores Windows de IaaS.

Os requisitos são os mesmos, independentemente se os componentes Web hospedam ou não o Model Manager.

- Configurar o Java.
 - Instale o Java 1.8, 64 bits, atualização 161 ou posterior. Não use 32 bits.
O JRE é suficiente. Você não precisa do JDK completo.
 - Defina a variável de ambiente JAVA_HOME como a pasta de instalação Java.
 - Verifique se o arquivo %JAVA_HOME%\bin\java.exe está disponível.
- Configure os Internet Information Services (IIS) de acordo com a tabela a seguir.

Você precisa do IIS 7.5 para as variantes do Windows 2008, IIS 8 para Windows 2012, IIS 8.5 para Windows 2012 R2 e IIS 10 para Windows 2016.

Além das definições de configuração, evite hospedar sites adicionais no IIS. O vRealize Automation define a associação na sua porta de comunicação com todos os endereços IP não atribuídos, impossibilitando associações adicionais. A porta de comunicação padrão do vRealize Automation é 443.

Tabela 1-16. Internet Information Services do Host do Serviço de Gerenciador do IaaS

| Componente do IIS | Configuração |
|--|---|
| Funções do Internet Information Services (IIS) | <ul style="list-style-type: none"> ■ Autenticação do Windows ■ Conteúdo Estático ■ Documento padrão ■ ASPNET 3.5 e ASPNET 4.5 ■ Extensões ISAPI ■ Filtro ISAPI |
| Funções Serviço de Ativação de Processos do Windows do IIS | <ul style="list-style-type: none"> ■ API de configuração ■ Ambiente Net ■ Modelo de processo ■ Ativação WCF (somente para variantes do Windows 2008) ■ Ativação HTTP ■ Ativação não HTTP (somente para variantes do Windows 2008) <p>(Variantes do Windows 2012: Vá até Recursos > Recursos do .Net Framework 3.5 > Ativação não HTTP)</p> |
| Configurações de Autenticação do IIS | <p>Defina os não padrões a seguir.</p> <ul style="list-style-type: none"> ■ Autenticação do Windows ativada ■ Autenticação anônima desativada <p>Não altere os padrões a seguir.</p> <ul style="list-style-type: none"> ■ Negotiate Provider ativado ■ NTLM Provider ativado ■ Modo Kernel da Autenticação do Windows ativado ■ Proteção Estendida da Autenticação do Windows desativada ■ Para certificados usando SHA512, o TLS1.2 deve estar desativado nas variantes do Windows 2012 |

Host do Serviço de Gerenciador do IaaS

Um servidor Windows que hospeda o componente do Serviço de Gerenciador deve satisfazer requisitos adicionais, além daqueles para todos os servidores Windows IaaS.

Os requisitos são os mesmos, se o host do Serviço de Gerenciador for primário ou um backup.

- Não pode existir firewalls entre um host do Serviço de Gerenciador e um host DEM. Para obter informações sobre portas, consulte [Portas do Servidor Windows de IaaS](#).
- O host do Serviço de Gerenciador deve ser capaz de resolver o nome NETBIOS do host do banco de dados do SQL Server. Se não for possível resolver o nome NETBIOS, adicione o nome NETBIOS do SQL Server no arquivo `/etc/hosts` da máquina do Serviço de Gerenciador.

Host do servidor SQL de IaaS

Um servidor Windows que hospeda o banco de dados SQL de IaaS deve atender a certos requisitos.

Seu SQL Server pode residir em um de seus servidores Windows de IaaS, ou em um host separado.

Quando hospedado junto com componentes de IaaS, esses requisitos são em adição àqueles para todos os servidores Windows de IaaS.

- Esta versão do vRealize Automation não tem suporte para o modo de compatibilidade 130 do SQL Server 2016 padrão. Se você criar separadamente um banco de dados vazio do SQL Server 2016 para ser usado com o IaaS, use o modo de compatibilidade 100 ou 120.

Se você criar o banco de dados por meio do instalador do vRealize Automation, a compatibilidade já estará configurada.

- O Grupo de Disponibilidade AlwaysOn (AAG) só tem suporte no SQL Server 2016. Enterprise. Ao usar o AAG, você especifica o FQDN do ouvinte AAG como host do SQL Server.
- Quando hospedado junto com componentes de IaaS, configure o Java.
 - Instale o Java 1.8, 64 bits, atualização 161 ou posterior. Não use 32 bits.
O JRE é suficiente. Você não precisa do JDK completo.
 - Defina a variável de ambiente JAVA_HOME como a pasta de instalação Java.
 - Verifique se o arquivo %JAVA_HOME%\bin\java.exe está disponível.
- Use uma versão compatível do SQL Server da [Matriz de Suporte do vRealize Automation](#).
- Ative o protocolo TCP/IP para o SQL Server.
- O SQL Server inclui um banco de dados modelo para todos os bancos de dados criados na instância do SQL. Para instalar o IaaS corretamente, não altere o tamanho do banco de dados modelo.
- Em geral, o servidor precisa de mais hardware que os mínimos descritos em [Servidores Windows do IaaS](#).

Para obter mais informações, consulte [Especificações de hardware do vRealize Automation e máximos de capacidade](#).

- Antes de executar o instalador do vRealize Automation, você precisa identificar contas e adicionar permissões no SQL. Consulte [Contas e senhas](#).

Host do Distributed Execution Manager do IaaS

Um servidor Windows que hospeda o componente orquestrador ou trabalhador do Distributed Execution Manager (DEM) deve satisfazer requisitos adicionais, além daqueles para todos os servidores Windows IaaS.

Nenhum firewall pode existir entre um host DEM e o host do Serviço de Gerenciador. Para obter informações sobre portas, consulte [Portas do Servidor Windows de IaaS](#).

Trabalhadores DEM podem ter requisitos adicionais dependendo dos recursos de provisionamento com os quais eles interagem.

Trabalhadores do DEM com o Amazon Web Services

Um Trabalhador do DEM IaaS do vRealize Automation que se comunica com o Amazon Web Services (AWS) deve satisfazer requisitos adicionais, além daqueles para todos os servidores Windows e DEMs IaaS em geral.

Um Trabalhador do DEM pode se comunicar com o AWS para obter provisionamento. O Trabalhador do DEM se comunica com a conta do Amazon EC2, além de coletar dados dela.

- O Trabalhador do DEM deve ter acesso à Internet.
- Se o Trabalhador do DEM estiver atrás de um firewall, o tráfego HTTPS deverá ser permitido de e para `aws.amazon.com`, bem como os URLs para as regiões do EC2 às quais as suas contas do AWS têm acesso, como `ec2.us-east-1.amazonaws.com` para a região EUA - Leste.

Como cada URL resolve um intervalo de endereços IP, talvez seja necessário usar uma ferramenta, como as que estão disponíveis no site Network Solutions, para listar e configurar esses endereços IP.

- Se o Trabalhador do DEM acessar a Internet por meio de um servidor proxy, o serviço DEM deverá ser executado com credenciais que possam ser autenticadas no servidor proxy.

DEM Workers com OpenStack ou PowerVC

Um DEM Worker de IaaS do vRealize Automation que se comunica com e coleta dados do OpenStack ou Power VC deve atender a requisitos adicionais, além daqueles para todos os servidores Windows de IaaS e DEMs em geral.

Tabela 1-17. Requisitos de OpenStack e PowerVC para DEM Worker

| Sua instalação | Requisitos |
|---|---|
| Tudo | <p>No Registro do Windows, habilite o suporte ao TLS v1.2 para .NET Framework. Por exemplo:</p> <pre>[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319] "SchUseStrongCrypto"=dword:00000001</pre> <pre>[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319] "SchUseStrongCrypto"=dword:00000001</pre> |
| Host DEM do Windows 2008 | <p>No Registro do Windows, habilite o protocolo TLS v1.2. Por exemplo:</p> <pre>[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2] [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client] "DisabledByDefault"=dword:00000000 "Enabled"=dword:00000001</pre> <pre>[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server] "DisabledByDefault"=dword:00000000 "Enabled"=dword:00000001</pre> |
| Certificados auto-assinados no seu host de endpoint de infraestrutura | <p>Se a sua instância do PowerVC ou OpenStack não estiver usando certificados confiáveis, importe o certificado SSL da sua instância do PowerVC ou OpenStack para o repositório de Autoridades de Certificação Raiz Confiáveis em cada servidor Windows IaaS no qual você pretende instalar um DEM do vRealize Automation.</p> |

DEM Workers com Red Hat Enterprise Virtualization

Um DEM Worker de IaaS do vRealize Automation que se comunica com e coleta dados do Red Hat Enterprise Virtualization (RHEV) deve atender a requisitos adicionais, além daqueles para todos os servidores Windows de IaaS e DEMs em geral.

- Você deve juntar cada ambiente de RHEV ao domínio contendo o servidor do DEM Worker.
- As credenciais utilizadas para gerenciar o endpoint que representa um ambiente RHEV devem ter privilégios de administrador no ambiente RHEV. Ao utilizar RHEV para provisionamento, o DEM Worker se comunica com dados dessa conta e os coleta.
- As credenciais também devem ter privilégios suficientes para criar objetos nos hosts no ambiente.

DEM Workers com SCVMM

Um DEM Worker de IaaS do vRealize Automation que gerencie máquinas virtuais através do System Center Virtual Machine Manager (SCVMM) deve atender a requisitos adicionais, além daqueles para todos os servidores Windows de IaaS e DEMs em geral.

- Instale o DEM Worker na mesma máquina do console de SCVMM.
Uma prática recomendada é instalar o console de SCVMM em um DEM Worker diferente.
- O DEM Worker deve ter acesso ao módulo SCVMM PowerShell instalado com o console.

- A Política de Execução do PowerShell deve ser definida como RemoteSigned ou Unrestricted.

Para verificar a Política de execução do PowerShell, insira um dos seguintes comandos no prompt de comando do PowerShell.

```
help about_signing  
help Set-ExecutionPolicy
```

- Se todos os DEM Workers na instância não estiverem em máquinas que atendem a esses requisitos, use os comandos do Skill para direcionar fluxos de trabalho relacionados ao SCVMM para os DEM Workers que estejam em máquinas adequadas.

O vRealize Automation não é compatível com um ambiente de implantação que usa a configuração de nuvem privada SCVMM. O vRealize Automation atualmente não pode coletar de, alocar para, ou provisionar com base em nuvens privadas de SCVMM.

Os requisitos adicionais a seguir se aplicam ao SCVMM.

- O vRealize Automation é compatível com o SCVMM 2012 R2, que requer o PowerShell 3 ou superior.
- Instale o console do SCVMM antes de instalar os DEM Workers do vRealize Automation que consomem os itens de trabalho do SCVMM.

Se você instalar o DEM Worker antes do console do SCVMM, verá erros de log semelhantes ao exemplo a seguir.

Falha no fluxo de trabalho 'ScvmmEndpointDataCollection' com a seguinte exceção: o termo 'Get-VMMServer' não é reconhecido como o nome de um cmdlet, uma função, um arquivo de script ou um programa operável. Verifique a ortografia do nome ou, se um caminho tiver sido incluído, verifique se o caminho está correto e tente novamente.

Para resolver o problema, verifique se o console do SCVMM está instalado e reinicie o serviço do DEM Worker.

- Cada instância do SCVMM deve estar associada ao domínio que contém o servidor.
- As credenciais utilizadas para gerenciar o endpoint que representa uma instância do SCVMM devem ter privilégios de administrador no servidor SCVMM.

As credenciais também devem ter privilégios de administrador nos servidores Hyper-V da instância.

- Para provisionar máquinas em um recurso de SCVMM, o usuário do vRealize Automation que está solicitando o item de catálogo deve ter a função de administrador na instância do SCVMM.
- Os servidores Hyper-V em uma instância do SCVMM a ser gerenciada devem ser servidores R2 SP1 do Windows 2008 com Hyper-V instalado. O processador deve dispor das extensões de virtualização necessárias, o .NET Framework 4.5.2, ou mais recente, deve estar instalado, e a Instrumentação de Gerenciamento do Windows (WMI) deve estar habilitada.

- Para provisionar uma máquina da Geração-2 em um recurso do SCVMM 2012 R2, você deve adicionar as seguintes propriedades em um blueprint.

```
Scvmm.Generation2 = true
Hyperv.Network.Type = synthetic
```

Os blueprints da Geração-2 devem ter um virtualHardDisk (vHDX) com coleta de dados existente na página de informações de compilação do blueprint. Se estiver em branco, o provisionamento da Geração-2 apresentará falhas.

Para informações adicionais sobre preparar para provisionamento da máquina, consulte [Preparar ambiente de SCVMM](#).

Certificados

O vRealize Automation usa certificados SSL para uma comunicação segura entre componentes e instâncias do IaaS do appliance vRealize Automation. Os dispositivos e as máquinas de instalação do Windows trocam esses certificados para estabelecer uma conexão confiável. Você pode obter certificados a partir de uma autoridade de certificação interna ou externa, ou pode gerar certificados autoassinados durante o processo de implantação de cada componente.

Para obter informações importantes sobre resolução de problemas, suporte e requisitos de confiança para certificados, consulte [Artigo da Base de Conhecimento da VMware 2106583](#).

Observação O vRealize Automation oferece suporte para certificados SHA2. Os certificados autoassinados gerados pelo sistema usam Criptografia SHA-256 com RSA. Talvez seja necessário atualizar para certificados SHA2 devido a requisitos de navegador ou sistema operacional.

Você pode atualizar ou substituir certificados após a implantação. Por exemplo, um certificado pode expirar ou você pode optar por usar certificados autoassinados durante a implantação inicial, mas depois obter certificados de uma autoridade confiável antes de ativar sua implementação do vRealize Automation.

Tabela 1-18. Implementações de certificados

| Componente | Implantação mínima (sem produção) | Implantação distribuída (pronta para produção) |
|----------------------------------|---|--|
| Appliance do vRealize Automation | Gere um certificado autoassinado durante a configuração de um dispositivo. | Para cada cluster de appliance, você pode usar um certificado de uma autoridade de certificação interna ou externa. Certificados de vários usuários e curingas são suportados. |
| Componentes do IaaS | Durante a instalação, aceite os certificados autoassinados gerados ou selecione a supressão dos certificados. | Obtenha um certificado de vários usuários, como o certificado SAN (nome alternativo da entidade), a partir de uma autoridade de certificação interna ou externa em que seu cliente Web confie. |

Cadeia de certificados

Se você usar cadeias de certificados, especifique os certificados na seguinte ordem.

- Certificado cliente/servidor assinado pelo certificado de autoridade de certificação intermediário

- Um ou mais certificados intermediários
- Um certificado de autoridade de certificação raiz

Inclua o cabeçalho BEGIN CERTIFICATE e o rodapé END CERTIFICATE para cada certificado a ser importado.

Alterações de certificado se personalizar a URL de login do vRealize Automation

Se desejar que os usuários façam login em um nome de URL que não seja um nome do balanceador de carga ou appliance do vRealize Automation, consulte as etapas de pré e pós instalação do CNAME em [Definir a URL de login do vRealize Automation como um nome personalizado](#).

Requisitos de certificado do vRealize Automation

Ao usar seus próprios certificados com o vRealize Automation, estes precisam atender a certos requisitos.

Tipos de certificados com suporte

Em muitas organizações, certificados são emitidos ou solicitados por autoridades externas de acordo com os requisitos da empresa.

Os seguintes requisitos abordam tipos comuns de certificado e formato de identidade usados com implantações típicas do vRealize Automation.

| Propriedade de certificado | Requisitos |
|----------------------------|-----------------------------|
| Algoritmo de hash | SHA1, SHA2, (256, 584, 512) |
| Algoritmo de assinatura | RSASSA-PKCS1_V1_5 |
| Comprimento da chave | 2084, 4096 |

Observação A assinatura RSASSA-PSS não tem suporte para implantações do vRealize Automation. Essa assinatura é o padrão para uma CA da Microsoft no Windows 2012 R2. A assinatura é um parâmetro configurável e, portanto, você deve garantir que ele seja definida corretamente ao usar uma CA da Microsoft.

Matriz de suporte de certificados do vRealize Automation

| Algoritmo de hash | SHA1 | | | | SHA2-256 | | | |
|------------------------------------|-------------------------|--------------------|-------------|-------------|--------------------|--------------------|-------------|-------------|
| | Algoritmo de assinatura | RSASSA-PKCS1_V1_5 | | RSASSA-PSS | | RSASSA-PKCS1_V1_5 | | RSASSA-PSS |
| Tamanho da chave | 2048 | 4096 | 2048 | 4096 | 2048 | 4096 | 2048 | 4096 |
| Com suporte no vRealize Automation | Suporte verificado | Suporte verificado | Sem suporte | Sem suporte | Suporte verificado | Suporte verificado | Sem suporte | Sem suporte |

| Algoritmo de hash | SHA2-384 | | | | SHA2-512 | | | |
|------------------------------------|-------------------------|--------------------|-------------|-------------|--------------------|--------------------|-------------|-------------|
| | Algoritmo de assinatura | RSASSA-PKCS1_V1_5 | | RSASSA-PSS | | RSASSA-PKCS1_V1_5 | | RSASSA-PSS |
| Tamanho da chave | 2048 | 4096 | 2048 | 4096 | 2048 | 4096 | 2048 | 4096 |
| Com suporte no vRealize Automation | Suporte verificado | Suporte verificado | Sem suporte | Sem suporte | Suporte verificado | Suporte verificado | Sem suporte | Sem suporte |

Extraindo certificados e chaves privadas

Os certificados que você usa com os appliances virtuais devem estar no formato de arquivo PEM.

Os exemplos na seguintes tabela usam comandos do Gnu `openssl` para extrair as informações de certificado que você precisa para configurar os appliances virtuais.

Tabela 1-19. Valores e comandos de certificado de amostra (openssl)

| A autoridade de certificação fornece | Comando | Entradas de appliance virtual |
|--------------------------------------|--|-------------------------------|
| Chave privada RSA | <code>openssl pkcs12 -in path_to_.pfx certificate_file -nocerts -out key.pem</code> | Chave privada RSA |
| Arquivo PEM | <code>openssl pkcs12 -in path_to_.pfx certificate_file -clcerts -nokeys -out cert.pem</code> | Cadeia de certificados |
| (Opcional) Código de acesso | n/d | Código de acesso |

Implantar appliance do vRealize Automation

O appliance do vRealize Automation é entregue como um arquivo de virtualização aberto que você implementa em uma infraestrutura virtualizada existente.

Sobre a implantação do appliance do vRealize Automation

Todas as instalações requerem primeiro um appliance do vRealize Automation implantado mas não configurado, antes de se prosseguir com uma das opções de instalação reais do vRealize Automation.

- O assistente de instalação consolidado, baseado em navegador
- Configuração separada do appliance baseado em navegador, seguida por instalações separadas do Windows para servidores IaaS
- Instalador silencioso baseado em linha de comando que aceita entrada de um arquivo de propriedades de resposta
- A API REST de instalação que aceita a entrada formatada para JSON

Implantar o appliance do vRealize Automation

Antes de executar qualquer um dos caminhos de instalação, o vRealize Automation requer a implantação de pelo menos um appliance do vRealize Automation.

Para criar o appliance, você usa o Cliente vSphere para baixar e implantar uma máquina virtual parcialmente configurada a partir de um modelo. Talvez seja necessário realizar o procedimento mais uma vez se você pretende criar uma implantação corporativa para alta disponibilidade e failover. Em geral, essa implantação tem vários appliances do vRealize Automation atrás de um balanceador de carga.

Pré-requisitos

- Faça login no Cliente vSphere com uma conta que tenha permissão para implantar modelos OVF no inventário.
- Baixe o arquivo `.ovf` ou `.ova` do appliance do vRealize Automation em um local acessível ao Cliente vSphere.

Procedimentos

- 1 Selecione a opção vSphere **Implantar modelo OVF**.
- 2 Insira o caminho no arquivo `.ovf` ou `.ova` do appliance do vRealize Automation.
- 3 Analise os detalhes do modelo.
- 4 Leia e aceite o contrato de licença do usuário final.
- 5 Digite um nome de appliance e um local de inventário.

Ao implantar appliances, use um nome diferente para cada um e não inclua caracteres não alfanuméricos, como sublinhados (`_`) nos nomes.

- 6 Selecione o host e o cluster no qual o appliance residirá.
- 7 Selecione o pool de recursos no qual o appliance residirá.
- 8 Selecione o armazenamento que hospedará o appliance.

9 Selecione um formato de disco.

Os formatos grossos melhoram o desempenho, e os formatos finos economizam espaço de armazenamento.

O formato não afeta o tamanho do disco do appliance. Se um appliance precisar de mais espaço para dados, adicione o disco usando vSphere após a implantação.

10 No menu suspenso, selecione uma Rede de destino.

11 Conclua as propriedades do appliance.

a Digite e confirme uma senha da raiz.

As credenciais da conta raiz conectam você à interface de administração baseada em navegador e hospedada pelo appliance ou ao console de linha de comando do sistema operacional do appliance.

b Selecione se você deseja ou não permitir conexões SSH remotas com o console de linha de comando.

Desativar o SSH é mais seguro, mas requer que você acesse o console diretamente no vSphere em vez de por meio de um cliente de terminal separado.

- c Para **Hostname**, insira o FQDN do appliance.

Para obter os melhores resultados, insira o FQDN, mesmo se estiver usando o DHCP.

Observação O vRealize Automation oferece suporte para DHCP, mas endereços IP estáticos são recomendados para implantações de produção.

- d Em Propriedades de Rede, ao usar endereços IP estáticos, insira os valores para gateway, máscara de rede e servidores DNS. Você também deve inserir o endereço IP, o FQDN e o domínio para o próprio appliance, conforme mostrado no exemplo a seguir.

Figura 1-13. Exemplo de propriedades do appliance virtual

| | |
|-------------------------------------|---|
| ▼ Application | 3 settings |
| Enable SSH service in the appliance | This will be used as an initial status of the SSH service in the appliance. You can change the status from the appliance Web console. <input checked="" type="checkbox"/> |
| Hostname | The host name for this virtual machine. Provide the fully qualified domain name if you use DHCP. Leave blank to try to reverse look up the IP address if you use DHCP. <input type="text" value="va1.mycompany.com"/> |
| Initial root password | This will be used as an initial password for the root user account. You can change the password using the passwd command or from the appliance Web console. Enter password <input type="password" value="*****"/> Confirm password <input type="password" value="*****"/> |
| ▼ Networking Properties | 6 settings |
| Default Gateway | The default gateway address for this VM. Leave blank if DHCP is desired. <input type="text" value="12.34.56.79"/> |
| Domain Name | The domain name of this VM. Leave blank if DHCP is desired. <input type="text" value="mycompany.com"/> |
| Domain Name Servers | The domain name server IP Addresses for this VM (comma separated). Leave blank if DHCP is desired. <input type="text" value="12.34.56.80, 12.34.56.81"/> |
| Domain Search Path | The domain search path (comma or space separated domain names) for this VM. Leave blank if DHCP is desired. <input type="text" value="mycompany.com"/> |
| Network 1 IP Address | The IP address for this interface. Leave blank if DHCP is desired. <input type="text" value="12.34.56.78"/> |
| Network 1 Netmask | The netmask or prefix for this interface. Leave blank if DHCP is desired. <input type="text" value="255.255.254.0"/> |

12 Dependendo da sua implantação, do vCenter Server e da configuração de DNS, selecione uma das seguintes maneiras de finalizar a implantação e ligar o appliance.

- Se você tiver implantado no vSphere e a opção **Ligar após a implantação** estiver disponível na página Pronto para ser Concluído, realize as etapas a seguir.
 - a Selecione **Ligar após a implantação** e clique em **Concluir**.
 - b Depois que o arquivo concluir a implantação no vCenter Server, clique em **Fechar**.
 - c Aguarde até que a máquina virtual seja iniciada, o que pode demorar até 5 minutos.
- Se você tiver implantado no vSphere e a opção **Ligar após a implantação** não estiver disponível na página Pronto para ser Concluído, realize as etapas a seguir.
 - a Depois que o arquivo concluir a implantação no vCenter Server, clique em **Fechar**.
 - b Ligue o appliance do vRealize Automation.
 - c Aguarde até que a máquina virtual seja iniciada, o que pode demorar até 5 minutos.
 - d Verifique se o appliance do vRealize Automation é implantado por ping de seu FQDN. Se você não puder executar um ping do appliance, reinicie a máquina virtual.
 - e Aguarde até que a máquina virtual seja iniciada, o que pode demorar até 5 minutos.
- Se você tiver implantado o appliance do vRealize Automation para vCloud usando o vCloud Director, o vCloud poderá substituir a senha inserida durante a implantação do OVA. Para evitar a substituição, realize as etapas a seguir.
 - a Depois de implantar no vCloud Director, clique no seu vApp para exibir o appliance do vRealize Automation.
 - b Clique com o botão direito do mouse no appliance do vRealize Automation e selecione **Propriedades**.
 - c Clique na guia **Personalização do SO Guest**.
 - d Em **Redefinição da Senha**, desmarque a opção **Permitir senha do administrador local** e clique em **OK**.
 - e Ligue o appliance do vRealize Automation.
 - f Aguarde até que a máquina virtual seja iniciada, o que pode demorar até 5 minutos.

13 Verifique se o appliance do vRealize Automation é implantado por ping de seu FQDN.

Próximo passo

- (Opcional) Adicione NICs. Consulte [Adicionar controladores de interface de rede antes de executar o instalador](#).
- Faça login na interface de administração baseada em navegador para executar o Assistente de Instalação consolidado ou configurar o appliance manualmente.
`https://vrealize-automation-appliance-FQDN:5480`
- Como alternativa, você pode ignorar o login para poder aproveitar a instalação com base em API ou silenciosa do vRealize Automation.

Adicionar controladores de interface de rede antes de executar o instalador

O vRealize Automation é compatível com vários controladores de interface de rede (NICs). Antes de executar o instalador, é possível adicionar NICs ao appliance do vRealize Automation ou ao servidor Windows do IaaS.

Se você precisar que vários NICs estejam instalados antes de executar o assistente de instalação do vRealize Automation, adicione-os após a implantação no vCenter, mas antes de iniciar o assistente. Os motivos pelos quais você pode querer NICs adicionais instalados no início incluem os seguintes exemplos:

- Você deseja redes separadas de infraestrutura e de usuário.
- É necessário um NIC adicional para que os servidores IaaS possam ingressar em um domínio do Active Directory.

Para obter mais informações sobre vários cenários de NIC, consulte esta [postagem de blog de Gerenciamento do VMware Cloud](#).

Para três ou mais NICs, esteja ciente das seguintes limitações.

- O VIDM precisa acessar o banco de dados Postgres e o Active Directory.
 - Em um cluster de alta disponibilidade, o VIDM precisa acessar a URL do balanceador de carga.
 - As conexões anteriores do VIDM devem passar pelos dois primeiros NICs.
 - Os NICs após o segundo NIC não devem ser usados ou reconhecidos pelo VIDM.
 - Os NICs após o segundo NIC não devem ser usados para se conectar ao Active Directory.
- Use o primeiro ou o segundo NIC ao configurar um diretório no vRealize Automation.

Pré-requisitos

Implante o OVF do appliance do vRealize Automation e as máquinas virtuais do Windows, mas não faça login ou inicie o assistente de instalação.

Procedimentos

- 1 No vCenter, adicione NICs em cada appliance do vRealize Automation.
 - a Clique com o botão direito do mouse no appliance recém-implantado e selecione **Editar Configurações**.
 - b Adicione NICs VMXNETn.
 - c Se estiver ligado, reinicie o appliance.

2 Faça login na linha de comando do appliance do vRealize Automation como raiz.

3 Configure os NICs executando o seguinte comando para cada NIC.

Certifique-se de incluir o endereço do gateway padrão. Você pode configurar rotas estáticas depois de concluir esse procedimento.

```
/opt/vmware/share/vami/vami_set_network network-interface (STATICV4|  
STATICV4+DHCPV6|STATICV4+AUTOV6) IPv4-address netmask gateway-v4-address
```

Por exemplo:

```
/opt/vmware/share/vami/vami_set_network eth1 STATICV4 192.168.100.20  
255.255.255.0 192.168.100.1
```

- 4 Verifique se todos os nós de vRealize Automation podem resolver uns aos outros pelo nome DNS.
- 5 Verifique se todos os nós de vRealize Automation podem acessar qualquer FQDNs de balanceamento de carga para componentes do vRealize Automation.
- 6 Se você estiver usando o Split-Brain DNS, verifique se todos os VIPs e nós de vRealize Automation têm o mesmo FQDN no DNS para cada nó IP e VIP.
- 7 No vCenter, adicione NICs aos servidores Windows do IaaS.
 - a Clique com o botão direito do mouse no servidor do IaaS e selecione **Editar Configurações**.
 - b Adicione NICs à máquina virtual do servidor do IaaS.
- 8 No Windows, configure os NICs do servidor do IaaS e seus endereços IP adicionados. Consulte a documentação da Microsoft, se necessário.

Próximo passo

- (Opcional) Se você precisar de rotas estáticas, siga as diretrizes em [Configurar rotas estáticas](#) antes de continuar com a instalação.
- Faça login na interface de administração baseada em navegador para executar o Assistente de Instalação consolidado ou configurar o appliance manualmente.
`https://vrealize-automation-appliance-FQDN:5480`
- Como alternativa, você pode ignorar o login para poder aproveitar a instalação com base em API ou silenciosa do vRealize Automation.

Instalando o vRealize Automation com o assistente de instalação

O assistente de instalação do vRealize Automation permite uma instalação simples e rápida de implantações mínimas ou corporativas.

Antes de iniciar o assistente, você implanta um appliance do vRealize Automation e configura servidores Windows IaaS para atender aos pré-requisitos. O Assistente de Instalação aparece na primeira vez que você faz login no recém-implantado appliance do vRealize Automation.

- Para parar o assistente e retornar mais tarde, clique em **Logoff**.
- Para desativar o assistente, clique em **Cancelar** ou saia e inicie a instalação manual usando as interfaces padrão.

O assistente é sua principal ferramenta para novas instalações do vRealize Automation. Se quiser expandir uma implantação do vRealize Automation existente depois de executar o assistente, consulte os procedimentos em [As interfaces de instalação padrão do vRealize Automation](#).

Usando o assistente de instalação para implantações mínimas

Implementações mínimas demonstram como o vRealize Automation funciona, mas não têm capacidade o suficiente para suportar ambientes de produção corporativos.

Instale uma implementação mínima para serviços de prova do conceito ou para se familiarizar com o vRealize Automation.

Iniciar o assistente de instalação para uma implantação mínima

Em geral, as implementações mínimas são compostas por um appliance do vRealize Automation, um servidor Windows do IaaS e o agente do vSphere para endpoints. A instalação mínima coloca todos os componentes do IaaS em um único servidor Windows.

Pré-requisitos

- Satisfaça os pré-requisitos no [Preparando para a instalação do vRealize Automation](#).
- Crie um appliance não configurado. Consulte [Implantar o appliance do vRealize Automation](#).

Procedimentos

- 1 Faça login como raiz na interface de administração do appliance do vRealize Automation.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Quando o assistente de instalação aparecer, clique em **Avançar**.
- 3 Aceite o contrato de licença e clique em **Avançar**.
- 4 Na página Tipo de Implementação, selecione **Implementação mínima e Instalar Infrastructure as a Service**, depois clique em **Avançar**.
- 5 Na página Pré-Requisitos de Instalação, pause para fazer login no servidor Windows do IaaS e instalar o Agente de Gerenciamento. O Agente de Gerenciamento permite que o appliance do vRealize Automation descubra e conecte-se ao servidor do IaaS.

Próximo passo

Instale o Agente de Gerenciamento no servidor Windows IaaS. Consulte [Instalar o Agente de gerenciamento do vRealize Automation](#).

Instalar o Agente de gerenciamento do vRealize Automation

Todos os servidores Windows IaaS requerem o Agente de gerenciamento, que os vincula a seu appliance específico do vRealize Automation.

Se você hospedar o banco de dados SQL Server do vRealize Automation em uma máquina Windows diferente, que não hospede os componentes do IaaS, o Agente de Gerenciamento não será necessário na máquina do SQL Server.

O Agente de Gerenciamento registra o servidor Windows IaaS com o appliance específico do vRealize Automation, automatiza a instalação e o gerenciamento de componentes IaaS e coleta informações de telemetria e suporte. O Agente de Gerenciamento é executado como um serviço do Windows em uma conta de domínio com direitos de administrador em servidores Windows IaaS.

Pré-requisitos

Crie um appliance do vRealize Automation e inicie o assistente de instalação.

Consulte [Implantar o appliance do vRealize Automation](#) e [Iniciar o assistente de instalação para uma implantação mínima](#).

Procedimentos

- 1 Faça login no console do appliance do vRealize Automation como raiz.
- 2 Insira o seguinte comando:

```
openssl x509 -in /opt/vmware/etc/lighttpd/server.pem -fingerprint -noout -sha1
```
- 3 Copie a impressão digital para poder verificá-la mais tarde. Por exemplo:

```
71:84:47:72:03:57:C8:C2:68:65:00:06:BC:D8:23:98:92:54:BF:89
```
- 4 Faça login no servidor Windows IaaS usando uma conta com direitos de administrador.
- 5 Abra um navegador da Web para o URL do instalador do appliance do vRealize Automation.

```
https://vrealize-automation-appliance-FQDN:5480/installer
```
- 6 Clique em **Instalador de Agente de gerenciamento**, salve e execute o arquivo .msi.
- 7 Leia as boas-vindas.
- 8 Aceite o contrato de licença de usuário final.
- 9 Aceite ou altere a pasta de instalação.

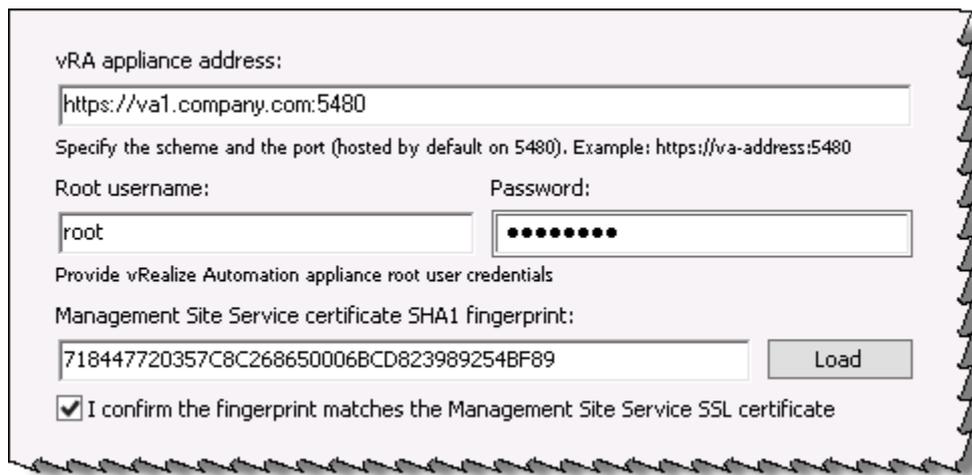
```
Program Files (x86)\VMware\VCAC\Management Agent
```

10 Insira os detalhes do appliance do vRealize Automation:

- a Insira o endereço HTTPS do dispositivo, incluindo o FQDN e o: número da porta 5480.
- b Digite as credenciais da conta raiz do appliance.
- c Clique em **Carregar** e confirme se a impressão digital corresponde à que foi copiada anteriormente. Ignore os dois pontos.

Se as impressões digitais não forem correspondentes, verifique se você possui o endereço correto do appliance.

Figura 1-14. Agente de gerenciamento – Detalhes do appliance do vRealize Automation



11 Digite o domínio/nome de usuário e senha para a conta de serviço.

A conta de serviço deve ser uma conta de domínio com direitos de administrador em servidores Windows IaaS. Use a mesma conta de serviço por toda parte.

12 Siga as instruções para concluir a instalação do Agente de gerenciamento.

Observação Como eles estão vinculados, você deve reinstalar o Agente de Gerenciamento caso substitua o appliance do vRealize Automation.

A desinstalação do IaaS de um servidor Windows não remove o Agente de Gerenciamento. Para desinstalar um Agente de Gerenciamento, use separadamente a opção Adicionar ou remover programas no Windows.

Próximo passo

Retorne ao assistente de instalação baseado no navegador. Os servidores Windows IaaS com o Agente de Gerenciamento instalado são exibidos em Hosts descobertos.

Concluindo o Assistente de Instalação

Após instalar o Agente de Gerenciamento, retorne ao assistente e siga os prompts. Se precisar de instruções adicionais sobre as configurações, clique no link Ajuda no canto superior do assistente.

- Ao concluir o assistente, a última página exibe o caminho e o nome para um arquivo de propriedades. Você pode editar esse arquivo e usá-lo para executar uma instalação silenciosa do vRealize Automation com configurações idênticas ou semelhantes da sua sessão assistente. Consulte [Instalação silenciosa do vRealize Automation](#).
- Se você criou o conteúdo inicial, poderá fazer login no locatário padrão como o usuário configurationadmin e solicitar os itens de catálogo. Para um exemplo sobre como solicitar o item e concluir a ação manual do usuário, consulte [Cenário: Solicitar conteúdo inicial para uma implementação de prova de conceito Rainpole](#).
- Para configurar o acesso ao locatário padrão para outros usuários, consulte [Configurar o acesso ao tenant padrão](#).

Usando o assistente de instalação para implantações corporativas

Você pode personalizar a implantação corporativa de acordo com as necessidades da organização. Uma implantação corporativa pode consistir em componentes distribuídos ou em implantações de alta disponibilidade configuradas com balanceadores de carga.

As implantações corporativas são projetadas para estruturas de instalação mais complexas com componentes distribuídos e redundantes e normalmente incluem balanceadores de carga. A instalação de componentes do IaaS é opcional para qualquer tipo de implantação.

Para implantações com balanceamento de carga, várias instâncias de servidor Web ativas e appliances do appliance do vRealize Automation fazem a instalação falhar. Apenas uma instância do servidor Web e um único appliance do vRealize Automation devem estar ativos durante a instalação.

Inicie o assistente de instalação para uma implantação corporativa

Implantações corporativas são grandes o suficiente para ambientes de produção. Você pode usar o assistente de instalação para implantar uma instalação distribuída ou uma instalação distribuída com balanceadores de carga para alta disponibilidade e failover.

Se você implantar uma instalação distribuída com balanceadores de carga, notifique a equipe responsável pela configuração do seu ambiente vRealize Automation. Seus administradores de locatário devem configurar o Gerenciamento de Diretórios para alta disponibilidade ao configurarem o link para o Active Directory.

Pré-requisitos

- Satisfaça os pré-requisitos no [Preparando para a instalação do vRealize Automation](#).
- Crie um appliance não configurado. Consulte [Implantar o appliance do vRealize Automation](#).

Procedimentos

- 1 Faça login como raiz na interface de administração do appliance do vRealize Automation.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Quando o assistente de instalação aparecer, clique em **Avançar**.
- 3 Aceite o Contrato de Licença de Usuário Final e clique em **Avançar**.

- 4 Na página Tipo de Implantação, selecione **Implantação corporativa e Instalar Infrastructure as a Service**.
- 5 Na página Pré-Requisitos de Instalação, pause para fazer login nos servidores Windows do IaaS e instalar o Agente de Gerenciamento. O Agente de Gerenciamento permite que o appliance do vRealize Automation descubra e conecte-se a esses servidores de IaaS.

Próximo passo

Instale o Agente de Gerenciamento nos seus servidores Windows IaaS. Consulte [Instalar o Agente de Gerenciamento do vRealize Automation](#).

Instalar o Agente de Gerenciamento do vRealize Automation

Todos os servidores Windows IaaS requerem o Agente de Gerenciamento, que os vincula a seu appliance específico do vRealize Automation.

Se você hospedar o banco de dados SQL Server do vRealize Automation em uma máquina Windows diferente, que não hospede os componentes do IaaS, o Agente de Gerenciamento não será necessário na máquina do SQL Server.

O Agente de Gerenciamento registra o servidor Windows IaaS com o appliance específico do vRealize Automation, automatiza a instalação e o gerenciamento de componentes IaaS e coleta informações de telemetria e suporte. O Agente de Gerenciamento é executado como um serviço do Windows em uma conta de domínio com direitos de administrador em servidores Windows IaaS.

Pré-requisitos

Crie um appliance do vRealize Automation e inicie o assistente de instalação.

Consulte [Implantar o appliance do vRealize Automation](#) e [Inicie o assistente de instalação para uma implantação corporativa](#).

Procedimentos

- 1 Faça login no console do appliance do vRealize Automation como raiz.
- 2 Insira o seguinte comando:

```
openssl x509 -in /opt/vmware/etc/lighttpd/server.pem -fingerprint -noout -sha1
```
- 3 Copie a impressão digital para poder verificá-la mais tarde. Por exemplo:

```
71:84:47:72:03:57:C8:C2:68:65:00:06:BC:D8:23:98:92:54:BF:89
```
- 4 Faça login no servidor Windows IaaS usando uma conta com direitos de administrador.
- 5 Abra um navegador da Web para o URL do instalador do appliance do vRealize Automation.

```
https://vrealize-automation-appliance-FQDN:5480/installer
```
- 6 Clique em **Instalador de Agente de Gerenciamento**, salve e execute o arquivo .msi.
- 7 Leia as boas-vindas.
- 8 Aceite o contrato de licença de usuário final.

9 Aceite ou altere a pasta de instalação.

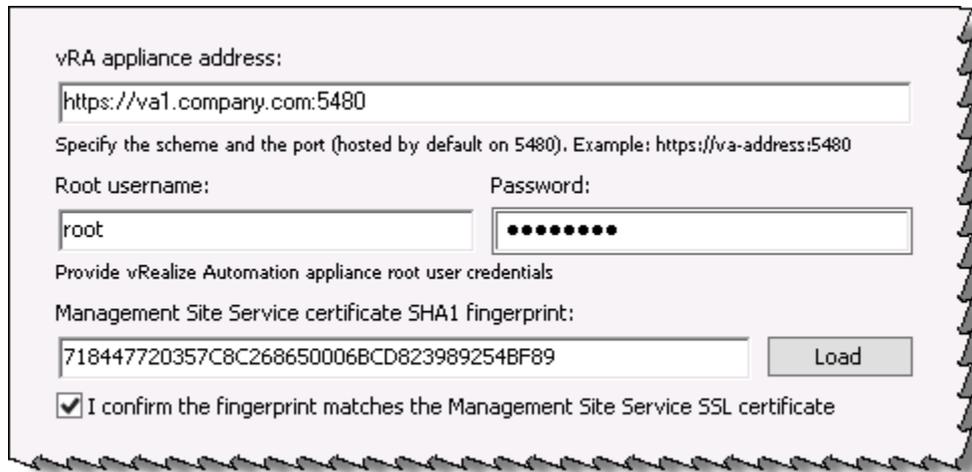
Program Files (x86)\VMware\VCAC\Management Agent

10 Insira os detalhes do appliance do vRealize Automation:

- a Insira o endereço HTTPS do dispositivo, incluindo o FQDN e o número da porta 5480.
- b Digite as credenciais da conta raiz do appliance.
- c Clique em **Carregar** e confirme se a impressão digital corresponde à que foi copiada anteriormente. Ignore os dois pontos.

Se as impressões digitais não forem correspondentes, verifique se você possui o endereço correto do appliance.

Figura 1-15. Agente de gerenciamento – Detalhes do appliance do vRealize Automation



11 Digite o domínio/nome de usuário e senha para a conta de serviço.

A conta de serviço deve ser uma conta de domínio com direitos de administrador em servidores Windows IaaS. Use a mesma conta de serviço por toda parte.

12 Siga as instruções para concluir a instalação do Agente de Gerenciamento.

Repita o procedimento para todos os servidores Windows que hospedarão componentes IaaS.

Observação Como eles estão vinculados, você deve reinstalar o Agente de Gerenciamento caso substitua o appliance do vRealize Automation.

A desinstalação do IaaS de um servidor Windows não remove o Agente de Gerenciamento. Para desinstalar um Agente de Gerenciamento, use separadamente a opção Adicionar ou remover programas no Windows.

Próximo passo

Retorne ao assistente de instalação baseado no navegador. Os servidores Windows IaaS com o Agente de Gerenciamento instalado são exibidos em Hosts descobertos.

Concluindo o Assistente de Instalação

Após instalar o Agente de Gerenciamento, retorne ao assistente e siga os prompts. Se precisar de instruções adicionais sobre as configurações, clique no link Ajuda no canto superior do assistente.

- Ao concluir o assistente, a última página exibe o caminho e o nome para um arquivo de propriedades. Você pode editar esse arquivo e usá-lo para executar uma instalação silenciosa do vRealize Automation com configurações idênticas ou semelhantes da sua sessão assistente. Consulte [Instalação silenciosa do vRealize Automation](#).
- Se você criou o conteúdo inicial, poderá fazer login no locatário padrão como o usuário configurationadmin e solicitar os itens de catálogo. Para um exemplo sobre como solicitar o item e concluir a ação manual do usuário, consulte [Cenário: Solicitar conteúdo inicial para uma implementação de prova de conceito Rainpole](#).
- Para configurar o acesso ao locatário padrão para outros usuários, consulte [Configurar o acesso ao tenant padrão](#).

Avançar pelas etapas do Assistente de Instalação do vRealize Automation

O Assistente de Instalação do vRealize Automation apresenta páginas de fácil uso nas quais você verifica pré-requisitos, insere configurações, valida configurações e instala componentes do vRealize Automation.

Observação O assistente inclui etapas em que você pausa para fazer login em outros sistemas, como balanceadores de carga ou servidores Windows IaaS.

Pré-requisitos

- Crie um ou mais appliance(s) não configurado(s). Consulte [Implantar o appliance do vRealize Automation](#).

Implantações mínimas usam um appliance do vRealize Automation. Implantações corporativas podem ter vários appliances atrás do balanceamento de carga.
- Tenha um ou mais sistemas Windows disponíveis para hospedar componentes do IaaS.
- Inicie o assistente fazendo login como raiz na interface de administração de appliance do vRealize Automation.

`https://vrealize-automation-appliance-FQDN:5480`

Procedimentos

1 Tipo de implantação

Na página Tipo de implantação, decida quais componentes do vRealize Automation, e quantos de cada, você deseja instalar.

2 Pré-requisitos da instalação

Na página Pré-requisitos da instalação, pause para estabelecer uma conexão com as máquinas Windows que hospedarão o IaaS. do vRealize Automation Além disso, selecione uma fonte de sincronização de hora.

3 [vRealize Appliances](#)

(Somente implantações corporativas) Na página vRealize Appliances, você tem a opção de criar uma implantação de alta disponibilidade com vários appliances do vRealize Automation.

4 [Funções de Servidor](#)

(Somente para implantações empresariais) Na página Funções de Servidor, você atribui funções de componente do vRealize Automation IaaS às máquinas do Windows onde instalou o Agente de gerenciamento anteriormente.

5 [Verificador de pré-requisitos](#)

Na página Verificador de pré-requisitos, verifique e corrija os servidores Windows do vRealize Automation para oferecer suporte à instalação do IaaS.

6 [Host do vRealize Automation](#)

Na página Host do vRealize Automation, defina o endereço da URL de base para o vRealize Automation. O endereço costuma ser o appliance do vRealize Automation ou, em ambientes de alta disponibilidade, um balanceador de carga.

7 [Single Sign On](#)

Na página Single Sign On, defina o log de administrador do sistema tenant padrão do vRealize Automation nas credenciais.

8 [Host do IaaS](#)

Na página Host do IaaS, você define os endereços de URL base para certos componentes do IaaS. Além disso, você cria uma senha de segurança para o banco de dados SQL do vRealize Automation IaaS.

9 [Microsoft SQL Server](#)

Na página Microsoft SQL Server, configure o banco de dados SQL IaaS do vRealize Automation. O banco de dados IaaS registra as máquinas provisionadas, os elementos associados e as políticas.

10 [Função da Web](#)

(Somente implantações corporativas) Na página Função da Web, configure separadamente o site da Web do vRealize Automation IaaS no IIS.

11 [Função do Manager Service](#)

(Somente implantações corporativas) Na página Função do Manager Service, configure a máquina Windows vRealize Automation separada que hospeda o Manager Service IaaS.

12 [Distributed Execution Managers](#)

Na página Distributed Execution Managers, configure as máquinas Windows do vRealize Automation que hospedam os DEMs do IaaS. Vários hosts DEM são suportados.

13 [Agentes](#)

Na página Agentes, crie a ligação entre o vRealize Automation IaaS e os recursos de virtualização para os quais a infraestrutura está implantada. Selecione um tipo de agente e preencha os detalhes para o endpoint correspondente.

14 [Certificado do vRealize Appliance](#)

Na página Certificado do vRealize Appliance, crie ou selecione o certificado de autenticação usado pelo appliance do vRealize Automation. Quando o certificado é autoassinado, os usuários finais podem ver e confirmar esse certificado quando fazem login no vRealize Automation em um navegador.

15 [Certificado Web](#)

Na página Certificado Web, crie ou selecione o certificado de autenticação usado pelo servidor Web do IaaS. O appliance do vRealize Automation se conecta ao servidor Web e precisa se autenticar e confiar nele.

16 [Certificado do Manager Service](#)

(Somente implantações corporativas) Na página Certificado do Manager Service, crie ou selecione o certificado de autenticação usado pelo host do Manager Service IaaS do vRealize Automation. Os outros servidores Windows IaaS se conectam ao host do Manager Service e precisam se autenticar e confiar nele.

17 [Balanceadores de Carga](#)

(Somente para implantações empresariais) Na página Balanceadores de Carga, pause para configurar os balanceadores de carga do pool correto dos sistemas membro do vRealize Automation.

18 [Validação](#)

Na página Validação, você verifica se a instalação de vRealize Automation pode continuar.

19 [Criar snapshots](#)

Na página Criar Snapshots, pause para criar snapshots de máquina virtual de todos os componentes do vRealize Automation antes de prosseguir com a instalação.

20 [Detalhes da instalação](#)

Na página Detalhes da instalação, inicie a instalação do vRealize Automation ou tente novamente se ocorrer algum problema.

21 [Licenciamento](#)

Na página Licenciamento, insira uma chave para ativar o produto vRealize Automation instalado.

22 [Telemetria](#)

Na página Telemetria, você decide se o vRealize Automation deve ou não enviar estatísticas de uso para a VMware como parte do Programa de Aperfeiçoamento da Experiência do Cliente.

23 [Opções após a instalação](#)

Na página Opções após a instalação, você pode criar novos dados do vRealize Automation ou migrar os dados da implantação antiga para a nova instalação.

24 [Configuração de conteúdo inicial](#)

Na página Configuração de conteúdo inicial, crie um novo usuário local de tenant padrão do vRealize Automation que possa iniciar um fluxo de trabalho de conteúdo para um endpoint do vSphere.

25 Configuração da migração

Na página Configuração da migração, você pode iniciar a transferência de outra implantação mais antiga do vRealize Automation para a implantação recém-instalada.

Tipo de implantação

Na página Tipo de implantação, decida quais componentes do vRealize Automation, e quantos de cada, você deseja instalar.

Mínima

As implantações mínimas usam apenas um appliance do vRealize Automation e um servidor Windows que hospeda os componentes do IaaS. Nas implantações mínimas, você pode hospedar o banco de dados do IaaS em um sistema SQL Server separado ou instalar o SQL no servidor Windows do IaaS.

Não é possível converter uma implantação mínima em uma implantação corporativa. Para expandir uma implantação, comece com uma pequena implantação corporativa e adicione componentes a ela. Não é possível iniciar com uma implantação mínima.

Corporativa

As implantações corporativas incluem vários hosts do Windows e appliances separados, geralmente com balanceamento de carga. As implantações corporativas também permitem que você hospede o banco de dados do IaaS em um sistema SQL Server separado ou em um dos servidores Windows do IaaS.

Quando você seleciona uma implantação corporativa, aparecem outras páginas do Assistente de Instalação na lista de resumo, na parte esquerda do assistente.

Infraestrutura como Serviço

A opção Infraestrutura como Serviço (IaaS) seleciona se as máquinas Windows existentes devem ou não ser configuradas com recursos de modelagem e provisionamento do vRealize Automation.

Quando você seleciona IaaS, aparecem outras páginas do Assistente de Instalação na lista de resumo, na parte esquerda do assistente.

Pré-requisitos da instalação

Na página Pré-requisitos da instalação, pause para estabelecer uma conexão com as máquinas Windows que hospedarão o IaaS. Além disso, selecione uma fonte de sincronização de hora.

Servidores Windows do IaaS

Para que uma máquina Windows sirva como um host de componente do IaaS, você deve baixar e instalar vCAC-IaaSManagementAgent-Setup.msi na máquina Windows.

A instalação do Agente de gerenciamento requer comunicação com um appliance do vRealize Automation em execução. Cada vez que você instala o Agente de Gerenciamento no Windows, esse sistema fica exclusivamente vinculado ao appliance e à implantação em questão.

Os possíveis servidores Windows IaaS que tenham o Agente de Gerenciamento correto instalado aparecem em **Hosts Descobertos**.

Para que o Assistente de Instalação ignore um host descoberto, clique em **Excluir**. A exclusão de um host Windows não remove seu Agente de Gerenciamento. Para desinstalar o agente, use o recurso Adicionar ou Remover Programas diretamente no Windows.

Fonte de horário

Você deve sincronizar cada appliance do vRealize Automation e o servidor Windows do IaaS com a mesma fonte de horário. As seguintes fontes são permitidas:

- Usar Horário do Host - Faz a sincronização com o host ESXi do appliance do vRealize Automation.
- Usar Servidor de Horário - Faz a sincronização com um servidor NTP (Network Time Protocol) externo. Insira o endereço IP ou o FQDN do servidor NTP.

Não misture fontes de horário em uma implantação do vRealize Automation.

vRealize Appliances

(Somente implantações corporativas) Na página vRealize Appliances, você tem a opção de criar uma implantação de alta disponibilidade com vários appliances do vRealize Automation.

Vários appliances devem ser hospedados atrás de um balanceador de carga que você instalou separadamente. Em uma página posterior do assistente, verifique e conclua a configuração dos appliances e do balanceador de carga. Para cada appliance do vRealize Automation que você adicionar, insira as credenciais raiz e de FQDN.

Funções de Servidor

(Somente para implantações empresariais) Na página Funções de Servidor, você atribui funções de componente do vRealize Automation IaaS às máquinas do Windows onde instalou o Agente de gerenciamento anteriormente.

As máquinas do Windows do IaaS servem com servidores da web primários e adicionais, como hosts do Serviço de gerenciador, hosts DEM e hosts do Agente. Para obter mais funções de componente do IaaS, consulte [Infraestrutura como Serviço](#).

A separação de funções de servidor do IaaS é somente possível em implantações empresariais. Em implantações mínimas, uma máquina do Windows executa todas as funções.

Verificador de pré-requisitos

Na página Verificador de pré-requisitos, verifique e corrija os servidores Windows do vRealize Automation para oferecer suporte à instalação do IaaS.

O verificador de pré-requisitos inspeciona as máquinas do Windows onde você instalou o Agente de Gerenciamento e onde hospedará os componentes do IaaS. Os pré-requisitos incluem Java, configurações do Internet Information Services (IIS), o serviço de Coordenador de Transações Distribuídas (DTC) Microsoft, entre outros. Para ver uma lista detalhada de pré-requisitos, clique em **Exibir detalhes**.

O Assistente de Instalação permite proceder sem verificar os pré-requisitos, mas saiba que a instalação poderá falhar.

- Para verificar os pré-requisitos, clique em **Executar**.

- Se os pré-requisitos estiverem ausentes, clique em **Exibir detalhes** para aprender mais e, em seguida, clique em **Corrigir**.

O Assistente de Instalação pode corrigir a maioria dos pré-requisitos baseados em software ou configuração. Após fazer as alterações, o Assistentes de Instalação reinicia seus hosts do IaaS.

O assistente não pode corrigir problemas de memória ou CPU insuficiente. Se esses problemas ocorrerem, eles deverão ser corrigidos no vSphere ou no seu hardware, caso venham a ocorrer.

Host do vRealize Automation

Na página Host do vRealize Automation, defina o endereço da URL de base para o vRealize Automation. O endereço costuma ser o appliance do vRealize Automation ou, em ambientes de alta disponibilidade, um balanceador de carga.

- Ao implantar apenas um appliance do vRealize Automation sem balanceador de carga, insira o FQDN do appliance do vRealize Automation. Você pode selecionar uma opção para que o Assistente de Instalação preencha o FQDN para você.
- Em vez disso, ao implantar uma configuração corporativa que inclua um ou mais appliances do vRealize Automation atrás do balanceamento de carga, insira o FQDN do balanceador de carga.

Um único appliance do vRealize Automation ainda pode ser implantado atrás de um balanceador de carga. Essa abordagem permite que você adicione outros appliances de forma mais fácil, para expandir a implantação.

Single Sign On

Na página Single Sign On, defina o log de administrador do sistema tenant padrão do vRealize Automation nas credenciais.

O administrador do sistema tenant padrão tem a maioria das permissões de qualquer usuário, incluindo a criação de tenants adicionais. As credenciais do administrador do sistema tenant padrão são separadas das credenciais de raiz do appliance do vRealize Automation.

Host do IaaS

Na página Host do IaaS, você define os endereços de URL base para certos componentes do IaaS. Além disso, você cria uma senha de segurança para o banco de dados SQL do vRealize Automation IaaS.

Implementações mínimas

| Configuração | Descrição |
|--------------------------------|--|
| Endereço Web do IaaS | Insira o FQDN do servidor Windows do IaaS. |
| Instale os componentes do IaaS | Selecione ou insira o FQDN do servidor Windows do IaaS. |
| Nome de usuário | No formato DOMÍNIO\nome de usuário, insira a conta de serviço. A conta deve ser uma conta de domínio com privilégios de administrador local no servidor Windows do IaaS. |
| Senha | Insira a senha da conta. |

| Configuração | Descrição |
|--------------------|---|
| Senha de segurança | <p>Cria uma senha para criptografar dados no banco de dados SQL do IaaS.</p> <ul style="list-style-type: none"> ■ Grave a senha, pois ela será necessária para restaurar o banco de dados se houver uma falha ou para adicionar componentes após a instalação inicial. ■ A senha não pode conter um caractere de citação dupla ("). |
| Confirme a senha | Insira a senha novamente. |

Implantações corporativas

| Configuração | Descrição |
|------------------------------------|---|
| Endereço Web do IaaS | Insira o FQDN primário do servidor da web do IaaS. Se estiver implantando uma configuração corporativa que inclua vários servidores da web do IaaS com carga balanceada, insira o FQDN do balanceador de carga no lugar. |
| Endereço do Serviço de Gerenciador | Insira o FQDN primário do host do Serviço de Gerenciador. Se estiver implantando uma configuração corporativa que inclua vários hosts do Serviço de Gerenciador com carga balanceada, insira o FQDN do balanceador de carga no lugar. |
| Senha de segurança | <p>Cria uma senha para criptografar dados no banco de dados SQL do IaaS.</p> <ul style="list-style-type: none"> ■ Grave a senha, pois ela será necessária para restaurar o banco de dados se houver uma falha ou para adicionar componentes após a instalação inicial. ■ A senha não pode conter um caractere de citação dupla ("). |
| Confirme a senha | Insira a senha novamente. |

Microsoft SQL Server

Na página Microsoft SQL Server, configure o banco de dados SQL IaaS do vRealize Automation. O banco de dados IaaS registra as máquinas provisionadas, os elementos associados e as políticas.

| Configuração | Descrição |
|---------------------------------------|--|
| Nome do servidor | <p>Insira o FQDN do host do SQL Server, que pode ser um servidor Windows IaaS ou um servidor separado.</p> <p>Se você precisar especificar um número de porta ou uma instância nomeada, use o formato FQDN,Port\Instance.</p> <p>Ao usar o Grupo de Disponibilidade AlwaysOn (AAG) do SQL, especifique o FQDN do ouvinte AAG.</p> |
| Nome do banco de dados | Aceite o padrão do vra , ou insira um nome diferente para o banco de dados IaaS. |
| Criar um novo banco de dados | <p>Permita que o Assistente de Instalação crie o banco de dados.</p> <p>Para que essa opção funcione, a conta que executa o Agente de Gerenciamento no servidor Web IaaSPrincipal deve ter a função sysadmin no SQL.</p> |
| Usar o banco de dados vazio existente | <p>Não permita que o Assistente de Instalação crie o banco de dados.</p> <p>Quando você cria um banco de dados separado, as credenciais de usuário Windows ou usuário SQL que você informa precisam da permissão dbo no banco de dados.</p> |
| Configurações padrão | <p>(Somente para banco de dados novo) Desmarque essa opção se você quiser usar um local de armazenamento alternativo para os arquivos de log e dados do IaaS.</p> <p>Quando estiver desmarcada, insira os diretórios para dados (MDF) e logs. Sua conta do serviço SQL Server deve ter permissão de gravação para os diretórios.</p> |

| Configuração | Descrição |
|--|---|
| Usar SSL para conexão com o banco de dados | Criptografe as conexões com o banco de dados. Para usar essa opção, você deve configurar um host separado do SQL Server para SSL. Além disso, o servidor Web IaaS e o host do Manager Service devem confiar no certificado SSL do host do SQL Server. |
| Autenticação do Windows | Desmarque essa opção apenas se quiser usar a autenticação SQL no lugar da autenticação do Windows. Quando estiver desmarcada, insira as credenciais de autenticação SQL. |
| Caminho de instalação | Deixe esta opção desmarcada para aceitar o padrão %ProgramFiles(x86)%\VMware ou insira um local alternativo. <ul style="list-style-type: none"> ■ Os arquivos do vRealize Automation não estão instalados no host do SQL Server. Eles são colocados no servidor Web IaaS principal. ■ Se você instalar vários componentes IaaS na mesma máquina Windows, instale-os no mesmo caminho de instalação. |

Função da Web

(Somente implantações corporativas) Na página Função da Web, configure separadamente o site da Web do vRealize Automation IaaS no IIS.

Em um ambiente corporativo, especifique separadamente a máquina Windows IaaS que hospeda o componente da Web. Para alta disponibilidade, vários hosts são suportados.

| Configuração | Descrição | |
|---------------------|--|---|
| Nome do site na Web | Personalize o nome ou deixe como o site padrão IIS. Evite hospedar outros sites da Web no IIS. O vRealize Automation define a associação na sua porta de comunicação com todos os endereços IP não atribuídos, impossibilitando associações adicionais. | |
| Porta | Personalize a porta ou aceite a porta padrão 443. | |
| Servidores Web IaaS | Nome do Host IaaS | Insira o FQDN de cada máquina Windows IaaS que hospeda o componente Web do IaaS. |
| | Nome de usuário | No formato DOMÍNIO\nome de usuário, insira a conta de serviço. A conta deve ser uma conta de domínio com privilégios de administrador local no servidor Windows do IaaS. |
| | Senha | Insira a senha da conta. |
| | Caminho de instalação | Deixe esta opção desmarcada para aceitar o padrão %ProgramFiles(x86)%\VMware ou insira um local alternativo. Se você instalar vários componentes IaaS na mesma máquina Windows, instale-os no mesmo caminho de instalação. |

Função do Manager Service

(Somente implantações corporativas) Na página Função do Manager Service, configure a máquina Windows vRealize Automation separada que hospeda o Manager Service IaaS.

Em uma implantação corporativa, especifique separadamente o host do Manager Service, que é um serviço Windows. Para alta disponibilidade, vários hosts são suportados.

| Configuração | Descrição |
|-----------------------|---|
| Ativo | <p>Selecione o host principal do Manager Service. Os outros hosts servem como backups do principal.</p> <p>Quando você faz a instalação usando o Assistente de Instalação, o serviço faz um failover transparente para um backup se ocorrer algum problema. Consulte Sobre o failover automático do Serviço de Gerenciador.</p> |
| Nome do Host IaaS | Insira o FQDN de cada máquina Windows IaaS que hospeda o Manager Service. |
| Nome de usuário | No formato DOMÍNIO\nome de usuário, insira a conta de serviço. A conta deve ser uma conta de domínio com privilégios de administrador local no servidor Windows do IaaS. |
| Senha | Insira a senha da conta. |
| Caminho de instalação | <p>Deixe esta opção desmarcada para aceitar o padrão %ProgramFiles(x86)%\VMware ou insira um local alternativo.</p> <p>Se você instalar vários componentes IaaS na mesma máquina Windows, instale-os no mesmo caminho de instalação.</p> |

Distributed Execution Managers

Na página Distributed Execution Managers, configure as máquinas Windows do vRealize Automation que hospedam os DEMs do IaaS. Vários hosts DEM são suportados.

| Configuração | Descrição |
|------------------------|--|
| Nome do Host IaaS | Insira o FQDN de cada máquina Windows IaaS que hospeda um DEM. |
| Nome da instância | Insira um identificador exclusivo para cada DEM. Todos os nomes DEM devem ser exclusivos, estejam eles no mesmo host ou em hosts diferentes. |
| Nome de usuário | No formato DOMÍNIO\nome de usuário, insira a conta de serviço. A conta deve ser uma conta de domínio com privilégios de administrador local no servidor Windows do IaaS. |
| Senha | Insira a senha da conta. |
| Descrição da instância | Se necessário, insira uma explicação dos fluxos de trabalho associados a cada DEM. |
| Caminho de instalação | <p>Deixe esta opção desmarcada para aceitar o padrão %ProgramFiles(x86)%\VMware ou insira um local alternativo.</p> <p>Se você instalar vários componentes IaaS na mesma máquina Windows, instale-os no mesmo caminho de instalação.</p> |

Agentes

Na página Agentes, crie a ligação entre o vRealize Automation IaaS e os recursos de virtualização para os quais a infraestrutura está implantada. Selecione um tipo de agente e preencha os detalhes para o endpoint correspondente.

- Vários agentes de tipos iguais ou diferentes são suportados.
- Você pode instalar agentes no mesmo servidor ou em servidores separados.

- Quando for no mesmo servidor, até 25 agentes de qualquer tipo são suportados.
- Quando vários agentes do mesmo tipo estão no mesmo servidor, cada um deve ter um nome exclusivo e um endpoint diferente.
- Para alta disponibilidade, você pode instalar um agente do mesmo tipo, nome e endpoint em servidores separados.
- O vSphere é geralmente um dos tipos de agentes.
- Você pode adicionar agentes pós-instalação.

Tipos de Agente

Tabela 1-20. vSphere

| Configuração | Descrição |
|-----------------------|---|
| Tipo de agente | Na lista suspensa, selecione vSphere. |
| Nome do Host IaaS | Na lista suspensa, selecione o FQDN da máquina Windows do IaaS que hospeda o agente. |
| Nome do agente | Insira um identificador exclusivo, a menos que você esteja adicionando o mesmo nome de agente e endpoint em servidores separados para alta disponibilidade. |
| Endpoint | Insira um nome para o endpoint do vSphere. |
| Caminho de instalação | Deixe esta opção desmarcada para aceitar o padrão %ProgramFiles(x86)%\VMware ou insira um local alternativo. Se você instalar vários componentes IaaS na mesma máquina Windows, instale-os no mesmo caminho de instalação. |
| Nome de usuário | No formato DOMÍNIO\nome de usuário, insira a conta de serviço. A conta deve ser uma conta de domínio com privilégios de administrador local no servidor Windows do IaaS. |
| Senha | Insira a senha da conta. |

Tabela 1-21. EPI PowerShell

| Configuração | Descrição |
|-----------------------|---|
| Tipo de agente | Na lista suspensa, selecione EpiPowerShell. |
| Nome do Host IaaS | Na lista suspensa, selecione o FQDN da máquina Windows do IaaS que hospeda o agente. |
| Nome do agente | Insira um identificador exclusivo, a menos que você esteja adicionando o mesmo nome de agente e endpoint em servidores separados para alta disponibilidade. |
| Tipo | Na lista suspensa, selecione qual marca de provisionamento o endpoint EPIServer está hospedando. |
| Servidor | Insira o FQDN do EPIServer. |
| Caminho de instalação | Deixe esta opção desmarcada para aceitar o padrão %ProgramFiles(x86)%\VMware ou insira um local alternativo. Se você instalar vários componentes IaaS na mesma máquina Windows, instale-os no mesmo caminho de instalação. |

Tabela 1-21. EPI PowerShell (Continuação)

| Configuração | Descrição |
|-----------------|--|
| Nome de usuário | No formato DOMÍNIO\nome de usuário, insira a conta de serviço. A conta deve ser uma conta de domínio com privilégios de administrador local no servidor Windows do IaaS. |
| Senha | Insira a senha da conta. |

Tabela 1-22. HyperV

| Configuração | Descrição |
|-----------------------|---|
| Tipo de agente | Na lista suspensa, selecione HyperV. |
| Nome do Host IaaS | Na lista suspensa, selecione o FQDN da máquina Windows do IaaS que hospeda o agente. |
| Nome do agente | Insira um identificador exclusivo, a menos que você esteja adicionando o mesmo nome de agente e endpoint em servidores separados para alta disponibilidade. |
| Nome de usuário | Insira a conta de login para a instância de endpoint HyperV. |
| Senha | Insira a senha da conta. |
| Caminho de instalação | Deixe esta opção desmarcada para aceitar o padrão %ProgramFiles(x86)%\VMware ou insira um local alternativo. Se você instalar vários componentes IaaS na mesma máquina Windows, instale-os no mesmo caminho de instalação. |
| Nome de usuário | No formato DOMÍNIO\nome de usuário, insira a conta de serviço. A conta deve ser uma conta de domínio com privilégios de administrador local no servidor Windows do IaaS. |
| Senha | Insira a senha da conta. |

Tabela 1-23. PowerShell de VDI

| Configuração | Descrição |
|-----------------------|---|
| Tipo de agente | Na lista suspensa, selecione VdiPowerShell. |
| Nome do Host IaaS | Na lista suspensa, selecione o FQDN da máquina Windows do IaaS que hospeda o agente. |
| Nome do agente | Insira um identificador exclusivo, a menos que você esteja adicionando o mesmo nome de agente e endpoint em servidores separados para alta disponibilidade. |
| Tipo | O tipo de endpoint padrão é XenDesktop e não pode ser mudado. |
| Servidor | Insira o FQDN do endpoint XenDesktop. |
| Versão XenDesktop | Na lista suspensa, selecione a versão. |
| Caminho de instalação | Deixe esta opção desmarcada para aceitar o padrão %ProgramFiles(x86)%\VMware ou insira um local alternativo. Se você instalar vários componentes IaaS na mesma máquina Windows, instale-os no mesmo caminho de instalação. |

Tabela 1-23. PowerShell de VDI (Continuação)

| Configuração | Descrição |
|-----------------|--|
| Nome de usuário | No formato DOMÍNIO\nome de usuário, insira a conta de serviço. A conta deve ser uma conta de domínio com privilégios de administrador local no servidor Windows do IaaS. |
| Senha | Insira a senha da conta. |

Tabela 1-24. Xen

| Configuração | Descrição |
|-----------------------|---|
| Tipo de agente | Na lista suspensa, selecione Xen. |
| Nome do Host IaaS | Na lista suspensa, selecione o FQDN da máquina Windows do IaaS que hospeda o agente. |
| Nome do agente | Insira um identificador exclusivo, a menos que você esteja adicionando o mesmo nome de agente e endpoint em servidores separados para alta disponibilidade. |
| Nome de usuário | Insira a conta de login para a instância de endpoint Xen. |
| Senha | Insira a senha da conta. |
| Caminho de instalação | Deixe esta opção desmarcada para aceitar o padrão %ProgramFiles(x86)%\VMware ou insira um local alternativo. Se você instalar vários componentes IaaS na mesma máquina Windows, instale-os no mesmo caminho de instalação. |
| Nome de usuário | No formato DOMÍNIO\nome de usuário, insira a conta de serviço. A conta deve ser uma conta de domínio com privilégios de administrador local no servidor Windows do IaaS. |
| Senha | Insira a senha da conta. |

Tabela 1-25. WMI

| Configuração | Descrição |
|-----------------------|---|
| Tipo de agente | Na lista suspensa, selecione WMI. |
| Nome do Host IaaS | Na lista suspensa, selecione o FQDN da máquina Windows do IaaS que hospeda o agente. |
| Nome do agente | Insira um identificador exclusivo, a menos que você esteja adicionando o mesmo nome de agente e endpoint em servidores separados para alta disponibilidade. |
| Caminho de instalação | Deixe esta opção desmarcada para aceitar o padrão %ProgramFiles(x86)%\VMware ou insira um local alternativo. Se você instalar vários componentes IaaS na mesma máquina Windows, instale-os no mesmo caminho de instalação. |
| Nome de usuário | No formato DOMÍNIO\nome de usuário, insira a conta de serviço. A conta deve ser uma conta de domínio com privilégios de administrador local no servidor Windows do IaaS. |
| Senha | Insira a senha da conta. |

Tabela 1-26. Testar

| Configuração | Descrição |
|-----------------------|---|
| Tipo de agente | Na lista suspensa, selecione Testar. |
| Nome do Host IaaS | Na lista suspensa, selecione o FQDN da máquina Windows do IaaS que hospeda o agente. |
| Nome do agente | Insira um identificador exclusivo, a menos que você esteja adicionando o mesmo nome de agente e endpoint em servidores separados para alta disponibilidade. |
| Caminho de instalação | Deixe esta opção desmarcada para aceitar o padrão %ProgramFiles(x86)%\VMware ou insira um local alternativo. Se você instalar vários componentes IaaS na mesma máquina Windows, instale-os no mesmo caminho de instalação. |
| Nome de usuário | No formato DOMÍNIO\nome de usuário, insira a conta de serviço. A conta deve ser uma conta de domínio com privilégios de administrador local no servidor Windows do IaaS. |
| Senha | Insira a senha da conta. |

Certificado do vRealize Appliance

Na página Certificado do vRealize Appliance, crie ou selecione o certificado de autenticação usado pelo appliance do vRealize Automation. Quando o certificado é autoassinado, os usuários finais podem ver e confirmar esse certificado quando fazem login no vRealize Automation em um navegador.

| Configuração | Descrição | |
|---------------------|---------------------------------|--|
| Ação do certificado | Manter Existentes | Use o certificado que já está neste appliance do vRealize Automation. Verifique os detalhes nas entradas abaixo, como o número de série e a impressão digital. |
| | Gerar Certificado | Use o assistente para gerar um certificado auto-assinado do appliance do vRealize Automation. |
| | Gerar solicitação de assinatura | Crie um arquivo de solicitação de assinatura de certificado (CSR) para a sua autoridade de certificação (CA). Uma CSR ajuda sua CA a criar um certificado com os valores corretos para você importar. <ol style="list-style-type: none"> 1 Insira a Organização, a Unidade Organizacional e o Código do País (veja abaixo). 2 Clique em Gerar solicitação de assinatura. 3 Para baixar o arquivo CSR para a sua CA, clique no link que aparece. |
| | Importar | Identifique um arquivo de certificado no formato PEM, use o assistente para adicioná-lo ao armazenamento correto e carregue-o para ser usado pelo vRealize Automation. A não ser que você esteja importando um certificado criado a partir da sua CSR, esta opção exige que você insira a chave privada do certificado, a senha do certificado (se houver) e a cadeia de certificados. Ao importar um PEM fornecido pela CA que foi criado a partir da sua CSR, deixe a chave privada e a senha em branco. |

| Configuração | Descrição |
|------------------------|--|
| Nome comum | O FQDN do appliance do vRealize Automation. Em vez disso, em implantações corporativas de alta disponibilidade com um balanceador de carga à frente de vários appliances, essa entrada corresponde ao FQDN do balanceador de carga. |
| Organização | Insira o texto para representar seu maior departamento ou unidade de negócios. |
| Unidade organizacional | Insira o texto para representar seu menor departamento ou grupo de trabalho. |
| Código do país | Insira uma abreviação para o seu país de operação. |
| Serial | Identificador alfanumérico exclusivo |
| Impressão digital | Cadeia de caracteres alfanumérica exclusiva para identificar um certificado ou fazer comparação entre os certificados. |
| Válido desde | Carimbo de data e hora após as quais o certificado pode ser usado. |
| Válido até | Carimbo de data e hora após as quais o certificado não pode mais ser usado. |

Certificado Web

Na página Certificado Web, crie ou selecione o certificado de autenticação usado pelo servidor Web do IaaS. O appliance do vRealize Automation se conecta ao servidor Web e precisa se autenticar e confiar nele.

| Configuração | Descrição |
|---------------------|---|
| Ação do certificado | <p>Manter Existentes</p> <p>Use o certificado que já está neste servidor Web do IaaS. Verifique os detalhes nas entradas abaixo, como o número de série e a impressão digital.</p> <hr/> <p>Gerar Certificado</p> <p>Use o assistente para gerar um certificado autoassinado do servidor Web do IaaS.</p> <hr/> <p>Gerar solicitação de assinatura</p> <p>Crie um arquivo de solicitação de assinatura de certificado (CSR) para a sua autoridade de certificação (CA). Uma CSR ajuda sua CA a criar um certificado com os valores corretos para você importar.</p> <ol style="list-style-type: none"> 1 Insira a Organização, a Unidade Organizacional e o Código do País (veja abaixo). 2 Clique em Gerar solicitação de assinatura. 3 Para baixar o arquivo CSR para a sua CA, clique no link que aparece. |

| Configuração | Descrição |
|---|---|
| Importar | <p>Identifique um arquivo de certificado no formato PEM, use o assistente para adicioná-lo ao armazenamento correto e carregue-o para ser usado pelo vRealize Automation.</p> <p>A não ser que você esteja importando um certificado criado a partir da sua CSR, esta opção exige que você insira a chave privada do certificado, a senha do certificado (se houver) e a cadeia de certificados.</p> <p>Ao importar um PEM fornecido pela CA que foi criado a partir da sua CSR, deixe a chave privada e a senha em branco.</p> |
| Fornecer impressão digital do certificado | Carregue um certificado que já tenha sido adicionado ao armazenamento correto. |
| Nome comum | <p>O FQDN do servidor Web do IaaS.</p> <p>Em vez disso, em implantações corporativas de alta disponibilidade com um balanceador de carga à frente de vários servidores Web, essa entrada corresponde ao FQDN do balanceador de carga.</p> |
| Organização | Insira o texto para representar seu maior departamento ou unidade de negócios. |
| Unidade organizacional | Insira o texto para representar seu menor departamento ou grupo de trabalho. |
| Código do país | Insira uma abreviação para o seu país de operação. |
| Serial | Identificador alfanumérico exclusivo |
| Impressão digital | Cadeia de caracteres alfanumérica exclusiva para identificar um certificado ou fazer comparação entre os certificados. |
| Válido desde | Carimbo de data e hora após as quais o certificado pode ser usado. |
| Válido até | Carimbo de data e hora após as quais o certificado não pode mais ser usado. |

Certificado do Manager Service

(Somente implantações corporativas) Na página Certificado do Manager Service, crie ou selecione o certificado de autenticação usado pelo host do Manager Service IaaS do vRealize Automation. Os outros servidores Windows IaaS se conectam ao host do Manager Service e precisam se autenticar e confiar nele.

Esta página aparece apenas quando você hospeda o Manager Service em uma máquina separada do servidor Web do IaaS. Quando estão hospedados na mesma máquina, o certificado Web oferece autenticação para ambas as funções.

| Configuração | | Descrição |
|------------------------|---|---|
| Ação do certificado | Manter Existentes | Use o certificado que já está neste host do Manager Service do IaaS. Verifique os detalhes nas entradas abaixo, como o número de série e a impressão digital. |
| | Gerar Certificado | Use o assistente para gerar um certificado autoassinado do host do Manager Service do IaaS. |
| | Gerar solicitação de assinatura | <p>Crie um arquivo de solicitação de assinatura de certificado (CSR) para a sua autoridade de certificação (CA). Uma CSR ajuda sua CA a criar um certificado com os valores corretos para você importar.</p> <ol style="list-style-type: none"> 1 Insira a Organização, a Unidade Organizacional e o Código do País (veja abaixo). 2 Clique em Gerar solicitação de assinatura. 3 Para baixar o arquivo CSR para a sua CA, clique no link que aparece. |
| | Importar | <p>Identifique um arquivo de certificado no formato PEM, use o assistente para adicioná-lo ao armazenamento correto e carregue-o para ser usado pelo vRealize Automation.</p> <p>A não ser que você esteja importando um certificado criado a partir da sua CSR, esta opção exige que você insira a chave privada do certificado, a senha do certificado (se houver) e a cadeia de certificados.</p> <p>Ao importar um PEM fornecido pela CA que foi criado a partir da sua CSR, deixe a chave privada e a senha em branco.</p> |
| | Fornecer impressão digital do certificado | Carregue um certificado que já tenha sido adicionado ao armazenamento correto. |
| Nome comum | | <p>O FQDN do host do Manager Service do IaaS.</p> <p>Em vez disso, em implantações corporativas de alta disponibilidade com um balanceador de carga à frente de vários hosts do Manager Service, essa entrada corresponde ao FQDN do balanceador de carga.</p> |
| Organização | | Insira o texto para representar seu maior departamento ou unidade de negócios. |
| Unidade organizacional | | Insira o texto para representar seu menor departamento ou grupo de trabalho. |
| Código do país | | Insira uma abreviação para o seu país de operação. |
| Serial | | Identificador alfanumérico exclusivo |
| Impressão digital | | Cadeia de caracteres alfanumérica exclusiva para identificar um certificado ou fazer comparação entre os certificados. |
| Válido desde | | Carimbo de data e hora após as quais o certificado pode ser usado. |
| Válido até | | Carimbo de data e hora após as quais o certificado não pode mais ser usado. |

Balancedores de Carga

(Somente para implantações empresariais) Na página Balanceadores de Carga, pause para configurar os balanceadores de carga do pool correto dos sistemas membro do vRealize Automation.

A lista de balanceadores de carga somente tem fins informativos. Com base nas suas entradas anteriores do assistente, ela apresenta cada balanceador de carga em sua implantação, juntamente com os membros, sua função de componente, FQDN e número de porta.

Pause aqui e utilize a lista enquanto efetua o login nos balanceadores de carga para adicionar membros do vRealize Automation e portas abertas.

Validação

Na página Validação, você verifica se a instalação de vRealize Automation pode continuar.

Para verificar se todos os componentes, funções e contas do vRealize Automation estão corretos e se os sistemas podem realizar a autenticação uns com os outros, clique em **Validar**. O processo pode demorar até meia hora ou mais, dependendo de seu ambiente.

Se houver erros, expanda o item de linha com falha e faça correções com base no status e nas mensagens apresentadas. Você não pode proceder com a instalação do vRealize Automation até que a validação seja realizada.

Criar snapshots

Na página Criar Snapshots, pause para criar snapshots de máquina virtual de todos os componentes do vRealize Automation antes de prosseguir com a instalação.

Embora a validação tenha ocorrido com sucesso, você é enfaticamente avisado para se preparar para problemas inesperados durante a instalação. Antes de iniciar a instalação, use o cliente vSphere para criar um snapshot de cada appliance do vRealize Automation e do servidor Windows IaaS. Caso contrário, será preciso reinserir todas as configurações do assistente para voltar a este ponto.

Se você tiver recursos suficientes, poderá criar snapshots das máquinas virtuais em execução. A prática recomendada é pará-las primeiro.

- 1 No canto superior direito do Assistente de Instalação, clique em **Fazer logoff**.

Importante Se você fechar o assistente usando qualquer outra opção que não seja **Fazer logoff**, não será possível reabrir o assistente.

- 2 No vSphere, encerre o sistema operacional de cada appliance do vRealize Automation e do servidor Windows IaaS.
- 3 Clique com o botão direito nas máquinas virtuais e selecione **Criar snapshot**.
- 4 Nomeie o snapshot.
- 5 Para incluir a memória da máquina no snapshot, selecione **Criar snapshot da memória da máquina virtual**.
- 6 Clique em **OK**.

Aguarde os snapshots serem criados.

- 7 Ligue o sistema operacional de cada appliance do vRealize Automation e do servidor Windows IaaS.
- 8 Volte à página de snapshot do Assistente de Instalação fazendo login como raiz novamente.

<https://vrealize-automation-appliance-FQDN:5480>

Detalhes da instalação

Na página Detalhes da instalação, inicie a instalação do vRealize Automation ou tente novamente se ocorrer algum problema.

Para iniciar a instalação, clique em **Instalar**. Dependendo do seu ambiente, a instalação pode demorar uma hora ou mais.

Durante ou após a instalação, você pode clicar no botão **Coletar Logs**.

- Ao coletar logs, um link de download do arquivo ZIP é exibido acima da tabela de status.
- Ao coletar logs mais de uma vez, cada coleta substituirá a anterior.

Se você quiser os logs atuais, baixe-os antes de clicar em **Coletar Logs** novamente.

Se ocorrer algum problema, o assistente para a instalação e exibe mensagens para ajudá-lo com as correções. Após avaliar as mensagens e anotar as correções necessárias, você pode ou não precisar dos snapshots que criou.

Não reverter para snapshots

Se o assistente ativar a opção **Repetir instalação com falha**, você poderá fazer as correções e repetir a instalação sem reverter as máquinas a snapshots.

Após fazer as correções, clique em **Repetir instalação com falha**.

Reverter os Windows Server do IaaS para snapshots

Se o assistente ativar a opção **Repetir todo IaaS**, siga estas etapas.

- 1 No vSphere, reverta todas as máquinas Windows IaaS aos snapshots criados na página anterior do assistente.
- 2 Se os snapshots tiverem sido criados após um encerramento, ligue os sistemas operacionais convidados.
- 3 Se você tiver usado um SQL Server externo, exclua o banco de dados SQL do vRealize Automation.
- 4 Faça as correções.
- 5 Clique em **Tentar novamente todo o IaaS**.

Reverter appliances e Windows Servers do IaaS para snapshots

Se o assistente exibir mensagens sobre o appliance do vRealize Automation, siga estas etapas.

- 1 No vSphere, reverta todos os appliances do vRealize Automation e máquinas Windows IaaS aos snapshots criados na página anterior do assistente.
- 2 Se os snapshots tiverem sido criados após um encerramento, ligue os sistemas operacionais convidados.

- 3 Se você tiver usado um SQL Server externo, exclua o banco de dados SQL do vRealize Automation.
- 4 Faça as correções.
- 5 Volte ao Assistente de Instalação fazendo login como raiz novamente.
`https://vrealize-automation-appliance-FQDN:5480`
- 6 Volte à página Detalhes da Instalação e clique em **Instalar**.

Licenciamento

Na página Licenciamento, insira uma chave para ativar o produto vRealize Automation instalado.

Em **Nova Chave de Licença**, insira sua chave e clique em **Enviar Chave**. Você pode enviar separadamente mais de uma chave, incluindo chaves para vRealize Automation, vRealize Suite, vRealize Business for Cloud e vRealize Code Stream autônomos.

Nesta página você também seleciona se o vRealize Code Stream deve ser ativado.

vRealize Code Stream não é suportado para implantações de alta disponibilidade ou de produção do vRealize Automation e requer o Pacote de Gerenciamento do vRealize Code Stream. Para obter mais informações, consulte [Licenciar o vRealize Code Stream](#).

Telemetria

Na página Telemetria, você decide se o vRealize Automation deve ou não enviar estatísticas de uso para a VMware como parte do Programa de Aperfeiçoamento da Experiência do Cliente.

Marque ou desmarque a opção para participar do Programa de Aperfeiçoamento da Experiência do Cliente (CEIP).

Para obter mais informações, veja [Programa de Aperfeiçoamento da Experiência do Cliente](#).

Opções após a instalação

Na página Opções após a instalação, você pode criar novos dados do vRealize Automation ou migrar os dados da implantação antiga para a nova instalação.

- A opção **Configurar o conteúdo inicial** cria um usuário local novo do tenant padrão. O usuário local pode iniciar o processo de configuração no tenant padrão.

Para essa opção, você precisa ter adicionado anteriormente pelo menos um endpoint do vSphere, na página Agentes do Assistente de Instalação.
- A opção **Migrar uma Implantação** transfere os dados do vRealize Automation antigo para esta nova implantação que acabou de ser instalada. A migração preserva elementos essenciais como grupos, blueprints e endpoints.
- A opção **Continuar** conduz você ao fim do Assistente de Instalação.

Configuração de conteúdo inicial

Na página Configuração de conteúdo inicial, crie um novo usuário local de tenant padrão do vRealize Automation que possa iniciar um fluxo de trabalho de conteúdo para um endpoint do vSphere.

Observação Esta opção não estará disponível se você tiver adicionado pelo menos um endpoint do vSphere anteriormente na página Agentes.

O novo nome de usuário local é configurationadmin. O vRealize Automation concede ao usuário configurationadmin os privilégios a seguir.

- Administrador de tenant
- Administrador do IaaS
- Administrador de aprovação
- Administrador do catálogo
- Arquiteto de infraestrutura
- Arquiteto do XaaS
- Administrador do vRealize Orchestrator

Insira e confirme uma senha de login para configurationadmin. Para gerar um item de catálogo de forma que o configurationadmin possa iniciar o processo de configuração após fazer login no tenant padrão, clique em **Criar conteúdo inicial**.

Configuração da migração

Na página Configuração da migração, você pode iniciar a transferência de outra implantação mais antiga do vRealize Automation para a implantação recém-instalada.

Antes de migrar uma implantação mais antiga, verifique as seguintes diretrizes.

- Leia com atenção o guia de migração do vRealize Automation referente à versão mais antiga da sua implantação. Os pré-requisitos e outros detalhes podem variar.
- Migre os tenants e os armazenamentos de identidade mais antigos para o VMware Identity Manager na nova implantação.
- Clone o banco de dados SQL Server IaaS mais antigo e restaure-o no banco de dados IaaS da nova implantação. Anote o nome do banco de dados clonado.
- Obtenha (e anote) a chave de criptografia para o banco de dados SQL Server IaaS mais antigo.
- Crie (e anote) uma nova senha para criptografar novamente os dados migrados.
- Anote as credenciais de login raiz e FQDN do balanceador de carga ou appliance do vRealize Automation mais antigo.
- Anote as credenciais de login raiz da nova implantação.

As interfaces de instalação padrão do vRealize Automation

Depois de executar o Assistente de Instalação, talvez você precise ou queira realizar certas tarefas de instalação manualmente, por meio das interfaces padrão.

O Assistente de Instalação descrito em [Instalando o vRealize Automation com o assistente de instalação](#) é a sua principal ferramenta para novas instalações do vRealize Automation. No entanto, depois de executar o assistente, algumas operações ainda exigem o processo de instalação manual antigo.

Você precisará das etapas manuais se quiser expandir uma implantação do vRealize Automation ou se o assistente tiver parado por qualquer motivo. Situações em que talvez você precise consultar os procedimentos nesta seção incluem os seguintes exemplos.

- Você optou por cancelar o assistente antes de terminar a instalação.
- A instalação por meio do assistente falhou.
- Você deseja adicionar outro appliance do vRealize Automation para alta disponibilidade.
- Você deseja adicionar outro servidor Web IaaS para alta disponibilidade.
- Você precisa de outro agente de proxy.
- Você precisa de outro orchestrator ou trabalhador DEM.

Você pode usar todos os processos manuais ou apenas alguns deles. Reveja o material desta seção e siga os procedimentos que se aplicam à sua situação.

Usando as interfaces padrão para implantações mínimas

Você pode instalar uma implantação mínima e autônoma para uso em um ambiente de desenvolvimento ou como uma prova de conceito. As implantações mínimas não são adequadas para um ambiente de produção.

Lista de verificação da implantação mínima

Você instala o vRealize Automation em uma configuração mínima para prova de conceito ou trabalho de desenvolvimento. Implantações mínimas exigem menos etapas de instalação, mas não têm a capacidade de produção de uma implantação empresarial.

Conclua as tarefas de alto nível na seguinte ordem.

Tabela 1-27. Lista de verificação da implantação mínima

| Tarefa | Detalhes |
|--|---|
| <input type="checkbox"/> Planeje o ambiente e satisfaça os pré-requisitos de instalação. | Preparando para a instalação do vRealize Automation |
| <input type="checkbox"/> Crie um appliance não configurado do vRealize Automation. | Implantar o appliance do vRealize Automation |
| <input type="checkbox"/> Configure o appliance do vRealize Automation manualmente. | Configurar o appliance do vRealize Automation |
| <input type="checkbox"/> Instale os componentes do IaaS em um único servidor do Windows. | Instalando componentes do IaaS |

Tabela 1-27. Lista de verificação da implantação mínima (Continuação)

| Tarefa | Detalhes |
|--|---|
| <input type="checkbox"/> Instale agentes adicionais, se necessário. | Instalando agentes do vRealize Automation |
| <input type="checkbox"/> Realize as tarefas pós-instalação como a configuração do tenant padrão. | Configurar o acesso ao tenant padrão |

Configurar o appliance do vRealize Automation

O appliance do vRealize Automation é uma máquina virtual parcialmente configurada que hospeda o portal da web do usuário e servidor do vRealize Automation. Baixe e implante o modelo de Formato de virtualização aberta (OVF) do appliance no vCenter Server ou no inventário do ESX/ESXi.

Pré-requisitos

- Crie um appliance não configurado. Consulte [Implantar o appliance do vRealize Automation](#).
- Obtenha um certificado de autenticação para o appliance do vRealize Automation.

Procedimentos

- 1 Faça login na interface de gerenciamento de appliance do vRealize Automation não configurada como raiz.

`https://vrealize-automation-appliance-FQDN:5480`

Ignore todos os avisos de certificado para continuar.

- 2 Se o assistente de instalação aparecer, cancele-o para que possa acessar a interface de gerenciamento em vez do assistente.
- 3 Selecione **Administração > Configurações de Hora** e defina a fonte de sincronização da hora.

| Opção | Descrição |
|----------------------------|--|
| Hora do host | Sincronize com o host ESXi do appliance do vRealize Automation. |
| Servidor de horário | Sincronize com um servidor NTP (Protocolo de tempo de rede) externo. Insira o endereço IP ou o FQDN do servidor NTP. |

Você deve sincronizar os appliances do vRealize Automation e servidores IaaS Windows para a mesma fonte de horário. Não misture fontes de horário em uma implantação do vRealize Automation.

4 Selecione **Configurações do vRA > Configurações do Host**.

| Opção | Ação |
|-----------------------------------|---|
| Solucionar automaticamente | Selecione Solucionar Automaticamente para especificar o nome do host atual do Appliance do vRealize Automation. |
| Atualizar host | <p>Para novos hosts, selecione Atualizar Host. Insira o nome de domínio totalmente qualificado do Appliance do vRealize Automation, <i>vra-hostname.domain.name</i> na caixa de texto Nome do Host.</p> <p>Para implantações distribuídas que usam balanceadores de carga, selecione Atualizar Host. Insira o nome de domínio totalmente qualificado do servidor do balanceador de carga, <i>vra-loadbalancername.domain.name</i> na caixa de texto Nome do Host.</p> |

Observação Defina configurações de SSO conforme descrito mais adiante neste procedimento sempre que você usar **Atualizar Host** para definir o nome do host.

5 Selecione o tipo de certificado no menu **Ação de Certificado**.

Se você estiver usando um certificado codificado por PEM, por exemplo, para um ambiente distribuído, selecione **Importar**.

Os certificados que você importa devem ser confiáveis e também aplicáveis a todas as instâncias do appliance do vRealize Automation e todos os balanceadores de carga por meio do uso de certificados de Nome Alternativo da Entidade (SAN).

Se quiser gerar uma solicitação CSR para um novo certificado que pode ser enviado a uma autoridade de certificação, selecione **Gerar Solicitação de Assinatura**. Uma CSR ajuda sua CA a criar um certificado com os valores corretos para você importar.

Observação Se você usar cadeias de certificados, especifique os certificados na seguinte ordem:

- a Certificado cliente/servidor assinado pelo certificado de autoridade de certificação intermediário
- b Um ou mais certificados intermediários
- c Um certificado de autoridade de certificação raiz

| Opção | Ação |
|--------------------------|---|
| Manter Existentes | Mantenha a configuração SSL atual. Selecione essa opção para cancelar as alterações. |
| Gerar Certificado | <ul style="list-style-type: none"> a O valor exibido na caixa de texto Nome comum é o Nome de host, conforme ele é exibido na parte superior da página. Se todas as instâncias adicionais do appliance do vRealize Automation estiverem disponíveis, os respectivos FQDN serão incluídos no atributo SAN do certificado. b Insira o nome da organização, como o nome da sua empresa, na caixa de texto Organização. c Insira a unidade organizacional, como o nome ou o local do departamento, na caixa de texto Unidade organizacional. d Insira um código de país ISO 3166 de duas letras, como PT_BR, na caixa de texto País. |

| Opção | Ação |
|--|---|
| Gerar solicitação de assinatura | <ul style="list-style-type: none"> a Selecione Gerar Solicitação de Assinatura. b Reveja as entradas nas caixas de texto Organização, Unidade Organizacional, Código do País e Nome Comum. Essas entradas são preenchidas do certificado existente. É possível editá-las se necessário. c Clique em Gerar CSR para gerar uma solicitação de assinatura de certificado e depois clique no link Baixar a CSR gerada aqui para abrir uma caixa de diálogo que permite salvar a CSR em um local onde ela pode ser enviada para uma autoridade de certificação. d Quando receber o certificado preparado, clique em Importar e siga as instruções para importar um certificado no vRealize Automation. |
| Importar | <ul style="list-style-type: none"> a Copie os valores do certificado, de BEGIN PRIVATE KEY até END PRIVATE KEY, incluindo o cabeçalho e o rodapé, e cole-os na caixa de texto Chave Privada RSA. b Copie os valores do certificado, de BEGIN PRIVATE KEY até END PRIVATE KEY, incluindo o cabeçalho e o rodapé, e cole-os na caixa de texto Cadeia de Certificados. Para vários valores de certificado, inclua um cabeçalho BEGIN CERTIFICATE e um rodapé END CERTIFICATE em cada certificado. <p>Observação No caso dos certificados encadeados, atributos adicionais podem estar disponíveis.</p> <ul style="list-style-type: none"> c (Opcional) Se o seu certificado usar um código de acesso para criptografar a chave do certificado, copie-o e cole-o na caixa de texto Código de Acesso. |

6 Clique em **Salvar Configurações** para salvar as informações do host e a configuração do SSL.

7 Defina as configurações do SSO.

8 Clique em **Mensagens**. As definições de configuração e o status de mensagens do seu appliance são exibidos. Não altere essas configurações.

9 Clique na guia **Telemetria** para escolher se deseja participar do Programa de Aperfeiçoamento da Experiência do Cliente (CEIP) da VMware.

Os detalhes sobre os dados recolhidos pelo CEIP e os fins para os quais eles são utilizados pelo VMware são estabelecidos pelo Centro de Confiança e Garantia, em <http://www.vmware.com/trustvmware/ceip.html>.

- Selecione **Participe do Programa de Aperfeiçoamento da Experiência do Cliente da VMware** para participar do programa.
- Desmarque **Participe do Programa de Aperfeiçoamento da Experiência do Cliente da VMware** para não participar do programa.

10 Clique em **Serviços** e verifique se os serviços estão registrados.

Dependendo da configuração do seu site, isso pode demorar cerca de 10 minutos.

Observação Você pode fazer login no appliance e executar o `tail -f /var/log/vcac/catalina.out` para monitorar a inicialização dos serviços.

11 Insira as informações da sua licença.

- a Clique em **Configurações do vRA > Licenciamento**.
- b Clique em **Licenciamento**.
- c Insira uma chave de licença válida do vRealize Automation que você baixou com os arquivos de instalação e clique em **Enviar Chave**.

Observação Se houver um erro de conexão, você poderá ter um problema com o balanceador de carga. Verifique a conectividade de rede do balanceador de carga.

12 Selecione se deseja ativar vRealize Code Stream e inserir uma licença vRealize Code Stream.

vRealize Code Stream não tem suporte para implantações do vRealize Automation de alta disponibilidade ou produção.

13 Confirme se você pode fazer login no vRealize Automation.

- a Abra um navegador da Web para a URL da interface de produto do vRealize Automation.
`https://vrealize-automation-appliance-FQDN/vcac`
- b Aceite o certificado do vRealize Automation.
- c Aceite o certificado do SSO.
- d Faça login com o `administrator@vsphere.local` e a senha que você especificou na configuração do SSO.

A interface é aberta na página Tenants na guia **Administração**. Um único tenant nomeado `vsphere.local` aparece na lista.

Você terminou a implantação e configuração do seu Appliance do vRealize Automation. Se o appliance não funcionar corretamente após a configuração, reimplante-o e reconfigure-o. Não faça alterações no appliance existente.

Próximo passo

Consulte [Instalar os componentes de infraestrutura](#).

Instalando componentes do IaaS

O administrador instala um conjunto completo de componentes de infraestrutura (IaaS) em uma máquina Windows (física ou virtual). Os direitos de administrador são obrigatórios para a execução dessas tarefas.

A instalação mínima instala todos os componentes no mesmo servidor Windows, exceto o banco de dados SQL, que você pode instalar em um servidor separado.

Ativar a sincronização de horário no servidor Windows

Os relógios no servidor do vRealize Automation e no servidor Windows devem estar sincronizados para garantir que a instalação seja bem-sucedida.

As etapas a seguir descrevem como ativar a sincronização de horário com o host ESX/ESXi usando o VMware Tools. Se você estiver instalando os componentes do IaaS em um host físico ou não desejar usar o VMware Tools para a sincronização de horário, verifique se o horário do servidor é preciso usando seu método preferido.

Procedimentos

- 1 Abra um prompt de comando na máquina de instalação do Windows.
- 2 Digite o comando a seguir para navegar até o diretório do VMware Tools.

```
cd C:\Program Files\VMware\VMware Tools
```

- 3 Digite o comando para exibir o status da sincronização de horário.

```
VMwareToolboxCmd.exe timesync status
```

- 4 Se a sincronização de horário estiver desativada, digite o comando a seguir para ativá-la.

```
VMwareToolboxCmd.exe timesync enable
```

Certificados do IaaS

Os componentes IaaS do vRealize Automation usam certificados e SSL para proteger as comunicações entre os componentes. Em uma instalação mínima para fins de prova de conceito, você pode usar certificados autoassinados.

Em um ambiente distribuído, obtenha um certificado de domínio de uma autoridade de certificação confiável. Para obter informações sobre como instalar certificados de domínio de componentes IaaS, consulte [Instalar certificados do IaaS](#) no capítulo sobre implantação distribuída.

Instalar os componentes de infraestrutura

O administrador do sistema faz login na máquina Windows e usa o assistente de instalação para instalar os serviços do IaaS na máquina virtual ou física do Windows.

Pré-requisitos

- Verifique se o servidor atende aos requisitos em [Servidores Windows do IaaS](#).
- [Ativar a sincronização de horário no servidor Windows](#).
- Verifique se você implantou e configurou totalmente o appliance do vRealize Automation e se os serviços necessários estão em execução (plugin-service, catalogue-service, iaas-proxy-provider).

Procedimentos

- 1 [Baixar o Instalador IaaS do vRealize Automation](#)

Para instalar o IaaS no seu servidor Windows virtual ou físico mínimo, é necessário baixar uma cópia do instalador do IaaS a partir do appliance do vRealize Automation.

2 Selecionar o tipo de instalação

O administrador do sistema executa o assistente de instalação na máquina de instalação do Windows 2008 ou 2012.

3 Verificar pré-requisitos

O Verificador de Pré-requisitos verifica se a sua máquina atende aos requisitos de instalação do IaaS.

4 Especificar as configurações do servidor e da conta

O administrador do sistema do vRealize Automation especifica as configurações de servidor e de conta para o servidor de instalação do Windows e seleciona uma instância e o método de autenticação do servidor de banco de dados SQL.

5 Especificar gerentes e agentes

A instalação mínima instala os Distributed Execution Managers necessários e o agente de proxy do vSphere padrão. O administrador do sistema pode instalar agentes adicionais de proxy (XenServer ou Hyper-V, por exemplo) após a instalação usando o instalador personalizado.

6 Registrar os componentes do IaaS

O administrador de sistema instala o certificado IaaS e registra os componentes IaaS com o SSO.

7 Concluir a instalação

O administrador do sistema conclui a instalação do IaaS.

Baixar o Instalador IaaS do vRealize Automation

Para instalar o IaaS no seu servidor Windows virtual ou físico mínimo, é necessário baixar uma cópia do instalador do IaaS a partir do appliance do vRealize Automation.

Se você vir avisos de certificado durante esse processo, ignore-os para concluir a instalação.

Pré-requisitos

- Revise os requisitos do Windows Server do IaaS. Consulte [Servidores Windows do IaaS](#).
- Se você estiver usando o Internet Explorer para fazer o download, verifique se a Configuração de Segurança Reforçada está ativada. Navegue para o `res://iesetup.dll/SoftAdmin.htm` no servidor Windows.

Procedimentos

- 1 Faça login no servidor Windows do IaaS usando uma conta com direitos de administrador.
- 2 Abra um navegador da Web diretamente para a URL do instalador do appliance do vRealize Automation.

`https://vrealize-automation-appliance-FQDN:5480/installer`

- 3 Clique em **Instalador do IaaS**.

- 4 Salve `setup__vrealize-automation-appliance-FQDN@5480` no servidor Windows.

Não altere o nome do arquivo do instalador. Ele é utilizado para conectar a instalação ao appliance do vRealize Automation.

Selecionar o tipo de instalação

O administrador do sistema executa o assistente de instalação na máquina de instalação do Windows 2008 ou 2012.

Pré-requisitos

[Baixar o Instalador IaaS do vRealize Automation.](#)

Procedimentos

- 1 Clique com o botão direito do mouse no arquivo de configuração `setup__vrealize-automation-appliance-FQDN@5480.exe` e selecione **Executar como administrador**.
- 2 Clique em **Avançar**.
- 3 Aceite o contrato de licença e clique em **Avançar**.
- 4 Na página Login, forneça as credenciais de administrador do appliance do vRealize Automation e verifique o Certificado SSL.
 - a Digite o nome de usuário, que é **root**, e a senha.
A senha é aquela que você especificou quando implantou o appliance do vRealize Automation.
 - b Selecione **Aceitar Certificado**.
 - c Clique em **Exibir Certificado**.
Compare a impressão digital do certificado com a impressão digital definida para o appliance do vRealize Automation. Você pode exibir o certificado do appliance do vRealize Automation no navegador do cliente quando o console de gerenciamento é acessado na porta 5480.
- 5 Selecione **Aceitar Certificado**.
- 6 Clique em **Avançar**.
- 7 Selecione **Instalação completa** na página **Tipo de instalação** se você estiver criando uma implantação mínima e clique em **Avançar**.

Verificar pré-requisitos

O Verificador de Pré-requisitos verifica se a sua máquina atende aos requisitos de instalação do IaaS.

Pré-requisitos

[Selecionar o tipo de instalação.](#)

Procedimentos

- 1 Conclua o Verificador de Pré-requisitos.

| Opção | Descrição |
|--------------------|--|
| Nenhum erro | Clique em Avançar . |
| Erros não críticos | Clique em Ignorar . |
| Erros críticos | Ignorar os erros críticos provoca falha na instalação. Se forem exibidos avisos, selecione o alerta no painel à esquerda e siga as instruções à direita. Resolva todos os erros críticos e clique em Verificar Novamente para realizar a verificação. |

- 2 Clique em **Avançar**.

A máquina atende aos requisitos de instalação.

Especificar as configurações do servidor e da conta

O administrador do sistema do vRealize Automation especifica as configurações de servidor e de conta para o servidor de instalação do Windows e seleciona uma instância e o método de autenticação do servidor de banco de dados SQL.

Pré-requisitos

[Verificar pré-requisitos.](#)

Procedimentos

- 1 Na página **Configurações do Servidor e da Conta** ou **Configurações Detectadas**, insira o nome de usuário e a senha para a conta de serviços do Windows. Essa conta de serviços deve ser uma conta de administrador local que também tenha privilégios administrativos para o SQL.

- 2 Insira uma frase na caixa de texto **Senha**.

A senha é uma série de palavras que gera a chave de criptografia usada para proteger os dados do banco de dados.

Observação Salve sua senha para que esteja disponível para futuras instalações ou recuperações do sistema.

- 3 Para instalar a instância de banco de dados no mesmo servidor com os componentes do IaaS, aceite o servidor padrão na caixa de texto **Servidor** na seção Informações de Instalação do Banco de Dados SQL Server.

Se o banco de dados estiver em uma máquina diferente, insira o servidor no seguinte formato.

machine-FQDN,port-number\named-database-instance

- 4 Aceite o padrão na caixa de texto **Nome do banco de dados** ou insira um nome apropriado, se aplicável.

5 Selecione o método de autenticação.

- ◆ Selecione **Usar autenticação do Windows** se você deseja criar o banco de dados usando as credenciais do Windows do usuário atual. O usuário deve ter privilégios sys_admin do SQL.
- ◆ Desmarque **Usar autenticação do Windows** se você deseja criar o banco de dados usando a autenticação SQL. Digite o **Nome do usuário** e a **Senha** do usuário do SQL Server com privilégios sys_admin do SQL na instância do SQL Server.

A autenticação do Windows é recomendada. Quando você escolhe a autenticação SQL, a senha do banco de dados não criptografada aparece em determinados arquivos de configuração.

6 (Opcional) Marque a caixa de seleção **Usar SSL para conexão do banco de dados**.

Por padrão, a caixa de seleção fica marcada. O SSL oferece uma conexão mais segura entre o servidor do IaaS e o banco de dados do SQL. No entanto, você deve configurar primeiro o SSL no SQL Server para oferecer suporte a essa opção. Para obter mais informações sobre como configurar o SSL no SQL Server, consulte [Artigo da Microsoft Technet 189067](#).

7 Clique em **Avançar**.

Especificar gerentes e agentes

A instalação mínima instala os Distributed Execution Managers necessários e o agente de proxy do vSphere padrão. O administrador do sistema pode instalar agentes adicionais de proxy (XenServer ou Hyper-V, por exemplo) após a instalação usando o instalador personalizado.

Pré-requisitos

[Especificar as configurações do servidor e da conta.](#)

Procedimentos

- 1 Na página **Distributed Execution Managers e agente de proxy do vSphere**, aceite os padrões ou altere os nomes, se apropriado.
- 2 Aceite o padrão para instalar um agente do vSphere para permitir o provisionamento com o vSphere ou desmarque-o, se aplicável.
 - a Selecione **Instalar e configurar agente do vSphere**.
 - b Aceite o agente e o endpoint padrão, ou digite um nome.

Anote o valor do nome do Endpoint. Você deve digitar essas informações corretamente ao configurar o endpoint do vSphere no console do vRealize Automation ou a configuração poderá falhar.

3 Clique em **Avançar**.

Registrar os componentes do IaaS

O administrador de sistema instala o certificado IaaS e registra os componentes IaaS com o SSO.

Pré-requisitos

[Baixar o Instalador IaaS do vRealize Automation.](#)

Procedimentos

- 1 Aceite o valor padrão do **Servidor**, que é preenchido com o nome do domínio totalmente qualificado do servidor do appliance do vRealize Automation do qual foi feito o download do instalador. Verifique se o nome do domínio totalmente qualificado é usado para identificar o servidor e não um endereço IP.

Se você tiver vários dispositivos virtuais e estão usando um balanceador de carga, insira o caminho do dispositivo virtual do balanceador de carga.

- 2 Clique em **Carregar** para preencher o valor de **Tenant padrão de SSO*** (vsphere.local).
- 3 Clique em **Baixar** para recuperar o certificado do appliance do vRealize Automation.
É possível clicar em **Ver certificado** para ver os detalhes do certificado.
- 4 Selecione **Aceitar certificado** para instalar o certificado SSO.
- 5 No painel Administrador SSO, digite **administrador** na caixa de texto **Nome do usuário** e a senha definida para esse usuário ao configurar o SSO em **Senha** e **Confirmar senha**.
- 6 Clique no link do teste à direita do campo **Nome do usuário** para validar a senha inserida.
- 7 Aceite o padrão em **Servidor do IaaS** contendo o nome do host da máquina Windows onde você está instalando.
- 8 Clique no link do teste à direita do campo **Servidor do IaaS** para validar a conectividade.
- 9 Clique em **Avançar**.

Se aparecer quaisquer erros depois de clicar em **Avançar**, resolva-os antes de continuar.

Concluir a instalação

O administrador do sistema conclui a instalação do IaaS.

Pré-requisitos

- [Registrar os componentes do IaaS.](#)
- Verifique se a máquina em que você está fazendo a instalação está conectada à rede e pode se conectar ao appliance do vRealize Automation a partir do qual você baixa o instalador do IaaS.

Procedimentos

- 1 Revise as informações na página **Pronto para instalação** e clique em **Instalar**.

A instalação é iniciada. A instalação pode levar de cinco minutos a uma hora, dependendo da configuração de rede.

- 2 Quando a mensagem de sucesso aparecer, deixe a caixa de seleção **Orientar-me pela configuração inicial** marcada e clique em **Avançar** e, depois, em **Concluir**.
- 3 Feche a caixa de mensagem **Configurar o sistema**.

Agora a instalação está concluída.

Próximo passo

[Verificar os serviços do IaaS.](#)

Usando as interfaces padrão para implantações distribuídas

Implantações empresariais são projetadas para maior capacidade do vRealize Automation em produção, e exigem que você distribua componentes por múltiplas máquinas. Implantações empresariais também podem incluir sistemas redundantes atrás de balanceadores de carga.

Lista de verificação de implantação distribuída

Um administrador de sistema pode implantar o vRealize Automation em uma configuração distribuída, o que fornece proteção contra failover e alta disponibilidade por meio de redundância.

A Lista de verificação de implantação distribuída fornece uma visão geral de alto nível das etapas necessárias para realizar uma instalação distribuída.

Tabela 1-28. Lista de verificação de implantação distribuída

| Tarefa | Detalhes |
|---|---|
| <input type="checkbox"/> Planejar e preparar o ambiente de instalação e verificar se todos os pré-requisitos de instalação foram atendidos. | Preparando para a instalação do vRealize Automation |
| <input type="checkbox"/> Planejar e obter os seus certificados SSL. | Requisitos de confiança de certificado em um ambiente distribuído |
| <input type="checkbox"/> Implantar o servidor do appliance do vRealize Automation principal e todos os appliances adicionais que você exigir para obter redundância e alta disponibilidade. | Implantar o appliance do vRealize Automation |
| <input type="checkbox"/> Configure o balanceador de carga para lidar com o tráfego do appliance do vRealize Automation. | Configurar o balanceador de carga |
| <input type="checkbox"/> Configurar o servidor do appliance do vRealize Automation principal e todos os appliances adicionais que você implantou para obter redundância e alta disponibilidade. | Configurando dispositivos para ovRealize Automation |
| <input type="checkbox"/> Configurar o balanceador de carga para lidar com o tráfego do componente do vRealize Automation IaaS e instalar os componentes do vRealize Automation IaaS. | Instalar os componentes do IaaS em uma configuração distribuída |
| <input type="checkbox"/> Se necessário, instalar os agentes para integração com sistemas externos. | Instalando agentes do vRealize Automation |
| <input type="checkbox"/> Configurar o tenant padrão e fornecer a licença do IaaS. | Configurar o acesso ao tenant padrão |

vRealize Orchestrator

O appliance do vRealize Automation inclui uma versão integrada do vRealize Orchestrator que agora é recomendada para uso com novas instalações. Porém, em implantações mais antigas ou em casos especiais, os usuários podem conectar o vRealize Automation a um vRealize Orchestrator separado externo. Consulte <https://www.vmware.com/products/vrealize-orchestrator.html>.

Para obter informações sobre como conectar o vRealize Automation e o vRealize Orchestrator, consulte [Plug-in do VMware vRealize Orchestrator para vRealize Automation](#).

Gerenciamento de Diretórios

Se você fizer uma instalação distribuída com balanceadores de carga para alta disponibilidade e failover, notifique a equipe responsável pela configuração do seu ambiente vRealize Automation. Seus administradores de tenant devem configurar o Gerenciamento de Diretórios para alta disponibilidade ao configurarem o link para o seu Active Directory.

Desativando verificações de integridade do balanceador de carga

Verificações de integridade garantem que um balanceador de carga envie tráfego apenas para os nós que estão operando. O balanceador de carga envia uma verificação de integridade a uma frequência especificada para cada nó. Nós que excedem o limite de falhas se tornam ineligíveis para o novo tráfego.

Para a distribuição e failover de cargas de trabalho, você pode colocar vários appliances do vRealize Automation atrás de um balanceador de carga. Além disso, você pode colocar vários servidores Web do IaaS e vários servidores Manager Service do IaaS atrás de seus respectivos balanceadores de carga.

Ao usar balanceadores de carga, não permita que eles enviem verificações de integridade a qualquer momento durante a instalação. Verificações de integridade podem interferir na instalação ou fazer com que ela se comporte de maneira imprevisível.

- Ao implantar componentes de IaaS ou appliance do vRealize Automation atrás de balanceadores de carga existentes, desative verificações de integridade em todos os balanceadores de carga na configuração proposta antes de instalar qualquer componente.
- Depois de instalar e configurar todo o vRealize Automation, incluindo todos os componentes de IaaS e appliance do vRealize Automation, você poderá reativar as verificações de integridade.

Requisitos de confiança de certificado em um ambiente distribuído

vRealize Automation usa certificados para manter relações confiáveis e fornecer comunicação segura entre componentes em implantações distribuídas.

Em uma implantação distribuída ou clusterizada, a organização do certificado vRealize Automation está amplamente em conformidade com a estrutura arquitetônica de três camadas do vRealize Automation. As três camadas são Appliance do vRealize Automation, componentes do Site IaaS e componentes do Manager Service. Em um sistema distribuído, cada máquina de hardware em uma camada específica compartilha um certificado. Isto é, cada Appliance do vRealize Automation compartilha um certificado comum e cada máquina do Manager Service compartilha o certificado comum que se aplica a essa camada.

Você pode usar certificados autoassinados gerados pelo sistema ou pelo usuário ou fornecidos pela CA com implantações distribuídas do vRealize Automation. Nas versões a partir do vRealize Automation 7.0 e mais recentes, se nenhum certificado for fornecido pelo usuário, o instalador gera automaticamente certificados autoassinados para todos os nós aplicáveis e os coloca nos armazenamentos confiáveis apropriados.

Você pode usar balanceadores de carga com componentes do vRealize Automation para proporcionar alta disponibilidade e suporte de failover. A VMware recomenda que as implantações do vRealize Automation usem uma configuração de passagem para implantações que usam balanceadores de carga. Em uma configuração de passagem, os balanceadores de carga passam solicitações junto com os componentes apropriados, em vez de descriptografá-los. O Appliance do vRealize Automation e os servidores IaaS Web devem, então, executar a descriptografia necessária.

Para obter mais informações sobre como usar e configurar balanceadores de carga, consulte *Balanceamento de carga do vRealize Automation*.

Se fornecer ou gerar seus próprios certificados usando Openssl ou outra ferramenta, você pode usar certificados SAN (nome alternativo da entidade). Observe que os certificados IaaS devem ser certificados multiuso.

Se estiver fornecendo certificados, você deverá obter um certificado multiuso que inclua o componente IaaS no cluster e copiar esse certificado no armazenamento confiável para cada componente. Se você usar balanceadores de carga, deverá incluir o FQDN do balanceador de carga no endereço confiável do certificado multiuso do cluster.

Se você precisar atualizar os certificados autoassinados gerados pelo sistema com certificados fornecidos pelo usuário ou pela CA, consulte [Atualizando certificados do vRealize Automation](#).

A tabela Requisitos de confiança de certificados resume os requisitos de registro de confiança para vários certificados importados.

Tabela 1-29. Requisitos de confiança de certificados

| Importar | Registrar |
|---|---|
| Cluster do appliance do vRealize Automation | Cluster de componentes IaaS Web |
| Cluster do componente IaaS Web | <ul style="list-style-type: none"> ■ Cluster do appliance do vRealize Automation ■ Cluster de componentes do Manager Service ■ Componentes DEM Orchestrator e DEM Worker |
| Cluster de componente do Manager Service | <ul style="list-style-type: none"> ■ Componentes DEM Orchestrator e DEM Worker ■ Agentes e agentes de proxy |

Configurar a confiança de certificado do componente Web, do serviço de gerenciador e do host DEM

Clientes que usam uma impressão digital com arquivos PFX pré-instalados para oferecer suporte à autenticação de usuários devem configurar a confiança de impressão digital no host Web, no serviço de gerenciador e nas máquinas host de Trabalhadores e do DEM Orchestrator.

Os clientes que importam arquivos PEM ou usam certificados autoassinados podem ignorar este procedimento.

Pré-requisitos

Arquivos `web.pfx` e `ms.pfx` válidos disponíveis para autenticação via impressão digital.

Procedimentos

- 1 Importe os arquivos `web.pfx` e `ms.pfx` para as seguintes localizações nas máquinas host de componentes Web e do serviço de gerenciador:

- *Computador Host/Certificados/Repositório de certificados pessoais*
- *Computador Host/Certificados/Repositório de certificados de pessoas confiáveis*

- 2 Importe os arquivos `web.pfx` e `ms.pfx` para as seguintes localizações das máquinas host de Trabalhadores e do DEM Orchestrator:

Computador Host/Certificados/Repositório de certificados de pessoas confiáveis

- 3 Abra uma janela do Console de Gerenciamento Microsoft em cada uma das máquinas host aplicáveis.

Observação Os caminhos e as opções reais no Console de Gerenciamento podem ser um pouco diferentes dependendo das versões do Windows e das configurações do sistema.

- a Selecione **Adicionar/Remover Snap-in**.
- b Selecione **Certificados**.
- c Selecione **Computador Local**.
- d Abra os arquivos de certificado que você importou anteriormente e copie as impressões digitais.

Próximo passo

Insira a impressão digital na página Certificado do assistente do vRealize Automation para o Manager Service, os componentes Web e os componentes DEM.

Planilhas de instalação

Planilhas registram informações importantes que você precisa para fazer referência durante a instalação.

As configurações diferenciam maiúsculas de minúsculas. Observe que haverá espaços adicionais para mais componentes se você estiver instalando uma implementação distribuída. Você pode não precisar de todos os espaços nas planilhas. Além disso, uma máquina pode hospedar mais de um componente de IaaS. Por exemplo, o servidor Web primário e o DEM Orchestrator podem estar no mesmo FQDN.

Tabela 1-30. Appliance do vRealize Automation

| Variável | Meu valor | Exemplo |
|---|--------------------------------------|----------------------------------|
| FQDN do appliance primário do vRealize Automation | | automation.mycompany.com |
| Endereço IP do appliance primário do vRealize Automation Somente para referência; não insira endereços IP | | 123.234.1.105 |
| FQDN do appliance adicional do vRealize Automation | | automation2.mycompany.com |
| Endereço IP do appliance adicional do vRealize Automation Somente para referência; não insira endereços IP | | 123.234.1.106 |
| FQDN do balanceador de carga do appliance do vRealize Automation | | automation-balance.mycompany.com |
| Endereço IP do balanceador de carga do appliance do vRealize Automation Somente para referência; não insira endereços IP | | 123.234.1.201 |
| Nome de usuário da interface de gerenciamento (https://appliance-FQDN:5480) | raiz (padrão) | raiz |
| Senha da interface de gerenciamento | | admin123 |
| Tenant padrão | vsphere.local (padrão) | vsphere.local |
| Nome de usuário do tenant padrão | administrator@vsphere.local (padrão) | administrator@vsphere.local |
| Senha do tenant padrão | | login123 |

Tabela 1-31. Servidores Windows do IaaS

| Variável | Meu valor | Exemplo |
|---|-----------|--------------------|
| FQDN do servidor Web do IaaS primário com Model Manager Data | | web.mycompany.com |
| Endereço IP do servidor Web do IaaS primário com Model Manager Data Somente para referência; não insira endereços IP | | 123.234.1.107 |
| FQDN do servidor Web do IaaS adicional | | web2.mycompany.com |

Tabela 1-31. Servidores Windows do IaaS (Continuação)

| Variável | Meu valor | Exemplo |
|--|-----------|-------------------------------|
| Endereço IP do servidor Web do IaaS adicional Somente para referência; não insira endereços IP | | 123.234.1.108 |
| FQDN do balanceador de carga do servidor Web do IaaS | | web-balance.mycompany.com |
| Endereço IP do balanceador de carga do servidor Web do IaaS Somente para referência; não insira endereços IP | | 123.234.1.202 |
| FQDN do host do Manager Service do IaaS ativo | | mgr-svc.mycompany.com |
| Endereço IP do host do Manager Service do IaaS ativo Somente para referência; não insira endereços IP | | 123.234.1.109 |
| FQDN do host do Manager Service do IaaS passivo | | mgr-svc2.mycompany.com |
| Endereço IP do host do Manager Service do IaaS passivo Somente para referência; não insira endereços IP | | 123.234.1.110 |
| FQDN do balanceador de carga do host do Manager Service do IaaS | | mgr-svc-balance.mycompany.com |
| Endereço IP do balanceador de carga do host do Manager Service do IaaS Somente para referência; não insira endereços IP | | 123.234.203 |
| Para serviços do IaaS, conta do domínio com direitos de administrador nos hosts | | SUPPORT\provisioner |
| Senha da conta | | login123 |

Tabela 1-32. Banco de dados SQL Server do IaaS

| Variável | Meu valor | Exemplo |
|---|---------------|----------|
| Instância do banco de dados | | IAASSQL |
| Nome do banco de dados | vcac (padrão) | vcac |
| Código de acesso (usando na instalação, atualização e migração) | | login123 |

Tabela 1-33. Distributed Execution Managers do IaaS

| Variável | Meu valor | Exemplo |
|--|-----------|--------------------|
| FQDN do host de DEM | | dem.mycompany.com |
| Endereço IP do host de DEM | | 123.234.1.111 |
| Somente para referência; não insira endereços IP | | |
| FQDN do host de DEM | | dem2.mycompany.com |
| Endereço IP do host de DEM | | 123.234.1.112 |
| Somente para referência; não insira endereços IP | | |
| Nome único do DEM Orchestrator | | Orchestrator-1 |
| Nome único do DEM Orchestrator | | Orchestrator-2 |
| Nome único do DEM Worker | | Worker-1 |
| Nome único do DEM Worker | | Worker-2 |
| Nome único do DEM Worker | | Worker-3 |
| Nome único do DEM Worker | | Worker-4 |

Configurar o balanceador de carga

Após implantar os aplicativos para o vRealize Automation, você pode configurar um balanceador de carga para distribuir o tráfego entre várias instâncias do Appliance do vRealize Automation.

A lista a seguir oferece uma visão geral das etapas necessárias para configurar um balanceador de carga para o tráfego do vRealize Automation:

- 1 Instale o balanceador de carga.
- 2 Habilite a afinidade de sessão, também conhecida como sessões complexas.
- 3 Certifique-se de que o tempo limite no balanceador de carga seja de, pelo menos, 100 segundos.
- 4 Se a rede ou o balanceador de carga assim exigir, importe um certificado para o balanceador de carga. Para obter informações sobre relações e certificados confiáveis, consulte [Requisitos de confiança de certificado em um ambiente distribuído](#). Para obter informações sobre a extração de certificados, consulte [Extraindo certificados e chaves privadas](#).
- 5 Configure o balanceador de carga para tráfego do Appliance do vRealize Automation.
- 6 Configure os dispositivos para o vRealize Automation. Consulte [Configurando dispositivos para vRealize Automation](#).

Observação Ao configurar os dispositivos virtuais no balanceador de carga, faça isso apenas para os dispositivos virtuais que foram configurados para uso com o vRealize Automation. Se dispositivos não configurados forem usados, você receberá respostas de falha.

Para obter mais informações sobre balanceadores de carga, consulte [Balanceamento de carga do vRealize Automation](#).

Para obter mais informações sobre escalabilidade e alta disponibilidade, consulte o guia *Arquitetura de Referência do vRealize Automation*.

Configurando dispositivos para o vRealize Automation

Após implantar seus dispositivos e configurar o balanceamento de carga, configure os dispositivos para o vRealize Automation.

Configurar o primeiro appliance do vRealize Automation em um cluster

O appliance do vRealize Automation é uma máquina virtual parcialmente configurada que hospeda o portal da web do usuário e servidor do vRealize Automation. Baixe e implante o modelo de Formato de virtualização aberta (OVF) do appliance no vCenter Server ou no inventário do ESX/ESXi.

Pré-requisitos

- Crie um appliance não configurado. Consulte [Implantar o appliance do vRealize Automation](#).
- Obtenha um certificado de autenticação para o appliance do vRealize Automation.

Se a rede ou o balanceador de carga exigir, os procedimentos posteriores copiarão o certificado para o balanceador de carga e para os appliances adicionais.

Procedimentos

- 1 Faça login na interface de gerenciamento de appliance do vRealize Automation não configurada como raiz.

`https://vrealize-automation-appliance-FQDN:5480`

Ignore todos os avisos de certificado para continuar.

- 2 Se o assistente de instalação aparecer, cancele-o para que possa acessar a interface de gerenciamento em vez do assistente.
- 3 Selecione **Administração > Configurações de Hora** e defina a fonte de sincronização da hora.

| Opção | Descrição |
|---------------------|--|
| Hora do host | Sincronize com o host ESXi do appliance do vRealize Automation. |
| Servidor de horário | Sincronize com um servidor NTP (Protocolo de tempo de rede) externo. Insira o endereço IP ou o FQDN do servidor NTP. |

Você deve sincronizar todos os appliances do vRealize Automation e servidores IaaS Windows para a mesma fonte de horário. Não misture fontes de horário em uma implantação do vRealize Automation.

4 Selecione **Configurações do vRA > Configurações do Host**.

| Opção | Ação |
|-----------------------------------|--|
| Solucionar automaticamente | Selecione Solucionar automaticamente para especificar o nome do host atual para o appliance do vRealize Automation. |
| Atualizar host | <p>Para novos hosts, selecione Atualizar Host. Insira o nome de domínio totalmente qualificado do appliance do vRealize Automation, <i>vra-hostname.domain.name</i> na caixa de texto Nome do host.</p> <p>Para implantações distribuídas que usam balanceadores de carga, selecione Atualizar Host. Insira o nome de domínio totalmente qualificado do servidor do balanceador de carga, <i>vra-loadbalancename.domain.name</i> na caixa de texto Nome do Host.</p> |

Observação Defina configurações de SSO conforme descrito mais adiante neste procedimento sempre que você usar **Atualizar Host** para definir o nome do host.

5 Selecione o tipo de certificado no menu **Ação de Certificado**.

Se você estiver usando um certificado codificado por PEM, por exemplo, para um ambiente distribuído, selecione **Importar**.

Os certificados que você importa devem ser confiáveis e também aplicáveis a todas as instâncias do appliance do vRealize Automation e todos os balanceadores de carga por meio do uso de certificados de Nome Alternativo da Entidade (SAN).

Se quiser gerar uma solicitação CSR para um novo certificado que pode ser enviado a uma autoridade de certificação, selecione **Gerar Solicitação de Assinatura**. Uma CSR ajuda sua CA a criar um certificado com os valores corretos para você importar.

Observação Se você usar cadeias de certificados, especifique os certificados na seguinte ordem:

- a Certificado cliente/servidor assinado pelo certificado de autoridade de certificação intermediário
- b Um ou mais certificados intermediários
- c Um certificado de autoridade de certificação raiz

| Opção | Ação |
|--------------------------|---|
| Manter Existentes | Mantenha a configuração SSL atual. Selecione essa opção para cancelar as alterações. |
| Gerar Certificado | <ol style="list-style-type: none"> a O valor exibido na caixa de texto Nome comum é o Nome de host, conforme ele é exibido na parte superior da página. Se todas as instâncias adicionais do appliance do vRealize Automation estiverem disponíveis, os respectivos FQDN serão incluídos no atributo SAN do certificado. b Insira o nome da organização, como o nome da sua empresa, na caixa de texto Organização. c Insira a unidade organizacional, como o nome ou o local do departamento, na caixa de texto Unidade organizacional. d Insira um código de país ISO 3166 de duas letras, como PT_BR, na caixa de texto País. |

| Opção | Ação |
|--|---|
| Gerar solicitação de assinatura | <ul style="list-style-type: none"> a Selecione Gerar Solicitação de Assinatura. b Reveja as entradas nas caixas de texto Organização, Unidade Organizacional, Código do País e Nome Comum. Essas entradas são preenchidas do certificado existente. É possível editá-las se necessário. c Clique em Gerar CSR para gerar uma solicitação de assinatura de certificado e depois clique no link Baixar a CSR gerada aqui para abrir uma caixa de diálogo que permite salvar a CSR em um local onde ela pode ser enviada para uma autoridade de certificação. d Quando receber o certificado preparado, clique em Importar e siga as instruções para importar um certificado no vRealize Automation. |
| Importar | <ul style="list-style-type: none"> a Copie os valores do certificado, de BEGIN PRIVATE KEY até END PRIVATE KEY, incluindo o cabeçalho e o rodapé, e cole-os na caixa de texto Chave Privada RSA. b Copie os valores do certificado, de BEGIN PRIVATE KEY até END PRIVATE KEY, incluindo o cabeçalho e o rodapé, e cole-os na caixa de texto Cadeia de Certificados. Para vários valores de certificado, inclua um cabeçalho BEGIN CERTIFICATE e um rodapé END CERTIFICATE em cada certificado. <p>Observação No caso dos certificados encadeados, atributos adicionais podem estar disponíveis.</p> <ul style="list-style-type: none"> c (Opcional) Se o seu certificado usar um código de acesso para criptografar a chave do certificado, copie-o e cole-o na caixa de texto Código de Acesso. |

- 6 Clique em **Salvar Configurações** para salvar as informações do host e a configuração do SSL.
- 7 Se exigido pela sua rede ou balanceador de carga, copie o certificado importado ou recém-criado no balanceador de carga do appliance virtual.

Talvez seja necessário permitir o acesso SSH raiz, a fim de exportar o certificado.

- a Se ainda não estiver conectado, faça login no console de gerenciamento do appliance do vRealize Automation como raiz.
- b Clique na guia **Administração**.
- c Clique no submenu **Administração**.
- d Marque a caixa de seleção **Serviço SSH ativado**.
Desmarque a caixa de seleção para desativar o SSH quando terminar.
- e Marque a caixa de seleção **Login SSH do administrador**.
Desmarque a caixa de seleção para desativar o SSH quando terminar.
- f Clique em **Salvar Configurações**.

- 8 Defina as configurações do SSO.

9 Clique em **Serviços**.

Todos os serviços devem estar em execução antes de você poder instalar uma licença ou fazer login no console. Eles geralmente começam em cerca de 10 minutos.

Observação Você também pode fazer login no appliance e executar o `tail -f /var/log/vcac/catalina.out` para monitorar a inicialização do serviço.

10 Insira as informações da sua licença.

- a Clique em **Configurações do vRA > Licenciamento**.
- b Clique em **Licenciamento**.
- c Insira uma chave de licença válida do vRealize Automation que você baixou com os arquivos de instalação e clique em **Enviar Chave**.

Observação Se houver um erro de conexão, você poderá ter um problema com o balanceador de carga. Verifique a conectividade de rede do balanceador de carga.

11 Selecione se deseja ativar vRealize Code Stream e inserir uma licença vRealize Code Stream.

vRealize Code Stream não tem suporte para implantações do vRealize Automation de alta disponibilidade ou produção.

12 Clique em **Mensagens**. As definições de configuração e o status de mensagens do seu appliance são exibidos. Não altere essas configurações.

13 Clique na guia **Telemetria** para escolher se deseja participar do Programa de Aperfeiçoamento da Experiência do Cliente (CEIP) da VMware.

Os detalhes sobre os dados recolhidos pelo CEIP e os fins para os quais eles são utilizados pelo VMware são estabelecidos pelo Centro de Confiança e Garantia, em

<http://www.vmware.com/trustvmware/ceip.html>.

- Selecione **Participe do Programa de Aperfeiçoamento da Experiência do Cliente da VMware** para participar do programa.
- Desmarque **Participe do Programa de Aperfeiçoamento da Experiência do Cliente da VMware** para não participar do programa.

14 Clique em **Salvar Configurações**.

15 Confirme se você pode fazer login no vRealize Automation.

- a Abra um navegador da Web para a URL da interface de produto do vRealize Automation.
`https://vrealize-automation-appliance-FQDN/vcac`
- b Se solicitado, continue após os avisos de certificado.
- c Faça login com o `administrator@vsphere.local` e a senha que você especificou na configuração do SSO.

A interface é aberta na página Tenants na guia **Administração**. Um único tenant nomeado `vsphere.local` aparece na lista.

Configurando instâncias adicionais do appliance do vRealize Automation

O administrador do sistema pode implantar várias instâncias do appliance do vRealize Automation para garantir a redundância em um ambiente de alta disponibilidade.

Para cada appliance do vRealize Automation, você deve habilitar a sincronização de data/hora e adicionar o appliance a um cluster. As informações de configuração baseadas nas configurações do appliance do vRealize Automation inicial (principal) são adicionadas automaticamente quando você adiciona o appliance ao cluster.

Se você fizer uma instalação distribuída com balanceadores de carga para alta disponibilidade e failover, notifique a equipe responsável pela configuração do seu ambiente vRealize Automation. Seus administradores de tenant devem configurar o Gerenciamento de Diretórios para alta disponibilidade ao configurarem o link para o seu Active Directory.

Adicionar outro appliance do vRealize Automation ao cluster

Para alta disponibilidade, instalações distribuídas podem usar um balanceador de carga na frente de um cluster de nós de appliance do vRealize Automation.

Você usa a interface de gerenciamento no novo appliance do vRealize Automation para uni-lo a um cluster existente de um ou mais appliances. A operação de união copia informações de configuração para o novo appliance que você está adicionando, incluindo informações de certificado, SSO, licenciamento, banco de dados e mensagens.

Você deve adicionar um appliance de cada vez a um cluster, e não em paralelo.

Pré-requisitos

- Você já tem um ou mais appliances do vRealize Automation no cluster, e um desses appliances deve ser o nó primário. Consulte [Configurar o primeiro appliance do vRealize Automation em um cluster](#).
Você pode definir um novo appliance para ser o nó primário somente depois de uni-lo ao cluster.
- Crie o novo nó do appliance. Consulte [Implantar o appliance do vRealize Automation](#).
- Verifique se o balanceador de carga está configurado para uso com o novo appliance.
- Verifique se o tráfego pode passar pelo balanceador de carga para alcançar todos os nós atuais e o novo nó que você está prestes a adicionar.
- Verifique se todos os serviços do vRealize Automation foram iniciados nos nós atuais.

Procedimentos

- 1 Faça login na nova interface de gerenciamento de appliance do vRealize Automation como raiz.

`https://vrealize-automation-appliance-FQDN:5480`

Ignore todos os avisos de certificado para continuar.

- 2 Se o assistente de instalação aparecer, cancele-o para que possa acessar a interface de gerenciamento em vez do assistente.
- 3 Selecione **Administração > Configurações de Hora** e defina a fonte de horário para a mesma fonte usada pelo restante dos appliances do cluster.
- 4 Selecione **Configurações do vRA > Cluster**.
- 5 Digite o FQDN de um appliance previamente configurado do vRealize Automation na caixa de texto **Nó de cluster principal**.

Você pode usar o FQDN do appliance do primário do vRealize Automation ou qualquer appliance do vRealize Automation que já tenha sido unido ao cluster.

- 6 Insira a senha raiz na caixa de texto **Senha**.
- 7 Clique em **Unir cluster**.
- 8 Ignore todos os avisos de certificado para continuar.
Os serviços do cluster são reiniciados.
- 9 Verifique se os serviços estão em execução.
 - a Clique na guia **Serviços**.
 - b Clique na guia **Atualizar** para monitorar o andamento da inicialização do serviço.

Desabilitar serviços não utilizados

Para a conservação dos recursos internos em casos nos quais uma instância externa do vRealize Orchestrator é usada, você pode desativar o serviço incorporado do vRealize Orchestrator.

Pré-requisitos

[Adicionar outro appliance do vRealize Automation ao cluster](#)

Procedimentos

- 1 Faça login no console do appliance do vRealize Automation.
- 2 Pare o serviço do vRealize Orchestrator.

```
service vco-server stop
chkconfig vco-server off
```

Validar a implantação distribuída

Depois de implantar instâncias adicionais do appliance do vRealize Automation, você valida que pode acessar os appliances clusterizados.

Procedimentos

- 1 Na interface de gerenciamento do balanceador de carga ou no arquivo de configuração, desabilite temporariamente todos os nós, exceto o nó que está testando.
- 2 Confirme que você pode fazer login no vRealize Automation através do endereço do balanceador de carga:

`https://vrealize-automation-appliance-load-balancer-FQDN/vcac`

- 3 Após verificar que você pode acessar o novo appliance do vRealize Automation através do balanceador de carga, reative os outros nós.

Instalar os componentes do IaaS em uma configuração distribuída

O administrador do sistema instala os componentes do IaaS depois que os dispositivos são implantados e totalmente configurados. Os componentes do IaaS fornecem acesso aos recursos de infraestrutura do vRealize Automation.

Todos os componentes devem ser executados sob o mesmo usuário da conta de serviço, que deve ser uma conta de domínio com privilégios em cada servidor IaaS distribuído. Não use contas locais do sistema.

Pré-requisitos

- [Configurar o primeiro appliance do vRealize Automation em um cluster.](#)
- Se seu site inclui vários appliances do vRealize Automation, [Adicionar outro appliance do vRealize Automation ao cluster.](#)
- Verifique se o servidor atende aos requisitos em [Servidores Windows do IaaS.](#)
- Obtenha um certificado de uma autoridade de certificação confiável para importar para o repositório de raiz confiável das máquinas nas quais deseja instalar os dados de Site de Componente e Gerenciador Modelo.
- Se você estiver usando balanceadores de carga no ambiente, verifique se eles atendem aos requisitos de configuração.

Procedimentos

1 [Instalar certificados do IaaS](#)

Em ambientes de produção, obtenha um certificado de domínio de uma autoridade de certificação confiável. Importe o certificado para o armazenamento de certificados raiz confiável de todas as máquinas nas quais você pretende instalar o Website Component e o Manager Service (as máquinas do IIS) durante a instalação do IaaS.

2 [Baixar o Instalador IaaS do vRealize Automation](#)

Para instalar o IaaS nos seus servidores Windows virtuais ou físicos distribuídos, você precisa baixar uma cópia do instalador do IaaS a partir do appliance do vRealize Automation.

3 Escolhendo um cenário de banco de dados do IaaS

O vRealize Automation IaaS usa um banco de dados do Microsoft SQL Server para manter informações sobre as máquinas que ele gerencia e seus próprios elementos e políticas.

4 Instalar um componente de site do IaaS e dados do Model Manager

O administrador de sistema instala o componente Website para fornecer acesso aos recursos de infraestrutura no console da Web do vRealize Automation. Você pode instalar uma ou várias instâncias do componente Site, mas deve configurar o Model Manager Data na máquina que hospeda o primeiro componente Site. Instale o Model Manager Data somente uma vez.

5 Instalar componentes do servidor Web adicionais do IaaS

O servidor Web fornece acesso a capacidades de infraestrutura no vRealize Automation. Após instalar o primeiro servidor Web, você pode aumentar o desempenho instalando servidores Web adicionais de IaaS.

6 Instalar o Active Manager Service

O Manager Service ativo é um serviço do Windows que coordena a comunicação entre Distributed Execution Managers IaaS, o banco de dados, agentes, agentes de proxy e o SMTP.

7 Instalar o componente de backup do Manager Service

O Service Manager de backup fornece redundância e alta disponibilidade e poderá ser iniciado manualmente se o serviço ativo parar.

8 Instalando Distributed Execution Managers

Instale o Distributed Execution Manager como uma destas duas funções: DEM Orchestrator ou DEM Worker. Você deve instalar pelo menos uma instância do DEM para cada função e pode instalar instâncias adicionais do DEM para oferecer suporte a failover e alta disponibilidade.

9 Configurando o Windows Service para acessar o banco de dados do IaaS

O administrador do sistema pode alterar o método de autenticação usado para acessar o banco de dados de SQL durante o tempo de execução (após a instalação ser concluída). Por padrão, a identidade do Windows da conta conectada no momento é usada para conectar o banco de dados depois que ele é instalado.

10 Verificar os serviços do IaaS

Após a instalação, o administrador do sistema verifica se os serviços de IaaS estão em execução. Se os serviços estiverem em execução, a instalação será um sucesso.

Próximo passo

Instale um DEM Orchestrator e ao menos uma instância do DEM Worker. Consulte [Instalando Distributed Execution Managers](#).

Instalar certificados do IaaS

Em ambientes de produção, obtenha um certificado de domínio de uma autoridade de certificação confiável. Importe o certificado para o armazenamento de certificados raiz confiável de todas as máquinas nas quais você pretende instalar o Website Component e o Manager Service (as máquinas do IIS) durante a instalação do IaaS.

Pré-requisitos

Em máquinas Windows 2012, você deve desativar o TLS1.2 para certificados que usam SHA512. Para obter mais informações sobre como desativar o TLS 1.2, consulte [Artigo da Base de Conhecimento da Microsoft 245030](#).

Procedimentos

- 1 Obtenha um certificado de uma autoridade de certificação confiável.
- 2 Abra o Internet Information Services (IIS) Manager.
- 3 Clique duas vezes em **Certificados de Servidor** na Exibição de Recursos.
- 4 Clique em **Importar** no painel Ações.
 - a Insira um nome de arquivo na caixa de texto **Arquivo de certificado** ou clique no botão Procurar (...) para navegar até o nome de um arquivo no qual o certificado exportado está armazenado.
 - b Insira uma senha na caixa de texto **Senha** se o certificado tiver sido exportado com uma senha.
 - c Selecione **Marcar esta chave como exportável**.
- 5 Clique em **OK**.
- 6 Clique no certificado importado e selecione **Exibir**.
- 7 Verifique se o certificado e a respectiva cadeia são confiáveis.

Se o certificado não for confiável, você verá a mensagem Este certificado raiz da CA não é confiável.

Observação Você deve resolver o problema de confiança antes de prosseguir com a instalação. Se você continuar, a implementação falhará.

- 8 Reinicie o IIS ou abra uma janela do prompt de comando elevado e digite `iisreset`.

Próximo passo

[Baixar o Instalador IaaS do vRealize Automation](#).

Baixar o Instalador IaaS do vRealize Automation

Para instalar o IaaS nos seus servidores Windows virtuais ou físicos distribuídos, você precisa baixar uma cópia do instalador do IaaS a partir do appliance do vRealize Automation.

Se você vir avisos de certificado durante esse processo, ignore-os para concluir a instalação.

Pré-requisitos

- [Configurar o primeiro appliance do vRealize Automation em um cluster](#) e, opcionalmente, [Adicionar outro appliance do vRealize Automation ao cluster](#).
- Verifique se o servidor atende aos requisitos em [Servidores Windows do IaaS](#).
- Verifique se você importou um certificado para o IIS e se a raiz do certificado ou a autoridade de certificação está na raiz confiável na máquina de instalação.

- Se você estiver usando balanceadores de carga no ambiente, verifique se eles atendem aos requisitos de configuração.

Procedimentos

- 1 (Opcional) Ative o HTTP se você estiver instalando em uma máquina Windows 2012.
 - a Selecione: **Recursos > Adicionar recursos** do Server Manager.
 - b Expanda os **Serviços do WCF** nos recursos do .NET Framework.
 - c Selecione o **Ativador do HTTP**.
- 2 Faça login no servidor Windows do IaaS usando uma conta com direitos de administrador.
- 3 Abra um navegador da Web diretamente para a URL do instalador do appliance do vRealize Automation. Não use um endereço de balanceador de carga.
`https://vrealize-automation-appliance-FQDN:5480/installer`
- 4 Clique em **Instalador do IaaS**.
- 5 Salve `setup__vrealize-automation-appliance-FQDN@5480` no servidor Windows.
Não altere o nome do arquivo do instalador. Ele é utilizado para conectar a instalação ao appliance do vRealize Automation.
- 6 Baixe o arquivo do instalador em cada servidor Windows do IaaS no qual você está instalando componentes.

Próximo passo

Instale um banco de dados do IaaS, consulte [Escolhendo um cenário de banco de dados do IaaS](#).

Escolhendo um cenário de banco de dados do IaaS

O vRealize Automation IaaS usa um banco de dados do Microsoft SQL Server para manter informações sobre as máquinas que ele gerencia e seus próprios elementos e políticas.

Dependendo das preferências e dos privilégios, há vários procedimentos a serem escolhidos para a criação do banco de dados do IaaS.

Observação Você pode habilitar o SSL seguro ao criar ou atualizar o banco de dados de SQL. Por exemplo, ao criar ou atualizar o banco de dados de SQL, você pode usar a opção SSL segura para especificar que a configuração SSL que já está especificada no servidor SQL seja aplicada ao conectar ao banco de dados de SQL. O SSL oferece uma conexão mais segura entre o servidor do IaaS e o banco de dados do SQL. Essa opção, que está disponível no assistente de instalação personalizado, requer que você já tenha configurado o SSL no servidor SQL. Para obter informações relacionadas sobre como configurar o SSL no SQL Server, consulte [Artigo da Microsoft Technet 189067](#).

Tabela 1-34. Escolhendo um cenário de banco de dados do IaaS

| Cenário | Procedimento |
|---|---|
| Crie o banco de dados do IaaS manualmente usando os scripts do banco de dados fornecidos. Essa opção permite que o administrador do banco de dados revise as alterações cuidadosamente antes de criar o banco de dados. | Criar o banco de dados IaaS manualmente. |
| Prepare um banco de dados vazio e use o instalador para preencher o esquema do banco de dados. Esta opção permite ao instalador utilizar um usuário de banco de dados com privilégios dbo para preencher o banco de dados. | Preparar um banco de dados vazio. |
| Use o instalador para criar o banco de dados. Essa é a opção mais simples, mas requer o uso de privilégios sysadmin no instalador. | Criar o banco de dados do IaaS usando o assistente de instalação. |

Criar o banco de dados IaaS manualmente

O administrador do sistema do vRealize Automation pode criar o banco de dados manualmente usando scripts fornecidos pela VMware.

Pré-requisitos

- Instale o Microsoft .NET Framework 4.5.2 ou posterior no host do SQL Server.
- Use a Autenticação do Windows, em vez de usar a Autenticação do SQL, para se conectar ao banco de dados.
- Verifique os pré-requisitos de instalação do banco de dados. Consulte [Host do servidor SQL de IaaS](#).
- Abra um navegador Web para a URL do instalador do appliance do vRealize Automation e baixe os scripts de instalação do banco de dados de IaaS.

<https://vrealize-automation-appliance-FQDN:5480/installer>

Procedimentos

- 1 Navegue para o subdiretório Banco de dados no diretório em que você extraiu o arquivo zip de instalação.
- 2 Extraia o arquivo DBInstall.zip para um diretório local.
- 3 Faça login no host do banco de dados Windows com direitos suficientes para criar e arrastar privilégios **sysadmin** do banco de dados na instância do SQL Server.
- 4 Revise os scripts de implantação do banco de dados conforme necessário. Revise, especialmente, as configurações na seção DBSettings do CreateDatabase.sql e edite-as, se necessário.

As configurações no script são as configurações recomendadas. Apenas ALLOW_SNAPSHOT_ISOLATION ON e READ_COMMITTED_SNAPSHOT ON são necessárias.

5 Execute o comando a seguir com os argumentos descritos na tabela.

```
BuildDB.bat /p:DBServer=db_server;
DBName=db_name;DBDir=db_dir;
LogDir=[log_dir];ServiceUser=service_user;
ReportLogin=web_user;
VersionString=version_string
```

Tabela 1-35. Valores do banco de dados

| Variável | Valor |
|-----------------------|--|
| <i>db_server</i> | Especifica a instância do SQL Server no formato dbhostname[,port number]\SQL instance. Especifique um número de porta apenas se você estiver usando uma porta que não seja padrão. O número de porta padrão do Microsoft SQL é 1433. O valor padrão para <i>db_server</i> é localhost. |
| <i>db_name</i> | Nome do banco de dados. O valor padrão é vra. Nomes de banco de dados não devem consistir em mais de 128 caracteres ASCII. |
| <i>db_dir</i> | Caminho para o diretório de dados do banco de dados, excluindo a barra final. |
| <i>log_dir</i> | Caminho para o diretório de log do banco de dados, excluindo a barra final. |
| <i>service_user</i> | Nome de usuário com o qual o Manager é executado. |
| <i>Web_user</i> | Nome de usuário com o qual o Web Services é executado. |
| <i>version_string</i> | A versão do vRealize Automation, encontrada depois de se fazer login no appliance do vRealize Automation e clicar na guia Atualizar. Por exemplo, a cadeia de caracteres de versão do vRealize Automation 6.1 é 6.1.0.1200. |

O banco de dados é criado.

Próximo passo

[Instalar os componentes do IaaS em uma configuração distribuída.](#)

Preparar um banco de dados vazio

Um administrador de sistema do vRealize Automation pode instalar o esquema do IaaS em um banco de dados vazio. Esse método de instalação fornece máximo controle sobre a segurança do banco de dados.

Pré-requisitos

- Verifique os pré-requisitos de instalação do banco de dados. Consulte [Host do servidor SQL de IaaS](#).
- Abra um navegador Web para a URL do instalador do appliance do vRealize Automation e baixe os scripts de instalação do banco de dados de IaaS.

<https://vrealize-automation-appliance-FQDN:5480/installer>

Procedimentos

- 1 Navegue até o diretório Banco de Dados no diretório no qual você extraiu o arquivo zip de instalação.
- 2 Extraia o arquivo DBInstall.zip para um diretório local.
- 3 Faça login no banco de dados do host Windows com privilégios de **sysadmin** na instância do SQL Server.
- 4 Edite os arquivos a seguir e substitua todas as instâncias das variáveis na tabela pelos valores corretos para o seu ambiente.

```
CreateDatabase.sql
SetDatabaseSettings.sql
```

Tabela 1-36. Valores do banco de dados

| Variável | Valor |
|------------|--|
| \$(DBName) | Nome do banco de dados, como vra. Nomes de banco de dados não devem consistir em mais de 128 caracteres ASCII. |
| \$(DBDir) | Caminho para o diretório de dados do banco de dados, excluindo a barra final. |
| \$(LogDir) | Caminho para o diretório de log do banco de dados, excluindo a barra final. |

- 5 Revise as configurações na seção Configurações de BD do arquivo SetDatabaseSettings.sql e edite-as, se necessário.

As configurações no script são as configurações recomendadas para o banco de dados do IaaS. Somente ALLOW_SNAPSHOT_ISOLATION ON e READ_COMMITTED_SNAPSHOT ON são obrigatórias.

- 6 Abra o SQL Server Management Studio.
- 7 Clique em **Nova Consulta**.
Uma janela de Consulta SQL é aberta.
- 8 No menu **Consulta**, verifique se a opção **Modo SQLCMD** está selecionada.
- 9 Cole o conteúdo modificado inteiro do arquivo CreateDatabase.sql no painel de consulta.
- 10 Abaixo do conteúdo CreateDatabase.sql, cole o conteúdo modificado inteiro de SetDatabaseSettings.sql.
- 11 Clique em **Executar**.

O script é executado e cria o banco de dados.

Próximo passo

[Instalar os componentes do IaaS em uma configuração distribuída.](#)

Criar o banco de dados do IaaS usando o assistente de instalação

O vRealize Automation usa um banco de dados do Microsoft SQL Server para manter informações sobre as máquinas que ele gerencia e seus próprios elementos e políticas.

As etapas a seguir descrevem como criar o banco de dados do IaaS usando o instalador ou preencher um banco de dados vazio existente. Também é possível criar o banco de dados manualmente. Consulte [Criar o banco de dados IaaS manualmente](#).

Pré-requisitos

- Se você estiver criando o banco de dados com autenticação do Windows em vez de usar autenticação do SQL, verifique se o usuário que executa o instalador possui direitos **sysadmin** no servidor SQL.
- [Baixar o Instalador IaaS do vRealize Automation](#).

Procedimentos

- 1 Clique com o botão direito do mouse no arquivo de configuração `setup__vrealize-automation-appliance-FQDN@5480.exe` e selecione **Executar como administrador**.
- 2 Clique em **Avançar**.
- 3 Aceite o contrato de licença e clique em **Avançar**.
- 4 Na página Login, forneça as credenciais de administrador do appliance do vRealize Automation e verifique o Certificado SSL.
 - a Digite o nome de usuário, que é **root**, e a senha.
A senha é aquela que você especificou quando implantou o appliance do vRealize Automation.
 - b Selecione **Aceitar Certificado**.
 - c Clique em **Exibir Certificado**.
Compare a impressão digital do certificado com a impressão digital definida para o appliance do vRealize Automation. Você pode exibir o certificado do appliance do vRealize Automation no navegador do cliente quando o console de gerenciamento é acessado na porta 5480.
- 5 Clique em **Avançar**.
- 6 Selecione **Instalação Personalizada** na página Tipo de Instalação.
- 7 Selecione **Servidor do IaaS** em Seleção de Componentes na página Tipo de Instalação.
- 8 Aceite o local de instalação raiz ou clique em **Alterar** e selecione um caminho de instalação.
Mesmo em uma implantação distribuída, às vezes é possível instalar mais de um componente de IaaS no mesmo servidor Windows.
Se você instalar mais de um componente de IaaS, sempre os instale no mesmo caminho.
- 9 Clique em **Avançar**.
- 10 Na página Instalação personalizada do servidor do IaaS, selecione **Banco de dados**.

11 Na caixa de texto **Instância do banco de dados**, especifique a instância do banco de dados ou clique em **Examinar** e faça a seleção na lista de instâncias. Se a instância do banco de dados estiver em uma porta que não seja padrão, inclua o número da porta em uma especificação de instância usando o formulário `dbhost,SQL_port_number\SQLInstance`. O número de porta padrão do Microsoft SQL é 1443.

12 (Opcional) Marque a caixa de seleção **Usar SSL para conexão do banco de dados**.

Por padrão, a caixa de seleção fica marcada. O SSL oferece uma conexão mais segura entre o servidor do IaaS e o banco de dados do SQL. No entanto, você deve configurar primeiro o SSL no SQL Server para oferecer suporte a essa opção. Para obter mais informações sobre como configurar o SSL no SQL Server, consulte [Artigo da Microsoft Technet 189067](#).

13 Escolha o tipo de instalação do banco de dados no painel **Nome do banco de dados**.

- Selecione **Usar um banco de dados vazio existente** para criar o esquema em um banco de dados existente.
- Digite um novo nome de banco de dados ou o nome padrão **vra** para criar um novo banco de dados. Nomes de banco de dados não devem consistir em mais de 128 caracteres ASCII.

14 Desmarque a opção **Usar dados e diretórios de registro padrão** para especificar localizações alternativas ou deixe-a selecionada para usar os diretórios padrão (recomendado).

15 Selecione um método de autenticação para instalar o banco de dados na lista **Autenticação**.

- Para usar as credenciais com as quais você está executando o instalador para criar o banco de dados, selecione **Usar identidade do Windows...**
- Para usar a autenticação do SQL, desmarque a opção **Usar identidade do Windows...** Digite as credenciais de SQL nas caixas de texto Usuário e Senha.

Por padrão, a conta de usuário do serviço Windows é usada durante o acesso do tempo de execução ao banco de dados e deve ter direitos sysadmin para a instância do SQL Server. As credenciais usadas para acessar o banco de dados no tempo de execução podem ser configuradas para usar as credenciais de SQL.

A autenticação do Windows é recomendada. Quando você escolhe a autenticação SQL, a senha do banco de dados não criptografada aparece em determinados arquivos de configuração.

16 Clique em **Avançar**.

17 Conclua o Verificador de Pré-requisitos.

| Opção | Descrição |
|--------------------|--|
| Nenhum erro | Clique em Avançar . |
| Erros não críticos | Clique em Ignorar . |
| Erros críticos | Ignorar os erros críticos provoca falha na instalação. Se forem exibidos avisos, selecione o alerta no painel à esquerda e siga as instruções à direita. Resolva todos os erros críticos e clique em Verificar Novamente para realizar a verificação. |

18 Clique em **Instalar**.

19 Quando a mensagem de sucesso aparecer, desmarque a opção **Oriente-me pela configuração inicial** e clique em **Avançar**.

20 Clique em **Concluir**.

O banco de dados está pronto para uso.

Instalar um componente de site do IaaS e dados do Model Manager

O administrador de sistema instala o componente Website para fornecer acesso aos recursos de infraestrutura no console da Web do vRealize Automation. Você pode instalar uma ou várias instâncias do componente Site, mas deve configurar o Model Manager Data na máquina que hospeda o primeiro componente Site. Instale o Model Manager Data somente uma vez.

Pré-requisitos

- Instale o IaaS Database, consulte [Escolhendo um cenário de banco de dados do IaaS](#).
- Se você já instalou outros componentes do IaaS, lembre-se da senha do banco de dados que criou.
- Se você estiver usando balanceadores de carga no ambiente, verifique se eles atendem aos requisitos de configuração.

Procedimentos

1 [Instalar o primeiro componente de servidor Web do IaaS](#)

Instale o componente de servidor Web do IaaS para fornecer acesso a capacidades de infraestrutura no vRealize Automation.

2 [Configurar o Model Manager Data](#)

Instale o componente Model Manager na mesma máquina que hospeda o primeiro componente do servidor Web. Você instala o Model Manager apenas uma vez.

Você pode instalar componentes adicionais do Website ou pode instalar o Manager Service. Consulte [Instalar componentes do servidor Web adicionais do IaaS](#) ou [Instalar o Active Manager Service](#).

Instalar o primeiro componente de servidor Web do IaaS

Instale o componente de servidor Web do IaaS para fornecer acesso a capacidades de infraestrutura no vRealize Automation.

Você pode instalar múltiplos servidores Web do IaaS, mas somente o primeiro inclui o Model Manager Data.

Pré-requisitos

- [Criar o banco de dados do IaaS usando o assistente de instalação](#).
- Verifique se o servidor atende aos requisitos em [Servidores Windows do IaaS](#).
- Se você já instalou outros componentes do IaaS, lembre-se da senha do banco de dados que criou.
- Se você estiver usando balanceadores de carga no ambiente, verifique se eles atendem aos requisitos de configuração.

Procedimentos

- 1 Se estiver usando um balanceador de carga, desabilite os outros nós sob ele e verifique se o tráfego está direcionado ao nó desejado.

Além disso, desabilite verificações de integridade do balanceador de carga até que todos os componentes do vRealize Automation sejam instalados e configurados.

- 2 Clique com o botão direito do mouse no arquivo de configuração `setup__vrealize-automation-appliance-FQDN@5480.exe` e selecione **Executar como administrador**.

- 3 Clique em **Avançar**.

- 4 Aceite o contrato de licença e clique em **Avançar**.

- 5 Na página Login, forneça as credenciais de administrador do appliance do vRealize Automation e verifique o Certificado SSL.

- a Digite o nome de usuário, que é **root**, e a senha.

A senha é aquela que você especificou quando implantou o appliance do vRealize Automation.

- b Selecione **Aceitar Certificado**.

- c Clique em **Exibir Certificado**.

Compare a impressão digital do certificado com a impressão digital definida para o appliance do vRealize Automation. Você pode exibir o certificado do appliance do vRealize Automation no navegador do cliente quando o console de gerenciamento é acessado na porta 5480.

- 6 Clique em **Avançar**.

- 7 Selecione **Instalação Personalizada** na página Tipo de Instalação.

- 8 Selecione **Servidor do IaaS** em Seleção de Componentes na página Tipo de Instalação.

- 9 Aceite o local de instalação raiz ou clique em **Alterar** e selecione um caminho de instalação.

Mesmo em uma implantação distribuída, às vezes é possível instalar mais de um componente de IaaS no mesmo servidor Windows.

Se você instalar mais de um componente de IaaS, sempre os instale no mesmo caminho.

- 10 Clique em **Avançar**.

- 11 Selecione **Site** e **ModelManagerData** na página **Instalação Personalizada do Servidor do IaaS**.

- 12 Selecione um site entre os disponíveis ou aceite o site padrão na guia **Administração e Site do Model Manager**.

- 13 Digite um número de porta disponível na caixa de texto **Número de porta** ou aceite a porta padrão 443.

- 14 Clique em **Associação de Teste** para confirmar se o número da porta está disponível para uso.

15 Selecione o certificado desse componente.

- a Se você tiver importado um certificado depois de iniciar a instalação, clique em **Atualizar** para atualizar a lista.
- b Selecione o certificado a ser usado em **Certificados disponíveis**.
- c Se você tiver importado um certificado que não tem um nome simples e ele não aparecer na lista, desmarque **Exibir certificados usando nomes simples** e clique em **Atualizar**.

Se estiver instalando em um ambiente que não usa balanceadores de carga, você poderá selecionar **Gerar um Certificado Autoassinado** em vez de selecionar um certificado. Se você estiver instalando componentes Website adicionais atrás de um balanceador de carga, não gere certificados autoassinados. Importe o certificado do servidor da Web principal do IaaS para certificar-se de usar o mesmo certificado em todos os servidores atrás do balanceador de carga.

16 (Opcional) Clique em **Exibir Certificado**, exiba o certificado e clique em **OK** para fechar a janela de informações.

17 (Opcional) Selecione **Suprimir incompatibilidade de certificado** para suprimir os erros de certificado. A instalação ignora erros de incompatibilidade de nome de certificado, bem como todos os erros de correspondência da lista certificate-revocation.

Essa é uma opção menos segura.

Configurar o Model Manager Data

Instale o componente Model Manager na mesma máquina que hospeda o primeiro componente do servidor Web. Você instala o Model Manager apenas uma vez.

Pré-requisitos

[Instalar o primeiro componente de servidor Web do IaaS.](#)

Procedimentos

1 Clique na guia **Model Manager Data**.

2 Na caixa de texto **Servidor**, insira o nome do domínio totalmente qualificado do appliance do vRealize Automation.

vrealize-automation-appliance.mycompany.com

Não insira um endereço IP.

3 Clique em **Carregar** para exibir o **Tenant padrão de SSO**.

O tenant padrão `vsphere.local` é criado automaticamente quando você configura o Single Sign-On. Não o modifique.

4 Clique em **Download** para importar o certificado do dispositivo virtual.

O download do certificado pode levar alguns minutos.

5 (Opcional) Clique em **Exibir Certificado**, exiba o certificado e clique em **OK** para fechar a janela de informações.

- 6 Clique em **Aceitar certificado**.
- 7 Digite **administrator@vsphere.local** na caixa de texto **Nome do usuário** e digite a senha que você criou quando configurou o SSO nas caixas de texto **Senha** e **Confirmar**.
- 8 (Opcional) Clique em **Testar** para verificar as credenciais.
- 9 Na caixa de texto **Servidor IaaS**, identifique o componente do servidor Web do IaaS.

| Opção | Descrição |
|------------------------------------|---|
| Com um balanceador de carga | Insira o nome do domínio totalmente qualificado e o número da porta do balanceador de carga para o componente do servidor Web do IaaS, <i>web-load-balancer.mycompany.com:443</i> . Não insira endereços IP. |
| Sem um balanceador de carga | Insira o nome do domínio totalmente qualificado e o número da porta da máquina na qual você instalou o componente do servidor Web do IaaS, <i>web.mycompany.com:443</i> . Não insira endereços IP. |

A porta padrão é 443.

- 10 Clique em **Testar** para verificar a conexão do servidor.
- 11 Clique em **Avançar**.
- 12 Conclua o Verificador de Pré-requisitos.

| Opção | Descrição |
|---------------------------|--|
| Nenhum erro | Clique em Avançar . |
| Erros não críticos | Clique em Ignorar . |
| Erros críticos | Ignorar os erros críticos provoca falha na instalação. Se forem exibidos avisos, selecione o alerta no painel à esquerda e siga as instruções à direita. Resolva todos os erros críticos e clique em Verificar Novamente para realizar a verificação. |

- 13 Na página Configurações do Servidor e da Conta, nas caixas de texto de **Informações de Instalação do Servidor**, insira o nome do usuário e a senha do usuário da conta de serviço que tem privilégios administrativos no servidor de instalação atual.

O usuário da conta de serviço deve ser uma conta de domínio com privilégios em cada servidor IaaS distribuído. Não use contas locais do sistema.

- 14 Forneça a senha utilizada para gerar a chave de criptografia que protege o banco de dados.

| Opção | Descrição |
|--|--|
| Se você já tiver instalado componentes neste ambiente | Digite o código de acesso que você criou anteriormente nas caixas de texto Código de Acesso e Confirmar . |
| Se esta for a primeira instalação | Digite um código de acesso nas caixas de texto Código de Acesso e Confirmar . Você deve usar esse código de acesso sempre que instalar um novo componente. |

Manter o código de acesso em um local seguro para uso posterior.

- 15 Especifique o servidor do banco de dados do IaaS, o nome do banco de dados e o método de autenticação do servidor de banco de dados na caixa de texto **Informações de Instalação do Banco de Dados Microsoft SQL**.

Elas são as informações de servidor de banco de dados do IaaS, nome e autenticação que você criou anteriormente.

- 16 Clique em **Avançar**.
- 17 Clique em **Instalar**.
- 18 Quando a instalação for concluída, desmarque **Oriente-me pela configuração inicial** e clique em **Avançar**.

Próximo passo

Você pode instalar componentes adicionais do servidor Web ou pode instalar o Manager Service. Consulte [Instalar componentes do servidor Web adicionais do IaaS](#) ou [Instalar o Active Manager Service](#).

Instalar componentes do servidor Web adicionais do IaaS

O servidor Web fornece acesso a capacidades de infraestrutura no vRealize Automation. Após instalar o primeiro servidor Web, você pode aumentar o desempenho instalando servidores Web adicionais de IaaS.

Não instale o Model Manager Data com um componente de servidor Web adicional. Somente o primeiro componente do servidor Web hospeda o Model Manager Data.

Pré-requisitos

- [Instalar um componente de site do IaaS e dados do Model Manager](#).
- Verifique se o novo servidor atende aos requisitos em [Servidores Windows do IaaS](#).
- Use a interface de gerenciamento do appliance do vRealize Automation para substituir o certificado a incluir o FQDN do novo nó. Consulte [Substituir certificados no appliance do vRealize Automation](#).
- Se você já instalou outros componentes do IaaS, lembre-se da senha do banco de dados que criou.
- Se você estiver usando balanceadores de carga no ambiente, verifique se eles atendem aos requisitos de configuração.

Procedimentos

- 1 Se estiver usando um balanceador de carga, desabilite os outros nós sob ele e verifique se o tráfego está direcionado ao nó desejado.

Além disso, desabilite verificações de integridade do balanceador de carga até que todos os componentes do vRealize Automation sejam instalados e configurados.

- 2 Clique com o botão direito do mouse no arquivo de configuração `setup__vrealize-automation-appliance-FQDN@5480.exe` e selecione **Executar como administrador**.
- 3 Clique em **Avançar**.
- 4 Aceite o contrato de licença e clique em **Avançar**.

- 5 Na página Login, forneça as credenciais de administrador do appliance do vRealize Automation e verifique o Certificado SSL.
 - a Digite o nome de usuário, que é **root**, e a senha.

A senha é aquela que você especificou quando implantou o appliance do vRealize Automation.
 - b Selecione **Aceitar Certificado**.
 - c Clique em **Exibir Certificado**.

Compare a impressão digital do certificado com a impressão digital definida para o appliance do vRealize Automation. Você pode exibir o certificado do appliance do vRealize Automation no navegador do cliente quando o console de gerenciamento é acessado na porta 5480.
- 6 Clique em **Avançar**.
- 7 Selecione **Instalação Personalizada** na página Tipo de Instalação.
- 8 Selecione **Servidor do IaaS** em Seleção de Componentes na página Tipo de Instalação.
- 9 Aceite o local de instalação raiz ou clique em **Alterar** e selecione um caminho de instalação.

Mesmo em uma implantação distribuída, às vezes é possível instalar mais de um componente de IaaS no mesmo servidor Windows.

Se você instalar mais de um componente de IaaS, sempre os instale no mesmo caminho.
- 10 Clique em **Avançar**.
- 11 Selecione **Site** e na página **Instalação Personalizada do Servidor do IaaS**.
- 12 Selecione um site entre os disponíveis ou aceite o site padrão na guia **Administração e Site do Model Manager**.
- 13 Digite um número de porta disponível na caixa de texto **Número de porta** ou aceite a porta padrão 443.
- 14 Clique em **Associação de Teste** para confirmar se o número da porta está disponível para uso.
- 15 Selecione o certificado desse componente.
 - a Se você tiver importado um certificado depois de iniciar a instalação, clique em **Atualizar** para atualizar a lista.
 - b Selecione o certificado a ser usado em **Certificados disponíveis**.
 - c Se você tiver importado um certificado que não tem um nome simples e ele não aparecer na lista, desmarque **Exibir certificados usando nomes simples** e clique em **Atualizar**.

Se estiver instalando em um ambiente que não usa balanceadores de carga, você poderá selecionar **Gerar um Certificado Autoassinado** em vez de selecionar um certificado. Se você estiver instalando componentes Website adicionais atrás de um balanceador de carga, não gere certificados autoassinados. Importe o certificado do servidor da Web principal do IaaS para certificar-se de usar o mesmo certificado em todos os servidores atrás do balanceador de carga.

16 (Opcional) Clique em **Exibir Certificado**, exiba o certificado e clique em **OK** para fechar a janela de informações.

17 (Opcional) Selecione **Suprimir incompatibilidade de certificado** para suprimir os erros de certificado. A instalação ignora erros de incompatibilidade de nome de certificado, bem como todos os erros de correspondência da lista certificate-revocation.

Essa é uma opção menos segura.

18 Na caixa de texto **Servidor IaaS**, identifique o primeiro componente do servidor Web do IaaS.

| Opção | Descrição |
|------------------------------------|---|
| Com um balanceador de carga | Insira o nome do domínio totalmente qualificado e o número da porta do balanceador de carga para o componente do servidor Web do IaaS, <i>web-load-balancer.mycompany.com:443</i> . Não insira endereços IP. |
| Sem um balanceador de carga | Insira o nome do domínio totalmente qualificado e o número da porta da máquina na qual você instalou o primeiro componente do servidor Web do IaaS, <i>web.mycompany.com:443</i> . Não insira endereços IP. |

A porta padrão é 443.

19 Clique em **Testar** para verificar a conexão do servidor.

20 Clique em **Avançar**.

21 Conclua o Verificador de Pré-requisitos.

| Opção | Descrição |
|---------------------------|--|
| Nenhum erro | Clique em Avançar . |
| Erros não críticos | Clique em Ignorar . |
| Erros críticos | Ignorar os erros críticos provoca falha na instalação. Se forem exibidos avisos, selecione o alerta no painel à esquerda e siga as instruções à direita. Resolva todos os erros críticos e clique em Verificar Novamente para realizar a verificação. |

22 Na página Configurações do Servidor e da Conta, nas caixas de texto de **Informações de Instalação do Servidor**, insira o nome do usuário e a senha do usuário da conta de serviço que tem privilégios administrativos no servidor de instalação atual.

O usuário da conta de serviço deve ser uma conta de domínio com privilégios em cada servidor IaaS distribuído. Não use contas locais do sistema.

23 Forneça a senha utilizada para gerar a chave de criptografia que protege o banco de dados.

| Opção | Descrição |
|---|--|
| Se você já tiver instalado componentes neste ambiente | Digite o código de acesso que você criou anteriormente nas caixas de texto Código de Acesso e Confirmar . |
| Se esta for a primeira instalação | Digite um código de acesso nas caixas de texto Código de Acesso e Confirmar . Você deve usar esse código de acesso sempre que instalar um novo componente. |

Manter o código de acesso em um local seguro para uso posterior.

24 Especifique o servidor do banco de dados do IaaS, o nome do banco de dados e o método de autenticação do servidor de banco de dados na caixa de texto **Informações de Instalação do Banco de Dados Microsoft SQL**.

Elas são as informações de servidor de banco de dados do IaaS, nome e autenticação que você criou anteriormente.

25 Clique em **Avançar**.

26 Clique em **Instalar**.

27 Quando a instalação for concluída, desmarque **Orientar-me pela configuração inicial** e clique em **Avançar**.

Próximo passo

[Instalar o Active Manager Service.](#)

Instalar o Active Manager Service

O Manager Service ativo é um serviço do Windows que coordena a comunicação entre Distributed Execution Managers IaaS, o banco de dados, agentes, agentes de proxy e o SMTP.

A menos que o failover automático do Serviço de Gerenciador esteja ativado, sua implantação do IaaS exige que apenas uma máquina do Windows execute o Serviço de Gerenciador ativamente por vez. Máquinas de backup devem ter o serviço interrompido e configurado para iniciar manualmente.

Consulte [Sobre o failover automático do Serviço de Gerenciador](#).

Pré-requisitos

- Se você já instalou outros componentes do IaaS, lembre-se da senha do banco de dados que criou.
- (Opcional) Se você deseja instalar o Manager Service em um site diferente do site padrão, crie primeiro um site no Internet Information Services.
- Verifique se você tem um certificado de uma autoridade de certificação importado para o IIS e se o certificado raiz ou a autoridade de certificação é confiável. Todos os componentes no balanceador de carga devem ter o mesmo certificado.
- Verifique se o balanceador de carga do site está configurado e se o valor de tempo limite do balanceador de carga está definido como um mínimo de 180 segundos.
- [Instalar um componente de site do IaaS e dados do Model Manager.](#)

Procedimentos

- 1 Se estiver usando um balanceador de carga, desabilite os outros nós sob ele e verifique se o tráfego está direcionado ao nó desejado.

Além disso, desabilite verificações de integridade do balanceador de carga até que todos os componentes do vRealize Automation sejam instalados e configurados.

- 2 Clique com o botão direito do mouse no arquivo de configuração `setup__vrealize-automation-appliance-FQDN@5480.exe` e selecione **Executar como administrador**.

- 3 Aceite o contrato de licença e clique em **Avançar**.

- 4 Na página Login, forneça as credenciais de administrador do appliance do vRealize Automation e verifique o Certificado SSL.

- a Digite o nome de usuário, que é **root**, e a senha.

A senha é aquela que você especificou quando implantou o appliance do vRealize Automation.

- b Selecione **Aceitar Certificado**.

- c Clique em **Exibir Certificado**.

Compare a impressão digital do certificado com a impressão digital definida para o appliance do vRealize Automation. Você pode exibir o certificado do appliance do vRealize Automation no navegador do cliente quando o console de gerenciamento é acessado na porta 5480.

- 5 Clique em **Avançar**.

- 6 Selecione **Instalação Personalizada** na página Tipo de Instalação.

- 7 Selecione **Servidor do IaaS** em Seleção de Componentes na página Tipo de Instalação.

- 8 Aceite o local de instalação raiz ou clique em **Alterar** e selecione um caminho de instalação.

Mesmo em uma implantação distribuída, às vezes é possível instalar mais de um componente de IaaS no mesmo servidor Windows.

Se você instalar mais de um componente de IaaS, sempre os instale no mesmo caminho.

- 9 Clique em **Avançar**.

- 10 Selecione **Manager Service** na página **Instalação Personalizada do Servidor do IaaS**.

11 Na caixa de texto **Servidor IaaS**, identifique o componente do servidor Web do IaaS.

| Opção | Descrição |
|------------------------------------|---|
| Com um balanceador de carga | Insira o nome do domínio totalmente qualificado e o número da porta do balanceador de carga para o componente do servidor Web do IaaS, <i>web-load-balancer.mycompany.com:443</i> . Não insira endereços IP. |
| Sem um balanceador de carga | Insira o nome do domínio totalmente qualificado e o número da porta da máquina na qual você instalou o componente do servidor Web do IaaS, <i>web.mycompany.com:443</i> . Não insira endereços IP. |

A porta padrão é 443.

12 Selecione **Nó ativo com o tipo de inicialização definido como automático**.

13 Selecione um site entre os disponíveis ou aceite o site padrão na guia **Administração e Site do Model Manager**.

14 Digite um número de porta disponível na caixa de texto **Número de porta** ou aceite a porta padrão 443.

15 Clique em **Associação de Teste** para confirmar se o número da porta está disponível para uso.

16 Selecione o certificado desse componente.

- a Se você tiver importado um certificado depois de iniciar a instalação, clique em **Atualizar** para atualizar a lista.
- b Selecione o certificado a ser usado em **Certificados disponíveis**.
- c Se você tiver importado um certificado que não tem um nome simples e ele não aparecer na lista, desmarque **Exibir certificados usando nomes simples** e clique em **Atualizar**.

Se estiver instalando em um ambiente que não usa balanceadores de carga, você poderá selecionar **Gerar um Certificado Autoassinado** em vez de selecionar um certificado. Se você estiver instalando componentes Website adicionais atrás de um balanceador de carga, não gere certificados autoassinados. Importe o certificado do servidor da Web principal do IaaS para certificar-se de usar o mesmo certificado em todos os servidores atrás do balanceador de carga.

17 (Opcional) Clique em **Exibir Certificado**, exiba o certificado e clique em **OK** para fechar a janela de informações.

18 Clique em **Avançar**.

19 Verifique os pré-requisitos e clique em **Avançar**.

20 Na página Configurações do Servidor e da Conta, nas caixas de texto de **Informações de Instalação do Servidor**, insira o nome do usuário e a senha do usuário da conta de serviço que tem privilégios administrativos no servidor de instalação atual.

O usuário da conta de serviço deve ser uma conta de domínio com privilégios em cada servidor IaaS distribuído. Não use contas locais do sistema.

21 Forneça a senha utilizada para gerar a chave de criptografia que protege o banco de dados.

| Opção | Descrição |
|---|--|
| Se você já tiver instalado componentes neste ambiente | Digite o código de acesso que você criou anteriormente nas caixas de texto Código de Acesso e Confirmar . |
| Se esta for a primeira instalação | Digite um código de acesso nas caixas de texto Código de Acesso e Confirmar . Você deve usar esse código de acesso sempre que instalar um novo componente. |

Manter o código de acesso em um local seguro para uso posterior.

22 Especifique o servidor do banco de dados do IaaS, o nome do banco de dados e o método de autenticação do servidor de banco de dados na caixa de texto **Informações de Instalação do Banco de Dados Microsoft SQL**.

Elas são as informações de servidor de banco de dados do IaaS, nome e autenticação que você criou anteriormente.

23 Clique em **Avançar**.

24 Clique em **Instalar**.

25 Quando a instalação for concluída, desmarque **Orientar-me pela configuração inicial** e clique em **Avançar**.

26 Clique em **Concluir**.

Próximo passo

- Para garantir que o Manager Service que você instalou seja a instância ativa, verifique se o Serviço do vCloud Automation Center está em execução e defina como o tipo de inicialização "Automático".
- É possível que você instale outra instância do componente Manager Service como um backup passivo que você pode iniciar manualmente se a instância ativa falhar. Consulte [Instalar o componente de backup do Manager Service](#).
- O administrador do sistema pode alterar o método de autenticação usado para acessar o banco de dados de SQL durante o tempo de execução (após a instalação ser concluída). Consulte [Configurando o Windows Service para acessar o banco de dados do IaaS](#).

Instalar o componente de backup do Manager Service

O Service Manager de backup fornece redundância e alta disponibilidade e poderá ser iniciado manualmente se o serviço ativo parar.

A menos que o failover automático do Serviço de Gerenciador esteja ativado, sua implantação do IaaS exige que apenas uma máquina do Windows execute o Serviço de Gerenciador ativamente por vez. Máquinas de backup devem ter o serviço interrompido e configurado para iniciar manualmente.

Consulte [Sobre o failover automático do Serviço de Gerenciador](#).

Pré-requisitos

- Se você já instalou outros componentes do IaaS, lembre-se da senha do banco de dados que criou.

- (Opcional) Se você deseja instalar o Manager Service em um site diferente do site padrão, crie primeiro um site no Internet Information Services.
- Use a interface de gerenciamento do appliance do vRealize Automation para substituir o certificado a incluir o FQDN do novo nó. Consulte [Substituir certificados no appliance do vRealize Automation](#).
- Verifique se você tem um certificado de uma autoridade de certificação importado para o IIS e se o certificado raiz ou a autoridade de certificação é confiável. Todos os componentes no balanceador de carga devem ter o mesmo certificado.
- Verifique se o balanceador de carga Website está configurado.
- [Instalar um componente de site do IaaS e dados do Model Manager](#).

Procedimentos

- 1 Se estiver usando um balanceador de carga, desabilite os outros nós sob ele e verifique se o tráfego está direcionado ao nó desejado.

Além disso, desabilite verificações de integridade do balanceador de carga até que todos os componentes do vRealize Automation sejam instalados e configurados.

- 2 Clique com o botão direito do mouse no arquivo de configuração `setup__vrealize-automation-appliance-FQDN@5480.exe` e selecione **Executar como administrador**.

- 3 Clique em **Avançar**.

- 4 Aceite o contrato de licença e clique em **Avançar**.

- 5 Na página Login, forneça as credenciais de administrador do appliance do vRealize Automation e verifique o Certificado SSL.

- a Digite o nome de usuário, que é **root**, e a senha.

A senha é aquela que você especificou quando implantou o appliance do vRealize Automation.

- b Selecione **Aceitar Certificado**.

- c Clique em **Exibir Certificado**.

Compare a impressão digital do certificado com a impressão digital definida para o appliance do vRealize Automation. Você pode exibir o certificado do appliance do vRealize Automation no navegador do cliente quando o console de gerenciamento é acessado na porta 5480.

- 6 Clique em **Avançar**.

- 7 Selecione **Instalação Personalizada** na página Tipo de Instalação.

- 8 Selecione **Servidor do IaaS** em Seleção de Componentes na página Tipo de Instalação.

- 9 Aceite o local de instalação raiz ou clique em **Alterar** e selecione um caminho de instalação.

Mesmo em uma implantação distribuída, às vezes é possível instalar mais de um componente de IaaS no mesmo servidor Windows.

Se você instalar mais de um componente de IaaS, sempre os instale no mesmo caminho.

- 10 Clique em **Avançar**.
- 11 Selecione **Manager Service** na página **Instalação Personalizada do Servidor do IaaS**.
- 12 Na caixa de texto **Servidor IaaS**, identifique o componente do servidor Web do IaaS.

| Opção | Descrição |
|------------------------------------|---|
| Com um balanceador de carga | Insira o nome do domínio totalmente qualificado e o número da porta do balanceador de carga para o componente do servidor Web do IaaS, <i>web-load-balancer.mycompany.com:443</i> . Não insira endereços IP. |
| Sem um balanceador de carga | Insira o nome do domínio totalmente qualificado e o número da porta da máquina na qual você instalou o componente do servidor Web do IaaS, <i>web.mycompany.com:443</i> . Não insira endereços IP. |

A porta padrão é 443.

- 13 Selecione **Nó de espera frio da recuperação de desastres**.
- 14 Selecione um site entre os disponíveis ou aceite o site padrão na guia **Administração e Site do Model Manager**.
- 15 Digite um número de porta disponível na caixa de texto **Número de porta** ou aceite a porta padrão 443.
- 16 Clique em **Associação de Teste** para confirmar se o número da porta está disponível para uso.
- 17 Selecione o certificado desse componente.
 - a Se você tiver importado um certificado depois de iniciar a instalação, clique em **Atualizar** para atualizar a lista.
 - b Selecione o certificado a ser usado em **Certificados disponíveis**.
 - c Se você tiver importado um certificado que não tem um nome simples e ele não aparecer na lista, desmarque **Exibir certificados usando nomes simples** e clique em **Atualizar**.

Se estiver instalando em um ambiente que não usa balanceadores de carga, você poderá selecionar **Gerar um Certificado Autoassinado** em vez de selecionar um certificado. Se você estiver instalando componentes Website adicionais atrás de um balanceador de carga, não gere certificados autoassinados. Importe o certificado do servidor da Web principal do IaaS para certificar-se de usar o mesmo certificado em todos os servidores atrás do balanceador de carga.

- 18 (Opcional) Clique em **Exibir Certificado**, exiba o certificado e clique em **OK** para fechar a janela de informações.
- 19 Clique em **Avançar**.
- 20 Verifique os pré-requisitos e clique em **Avançar**.

- 21 Na página Configurações do Servidor e da Conta, nas caixas de texto de **Informações de Instalação do Servidor**, insira o nome do usuário e a senha do usuário da conta de serviço que tem privilégios administrativos no servidor de instalação atual.

O usuário da conta de serviço deve ser uma conta de domínio com privilégios em cada servidor IaaS distribuído. Não use contas locais do sistema.

- 22 Forneça a senha utilizada para gerar a chave de criptografia que protege o banco de dados.

| Opção | Descrição |
|---|--|
| Se você já tiver instalado componentes neste ambiente | Digite o código de acesso que você criou anteriormente nas caixas de texto Código de Acesso e Confirmar . |
| Se esta for a primeira instalação | Digite um código de acesso nas caixas de texto Código de Acesso e Confirmar . Você deve usar esse código de acesso sempre que instalar um novo componente. |

Manter o código de acesso em um local seguro para uso posterior.

- 23 Especifique o servidor do banco de dados do IaaS, o nome do banco de dados e o método de autenticação do servidor de banco de dados na caixa de texto **Informações de Instalação do Banco de Dados Microsoft SQL**.

Elas são as informações de servidor de banco de dados do IaaS, nome e autenticação que você criou anteriormente.

- 24 Clique em **Avançar**.

- 25 Clique em **Instalar**.

- 26 Quando a instalação for concluída, desmarque **Oriente-me pela configuração inicial** e clique em **Avançar**.

- 27 Clique em **Concluir**.

Próximo passo

- Para garantir que o Manager Service que você instalou seja uma instância de backup passivo, verifique se o Serviço do vRealize Automation está em execução e defina como o tipo de inicialização "Manual".
- O administrador do sistema pode alterar o método de autenticação usado para acessar o banco de dados de SQL durante o tempo de execução (após a instalação ser concluída). Consulte [Configurando o Windows Service para acessar o banco de dados do IaaS](#).

Instalando Distributed Execution Managers

Instale o Distributed Execution Manager como uma destas duas funções: DEM Orchestrator ou DEM Worker. Você deve instalar pelo menos uma instância do DEM para cada função e pode instalar instâncias adicionais do DEM para oferecer suporte a failover e alta disponibilidade.

O administrador de sistema deve escolher as máquinas de instalação que atendam aos requisitos de sistema predefinidos. O DEM Orchestrator e Worker podem residir na mesma máquina.

Quando você planejar a instalação de Distributed Execution Managers, tenha em mente as seguintes considerações:

- Os DEM Orchestrators oferecem suporte à alta disponibilidade ativa-ativa. Normalmente, você instala um DEM Orchestrator em cada máquina do Manager Service.
- Instale o Orchestrator em uma máquina com uma conectividade de rede forte com o host do Model Manager.
- Instale um segundo DEM Orchestrator em uma máquina diferente para obter failover.
- Normalmente, você instala DEM Workers no servidor do IaaS Manager Service ou em um servidor separado. O servidor deve ter conectividade de rede com o host do Model Manager.
- Você pode instalar instâncias adicionais do DEM para obter redundância e escalabilidade, incluindo várias instâncias na mesma máquina.

Há requisitos específicos para a instalação do DEM que dependem dos parâmetros que você usa. Consulte [Host do Distributed Execution Manager do IaaS](#).

Instalar os Distributed Execution Managers

Você deve instalar pelo menos um DEM Worker e um DEM Orchestrator. O procedimento de instalação é o mesmo para ambas as funções.

Os DEM Orchestrators oferecem suporte à alta disponibilidade ativa-ativa. Normalmente, você instala um único DEM Orchestrator em cada máquina do Manager Service. Você pode instalar DEM Orchestrators e DEM Workers na mesma máquina.

Pré-requisitos

[Baixar o Instalador IaaS do vRealize Automation](#).

Procedimentos

- 1 Clique com o botão direito do mouse no arquivo de configuração `setup__vrealize-automation-appliance-FQDN@5480.exe` e selecione **Executar como administrador**.
- 2 Clique em **Avançar**.
- 3 Aceite o contrato de licença e clique em **Avançar**.
- 4 Na página Login, forneça as credenciais de administrador do appliance do vRealize Automation e verifique o Certificado SSL.
 - a Digite o nome de usuário, que é **root**, e a senha.
A senha é aquela que você especificou quando implantou o appliance do vRealize Automation.
 - b Selecione **Aceitar Certificado**.
 - c Clique em **Exibir Certificado**.

Compare a impressão digital do certificado com a impressão digital definida para o appliance do vRealize Automation. Você pode exibir o certificado do appliance do vRealize Automation no navegador do cliente quando o console de gerenciamento é acessado na porta 5480.

- 5 Clique em **Avançar**.
- 6 Selecione **Instalação Personalizada** na página Tipo de Instalação.
- 7 Selecione **Distributed Execution Managers** em Seleção de Componentes na página Tipo de Instalação.

- 8 Aceite o local de instalação raiz ou clique em **Alterar** e selecione um caminho de instalação.

Mesmo em uma implantação distribuída, às vezes é possível instalar mais de um componente de IaaS no mesmo servidor Windows.

Se você instalar mais de um componente de IaaS, sempre os instale no mesmo caminho.

- 9 Clique em **Avançar**.
- 10 Verifique os pré-requisitos e clique em **Avançar**.
- 11 Insira as credenciais de login sob as quais o serviço será executado.

A conta de serviço deve ter privilégios de administrador local e deve ser a conta de domínio em uso por toda a instalação do IaaS. A conta de serviço tem privilégios em cada servidor IaaS distribuído e não deve ser uma conta de sistema local.

- 12 Clique em **Avançar**.
- 13 Selecione o tipo de instalação no menu suspenso **Função do DEM**.

| Opção | Descrição |
|--------------|---|
| Worker | O Worker executa fluxos de trabalho. |
| Orchestrator | O Orchestrator supervisiona as atividades dos DEM Workers, incluindo o agendamento e o pré-processamento de fluxos de trabalho, e monitora o status online do DEM Worker. |

- 14 Insira um nome exclusivo que identifica esse DEM na caixa de texto **Nome do DEM**.

O nome não pode incluir espaços e nem exceder 128 caracteres. Se você inserir um nome usado anteriormente, a seguinte mensagem será exibida: "O nome do DEM já existe. Para inserir um nome diferente para esse DEM, clique em Sim. Se estiver restaurando ou reinstalando um DEM com o mesmo nome, clique em Não."
- 15 (Opcional) Insira uma descrição dessa instância em **Descrição do DEM**.

- 16 Insira os nomes do host e as portas nas caixas de texto **Nome do Host do Manager Service** e **Nome do Host do Serviço da Web do Model Manager**.

| Opção | Descrição |
|-----------------------------|--|
| Com um balanceador de carga | Insira o nome do domínio totalmente qualificado e o número da porta dos balanceadores de carga para o componente do Manager Service e do servidor Web que hospeda o Model Manager, <i>mgr-svc-load-balancer.mycompany.com:443</i> e <i>web-load-balancer.mycompany.com:443</i> . Não insira endereços IP. |
| Sem um balanceador de carga | Insira o nome do domínio totalmente qualificado e o número da porta da máquina onde você instalou o Manager Service e do servidor Web que hospeda o Model Manager, <i>mgr-svc.mycompany.com:443</i> e <i>web.mycompany.com:443</i> . Não insira endereços IP. |

A porta padrão é 443.

- 17 (Opcional) Clique em **Testar** para testar as conexões com o Manager Service e o Serviço da Web do Model Manager.
- 18 Clique em **Adicionar**.
- 19 Clique em **Avançar**.
- 20 Clique em **Instalar**.
- 21 Quando a instalação for concluída, desmarque **Oriente-me pela configuração inicial** e clique em **Avançar**.
- 22 Clique em **Concluir**.

Próximo passo

- Verifique se o serviço está em execução e se o registro mostra algum erro. O nome do serviço é VMware DEM *Função - Nome*, onde a função é Orchestrator ou Worker. O local do registro é *Local de instalação*\Distributed Execution Manager\Name\Logos.
- Repita esse procedimento para instalar instâncias adicionais do DEM.

Configurar o DEM para se conectar ao SCVMM em um caminho de instalação diferente

Por padrão, o arquivo de configuração do DEM Worker usa o caminho de instalação padrão do console do Microsoft System Center Virtual Machine Manager (SCVMM). Se você instalar o console do SCVMM em um local não padrão, deverá atualizar o arquivo.

Este procedimento só será necessário se você tiver endpoints e agentes do SCVMM.

Pré-requisitos

- Saiba o caminho não padrão onde você instalou o console do SCVMM.

O caminho a seguir é o caminho padrão que você deve substituir no arquivo de configuração.

```
path="{ProgramFiles}\Microsoft System Center 2012 R2\Virtual Machine Manager\bin"
```

Procedimentos

- 1 Pare o serviço do DEM Worker.
- 2 Abra o seguinte arquivo no editor de texto.

Program Files (x86)\VMware\VCAC\Distributed Execution Manager*instance-name*\DynamicOps.DEM.exe.config

- 3 Localize a seção <assemblyLoadConfiguration>.
- 4 Atualize cada caminho usando o exemplo a seguir como diretriz.

```
<assemblyLoadConfiguration>
  <assemblies>
    <!-- List of required assemblies for Scvmm -->
    <add name="Errors" path="D:\Microsoft System Center 2012 R2\Virtual Machine Manager\bin"/>
    <add name="Microsoft.SystemCenter.VirtualMachineManager" path="D:\Microsoft System Center 2012
R2\Virtual Machine Manager\bin"/>
    <add name="Remoting" path="D:\Microsoft System Center 2012 R2\Virtual Machine Manager\bin"/>
    <add name="TraceWrapper" path="D:\Microsoft System Center 2012 R2\Virtual Machine Manager\bin"/>
    <add name="Utils" path="D:\Microsoft System Center 2012 R2\Virtual Machine Manager\bin"/>
  </assemblies>
</assemblyLoadConfiguration>
```

- 5 Salve e feche DynamicOps.DEM.exe.config.
- 6 Reinicie o serviço do DEM Worker.

Para obter mais informações, consulte [DEM Workers com SCVMM](#).

Informações adicionais sobre como preparar o ambiente do SCVMM e criar um endpoint do SCVMM estão disponíveis em [Preparando seu ambiente do SCVMM](#) e [Criar um endpoint do Hyper-V \(SCVMM\)](#).

Configurando o Windows Service para acessar o banco de dados do IaaS

O administrador do sistema pode alterar o método de autenticação usado para acessar o banco de dados de SQL durante o tempo de execução (após a instalação ser concluída). Por padrão, a identidade do Windows da conta conectada no momento é usada para conectar o banco de dados depois que ele é instalado.

Habilitar o acesso ao banco de dados do IaaS do usuário de serviço

Se o banco de dados SQL estiver instalado em um host separado do Serviço de Gerenciador, o acesso ao banco de dados do Serviço de Gerenciador deverá ser habilitado. Se o nome do usuário sob o qual o Serviço de Gerenciador será executado for o proprietário do banco de dados, nenhuma ação será necessária. Se o usuário não for o proprietário do banco de dados, o administrador do sistema deverá conceder o acesso.

Pré-requisitos

- [Escolhendo um cenário de banco de dados do IaaS](#).

- Verifique se o nome do usuário sob o qual o Serviço de Gerenciador será executado é o proprietário do banco de dados.

Procedimentos

- 1 Navegue para o diretório Banco de Dados no subdiretório para o qual você extraiu o arquivo zip de instalação.
- 2 Extraia o arquivo DBInstall.zip para um diretório local.
- 3 Faça login no host do banco de dados como um usuário com a função **sysadmin** na instância do SQL Server.
- 4 Edite o VMPS0psUser.sql e substitua todas as instâncias do \$(Usuário de Serviço) com o usuário (da Etapa 3) sob o qual o Serviço de Gerenciador será executado.
Não substitua o ServiceUser na linha que termina com WHERE name = N'ServiceUser').
- 5 Abra o SQL Server Management Studio.
- 6 Selecione o banco de dados (vCAC por padrão) em **Bancos de Dados** no painel esquerdo.
- 7 Clique em **Nova Consulta**.
A janela do SQL Query se abre no painel do lado direito.
- 8 Cole o conteúdo modificado do arquivo do VMPS0psUser.sql na janela de consulta.
- 9 Clique em **Executar**.

O acesso ao banco de dados é habilitado do Serviço de Gerenciador.

Configurar a conta de serviços do Windows para usar a autenticação SQL

Por padrão, a conta de serviço do Windows acessa o banco de dados durante o tempo de execução, mesmo que você tenha configurado o banco de dados para a autenticação SQL. Você pode alterar a autenticação em tempo de execução de Windows para SQL.

Um motivo para alterar a autenticação em tempo de execução pode ser quando, por exemplo, o banco de dados estiver em um domínio não confiável.

Pré-requisitos

Verifique se o banco de dados SQL Server do vRealize Automation existe. Comece com [Escolhendo um cenário de banco de dados do IaaS](#)

Procedimentos

- 1 Usando uma conta com privilégios de administrador, faça login no servidor Windows de IaaS que hospeda o Manager Service.
- 2 Em **Ferramentas Administrativas > Serviços**, pare o serviço do **VMware vCloud Automation Center**.

- 3 Abra os seguintes arquivos no editor de texto.

```
C:\Program Files (x86)\VMware\VCAC\Server\ManagerService.exe.config  
C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Web\Web.config
```

- 4 Em cada arquivo, localize a seção <connectionStrings>.

- 5 Substitua

```
Integrated Security=True;
```

com

```
User Id=database-username;Password=database-password;
```

- 6 Salve e feche os arquivos.

```
ManagerService.exe.config  
Web.config
```

- 7 Inicie o serviço do **VMware vCloud Automation Center**.

- 8 Use o comando `iisreset` para reiniciar o IIS.

Verificar os serviços do IaaS

Após a instalação, o administrador do sistema verifica se os serviços de IaaS estão em execução. Se os serviços estiverem em execução, a instalação será um sucesso.

Procedimentos

- 1 Na área de trabalho do Windows na máquina do IaaS, selecione **Ferramentas Administrativas > Serviços**.
- 2 Localize os serviços a seguir e verifique se o status deles é Iniciado e se o Tipo de inicialização está definido como Automático.
 - VMware DEM – Orchestrator – *Nome* em que *Nome* é a cadeia de caracteres fornecida na caixa **Nome do DEM** durante a instalação.
 - VMware DEM – Trabalhador – *Nome* em que *Nome* é a cadeia de caracteres fornecida na caixa **Nome do DEM** durante a instalação.
 - Agente do VMware vCloud Automation Center *Nome do agente*
 - VMware vCloud Automation Center Service
- 3 Feche a janela **Serviços**.

Instalando agentes do vRealize Automation

O vRealize Automation usa agentes para fazer integração a sistemas externos. Um administrador de sistema pode selecionar os agentes a serem instalados para comunicação com outras plataformas de virtualização.

O vRealize Automation usa os seguintes tipos de agentes para gerenciar sistemas externos:

- Agentes de proxy do Hypervisor (servidores vSphere, Citrix Xen Servers e Microsoft Hyper-V)
- Agentes de integração do External Provisioning Infrastructure (EPI)
- Agentes do Virtual Desktop Infrastructure (VDI)
- Agentes da Instrumentação de Gerenciamento do Windows (WMI)

Para obter alta disponibilidade, você pode instalar vários agentes para um único endpoint. Instale cada agente redundante em um servidor separado, mas nomeie-os e configure-os de forma idêntica. Os agentes redundantes fornecem alguma tolerância a falhas, mas não fornecem failover. Por exemplo, se você instalar dois agentes do vSphere, um no servidor A e um no servidor B, e o servidor A estiver disponível, o agente instalado no servidor B continuará a processar itens de trabalho. No entanto, o agente do servidor B não poderá terminar o processamento de um item de trabalho que o agente do servidor A já tiver iniciado.

Você tem a opção de instalar um agente do vSphere como parte da instalação mínima, mas, após a instalação, você também poderá adicionar outros agentes, incluindo um agente do vSphere adicional. Em uma implantação distribuída, instale todos os seus agentes depois de concluir a instalação distribuída base. Os agentes que você instala dependem dos recursos na sua infraestrutura.

Para obter informações sobre o uso de agentes do vSphere, consulte [Requisitos do agente do vSphere](#).

Definir a política de execução do PowerShell como RemoteSigned

Você deve definir a Política de execução do PowerShell de Restricted como RemoteSigned ou Unrestricted para permitir que os scripts locais do PowerShell sejam executados.

Para obter mais informações sobre a Política de Execução do PowerShell, consulte o [Artigo do Microsoft PowerShell sobre as Políticas de Execução](#). Se a sua Política de Execução do PowerShell for gerenciada em nível de política de grupo, entre em contato com o suporte de TI sobre suas restrições sobre as mudanças de políticas e consulte o [Artigo do Microsoft PowerShell sobre as Configurações de Política de Grupo](#).

Pré-requisitos

- Verifique se o Microsoft PowerShell está instalado no host de instalação antes da instalação do agente. A versão exigida depende do sistema operacional do host de instalação. Consulte a Ajuda e Suporte da Microsoft.
- Para obter mais informações sobre a Política de Execução do PowerShell, execute `help about_signing` ou `help Set-ExecutionPolicy` no prompt de comando do PowerShell.

Procedimentos

- 1 Usando uma conta de administrador, faça login na máquina de host do IaaS em que o agente está instalado.
- 2 Selecione **Iniciar > Todos os Programas > Versão do Windows PowerShell > Windows PowerShell**.
- 3 Para Remote Signed, execute `Set-ExecutionPolicy RemoteSigned`.

- 4 Para Unrestricted, execute `Set-ExecutionPolicy Unrestricted`.
- 5 Verifique se o comando gerou algum erro.
- 6 Digite `Exit` no prompt de comando do PowerShell.

Escolhendo o cenário de instalação do agente

Os agentes que você precisa instalar dependem dos sistemas externos aos quais você planeja fazer a integração.

Tabela 1-37. Escolhendo um cenário de agente

| Cenário de integração | Requisitos e procedimentos do agente |
|--|---|
| Provisione máquinas na nuvem fazendo a integração a um ambiente na nuvem como o Amazon Web Services ou Red Hat Enterprise Linux OpenStack Platform. | Você não precisa instalar um agente. |
| Provisione máquinas virtuais fazendo a integração a um ambiente vSphere. | Instalando e configurando o agente de proxy do vSphere |
| Provisione máquinas virtuais fazendo a integração a um ambiente Microsoft Hyper-V Server. | Instalando o agente de proxy do Hyper-V ou do XenServer |
| Provisione máquinas virtuais fazendo a integração a um ambiente XenServer. | <ul style="list-style-type: none"> ■ Instalando o agente de proxy do Hyper-V ou do XenServer ■ Instalando o agente do EPI para Citrix |
| Provisione máquinas virtuais fazendo a integração a um ambiente XenDesktop. | <ul style="list-style-type: none"> ■ Instalando o agente do VDI do XenDesktop ■ Instalando o agente do EPI para Citrix |
| Execute scripts do Visual Basic como etapas adicionais no processo de provisionamento antes ou depois de provisionar uma máquina ou ao cancelar o provisionamento. | Instalando o agente do EPI para scripts do Visual Basic |
| Colete dados das máquinas Windows provisionadas, por exemplo, o status do Active Directory do proprietário de uma máquina. | Instalando o agente do WMI para solicitações remotas do WMI |
| Provisione máquinas virtuais fazendo a integração a outra plataforma virtual suportada. | Você não precisa instalar um agente. |

Localização e requisitos de instalação de agente

O administrador do sistema costuma instalar os agentes no servidor do vRealize Automation que hospeda o componente do Manager Service.

Se um agente estiver instalado em outro host, a configuração de rede deverá permitir a comunicação entre o agente e a máquina de instalação do Manager Services.

Cada agente é instalado com um nome exclusivo em seu próprio diretório, `Agents\agentname`, no diretório de instalação do vRealize Automation (normalmente `Program Files(x86)\VMware\vCAC`), com sua configuração armazenada no arquivo `VRMAgent.exe.config` nesse diretório.

Instalando e configurando o agente de proxy do vSphere

Um administrador de sistema instala os agentes de proxy para comunicação com as instâncias de servidor do vSphere. Os agentes descobrem trabalhos disponíveis, recuperam informações do host e relatam itens de trabalho concluídos, além de outras alterações de status do host.

Requisitos do agente do vSphere

As credenciais do endpoint do vSphere, ou as credenciais sob as quais o serviço do agente é executado, devem ter acesso administrativo ao host de instalação. Vários agentes do vSphere devem atender aos requisitos de configuração do vRealize Automation.

Credenciais

Ao criar um endpoint que representa a instância do vCenter Server a ser gerenciada por um agente do vSphere, o agente pode usar as credenciais sob as quais o serviço está sendo executado para interagir com o vCenter Server ou especificar credenciais de endpoint separadas.

A tabela a seguir lista as permissões que as credenciais de endpoint do vSphere devem ter para gerenciar uma instância do vCenter Server. As permissões devem ser habilitadas para todos os clusters do vCenter Server, e não apenas para clusters que hospedarão endpoints.

Tabela 1-38. Permissões necessárias para o agente do vSphere gerenciar a instância do vCenter Server

| Valor do atributo | Permissão | |
|---------------------------------|---|-----------------------------|
| Repositório de dados | Alocar espaço | |
| | Navegar no repositório de dados | |
| Cluster de repositório de dados | Configurar um cluster de repositório de dados | |
| Pasta | Criar pasta | |
| | Excluir pasta | |
| Global | Gerenciar atributos personalizados | |
| | Definir atributo personalizado | |
| Rede | Atribuir rede | |
| Permissões | Modificar permissão | |
| Recurso | Atribuir VM ao pool de res | |
| | Migrar máquina virtual desligada | |
| | Migrar máquina virtual ligada | |
| Máquina virtual | Inventário | Criar com base no existente |
| | | Criar novo |
| | Interação | Mover |
| | | Remover |
| | | Configurar mídia de CD |
| | | Interação do console |

Tabela 1-38. Permissões necessárias para o agente do vSphere gerenciar a instância do vCenter Server (Continuação)

| Valor do atributo | Permissão |
|------------------------|---|
| Configuração | Interação do dispositivo |
| | Desligar (forçado) |
| | Ligar |
| | Redefinir |
| | Suspender |
| | Instalação de ferramentas |
| | Adicionar disco existente |
| | Adicionar novo disco |
| | Adicionar ou remover dispositivo |
| | Remover disco |
| | Avançado |
| | Alterar contagem de CPU |
| | Alterar recurso |
| | Estender Disco Virtual |
| | Rastreamento de alterações do dispositivo |
| Provisionamento | Memória |
| | Modificar configurações do dispositivo |
| | Renomear |
| | Definir anotação (versão 5.0 e posterior) |
| | Configurações |
| | Posicionamento de Swapfile |
| | Personalizar |
| Estado | Clonar modelo |
| | Clonar máquina virtual |
| | Implantar modelo |
| | Ler especificações de personalização |
| | Criar snapshot |
| Remover snapshot | |
| Reverter para snapshot | |

Desabilitar ou reconfigurar qualquer software de terceiros pode alterar o estado de energia de máquinas virtuais fora do vRealize Automation. Tais alterações podem interferir no gerenciamento do ciclo de vida da máquina pelo vRealize Automation.

Instalar o agente do vSphere

Instale um agente do vSphere para gerenciar as instâncias do vCenter Server. Para obter alta disponibilidade, você pode instalar um segundo agente do vSphere redundante para a mesma instância do vCenter Server. Nomeie e configure os dois agentes do vSphere de forma idêntica e instale-os em máquinas diferentes.

Pré-requisitos

- Instale o IaaS, incluindo o servidor Web e o host do Manager Service.
- Verifique se a máquina na qual você instala o agente está em um domínio confiável pelo domínio em que os componentes do IaaS estejam instalados.
- Verifique se os requisitos em [Requisitos do agente do vSphere](#) foram atendidos.
- Se você já tiver criado um endpoint do vSphere para uso com esse agente, anote o nome do endpoint.
- [Baixar o Instalador IaaS do vRealize Automation](#).

Procedimentos

- 1 Clique com o botão direito do mouse no arquivo de configuração `setup__vrealize-automation-appliance-FQDN@5480.exe` e selecione **Executar como administrador**.
- 2 Clique em **Avançar**.
- 3 Aceite o contrato de licença e clique em **Avançar**.
- 4 Na página Login, forneça as credenciais de administrador do appliance do vRealize Automation e verifique o Certificado SSL.
 - a Digite o nome de usuário, que é **root**, e a senha.
A senha é aquela que você especificou quando implantou o appliance do vRealize Automation.
 - b Selecione **Aceitar Certificado**.
 - c Clique em **Exibir Certificado**.
Compare a impressão digital do certificado com a impressão digital definida para o appliance do vRealize Automation. Você pode exibir o certificado do appliance do vRealize Automation no navegador do cliente quando o console de gerenciamento é acessado na porta 5480.
- 5 Selecione **Instalação Personalizada** na página Tipo de Instalação.
- 6 Na área da Seleção de Componente, selecione **Agentes de Proxy**.
- 7 Aceite o local de instalação raiz ou clique em **Alterar** e selecione um caminho de instalação.
Mesmo em uma implantação distribuída, às vezes é possível instalar mais de um componente de IaaS no mesmo servidor Windows.
Se você instalar mais de um componente de IaaS, sempre os instale no mesmo caminho.
- 8 Clique em **Avançar**.

- 9 Faça login com privilégios de administrador para os serviços do Windows na máquina de instalação.
O serviço deve ser executado na mesma máquina de instalação.
- 10 Clique em **Avançar**.
- 11 Selecione vSphere na lista **Tipo do agente**.
- 12 Insira um identificador para esse agente na caixa de texto **Nome do agente**.

Mantenha um registro do nome do agente, das credenciais, do nome do endpoint e da instância da plataforma de cada agente. Você precisará dessas informações para configurar endpoints e adicionar hosts no futuro.

Importante Para alta disponibilidade, você pode adicionar agentes redundantes e configurá-los de forma idêntica. Caso contrário, mantenha os agentes exclusivos.

| Opção | Descrição |
|--------------------------|--|
| Agente redundante | Instale agentes redundantes em servidores diferentes. Nomeie e configure agentes redundantes de forma idêntica. |
| Agente autônomo | Atribua um nome exclusivo ao agente. |

- 13 Configure uma conexão com o host IaaS Manager Service.

| Opção | Descrição |
|------------------------------------|---|
| Com um balanceador de carga | Insira o nome do domínio totalmente qualificado e o número da porta do balanceador de carga para o componente Manager Service, <i>mgr-svc-load-balancer.mycompany.com:443</i> . Não insira endereços IP. |
| Sem um balanceador de carga | Insira o nome do domínio totalmente qualificado e o número da porta da máquina na qual você instalou o componente Manager Service, <i>mgr-svc.mycompany.com:443</i> . Não insira endereços IP. |

A porta padrão é 443.

- 14 Configure uma conexão com o servidor Web IaaS.

| Opção | Descrição |
|------------------------------------|---|
| Com um balanceador de carga | Insira o nome do domínio totalmente qualificado e o número da porta do balanceador de carga para o componente de servidor Web, <i>web-load-balancer.mycompany.com:443</i> . Não insira endereços IP. |
| Sem um balanceador de carga | Insira o nome do domínio totalmente qualificado e o número da porta da máquina na qual você instalou o componente de servidor Web, <i>web.mycompany.com:443</i> . Não insira endereços IP. |

A porta padrão é 443.

- 15 Clique em **Testar** para verificar a conectividade com cada host.

16 Insira o nome do endpoint.

O nome do endpoint configurado no vRealize Automation deve corresponder ao nome do endpoint fornecido ao agente de proxy do vSphere durante a instalação, ou o endpoint não funcionará.

17 Clique em **Adicionar**.

18 Clique em **Avançar**.

19 Clique em **Instalar** para iniciar a instalação.

Depois de vários minutos, será exibida uma mensagem de êxito.

20 Clique em **Avançar**.

21 Clique em **Concluir**.

22 Verifique se a instalação foi bem-sucedida.

23 (Opcional) Adicionar vários agentes com diferentes configurações e um endpoint no mesmo sistema.

Próximo passo

[Configurar o agente do vSphere.](#)

Configurar o agente do vSphere

Configure o agente do vSphere em preparação para criar e usar endpoints do vSphere em blueprints do vRealize Automation.

Você usa o utilitário do agente de proxy para modificar as porções criptografadas do arquivo de configuração do agente, ou para alterar a política de exclusão da máquina para as plataformas de virtualização. Somente parte do arquivo de configuração do agente `VRMAgent.exe.config` está criptografada. Por exemplo, a seção `serviceConfiguration` não está criptografada.

Pré-requisitos

Usando uma conta com privilégios de administrador, faça login no servidor Windows de IaaS onde você instalou o agente do vSphere.

Procedimentos

1 Abra um prompt de comando do Windows como administrador.

2 Altere a pasta de instalação do agente, onde *nome-do-agente* é a pasta contendo o agente do vSphere.

```
cd %SystemDrive%\Program Files (x86)\VMware\VCAC\Agents\nome-do-agente
```

3 (Opcional) Para visualizar as configurações atuais, insira o comando a seguir.

```
DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config get
```

Veja a seguir um exemplo da saída do comando.

```
managementEndpointName: VCendpoint
doDeletes: True
```

- 4 (Opcional) Para alterar o nome do endpoint que você configurou na instalação, use o comando a seguir.

```
set managementEndpointName
```

Por exemplo: `DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set managementEndpointName meu-endpoint`

Você usa este processo para renomear o endpoint no vRealize Automation em vez de alterar os endpoints.

- 5 (Opcional) Para configurar a política de exclusão da máquina virtual, use o comando a seguir.

```
set doDeletes
```

Por exemplo: `DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set doDeletes falso`

| Opção | Descrição |
|------------|--|
| verdadeiro | (Padrão) Exclua máquinas virtuais destruídas no vRealize Automation do vCenter Server. |
| falso | Mova as máquinas virtuais destruídas no vRealize Automation para o diretório VRMDeleted no vCenter Server. |

- 6 Abra **Ferramentas Administrativas > Serviços** e reinicie o serviço Agente do vRealize Automation – *nome-do-agente*.

Próximo passo

Para obter alta disponibilidade, você pode instalar e configurar um agente redundante para o endpoint. Instale cada agente redundante em um servidor separado, mas nomeie-os e configure-os de forma idêntica.

Instalando o agente de proxy do Hyper-V ou do XenServer

Um administrador de sistema instala os agentes de proxy para comunicação com as instâncias de servidor do Hyper-V e do XenServer. Os agentes descobrem trabalhos disponíveis, recuperam informações do host e relatam itens de trabalho concluídos, além de outras alterações de status do host.

Requisitos do Hyper-V e do XenServer

Os agentes de proxy do Hyper-V Hypervisor exigem credenciais de administrador de sistema para a instalação.

As credenciais sob as quais o serviço do agente é executado devem ter acesso administrativo ao host de instalação.

São exigidas credenciais de nível de administrador para todas as instâncias do XenServer ou do Hyper-V nos hosts a serem gerenciados pelo agente.

Se você estiver usando pools Xen, todos os nós no pool Xen deverão ser identificados pelos respectivos nomes de domínio totalmente qualificados.

Observação Por padrão, o Hyper-V não está configurado para gerenciamento remoto. Um agente de proxy do vRealize Automation Hyper-V não pode comunicar-se com um servidor do Hyper-V, a menos que o gerenciamento remoto tenha sido ativado.

Consulte a documentação do Microsoft Windows Server para obter informações sobre como configurar o Hyper-V para gerenciamento remoto.

Instalar o agente do Hyper-V ou do XenServer

O agente do Hyper-V gerencia as instâncias do servidor do Hyper-V. O agente do XenServer gerencia as instâncias do servidor do XenServer.

Pré-requisitos

- Instale o IaaS, incluindo o servidor Web e o host do Manager Service.
- [Baixar o Instalador IaaS do vRealize Automation.](#)
- Verifique se agentes de proxy do Hyper-V Hypervisor têm credenciais de administrador do sistema.
- Verifique se as credenciais sob as quais o serviço do agente é executado têm acesso administrativo ao host de instalação.
- Verifique se todas as instâncias do XenServer ou do Hyper-V nos hosts a serem gerenciados pelo agente têm credenciais de nível de administrador.
- Se você estiver usando pools Xen, observe que todos os nós no pool Xen deverão ser identificados pelos respectivos nomes de domínio totalmente qualificados.

O vRealize Automation não pode se comunicar com ou gerenciar qualquer nó que não esteja identificado por seu nome de domínio totalmente qualificado no pool Xen.

- Configure o Hyper-V para gerenciamento remoto para ativar a comunicação do servidor do Hyper-V com os agentes de proxy do vRealize Automation Hyper-V.

Consulte a documentação do Microsoft Windows Server para obter informações sobre como configurar o Hyper-V para gerenciamento remoto.

Procedimentos

- 1 Clique com o botão direito do mouse no arquivo de configuração `setup__vrealize-automation-appliance-FQDN@5480.exe` e selecione **Executar como administrador**.
- 2 Clique em **Avançar**.
- 3 Aceite o contrato de licença e clique em **Avançar**.

- 4 Na página Login, forneça as credenciais de administrador do appliance do vRealize Automation e verifique o Certificado SSL.
 - a Digite o nome de usuário, que é **root**, e a senha.
A senha é aquela que você especificou quando implantou o appliance do vRealize Automation.
 - b Selecione **Aceitar Certificado**.
 - c Clique em **Exibir Certificado**.
Compare a impressão digital do certificado com a impressão digital definida para o appliance do vRealize Automation. Você pode exibir o certificado do appliance do vRealize Automation no navegador do cliente quando o console de gerenciamento é acessado na porta 5480.
- 5 Selecione **Instalação Personalizada** na página Tipo de Instalação.
- 6 Selecione **Seleção de Componentes** na página Tipo de Instalação.
- 7 Aceite o local de instalação raiz ou clique em **Alterar** e selecione um caminho de instalação.
Mesmo em uma implantação distribuída, às vezes é possível instalar mais de um componente de IaaS no mesmo servidor Windows.
Se você instalar mais de um componente de IaaS, sempre os instale no mesmo caminho.
- 8 Clique em **Avançar**.
- 9 Faça login com privilégios de administrador para os serviços do Windows na máquina de instalação.
O serviço deve ser executado na mesma máquina de instalação.
- 10 Clique em **Avançar**.
- 11 Selecione o agente na lista **Tipo do agente**.
 - Xen
 - Hyper-V
- 12 Insira um identificador para esse agente na caixa de texto **Nome do agente**.
Mantenha um registro do nome do agente, das credenciais, do nome do endpoint e da instância da plataforma de cada agente. Você precisará dessas informações para configurar endpoints e adicionar hosts no futuro.

Importante Para alta disponibilidade, você pode adicionar agentes redundantes e configurá-los de forma idêntica. Caso contrário, mantenha os agentes exclusivos.

| Opção | Descrição |
|--------------------------|--|
| Agente redundante | Instale agentes redundantes em servidores diferentes. Nomeie e configure agentes redundantes de forma idêntica. |
| Agente autônomo | Atribua um nome exclusivo ao agente. |

- 13 Informe o **Nome do agente** ao administrador do IaaS que configura endpoints.

Para ativar o acesso e a coleta de dados, o endpoint deve ser vinculado ao agente configurado para ele.

- 14 Configure uma conexão com o host IaaS Manager Service.

| Opção | Descrição |
|-----------------------------|---|
| Com um balanceador de carga | Insira o nome do domínio totalmente qualificado e o número da porta do balanceador de carga para o componente Manager Service, <i>mgr-svc-load-balancer.mycompany.com:443</i> . Não insira endereços IP. |
| Sem um balanceador de carga | Insira o nome do domínio totalmente qualificado e o número da porta da máquina na qual você instalou o componente Manager Service, <i>mgr-svc.mycompany.com:443</i> . Não insira endereços IP. |

A porta padrão é 443.

- 15 Configure uma conexão com o servidor Web IaaS.

| Opção | Descrição |
|-----------------------------|---|
| Com um balanceador de carga | Insira o nome do domínio totalmente qualificado e o número da porta do balanceador de carga para o componente de servidor Web, <i>web-load-balancer.mycompany.com:443</i> . Não insira endereços IP. |
| Sem um balanceador de carga | Insira o nome do domínio totalmente qualificado e o número da porta da máquina na qual você instalou o componente de servidor Web, <i>web.mycompany.com:443</i> . Não insira endereços IP. |

A porta padrão é 443.

- 16 Clique em **Testar** para verificar a conectividade com cada host.
- 17 Insira as credenciais de um usuário com permissões de nível administrativo na instância do servidor gerenciado.
- 18 Clique em **Adicionar**.
- 19 Clique em **Avançar**.
- 20 (Opcional) Adicione outro agente.
Por exemplo, você pode adicionar um agente do Xen se tiver adicionado anteriormente o agente do Hyper-V.
- 21 Clique em **Instalar** para iniciar a instalação.
Depois de vários minutos, será exibida uma mensagem de êxito.
- 22 Clique em **Avançar**.
- 23 Clique em **Concluir**.
- 24 Verifique se a instalação foi bem-sucedida.

Próximo passo

Para obter alta disponibilidade, você pode instalar e configurar um agente redundante para o endpoint. Instale cada agente redundante em um servidor separado, mas nomeie-os e configure-os de forma idêntica.

[Configurar o agente do Hyper-V ou do XenServer.](#)

Configurar o agente do Hyper-V ou do XenServer

O administrador do sistema pode modificar as configurações do agente de proxy, como a política de exclusão de plataformas de virtualização. Você pode usar o utilitário de agente de proxy para modificar as configurações iniciais que são criptografadas no arquivo de configuração do agente.

Pré-requisitos

Faça login como **administrador do sistema** na máquina em que você instalou o agente.

Procedimentos

- 1 Altere o diretório de instalação dos agentes, onde *agent_name* é o diretório que contém o agente de proxy, que também corresponde ao nome com o qual o agente está instalado.

```
cd Program Files (x86)\VMware\VCAC Agents\agent_name
```

- 2 Exiba as configurações atuais.

```
DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config get
```

Veja a seguir um exemplo do comando de saída:

```
Username: XAdmin
```

- 3 Insira o comando set para alterar uma propriedade, onde *property* corresponde a uma das opções mostradas na tabela.

```
DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set property value
```

Se você omitir *value*, o utilitário solicitará um novo valor.

| Propriedade | Descrição |
|-------------|--|
| username | O nome de usuário representando as credenciais no nível do administrador para o servidor XenServer ou Hyper-V com o qual o agente de comunica. |
| password | A senha para o nome de usuário no nível do administrador. |

- 4 Clique em **Iniciar > Ferramentas administrativas > Serviços** e reinicie o serviço vRealize Automation Agent – *agentname*.

Exemplo: Alterar as credenciais no nível do administrador

Insira o comando a seguir para alterar as credenciais no nível do administrador para a plataforma de virtualização especificada durante a instalação do agente.

```
DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set username jsmith
```

```
DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set password
```

Próximo passo

Para obter alta disponibilidade, você pode instalar e configurar um agente redundante para o endpoint. Instale cada agente redundante em um servidor separado, mas nomeie-os e configure-os de forma idêntica.

Instalando o agente do VDI do XenDesktop

O vRealize Automation usa agentes do Desktop Integration (VDI) PowerShell para registrar as máquinas XenDesktop que eles provisionam em sistemas externos de gerenciamento de desktop.

O agente de integração do VDI fornece aos proprietários das máquinas registradas uma conexão direta com a interface da Web do XenDesktop. Você pode instalar um agente do VDI como um agente dedicado para interação com um único Desktop Delivery Controller (DDC) ou como um agente geral que pode interagir com vários DDCs.

Requisitos do XenDesktop

Um administrador do sistema instala um agente de infraestrutura desktop virtual (VDI) para integrar os servidores XenDesktop no vRealize Automation.

Você pode instalar um agente de VDI geral para interagir com vários servidores. Se você estiver instalando um agente dedicado por servidor por razões de balanceamento de carga ou de autorização, deverá fornecer o nome do servidor XenDesktop DDC ao instalar o agente. Um agente dedicado pode manipular apenas as solicitações de registro direcionadas para o servidor especificado na respectiva configuração.

Consulte o *Matriz de suporte do vRealize Automation* no site da VMware para obter informações sobre as versões compatíveis do XenDesktop para servidores XenDesktop DDC.

Host e credenciais de instalação

As credenciais sob as quais o agente é executado deve ter acesso administrativo a todos os servidores XenDesktop DDC com as quais ele interage.

Requisitos do XenDesktop

O nome dado ao Host do XenServer no seu servidor XenDesktop deve coincidir com o UUID do Pool Xen no XenCenter. Consulte [Definir o nome de host do XenServer](#) para obter mais informações.

Cada servidor XenDesktop DDC com o qual você pretende registrar máquinas deve ser configurado da seguinte maneira:

- O tipo de grupo/catálogo deve ser definido como **Existente** para ser usado com o vRealize Automation.
- O nome de um host do vCenter Server em um servidor DDC deve coincidir com o nome da instância do vCenter Server, como inserido no endpoint do vRealize Automation vSphere, sem o domínio. O endpoint deve ser configurado com um nome de domínio totalmente qualificado (FQDN) e não com um endereço IP. Por exemplo, se o endereço no endpoint for `https://virtual-center27.domain/sdk`, o nome do host no servidor DDC deverá ser definido como `virtual-center27`.

Se o seu endpoint do vRealize Automation vSphere tiver sido configurado com um endereço IP, você deverá alterá-lo para usar um FQDN. Consulte *Configuração do IaaS* para obter mais informações sobre como configurar endpoints.

Requisitos do host do agente do XenDesktop

O SDK do Citrix XenDesktop deve ser instalado. O SDK do XenDesktop está incluído no disco de instalação do XenDesktop.

Verifique se o Microsoft PowerShell está instalado no host de instalação antes da instalação do agente. A versão exigida depende do sistema operacional do host de instalação. Consulte a Ajuda e Suporte da Microsoft.

A Política de Execução do MS PowerShell é definida como RemoteSigned ou Unrestricted. Consulte [Definir a política de execução do PowerShell como RemoteSigned](#).

Para obter mais informações sobre a Política de Execução do PowerShell, execute `help about_signing` ou `help Set-ExecutionPolicy` no prompt de comando do PowerShell.

Definir o nome de host do XenServer

No XenDesktop, o nome dado ao Host do XenServer no seu servidor XenDesktop deve coincidir com o UUID do Pool Xen no XenCenter. Se nenhum XenPool for configurado, o nome deverá coincidir com o UUID do XenServer em si.

Procedimentos

- 1 No Citrix XenCenter, selecione seu XenPool ou XenServer autônomo e clique na guia **Geral**. Grave o UUID.
- 2 Ao adicionar seu Pool XenServer ou host autônomo ao XenDesktop, digite o UUID que foi gravado na etapa anterior como o nome de **Conexão**.

Instalar o agente do XenDesktop

Os agentes do Virtual Desktop Integration (VDI) PowerShell se integram sistemas de desktop virtual externos, como o XenDesktop e o Citrix. Use um agente do VDI PowerShell para gerenciar a máquina XenDesktop.

Pré-requisitos

- Instale o IaaS, incluindo o servidor Web e o host do Manager Service.
- Verifique se os requisitos em [Requisitos do XenDesktop](#) foram atendidos.
- [Baixar o Instalador IaaS do vRealize Automation](#).

Procedimentos

- 1 Clique com o botão direito do mouse no arquivo de configuração `setup__vrealize-automation-appliance-FQDN@5480.exe` e selecione **Executar como administrador**.
- 2 Clique em **Avançar**.
- 3 Aceite o contrato de licença e clique em **Avançar**.
- 4 Na página Login, forneça as credenciais de administrador do appliance do vRealize Automation e verifique o Certificado SSL.
 - a Digite o nome de usuário, que é **root**, e a senha.

A senha é aquela que você especificou quando implantou o appliance do vRealize Automation.
 - b Selecione **Aceitar Certificado**.
 - c Clique em **Exibir Certificado**.

Compare a impressão digital do certificado com a impressão digital definida para o appliance do vRealize Automation. Você pode exibir o certificado do appliance do vRealize Automation no navegador do cliente quando o console de gerenciamento é acessado na porta 5480.
- 5 Clique em **Avançar**.
- 6 Selecione **Instalação Personalizada** na página Tipo de Instalação.
- 7 Selecione **Agentes Proxy** no painel Seleção do Componente.
- 8 Aceite o local de instalação raiz ou clique em **Alterar** e selecione um caminho de instalação.

Mesmo em uma implantação distribuída, às vezes é possível instalar mais de um componente de IaaS no mesmo servidor Windows.

Se você instalar mais de um componente de IaaS, sempre os instale no mesmo caminho.
- 9 Clique em **Avançar**.
- 10 Faça login com privilégios de administrador para os serviços do Windows na máquina de instalação.

O serviço deve ser executado na mesma máquina de instalação.
- 11 Clique em **Avançar**.
- 12 Selecione **VdiPowerShell** na lista **Tipo do agente**.

13 Insira um identificador para esse agente na caixa de texto **Nome do agente**.

Mantenha um registro do nome do agente, das credenciais, do nome do endpoint e da instância da plataforma de cada agente. Você precisará dessas informações para configurar endpoints e adicionar hosts no futuro.

Importante Para alta disponibilidade, você pode adicionar agentes redundantes e configurá-los de forma idêntica. Caso contrário, mantenha os agentes exclusivos.

| Opção | Descrição |
|--------------------------|--|
| Agente redundante | Instale agentes redundantes em servidores diferentes. Nomeie e configure agentes redundantes de forma idêntica. |
| Agente autônomo | Atribua um nome exclusivo ao agente. |

14 Configure uma conexão com o host IaaS Manager Service.

| Opção | Descrição |
|------------------------------------|---|
| Com um balanceador de carga | Insira o nome do domínio totalmente qualificado e o número da porta do balanceador de carga para o componente Manager Service, <i>mgr-svc-load-balancer.mycompany.com:443</i> . Não insira endereços IP. |
| Sem um balanceador de carga | Insira o nome do domínio totalmente qualificado e o número da porta da máquina na qual você instalou o componente Manager Service, <i>mgr-svc.mycompany.com:443</i> . Não insira endereços IP. |

A porta padrão é 443.

15 Configure uma conexão com o servidor Web IaaS.

| Opção | Descrição |
|------------------------------------|---|
| Com um balanceador de carga | Insira o nome do domínio totalmente qualificado e o número da porta do balanceador de carga para o componente de servidor Web, <i>web-load-balancer.mycompany.com:443</i> . Não insira endereços IP. |
| Sem um balanceador de carga | Insira o nome do domínio totalmente qualificado e o número da porta da máquina na qual você instalou o componente de servidor Web, <i>web.mycompany.com:443</i> . Não insira endereços IP. |

A porta padrão é 443.

16 Clique em **Testar** para verificar a conectividade com cada host.

17 Selecione a **Versão do VDI**.

18 Insira o nome de domínio totalmente qualificado do servidor de gerenciado na caixa de texto **Servidor do VDI**.

19 Clique em **Adicionar**.

20 Clique em **Avançar**.

21 Clique em **Instalar** para iniciar a instalação.

Depois de vários minutos, será exibida uma mensagem de êxito.

22 Clique em **Avançar**.

23 Clique em **Concluir**.

24 Verifique se a instalação foi bem-sucedida.

25 (Opcional) Adicionar vários agentes com diferentes configurações e um endpoint no mesmo sistema.

Próximo passo

Para obter alta disponibilidade, você pode instalar e configurar um agente redundante para o endpoint. Instale cada agente redundante em um servidor separado, mas nomeie-os e configure-os de forma idêntica.

Instalando o agente do EPI para Citrix

Os agentes do External provisioning Integration (EPI) PowerShell integram máquinas Citrix externas ao processo de provisionamento. O agente do EPI fornece streaming sob demanda das imagens de disco Citrix das quais as máquinas são inicializadas e executadas.

Os agentes do EPI dedicados interagem com um único servidor de provisionamento externo. Você deve instalar um agente do EPI para cada instância do servidor de provisionamento Citrix.

Requisitos do servidor de provisionamento Citrix

O administrador do sistema usa agentes de EPI (infraestrutura de provisionamento externo) para integrar os servidores de provisionamento Citrix e para habilitar o uso de scripts do Visual Basic no processo de provisionamento.

Credenciais e localização da instalação

Instale o agente no host PVS para as instâncias dos serviços de provisionamento Citrix. Verifique se o host de instalação atende aos [Requisitos do host do agente Citrix](#) antes de instalar o agente.

Embora um agente de EPI geralmente possa interagir com múltiplos servidores, o servidor de provisionamento Citrix requer um agente de EPI dedicado. Você deve instalar um agente de EPI para cada instância do servidor de provisionamento Citrix, informando o nome do servidor que o hospeda. As credenciais utilizadas pelo agente devem ter direitos administrativos para a instância do servidor de provisionamento Citrix.

Consulte o *Matriz de suporte do vRealize Automation* para obter informações sobre as versões suportadas do Citrix PVS.

Requisitos do host do agente Citrix

O PowerShell e o SDK dos serviços de provisionamento Citrix devem ser instalados no host de instalação antes da instalação do agente. Consulte *Matriz de suporte do vRealize Automation* no site da VMware para obter mais informações.

Verifique se o Microsoft PowerShell está instalado no host de instalação antes da instalação do agente. A versão exigida depende do sistema operacional do host de instalação. Consulte a Ajuda e Suporte da Microsoft.

Você também deve ter certeza de que o snap-in do PowerShell esteja instalado. Para obter mais informações, consulte o *Guia do programador de PowerShell de serviços de provisionamento Citrix* no site da Citrix.

A Política de Execução do MS PowerShell é definida como RemoteSigned ou Unrestricted. Consulte [Definir a política de execução do PowerShell como RemoteSigned](#).

Para obter mais informações sobre a Política de Execução do PowerShell, execute `help about_signing` ou `help Set-ExecutionPolicy` no prompt de comando do PowerShell.

Instalar o agente do Citrix

Os agentes do External provisioning integration (EPI) PowerShell integram sistemas externos ao processo de provisionamento de máquinas. Use o agente do EPI PowerShell para integração com servidor de provisionamento Citrix para permitir o provisionamento de máquinas por streaming de disco sob demanda.

Pré-requisitos

- Instale o IaaS, incluindo o servidor Web e o host do Manager Service.
- Verifique se os requisitos em [Requisitos do servidor de provisionamento Citrix](#) foram atendidos.
- [Baixar o Instalador IaaS do vRealize Automation](#).

Procedimentos

- 1 Clique com o botão direito do mouse no arquivo de configuração `setup__vrealize-automation-appliance-FQDN@5480.exe` e selecione **Executar como administrador**.
- 2 Clique em **Avançar**.
- 3 Aceite o contrato de licença e clique em **Avançar**.
- 4 Na página Login, forneça as credenciais de administrador do appliance do vRealize Automation e verifique o Certificado SSL.
 - a Digite o nome de usuário, que é **root**, e a senha.
A senha é aquela que você especificou quando implantou o appliance do vRealize Automation.
 - b Selecione **Aceitar Certificado**.
 - c Clique em **Exibir Certificado**.
Compare a impressão digital do certificado com a impressão digital definida para o appliance do vRealize Automation. Você pode exibir o certificado do appliance do vRealize Automation no navegador do cliente quando o console de gerenciamento é acessado na porta 5480.
- 5 Selecione **Instalação Personalizada** na página Tipo de Instalação.
- 6 Selecione **Seleção de Componentes** na página Tipo de Instalação.

- 7 Aceite o local de instalação raiz ou clique em **Alterar** e selecione um caminho de instalação.

Mesmo em uma implantação distribuída, às vezes é possível instalar mais de um componente de IaaS no mesmo servidor Windows.

Se você instalar mais de um componente de IaaS, sempre os instale no mesmo caminho.

- 8 Clique em **Avançar**.
- 9 Faça login com privilégios de administrador para os serviços do Windows na máquina de instalação. O serviço deve ser executado na mesma máquina de instalação.
- 10 Clique em **Avançar**.
- 11 Selecione **EPIPowerShell** na lista Tipo do agente.
- 12 Insira um identificador para esse agente na caixa de texto **Nome do agente**.

Mantenha um registro do nome do agente, das credenciais, do nome do endpoint e da instância da plataforma de cada agente. Você precisará dessas informações para configurar endpoints e adicionar hosts no futuro.

Importante Para alta disponibilidade, você pode adicionar agentes redundantes e configurá-los de forma idêntica. Caso contrário, mantenha os agentes exclusivos.

| Opção | Descrição |
|--------------------------|--|
| Agente redundante | Instale agentes redundantes em servidores diferentes. Nomeie e configure agentes redundantes de forma idêntica. |
| Agente autônomo | Atribua um nome exclusivo ao agente. |

- 13 Configure uma conexão com o host IaaS Manager Service.

| Opção | Descrição |
|------------------------------------|---|
| Com um balanceador de carga | Insira o nome do domínio totalmente qualificado e o número da porta do balanceador de carga para o componente Manager Service, <i>mgr-svc-load-balancer.mycompany.com:443</i> . Não insira endereços IP. |
| Sem um balanceador de carga | Insira o nome do domínio totalmente qualificado e o número da porta da máquina na qual você instalou o componente Manager Service, <i>mgr-svc.mycompany.com:443</i> . Não insira endereços IP. |

A porta padrão é 443.

14 Configure uma conexão com o servidor Web IaaS.

| Opção | Descrição |
|-----------------------------|---|
| Com um balanceador de carga | Insira o nome do domínio totalmente qualificado e o número da porta do balanceador de carga para o componente de servidor Web, <i>web-load-balancer.mycompany.com:443</i> . Não insira endereços IP. |
| Sem um balanceador de carga | Insira o nome do domínio totalmente qualificado e o número da porta da máquina na qual você instalou o componente de servidor Web, <i>web.mycompany.com:443</i> . Não insira endereços IP. |

A porta padrão é 443.

15 Clique em **Testar** para verificar a conectividade com cada host.

16 Selecione o tipo do EPI.

17 Insira o nome de domínio totalmente qualificado do servidor de gerenciado na caixa de texto **Servidor do EPI**.

18 Clique em **Adicionar**.

19 Clique em **Avançar**.

20 Clique em **Instalar** para iniciar a instalação.

Depois de vários minutos, será exibida uma mensagem de êxito.

21 Clique em **Avançar**.

22 Clique em **Concluir**.

23 Verifique se a instalação foi bem-sucedida.

24 (Opcional) Adicionar vários agentes com diferentes configurações e um endpoint no mesmo sistema.

Próximo passo

Para obter alta disponibilidade, você pode instalar e configurar um agente redundante para o endpoint. Instale cada agente redundante em um servidor separado, mas nomeie-os e configure-os de forma idêntica.

Instalando o agente do EPI para scripts do Visual Basic

Um administrador de sistema pode especificar scripts do Visual Basic como etapas adicionais no processo de provisionamento antes ou depois do provisionamento de uma máquina ou ao cancelar o provisionamento de uma máquina. Você deve instalar um External Provisioning Integration (EPI) PowerShell antes executar scripts do Visual Basic.

Os scripts do Visual Basic são especificados no blueprint do qual as máquinas são provisionadas. Esses scripts têm acesso a todas as propriedades personalizadas associadas à máquina e podem atualizar os valores delas. Em seguida, a próxima etapa no fluxo de trabalho tem acesso a esses novos valores.

Por exemplo, você poderia usar um script para gerar certificados ou tokens de segurança antes do provisionamento e usá-los no provisionamento de máquinas.

Para ativar scripts no provisionamento, você deve instalar um tipo específico de agente do EPI e colocar os scripts que deseja usar no sistema no qual o agente está instalado.

Ao executar um script, o agente do EPI passa todas as propriedades personalizadas da máquina como argumentos para o script. Para retornar os valores de propriedade atualizados, você deve colocar essas propriedades em um dicionário e chame uma função do vRealize Automation. Um script de amostra está incluído no subdiretório de scripts do diretório de instalação do agente do EPI. Esse script contém um cabeçalho para carregar todos os argumentos para um dicionário, um corpo no qual você pode incluir suas funções e um rodapé para retornar os valores das propriedades personalizadas atualizadas.

Observação Você pode instalar vários agentes do EPI/VBScript em vários servidores e provisionar utilizando um agente específico e os scripts do Visual Basic no host do agente. Se você precisar fazer isso, entre em contato com o suporte ao cliente da VMware.

Requisitos dos scripts do Visual Basic

Um administrador do sistema instala os agentes da Infraestrutura de provisionamento externo (EPI) para habilitar o uso dos scripts do Visual Basic no processo de provisionamento.

A tabela a seguir descreve os requisitos aplicáveis à instalação de um agente do EPI para habilitar o uso dos scripts do Visual Basic no processo de provisionamento.

Tabela 1-39. Agentes do EPI para script visual

| Requisito | Descrição |
|---------------------------------------|--|
| Credenciais | As credenciais sob as quais o agente será executado devem ter acesso administrativo ao host de instalação. |
| Microsoft PowerShell | O Microsoft PowerShell deve ser instalado no host de instalação antes da instalação do agente: a versão necessária depende do sistema operacional do host de instalação e pode ter sido instalada com esse sistema operacional. Acesse http://support.microsoft.com para mais informações. |
| Política de execução do MS PowerShell | A Política de execução do MS PowerShell deve ser definida como RemoteSigned ou Unrestricted . Para obter informações sobre a Política de execução do PowerShell, emita um dos seguintes comandos no prompt de comando do PowerShell: <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <pre>help about_signing help Set-ExecutionPolicy</pre> </div> |

Instalar o agente do EPI para scripts do Visual Basic

Os agentes do External provisioning integration (EPI) PowerShell permitem a integração de sistemas externos ao processo de provisionamento de máquinas. Use um agente do EPI para executar scripts do Visual Basic como etapas adicionais durante o processo de provisionamento.

Pré-requisitos

- Instale o IaaS, incluindo o servidor Web e o host do Manager Service.
- Verifique se os requisitos em [Requisitos dos scripts do Visual Basic](#) foram atendidos.

- [Baixar o Instalador IaaS do vRealize Automation.](#)

Procedimentos

- 1 Clique com o botão direito do mouse no arquivo de configuração `setup__vrealize-automation-appliance-FQDN@5480.exe` e selecione **Executar como administrador**.
- 2 Clique em **Avançar**.
- 3 Aceite o contrato de licença e clique em **Avançar**.
- 4 Na página Login, forneça as credenciais de administrador do appliance do vRealize Automation e verifique o Certificado SSL.
 - a Digite o nome de usuário, que é **root**, e a senha.

A senha é aquela que você especificou quando implantou o appliance do vRealize Automation.
 - b Selecione **Aceitar Certificado**.
 - c Clique em **Exibir Certificado**.

Compare a impressão digital do certificado com a impressão digital definida para o appliance do vRealize Automation. Você pode exibir o certificado do appliance do vRealize Automation no navegador do cliente quando o console de gerenciamento é acessado na porta 5480.
- 5 Selecione **Instalação Personalizada** na página Tipo de Instalação.
- 6 Selecione **Seleção de Componentes** na página Tipo de Instalação.
- 7 Aceite o local de instalação raiz ou clique em **Alterar** e selecione um caminho de instalação.

Mesmo em uma implantação distribuída, às vezes é possível instalar mais de um componente de IaaS no mesmo servidor Windows.

Se você instalar mais de um componente de IaaS, sempre os instale no mesmo caminho.
- 8 Clique em **Avançar**.
- 9 Faça login com privilégios de administrador para os serviços do Windows na máquina de instalação.

O serviço deve ser executado na mesma máquina de instalação.
- 10 Clique em **Avançar**.
- 11 Selecione **EPIPowerShell** na lista Tipo do agente.

12 Insira um identificador para esse agente na caixa de texto **Nome do agente**.

Mantenha um registro do nome do agente, das credenciais, do nome do endpoint e da instância da plataforma de cada agente. Você precisará dessas informações para configurar endpoints e adicionar hosts no futuro.

Importante Para alta disponibilidade, você pode adicionar agentes redundantes e configurá-los de forma idêntica. Caso contrário, mantenha os agentes exclusivos.

| Opção | Descrição |
|--------------------------|--|
| Agente redundante | Instale agentes redundantes em servidores diferentes. Nomeie e configure agentes redundantes de forma idêntica. |
| Agente autônomo | Atribua um nome exclusivo ao agente. |

13 Configure uma conexão com o host IaaS Manager Service.

| Opção | Descrição |
|------------------------------------|---|
| Com um balanceador de carga | Insira o nome do domínio totalmente qualificado e o número da porta do balanceador de carga para o componente Manager Service, <i>mgr-svc-load-balancer.mycompany.com:443</i> . Não insira endereços IP. |
| Sem um balanceador de carga | Insira o nome do domínio totalmente qualificado e o número da porta da máquina na qual você instalou o componente Manager Service, <i>mgr-svc.mycompany.com:443</i> . Não insira endereços IP. |

A porta padrão é 443.

14 Configure uma conexão com o servidor Web IaaS.

| Opção | Descrição |
|------------------------------------|---|
| Com um balanceador de carga | Insira o nome do domínio totalmente qualificado e o número da porta do balanceador de carga para o componente de servidor Web, <i>web-load-balancer.mycompany.com:443</i> . Não insira endereços IP. |
| Sem um balanceador de carga | Insira o nome do domínio totalmente qualificado e o número da porta da máquina na qual você instalou o componente de servidor Web, <i>web.mycompany.com:443</i> . Não insira endereços IP. |

A porta padrão é 443.

15 Clique em **Testar** para verificar a conectividade com cada host.

16 Selecione o tipo do EPI.

17 Insira o nome de domínio totalmente qualificado do servidor de gerenciado na caixa de texto **Servidor do EPI**.

18 Clique em **Adicionar**.

19 Clique em **Avançar**.

20 Clique em **Instalar** para iniciar a instalação.

Depois de vários minutos, será exibida uma mensagem de êxito.

21 Clique em **Avançar**.

22 Clique em **Concluir**.

23 Verifique se a instalação foi bem-sucedida.

24 (Opcional) Adicionar vários agentes com diferentes configurações e um endpoint no mesmo sistema.

Instalando o agente do WMI para solicitações remotas do WMI

Um administrador de sistema ativa que o protocolo Instrumentação de Gerenciamento do Windows (WMI) e instala o agente do WMI em todas as máquinas Windows gerenciadas para ativar o gerenciamento de dados e operações. O agente é obrigado a coletar dados de máquinas Windows, como o status do Active Directory do proprietário de uma máquina.

Ativar solicitações WMI remotas em máquinas Windows

Para usar os agentes WMI, as solicitações WMI remotas devem estar ativadas nos servidores Windows gerenciados.

Procedimentos

- 1 Em cada domínio que contém máquinas virtuais do Windows provisionadas e gerenciadas, crie um grupo do Active Directory e adicione a ele as credenciais de serviço dos agentes WMI que executam solicitações WMI remotas nas máquinas provisionadas.
- 2 Ative as solicitações WMI remotas para os grupos do Active Directory que contém as credenciais do agente em cada máquina do Windows provisionada.

Instalar o agente do WMI

O agente do Windows Management Instrumentation (WMI) permite a coleta de dados de máquinas Windows gerenciadas.

Pré-requisitos

- Instale o IaaS, incluindo o servidor Web e o host do Manager Service.
- Verifique se os requisitos em [Ativar solicitações WMI remotas em máquinas Windows](#) foram atendidos.
- [Baixar o Instalador IaaS do vRealize Automation](#).

Procedimentos

- 1 Clique com o botão direito do mouse no arquivo de configuração `setup__vrealize-automation-appliance-FQDN@5480.exe` e selecione **Executar como administrador**.
- 2 Clique em **Avançar**.
- 3 Aceite o contrato de licença e clique em **Avançar**.

- 4 Na página Login, forneça as credenciais de administrador do appliance do vRealize Automation e verifique o Certificado SSL.
 - a Digite o nome de usuário, que é **root**, e a senha.
A senha é aquela que você especificou quando implantou o appliance do vRealize Automation.
 - b Selecione **Aceitar Certificado**.
 - c Clique em **Exibir Certificado**.
Compare a impressão digital do certificado com a impressão digital definida para o appliance do vRealize Automation. Você pode exibir o certificado do appliance do vRealize Automation no navegador do cliente quando o console de gerenciamento é acessado na porta 5480.
- 5 Selecione **Instalação Personalizada** na página Tipo de Instalação.
- 6 Selecione **Seleção de Componentes** na página Tipo de Instalação.
- 7 Aceite o local de instalação raiz ou clique em **Alterar** e selecione um caminho de instalação.
Mesmo em uma implantação distribuída, às vezes é possível instalar mais de um componente de IaaS no mesmo servidor Windows.
Se você instalar mais de um componente de IaaS, sempre os instale no mesmo caminho.
- 8 Clique em **Avançar**.
- 9 Faça login com privilégios de administrador para os serviços do Windows na máquina de instalação.
O serviço deve ser executado na mesma máquina de instalação.
- 10 Clique em **Avançar**.
- 11 Selecione **WMI** na lista **Tipo do agente**.
- 12 Insira um identificador para esse agente na caixa de texto **Nome do agente**.
Mantenha um registro do nome do agente, das credenciais, do nome do endpoint e da instância da plataforma de cada agente. Você precisará dessas informações para configurar endpoints e adicionar hosts no futuro.

Importante Para alta disponibilidade, você pode adicionar agentes redundantes e configurá-los de forma idêntica. Caso contrário, mantenha os agentes exclusivos.

| Opção | Descrição |
|--------------------------|--|
| Agente redundante | Instale agentes redundantes em servidores diferentes. Nomeie e configure agentes redundantes de forma idêntica. |
| Agente autônomo | Atribua um nome exclusivo ao agente. |

13 Configure uma conexão com o host IaaS Manager Service.

| Opção | Descrição |
|-----------------------------|---|
| Com um balanceador de carga | Insira o nome do domínio totalmente qualificado e o número da porta do balanceador de carga para o componente Manager Service, <i>mgr-svc-load-balancer.mycompany.com:443</i> . Não insira endereços IP. |
| Sem um balanceador de carga | Insira o nome do domínio totalmente qualificado e o número da porta da máquina na qual você instalou o componente Manager Service, <i>mgr-svc.mycompany.com:443</i> . Não insira endereços IP. |

A porta padrão é 443.

14 Configure uma conexão com o servidor Web IaaS.

| Opção | Descrição |
|-----------------------------|---|
| Com um balanceador de carga | Insira o nome do domínio totalmente qualificado e o número da porta do balanceador de carga para o componente de servidor Web, <i>web-load-balancer.mycompany.com:443</i> . Não insira endereços IP. |
| Sem um balanceador de carga | Insira o nome do domínio totalmente qualificado e o número da porta da máquina na qual você instalou o componente de servidor Web, <i>web.mycompany.com:443</i> . Não insira endereços IP. |

A porta padrão é 443.

15 Clique em **Testar** para verificar a conectividade com cada host.

16 Clique em **Adicionar**.

17 Clique em **Avançar**.

18 Clique em **Instalar** para iniciar a instalação.

Depois de vários minutos, será exibida uma mensagem de êxito.

19 Clique em **Avançar**.

20 Clique em **Concluir**.

21 Verifique se a instalação foi bem-sucedida.

22 (Opcional) Adicionar vários agentes com diferentes configurações e um endpoint no mesmo sistema.

Instalação silenciosa do vRealize Automation

O vRealize Automation inclui opções para instalação silenciosa com scripts a partir da linha de comando, e instalação silenciosa baseada em API. Ambas as abordagens exigem que você prepare, com antecedência, os valores que iria inserir a mão normalmente durante uma instalação convencional.

Sobre a instalação silenciosa do vRealize Automation

A instalação silenciosa do vRealize Automation utiliza um executável que faz referência a um arquivo de resposta baseado em texto.

No arquivo de resposta, pré-configura FQDNs do sistema, credenciais de conta e outras configurações que normalmente são adicionadas durante uma instalação convencional baseada em assistente ou manual. A instalação silenciosa é útil para os seguintes tipos de implantações.

- Implantando vários ambientes quase idênticos
- Reimplantando repetidamente o mesmo ambiente
- Realizando instalações autônomas
- Realizando instalações com script

Realizar uma instalação silenciosa do vRealize Automation

Você pode realizar uma instalação autônoma e silenciosa do vRealize Automation a partir do console de um appliance recém-implantado do vRealize Automation.

Pré-requisitos

- Crie um appliance não configurado. Consulte [Implantar o appliance do vRealize Automation](#).
- Crie ou identifique seus servidores Windows IaaS e configure seus pré-requisitos.
- Instale o Agente de Gerenciamento nos seus servidores Windows IaaS.

Você pode instalar o Agente de Gerenciamento usando o download de arquivo .msi tradicional ou o processo silencioso descrito em [Realizar uma instalação silenciosa do Agente de Gerenciamento do vRealize Automation](#).

Procedimentos

- 1 Faça login no console do appliance do vRealize Automation como raiz.
- 2 Navegue até o seguinte diretório.

```
/usr/lib/vcac/tools/install
```
- 3 Abra o arquivo de resposta `ha.properties` em um editor de texto.
- 4 Adicione entradas específicas para a sua implantação em `ha.properties` e salve e feche o arquivo.
Como alternativa, você pode economizar tempo copiando e modificando um arquivo `ha.properties` de outra implantação em vez de editar o arquivo padrão inteiro.
- 5 No mesmo diretório, inicie a instalação executando o comando a seguir.

```
vra-ha-config.sh
```

A instalação pode demorar até uma hora ou mais para ser concluída, dependendo do ambiente e do tamanho da implantação.

- 6 (Opcional) Quando a instalação terminar, examine o arquivo de log.

`/var/log/vcac/vra-ha-config.log`

O instalador silencioso não salva dados de propriedades no registro, como senhas, licenças ou certificados.

Realizar uma instalação silenciosa do Agente de Gerenciamento do vRealize Automation

Você pode realizar uma instalação do Agente de Gerenciamento do vRealize Automation baseada na linha de comando em qualquer servidor Windows IaaS.

A instalação silenciosa do Agente de Gerenciamento consiste em um script do Windows PowerShell no qual você personaliza algumas configurações. Depois de adicionar configurações específicas da implantação, você pode instalar silenciosamente o Agente de Gerenciamento em todos os seus servidores Windows IaaS executando cópias do mesmo script em cada um deles.

Pré-requisitos

- Crie um appliance não configurado. Consulte [Implantar o appliance do vRealize Automation](#).
- Crie ou identifique seus servidores Windows IaaS e configure seus pré-requisitos.

Procedimentos

- 1 Faça login no servidor Windows do IaaS usando uma conta com direitos de administrador.
- 2 Abra um navegador da Web para o URL do instalador do appliance do vRealize Automation.
`https://vrealize-automation-appliance-FQDN:5480/installer`
- 3 Clique com o botão direito do mouse no arquivo de script PowerShell `InstallManagementAgent.ps1` e salve-o na área de trabalho ou em uma pasta no servidor Windows IaaS.
- 4 Abra `InstallManagementAgent.ps1` em um editor de texto.
- 5 Próximo do início do arquivo de script, adicione as configurações específicas da implantação.
 - O URL do appliance do vRealize Automation
`https://vrealize-automation-appliance-FQDN:5480`
 - Credenciais de conta de usuário raiz do appliance do vRealize Automation
 - Credenciais do usuário de serviços do vRealize Automation, uma conta de domínio com privilégios de administrador nos servidores Windows IaaS
 - A pasta em que você deseja instalar o Agente de Gerenciamento, Arquivos de Programas (x86) por padrão
 - (Opcional) A impressão digital do certificado no formato PEM que você está usando para autenticação
- 6 Salve e feche `InstallManagementAgent.ps1`.

- 7 Para instalar silenciosamente o Agente de Gerenciamento, clique duas vezes em `InstallManagementAgent.ps1`.
- 8 (Opcional) Verifique se a instalação foi concluída localizando **Agente de Gerenciamento do VMware vCloud Automation Center** na lista Programas e Recursos do Painel de Controle do Windows e na lista de serviços do Windows em execução.

Arquivo de resposta de instalação silenciosa do vRealize Automation

Instalações silenciosas do vRealize Automation exigem que você prepare um arquivo de resposta baseado em texto com antecedência.

Todos os Appliance do vRealize Automations recém-implantados contêm um arquivo de resposta padrão.

```
/usr/lib/vcac/tools/install/ha.properties
```

Para realizar uma instalação silenciosa, é necessário usar um editor de texto para personalizar as configurações em `ha.properties` para a implantação que você deseja instalar. Os exemplos a seguir são algumas das configurações e informações que você deve adicionar.

- Seu vRealize Automation ou a chave de licença de pacote
- FQDNs de nós do Appliance do vRealize Automation
- Credenciais da conta do usuário root do Appliance do vRealize Automation
- FQDNs de servidores Windows IaaS que atuarão agir como nós da Web, nós do Service Manager e assim por diante
- Credenciais do usuário de serviços do vRealize Automation, uma conta de domínio com privilégios de administrador nos servidores Windows IaaS
- FQDNs de balanceadores de carga
- Parâmetros do banco de dados SQL Server
- Parâmetros do agente de proxy para conexão com recursos de virtualização
- Se o instalador silencioso deve tentar corrigir pré-requisitos ausentes do servidor Windows IaaS

O instalador silencioso pode corrigir muitos pré-requisitos ausentes do Windows. Porém, alguns problemas de configuração, como CPU insuficiente, não podem ser alterados pelo instalador silencioso.

Para poupar tempo, é possível reutilizar e modificar um arquivo `ha.properties` que foi configurado para outra implantação, uma em que as configurações eram semelhantes. Além disso, quando você instala o vRealize Automation não silenciosamente usando o Assistente de Instalação, o assistente cria e salva suas configurações no arquivo `ha.properties`. O arquivo pode ser útil para reutilização e modificação ao instalar silenciosamente uma implementação semelhante.

O assistente não salva configurações de propriedade no arquivo `ha.properties`, como senhas, licenças ou certificados.

A linha de comando de instalação do vRealize Automation

O vRealize Automation inclui uma interface de linha de comando baseada em console para a realização de ajustes de instalação que podem ser necessários após a instalação inicial.

A interface de linha de comando (CLI) pode executar tarefas de instalação e configuração que não estão mais disponíveis na interface baseada em navegador após a instalação inicial. Os recursos da CLI incluem a nova verificação de pré-requisitos, a instalação de componentes IaaS, a instalação de certificados ou a definição do nome do host do vRealize Automation para o qual os usuários apontam seus navegadores da Web.

A CLI também é útil para usuários avançados que desejam certas operações de script. Algumas funções da CLI são usadas pela instalação silenciosa e, por isso, conhecer ambos os recursos reforçará seus conhecimentos sobre scripts de instalação do vRealize Automation.

Noções básicas sobre linha de comando de instalação do vRealize Automation

A interface de linha de comando de instalação do vRealize Automation inclui operações básicas de nível superior.

As operações básicas exibem IDs de nó do vRealize Automation, executam comandos, reportam o status do comando ou exibem as informações de ajuda. Para mostrar essas operações e suas opções na exibição do console, insira o seguinte comando sem opções ou qualificadores.

```
vra-command
```

Exibir IDs de nó

Você precisa de IDs de nó do vRealize Automation para poder executar comandos nos sistemas de destino corretos. Para exibir IDs de nó, insira o seguinte comando.

```
vra-command list-nodes
```

Anote os IDs do nó antes de executar comandos em máquinas específicas.

Executar comandos

A maioria das funções de linha de comando envolve executar um comando em um nó no cluster do vRealize Automation. Para executar um comando, use a seguinte sintaxe.

```
vra-command execute --node ID-do-nó nome-do-comando --nome-do-parâmetro valor-do-parâmetro
```

Como mostra a sintaxe anterior, muitos comandos exigem parâmetros e valores de parâmetros selecionados pelo usuário.

Exibir status do comando

Alguns comandos demoram alguns minutos ou até mais para serem concluídos. Para monitorar o progresso de um comando inserido, digite o seguinte comando.

```
vra-command status
```

O comando de status é especialmente útil para monitorar uma instalação silenciosa, que pode levar bastante tempo para tamanhos maiores de implementação.

Exibir a ajuda

Para exibir a ajuda de todos os comandos disponíveis, insira o seguinte comando.

```
vra-command help
```

Para exibir a ajuda de um único comando, insira o seguinte comando.

```
vra-command help nome-do-comando
```

Nomes de comandos de instalação do vRealize Automation

Comandos dão acesso via console a muitas tarefas de instalação e configuração do vRealize Automation que talvez você queira realizar após a instalação inicial.

Exemplos de comandos disponíveis incluem as seguintes funções.

- Adicionando outro appliance do vRealize Automation a uma instalação existente
- Definindo o nome do host para o qual os usuários apontam um navegador da Web quando acessam o vRealize Automation
- Criando o banco de dados SQL Server IaaS
- Executando o verificador de pré-requisitos em um servidor Windows IaaS
- Importando certificados

Para obter uma lista completa de comandos disponíveis do vRealize Automation, faça login no appliance do vRealize Automation e digite o seguinte comando.

```
vra-command help
```

A longa lista de nomes de comandos e parâmetros não é reproduzida em uma documentação separada. Use a lista efetivamente, identifique um comando de interesse e restrinja o seu foco inserindo o seguinte comando.

```
vra-command help nome-do-comando
```

O API de instalação do vRealize Automation

O API REST do vRealize Automation para instalação permite que você crie instalações controladas puramente por software para o vRealize Automation.

O API de instalação requer uma versão formatada do JSON das mesmas entradas que a instalação baseada em CLI obtém do arquivo de resposta `ha.properties`. As diretrizes a seguir familiarizam você com o funcionamento do API. Desse ponto, você deverá ser capaz de desenvolver chamadas programáticas ao API para instalar o vRealize Automation.

- Para acessar a documentação da API, aponte um navegador Web para a seguinte página do appliance do vRealize Automation.

`https://vrealize-automation-appliance-FQDN:5480/config`

É necessário ter um appliance do vRealize Automation não configurado. Consulte [Implantar o appliance do vRealize Automation](#).

- Para testar a instalação baseada em API, localize e execute o seguinte comando PUT:

```
PUT /vra-install
```

- Copie o JSON não populado da caixa **install_json** para um editor de texto. Preencha os valores de resposta da mesma forma que você faria em `ha.properties`. Quando suas respostas formatadas para JSON estiverem prontas, copie o código de volta para **install_json** e sobrescreva o JSON não populado.

Alternativamente, você pode editar o JSON de modelo a seguir e copiar o resultado para **install_json**.

```
/usr/lib/vcac/tools/install/installationProperties.json
```

Você também pode converter um `ha.properties` preenchido para JSON ou vice-versa.

- Na caixa de ação, selecione **validar** e clique em **Testar**.

A ação de validação executa o verificador e corretor de pré-requisito do vRealize Automation.

- A resposta da validação inclui um ID de comando alfanumérico que você pode inserir no seguinte comando GET.

```
GET /commands/command-id/aggregated-status
```

A resposta ao comando GET inclui o progresso da operação de validação.

- Ao concluir a validação com sucesso, você pode executar a instalação em si repetindo o processo. Na caixa de ação, selecione **instalar** em vez de **validar**.

A instalação pode demorar bastante dependendo do tamanho da implementação. Novamente, localize o ID de comando e use o comando GET de status agregado para obter o progresso da instalação. A resposta do GET pode ser semelhante ao exemplo a seguir.

```
"progress": "78%", "counts": {"failed": 0, "completed": 14, "total": 18, "queued": 3, "processing": 1}, "failed-commands": 0
```

- Se algo der errado durante a instalação, você pode ativar a coleta de log para todos os nós usando o comando a seguir.

```
PUT /commands/log-bundle
```

Semelhante à instalação, o ID de comando alfanumérico retornado permite que você monitore o status da coleta de log.

Converter entre Propriedades Silenciosas do vRealize Automation e JSON

Para instalações silenciosas do vRealize Automation baseadas em CLI ou API, você pode converter um arquivo de resposta de propriedades concluído para JSON ou vice-versa. A instalação silenciosa do CLI requer o arquivo de propriedades, enquanto o API requer o formato JSON.

Pré-requisitos

Um arquivo de resposta de propriedades concluído um arquivo de JSON completo

```
/usr/lib/vcac/tools/install/ha.properties
```

ou

```
/usr/lib/vcac/tools/install/installationProperties.json
```

Procedimentos

- 1 Faça login em uma sessão do console do appliance do vRealize Automation como raiz.
- 2 Execute o script do conversor adequado.

- Converter JSON para propriedades

```
/usr/lib/vcac/tools/install/convert-properties --from-json  
installationProperties.json
```

O script cria um novo arquivo de propriedades com o timestamp no nome, por exemplo:

```
ha.2016-10-17_13.02.15.properties
```

- Converter propriedades para JSON

```
/usr/lib/vcac/tools/install/convert-properties --to-json ha.properties
```

O script cria um novo arquivo `installationProperties.json` com o timestamp no nome, por exemplo:

```
installationProperties.2016-10-17_13.36.13.json
```

Você também pode exibir a ajuda para o script.

```
/usr/lib/vcac/tools/install/convert-properties --help
```

Tarefas pós instalação do vRealize Automation

Após a instalação do vRealize Automation, existem tarefas que podem exigir a sua atenção.

Configurar a criptografia em conformidade com o Padrão Federal de Processamento de Informações (FIPS)

Você pode ativar ou desativar a criptografia em conformidade com o Padrão Federal de Processamento de Informações (FIPS) 140-2 para tráfego de rede de entrada e saída do appliance do vRealize Automation.

Para alterar a configuração do FIPS, é preciso reiniciar o vRealize Automation. O FIPS é desabilitado por padrão.

Procedimentos

- 1 Faça login como raiz na interface de gerenciamento do appliance do vRealize Automation.

```
https://vrealize-automation-appliance-FQDN:5480
```

- 2 Clique em **Configurações do vRA > Configurações do Host**.
- 3 Próximo ao canto superior direito, clique no botão para ativar ou desativar o FIPS.

Quando ativado, o tráfego de rede de entrada e saída do appliance do vRealize Automation na porta 443 usa a criptografia em conformidade com FIPS 140–2. Independentemente da configuração de FIPS, o vRealize Automation usa algoritmos em conformidade com AES–256 para proteger os dados seguros armazenados no appliance do vRealize Automation.

Observação Esta versão do vRealize Automation só pode ativar parcialmente a conformidade com FIPS, porque alguns componentes internos não usam ainda os módulos criptográficos certificados. Em casos onde os módulos certificados ainda não tenham sido implementados, os algoritmos em conformidade com AES–256 são utilizados.

- 4 Clique em **Sim** para reiniciar o vRealize Automation.

Você também pode configurar o FIPS em uma sessão do console do appliance do vRealize Automation como raiz, usando os comandos a seguir.

```
vcac-vami fips enable
vcac-vami fips disable
vcac-vami fips status
```

Ativar o failover automático do Serviço de Gerenciador

O failover automático do Serviço de Gerenciador será desativado por padrão se você instalar ou atualizar o Serviço de Gerenciador com o instalador do Windows do vRealize Automation padrão.

Para ativar o failover automático do Serviço de Gerenciador após executar o instalador padrão do Windows, execute as seguintes etapas.

Procedimentos

- 1 Faça login como raiz em uma sessão de console no appliance do vRealize Automation.
- 2 Navegue até o seguinte diretório.

```
/usr/lib/vcac/tools/vami/commands
```

- 3 Insira o seguinte comando.

```
python ./manager-service-automatic-failover ENABLE
```

Se for necessário desativar o failover automático durante uma implantação do IaaS, insira o seguinte comando.

```
python ./manager-service-automatic-failover DISABLE
```

Sobre o failover automático do Serviço de Gerenciador

Você pode configurar o vRealize Automation IaaS Manager Service para fazer failover em um backup quando o Manager Service primário é interrompido.

A partir do vRealize Automation 7.3, não é mais necessário iniciar ou parar manualmente o Manager Service em cada servidor Windows para controlar qual deles atua como servidor primário ou de backup. O failover automático do Serviço de Gerenciador está ativado por padrão nos seguintes casos.

- Quando você instala o vRealize Automation silenciosamente ou com o Assistente de Instalação.
- Ao atualizar o IaaS por meio da interface de administração ou com o script de atualização automática.

O failover não é ativado quando você usa o instalador padrão baseado no Windows para adicionar um host do Manager Service ou atualizar o IaaS. Para ativá-lo, consulte [Ativar o failover automático do Serviço de Gerenciador](#).

Quando o failover automático está ativado, o Serviço de Gerenciador é iniciado automaticamente em todos os hosts do Serviço de Gerenciador, incluindo backups. O recurso de failover automático permite que os hosts monitorem uns aos outros de maneira transparente e realizem o failover quando necessário. Ele requer que o serviço do Windows esteja em execução em todos os hosts.

Observação Não é obrigatório utilizar o failover automático. É possível desativá-lo e continuar a iniciar e parar manualmente o serviço Windows para controlar qual host servirá como primário ou backup. Se você optar pela abordagem de failover, será necessário iniciar o serviço em um host por vez. Com o failover automático desativado, executar o serviço simultaneamente em vários servidores IaaS torna o vRealize Automation inutilizável.

Não tente ativar ou desativar seletivamente o failover automático. O failover automático deve estar sempre sincronizado como ligado ou desligado, em todos os hosts do Serviço de Gerenciador em uma implantação do IaaS.

Se o failover automático não estiver funcionando, consulte [O failover automático do Manager Service não é ativado](#) para obter dicas de solução de problemas.

Failover automático do banco de dados PostgreSQL do vRealize Automation

Em uma implantação do vRealize Automation de alta disponibilidade, algumas configurações permitem que o banco de dados PostgreSQL integrado do vRealize Automation realize o failover automaticamente.

O failover automático é ativado silenciosamente sob as seguintes condições.

- A implantação de alta disponibilidade inclui três appliances do vRealize Automation.
O failover automático não é compatível com apenas dois appliances.
- A replicação de banco de dados está definida como Modo Síncrono em Configurações do vRA > Banco de dados na interface de administração do vRealize Automation.

Normalmente, você deve evitar realizar um failover manual enquanto o failover automático está ativado. No entanto, para alguns problemas de nó, o failover automático poderá não ocorrer mesmo se ele estiver ativado. Quando isso acontecer, verifique se é necessário realizar um failover manual.

- 1 Após o nó primário do banco de dados PostgreSQL falhar, espere até 5 minutos para que o restante do cluster se estabilize.

- 2 Em um nó sobrevivente do appliance do vRealize Automation, abra um navegador e vá até o seguinte URL.

<https://vrealize-automation-appliance-FQDN:5434/api/status>

- 3 Pesquise por `manualFailoverNeeded`.
- 4 Se `manualFailoverNeeded` for verdadeiro, execute um failover manual.

Para obter mais informações, consulte [Executar failover manual do banco de dados do appliance do vRealize Automation](#).

Substituindo certificados autoassinados por certificados fornecidos por uma autoridade

Se o vRealize Automation foi instalado com certificados autoassinados, é possível substituí-los por certificados fornecidos por uma autoridade de certificação antes de implantar para produção.

Para obter mais informações sobre a atualização de certificados, consulte [Atualizando certificados do vRealize Automation](#).

Alterando nomes de host e endereços IP

Em geral, você deve esperar manter os nomes de host e FQDNs e endereços IP que você planejou para sistemas vRealize Automation. É possível fazer algumas alterações pós-instalação, mas isso pode ser complicado.

- Se você alterar o nome do host da máquina do Windows que hospeda o banco de dados do SQL Server do IaaS, consulte [Configurar o banco de dados do SQL Server para um novo nome de host](#).
- Na restauração dos componentes IaaS, a renomeação de um host pode afetar o host da Web IaaS, o host do Manager Service ou seus respectivos balanceadores de carga. Restaure esses hosts ou balanceadores de carga de acordo com as instruções para fazer backup e restaurar o *vRealize Suite*.

Para alterar um nome de host ou endereço IP do appliance do vRealize Automation, consulte as seções a seguir.

Alterar o nome de host do appliance do vRealize Automation

Ao manter um ambiente ou rede, pode ser necessário atribuir um nome de host diferente a um appliance do vRealize Automation.

Importante Renomear deixa o vRealize Automation off-line por vários minutos.

As mesmas etapas se aplicam para appliances do vRealize Automation independentes, mestres e de réplica.

Procedimentos

- 1 No DNS, crie um registro adicional com o novo nome do host de nó.
Não remova ainda o registro de DNS existente com o nome do host de antigo.
- 2 Aguarde que ocorra a replicação de DNS e distribuição de zona.

- 3 Faça login como raiz na linha de comando do appliance do vRealize Automation.
- 4 Execute o seguinte comando.

```
vcac-config hostname-change --host novo nome do host --certificate nome do arquivo de certificado
```

Um arquivo de certificado é opcional, a menos que o nome de host do appliance antigo tenha sido usado em um certificado. Em caso afirmativo, forneça um certificado atualizado com o novo nome de host.

Quando você especifica um arquivo de certificado, o comando de renomeação também importa o certificado e retorna o ID do certificado.

O arquivo de certificado deve estar no mesmo formato que a saída de texto do comando da API `/config/ssl/generate-certificate` e conter o novo nome do DNS em seu campo de SAN.

- 5 Espere até 15 minutos ou mais para que o processo de renomeação seja concluído. As ações de comando levam alguns minutos, seguidos por vários minutos adicionais para o novo registro de serviço.
- 6 Se o nome antigo do host do appliance tiver sido usado com um balanceador de carga em um ambiente de alta disponibilidade, verifique e reconfigure o balanceador de carga com o novo nome.
- 7 No DNS, remova o registro de DNS existente com o nome do host antigo.

Se você tiver problemas para alterar um nome de host, tente os procedimentos separados da documentação do vRealize Automation 7.3.

Alterar o endereço IP do Appliance vRealize Automation

Ao manter um ambiente ou rede, pode ser necessário atribuir um endereço de IP diferente a um appliance existente do vRealize Automation.

Pré-requisitos

- Como precaução, faça snapshots dos appliances do vRealize Automation e dos servidores do IaaS.
- A partir de uma sessão de console como raiz nos appliances do vRealize Automation, inspecione as entradas no arquivo `/etc/hosts`.

Procure por endereços atribuídos que podem causar conflito com o novo plano de endereços IP e faça alterações, conforme necessário.

Em todos os servidores IaaS, repita o processo para o arquivo `Windows\system32\drivers\etc\hosts`.

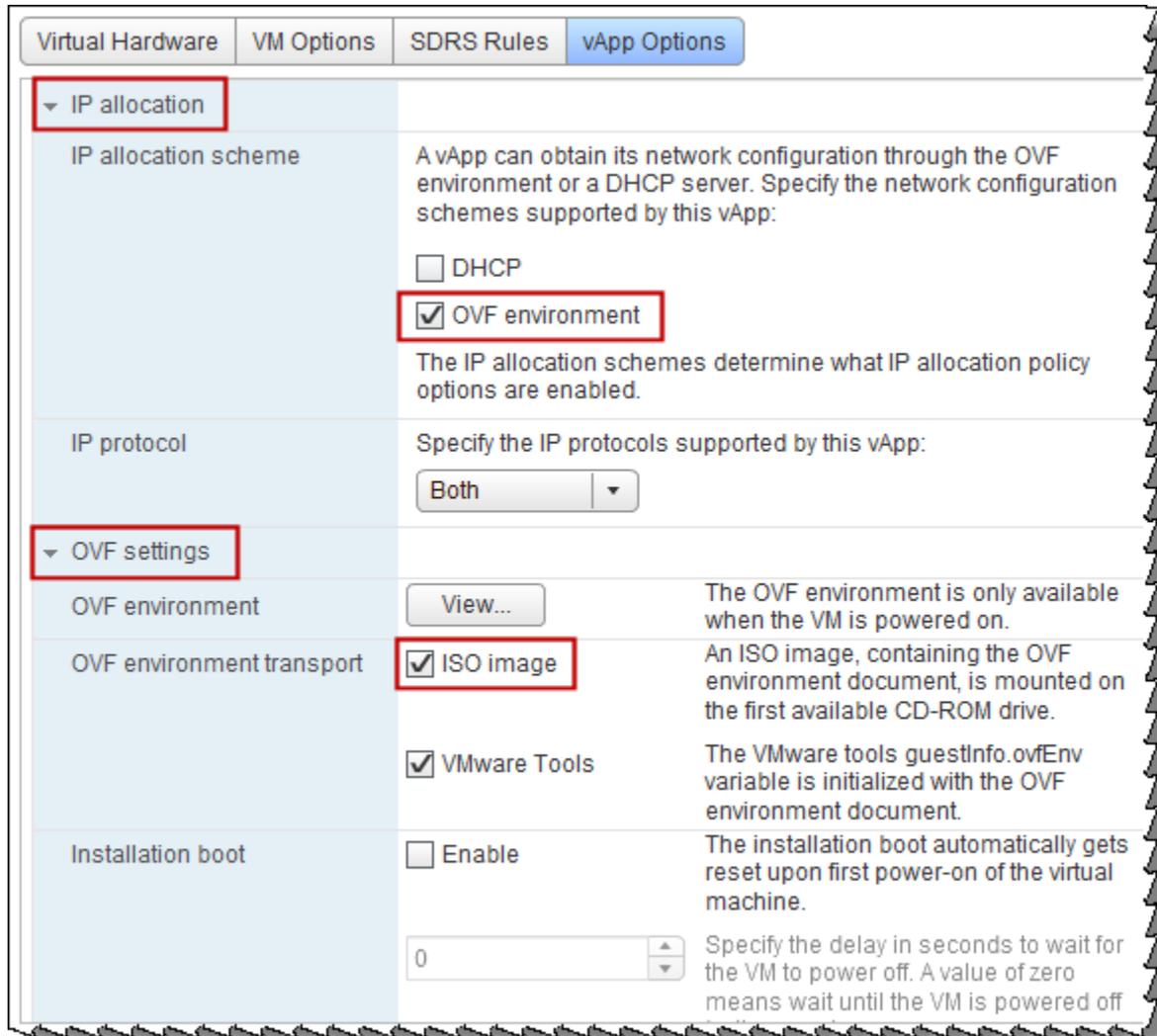
- Desligue todos os appliances do vRealize Automation.
- Pare todos os serviços do vRealize Automation em todos os servidores do IaaS.

Procedimentos

- 1 Em vSphere, localize o appliance do vRealize Automation que você deseja alterar e selecione **Ações > Editar Configurações**.

- 2 Clique em **Opções vApp**.
- 3 Expandir **Alocação de IP** e ativar a opção **Ambiente OVF**.
- 4 Expandir **Configurações OVF** e ativar a opção **Imagem ISO**.

Figura 1-16. Opções Ambiente OVF e Imagem ISO



- 5 Clique em **OK**.
- 6 Inicie o appliance do vRealize Automation que você está alterando.
- 7 Faça login como raiz na interface de gerenciamento do appliance do vRealize Automation.
<https://vrealize-automation-appliance-FQDN:5480>
- 8 Clique na guia **Rede**.
- 9 Abaixo das guias, clique em **Endereço**.
- 10 Atualizar o endereço IP.
- 11 No canto direito superior, clique em **Salvar configurações**.

12 Desligue o appliance do vRealize Automation que você está alterando.

13 No DNS, atualize as entradas para os novos endereços de IP.

Atualize apenas registros existentes do tipo A. Não altere os FQDNs.

Caso esteja usando um balanceador de carga, atualize também as configurações de IP do balanceador de carga para os nós de back-end, service pools e servidores virtuais, conforme necessário.

14 Aguarde que ocorra a replicação de DNS e distribuição de zona.

15 Inicie todos os appliances do vRealize Automation.

16 Inicie os serviços do vRealize Automation nos servidores do IaaS.

17 Faça login como raiz na interface de gerenciamento do appliance do vRealize Automation.

`https://vrealize-automation-appliance-FQDN:5480`

18 Verifique o status do appliance do vRealize Automation nas seguintes áreas.

- Status da conexão do banco de dados em **Configurações do vRA > Banco de Dados**
- Status do RabbitMQ em **Configurações do vRA > Mensagens**
- Status do Xenon em **Configurações do vRA > Xenon**
- Todos os serviços como REGISTRADO em **Serviços**

Ajustando o banco de dados SQL para um nome de host alterado

Você deve rever as definições de configuração se mover o banco de dados SQL do vRealize Automation IaaS para um nome de host diferente.

No mesmo nome de host, é possível restaurar o banco de dados SQL a partir de um backup sem etapas adicionais necessárias. Se você restaurar para um nome de host diferente, será necessário editar arquivos de configuração para fazer alterações adicionais.

Consulte [Artigo da Base de Conhecimento da VMware 2074607](#) para verificar as alterações necessárias ao mover o banco de dados SQL para um outro nome de host.

Alterar um endereço de servidor IP do IaaS

Ao manter um ambiente ou rede, pode ser necessário atribuir um endereço de IP diferente a um servidor Windows vRealize Automation IaaS existente.

Pré-requisitos

- Se o endereço IP do appliance do vRealize Automation precisar ser alterado, primeiro faça o seguinte. Consulte [Alterar o endereço IP do Appliance vRealize Automation](#).
- Como precaução, faça snapshots dos appliances do vRealize Automation e dos servidores do IaaS.
- A partir de uma sessão de console como raiz no appliance do vRealize Automation, inspecione as entradas no arquivo `/etc/hosts`.

Procure por endereços atribuídos que podem causar conflito com o novo plano de endereços IP e faça alterações, conforme necessário.

Em todos os servidores IaaS, repita o processo para o arquivo `Windows\system32\drivers\etc\hosts`.

- Desligue o appliance do vRealize Automation.
- Pare todos os serviços do vRealize Automation em todos os servidores do IaaS.

Procedimentos

1 Faça login no servidor IaaS com uma conta com direitos de administrador.

2 No Windows, altere o endereço IP.

Procure pelo endereço IP nas configurações de adaptador de rede do Windows, em propriedades do Protocolo de Internet.

3 Atualize o seu DNS local com as alterações.

Atualizar o DNS garante que os servidores Windows IaaS podem encontrar uns aos outros e que você pode reconectar a um servidor Windows se você for desconectado.

4 No host do Manager Service, inspecione o seguinte arquivo em um editor de texto.

```
install-folder\vCAC\Server\ManagerService.exe.config
```

A pasta de instalação padrão é `C:\Program Files (x86)\VMware`.

Verifique os endereços IP ou FQDNs das appliances vRealize Automation e dos servidores Windows IaaS.

5 Em todos os servidores Windows IaaS, inspecione o seguinte arquivo em um editor de texto.

```
install-folder\vCAC\Management Agent\VMware.IaaS.Management.Agent.exe.Config
```

Verifique o endereço IP ou FQDN do appliance vRealize Automation.

6 Faça login ao host do Servidor SQL.

7 Verifique se o endereço do repositório está configurado corretamente para usar o FQDN na coluna `ConnectionString`.

Por exemplo, abra o SQL Management Studio e execute a seguinte pesquisa.

```
"SELECT Name, ConnectionString FROM [database-name].[DynamicOps.RepositoryModel].[Models]"
```

8 Iniciar o appliance do vRealize Automation.

9 Inicie os serviços do vRealize Automation nos servidores do IaaS.

10 Inspecione arquivos de registro para verificar se os serviços Agent, DEM Worker, Manager Service e Web host foram iniciados com sucesso.

11 Faça login à vRealize Automation como um usuário com função de Administrador de Infraestrutura.

- 12 Navegue para **Infraestrutura > Monitoramento > Status de Distributed Execution** e verifique se todos os serviços estão sendo executados.
- 13 Faça teste para uma operação correta verificando os serviços de appliance, testando o provisionamento ou usando a ferramenta de Teste de Produção vRealize.

Alterar um nome do host do servidor do IaaS

Ao manter um ambiente ou rede, pode ser necessário atribuir um nome de host diferente a um servidor Windows vRealize Automation IaaS existente.

Procedimentos

- 1 Obtenha um snapshot do servidor do IaaS.
- 2 No servidor do IaaS, use o Gerenciador do IIS para interromper os pools de aplicativos do vRealize Automation: Repositório, VMware vRealize Automation e Wapi.
- 3 No servidor do IaaS, use Ferramentas Administrativas > Serviços para interromper todos os serviços, agentes e DEMs do vRealize Automation.
- 4 No DNS, crie um registro adicional com o novo nome do host.
Não remova ainda o registro de DNS existente com o nome do host de antigo.
- 5 Aguarde que ocorra a replicação de DNS e distribuição de zona.
- 6 No servidor do IaaS, altere o nome do host, mas não reinicie quando solicitado.
Procure o nome do host nas propriedades do sistema do Windows, sob o nome do computador, domínio e configurações do grupo de trabalho.
Quando solicitado a reiniciar, clique na opção para reiniciar mais tarde.
- 7 Se você usou o nome do host antigo para gerar certificados, atualize os certificados.
Para obter mais informações, consulte [Atualizando os certificados do vRealize Automation](#).
- 8 Use um editor de texto para localizar e atualizar o nome do host dentro dos arquivos de configuração.

Faça as atualizações com base em qual nome de host do servidor do IaaS você alterou. Em uma implantação de alta disponibilidade distribuída, talvez seja necessário acessar mais de um servidor. Não há nenhuma atualização se você alterar o nome do host de um DEM Orchestrator ou DEM Worker.

Observação Atualize apenas o nome de host do servidor Windows antigo. Se você encontrar um nome do balanceador de carga em vez disso, mantenha o nome.

Tabela 1-40. Arquivos para a atualização ao alterar um nome do host de nó da Web

| Servidor do IaaS | Caminho | Arquivo |
|------------------|--|------------------------|
| Nós da Web | <i>install-folder</i> \Server\Website | Web.config |
| | <i>install-folder</i> \Server\Website\Cafe | Vcac-Config.exe.config |

Tabela 1-40. Arquivos para a atualização ao alterar um nome do host de nó da Web (Continuação)

| Servidor do IaaS | Caminho | Arquivo |
|---|--|---------------------------|
| | <i>install-folder\Web API</i> | Web.config |
| | <i>install-folder\Web API\ConfigTool</i> | Vcac-Config.exe.config |
| Nó com o componente Model Manager instalado | <i>install-folder\Server\Model Manager Data</i> | Repoutil.exe.config |
| | <i>install-folder\Server\Model Manager Data\Cafe</i> | Vcac-Config.exe.config |
| Nós do Manager Service | <i>install-folder\Server</i> | ManagerService.exe.config |
| Nós do DEM Orchestrator | <i>install-folder\Distributed Execution Manager\dem</i> | DynamicOps.DEM.exe.config |
| Nós do DEM Worker | <i>install-folder\Distributed Execution Manager\DEM-name</i> | DynamicOps.DEM.exe.config |
| Nós do agente | <i>install-folder\Agents\agent-name</i> | RepoUtil.exe.config |
| | <i>install-folder\Agents\agent-name</i> | VRMAgent.exe.config |

Tabela 1-41. Arquivos para a atualização ao alterar um nome do host de nó do Manager Service

| Servidor do IaaS | Caminho | Arquivo |
|-------------------------|--|---------------------------|
| Nós do DEM Orchestrator | <i>install-folder\Distributed Execution Manager\DEM-name</i> | DynamicOps.DEM.exe.config |
| Nós do DEM Worker | <i>install-folder\Distributed Execution Manager\dem</i> | DynamicOps.DEM.exe.config |
| Nós do agente | <i>install-folder\Agents\agent-name</i> | VRMAgent.exe.config |

Tabela 1-42. Arquivos para atualização ao alterar um nome do host de nó do agente

| Servidor do IaaS | Caminho | Arquivo |
|------------------|---|---------------------|
| Nó do agente | <i>install-folder\Agents\agent-name</i> | VRMAgent.exe.config |

- 9 Reinicie o servidor do IaaS onde você alterou o nome do host.
- 10 Inicie os pools de aplicativos do vRealize Automation que você tenha interrompido anteriormente.
- 11 Inicie os serviços, agentes e DEMs do vRealize Automation que você tenha interrompido anteriormente.
- 12 Se o nome antigo do host do servidor IaaS tiver sido usado com um balanceador de carga em um ambiente de alta disponibilidade, verifique e reconfigure o balanceador de carga com o novo nome.
- 13 No DNS, remova o registro de DNS existente com o nome do host antigo.
- 14 Aguarde que ocorra a replicação de DNS e distribuição de zona.

- 15 Se você tiver alterado o nome de um host do Manager Service, execute as etapas adicionais a seguir.
 - a Atualize os agentes de software nas máquinas virtuais existentes.
 - b Recrie quaisquer ISOs ou modelos que contenham um agente guest.

Próximo passo

Valide que vRealize Automation está pronto para ser usado. Consulte a documentação de [Backup e restauração do vRealize Suite](#).

Definir a URL de login do vRealize Automation como um nome personalizado

Se você deseja que os usuários do vRealize Automation façam login em um nome de URL diferente do nome do balanceador de carga ou do appliance do vRealize Automation, siga as etapas de personalização antes e após a instalação.

Procedimentos

- 1 Antes da instalação, prepare um certificado que inclua o CNAME desejado, bem como os nomes do balanceador de carga e do appliance do vRealize Automation.
- 2 Instale o vRealize Automation inserindo o nome do appliance ou do balanceador de carga normalmente. Durante a instalação, importe o certificado personalizado.
- 3 Após a instalação, no DNS, crie um alias do CNAME de Nome Comum e aponte-o para o appliance ou para endereço VIP do balanceador de carga.
- 4 Faça login na interface do administrador de appliance do vRealize Automation como raiz.
`https://vrealize-automation-appliance-FQDN:5480`
- 5 Em **Configurações do vRA > Configurações do Host**, altere o **Nome do Host** para o CNAME que você escolheu.

Licenciar o vRealize Code Stream

Você pode ativar o vRealize Code Stream inserindo uma licença vRealize Code Stream em vRealize Automation.

Você pode inserir a licença vRealize Code Stream em qualquer um dos seguintes locais:

- Na página Licenciamento do assistente de instalação do vRealize Automation. Para obter mais informações, consulte [Instalação do vRealize Code Stream](#).
- Na guia Licenciamento na interface de gerenciamento do appliance do vRealize Automation. Para obter mais informações, consulte [Aplicar uma licença do vRealize Code Stream a um appliance](#).

Instalando o agente do vRealize Log Insight em servidores IaaS

Os servidores Windows em uma configuração de IaaS do vRealize Automation não incluem o agente do vRealize Log Insight por padrão.

O vRealize Log Insight fornece agregação e indexação de registros e pode coletar, importar e analisar registros para expor problemas do sistema. Se você deseja capturar e analisar registros de servidores IaaS usando o vRealize Log Insight, deve instalar separadamente o agente do vRealize Log Insight para Windows.

Para obter mais informações, consulte a [documentação do VMware vRealize Log Insight](#).

Appliance do vRealize Automations incluem o agente do vRealize Log Insight por padrão.

Alterar a porta de proxy do VMware Remote Console

Se o seu site bloquear ou de outra forma reservar a porta 8444, você poderá alterar a porta de proxy padrão usada pelo VMware Remote Console.

Procedimentos

- 1 Acesse o prompt de comando do appliance do vRealize Automation como root.
- 2 Abra o seguinte arquivo no editor de texto.
`/etc/vcac/security.properties`
- 3 Altere `consoleproxy.service.port` do padrão de 8444 para uma porta não utilizada.
- 4 Salve e feche o `security.properties`.
- 5 Reinicie o appliance do vRealize Automation.

Em um ambiente de HA, faça a mesma alteração em todos os appliances do vRealize Automation.

Alterar um FQDN do appliance do vRealize Automation de volta ao FQDN original

Em alguns casos, um FQDN do appliance do vRealize Automation pode ser alterado quando você não quer. Por exemplo, o FQDN é alterado se você cria um Diretório de Autenticação Integrada do Windows (IWA) para um domínio diferente daquele que o appliance está ligado.

Se você criar um diretório IWA para outro domínio, siga estas etapas para alterar o FQDN do appliance de volta para o FQDN original.

Procedimentos

- 1 Faça login no vRealize Automation e crie o diretório IWA normalmente.
Consulte [Configurar um Active Directory sobre um Link LDAP/IWA](#).
- 2 Se esse for um ambiente de alta disponibilidade, também siga as etapas em [Configurar o Gerenciamento de Diretórios para alta disponibilidade](#).
- 3 Criar um diretório IWA para um domínio diferente daquele que um appliance esteja ligado silenciosamente altera o FQDN do appliance.

Por exemplo, `va1.domain1.local` muda para `va1.domain2.local` quando você cria um diretório IWA para `domain2.local`.

Desfaça a alteração renomeando cada appliance de volta para seu FQDN original. Consulte o procedimento associado em [Alterando nomes de host e endereços IP](#).

- 4 Depois que os appliances são voltam a ficar online completamente com o FQDN original, faça login em cada nó do IaaS e siga as etapas abaixo.

- a Abra o seguinte arquivo no editor de texto.

```
C:\Program Files (x86)\VMware\vCAC\Management
Agent\VMware.IaaS.Management.Agent.exe.Config
```

- b Altere cada FQDN do endpoint address= do appliance novamente para o FQDN original.

Por exemplo, de:

```
<endpoint address="https://va1.domain2.local:5480/"
thumbprint="90C55BAEC53E31609EE1614CE4A8336848A8D4CF" />
<endpoint address="https://va2.domain2.local:5480/"
thumbprint="0468BF6EDBC6F2209BE01D0D7FD1094197E324ED" />
```

Para:

```
<endpoint address="https://va1.domain1.local:5480/"
thumbprint="90C55BAEC53E31609EE1614CE4A8336848A8D4CF" />
<endpoint address="https://va2.domain1.local:5480/"
thumbprint="0468BF6EDBC6F2209BE01D0D7FD1094197E324ED" />
```

- c Salve e feche o VMware.IaaS.Management.Agent.exe.Config.

- 5 Faça login como raiz na interface de gerenciamento do appliance do vRealize Automation.

`https://vrealize-automation-appliance-FQDN:5480`

- 6 Vá para **Configurações do vRA > Mensagens** e clique em **Redefinir Cluster RabbitMQ**.
- 7 Após a conclusão da redefinição, faça login em cada interface de gerenciamento do appliance.
- 8 Vá para **Configurações do vRA > Cluster** e verifique se todos os nós estão conectados ao cluster.

Configurar Grupo de Disponibilidade AlwaysOn do SQL

Se você definir o Grupo de Disponibilidade AlwaysOn (AAG) do SQL após a instalação do vRealize Automation, deverá fazer alterações na configuração.

Ao configurar o AAG do SQL após a instalação, siga as etapas em [Artigo da Base de Conhecimento da VMware 2074607](#) para configurar o vRealize Automation com o FQDN ouvinte do AAG como o host do SQL Server.

Adicionar controladores de interface de rede após a instalação do vRealize Automation

O vRealize Automation é compatível com vários controladores de interface de rede (NICs). Após a instalação, você pode adicionar NICs ao appliance do vRealize Automation ou ao servidor Windows do IaaS.

Vários NICs poderão ser necessários para algumas implantações do vRealize Automation, por exemplo:

- Você deseja redes separadas de infraestrutura e de usuário.
- É necessário um NIC adicional para que os servidores IaaS possam ingressar em um domínio do Active Directory.

Para obter mais informações sobre vários cenários de NIC, consulte esta [postagem de blog de Gerenciamento do VMware Cloud](#).

Para três ou mais NICs, esteja ciente das seguintes limitações.

- O VIDM precisa acessar o banco de dados Postgres e o Active Directory.
- Em um cluster de alta disponibilidade, o VIDM precisa acessar a URL do balanceador de carga.
- As conexões anteriores do VIDM devem passar pelos dois primeiros NICs.
- Os NICs após o segundo NIC não devem ser usados ou reconhecidos pelo VIDM.
- Os NICs após o segundo NIC não devem ser usados para se conectar ao Active Directory.

Use o primeiro ou o segundo NIC ao configurar um diretório no vRealize Automation.

Pré-requisitos

Instale completamente o vRealize Automation ao seu ambiente do vCenter.

Procedimentos

- 1 No vCenter, adicione NICs em cada appliance do vRealize Automation.
 - a Clique com o botão direito do mouse no appliance e selecione **Editar Configurações**.
 - b Adicione NICs VMXNETn.
 - c Se estiver ligado, reinicie o appliance.
- 2 Faça login na interface de gerenciamento de appliance do vRealize Automation como raiz.
<https://vrealize-automation-appliance-FQDN:5480>
- 3 Selecione a **Rede** e verifique se vários NICs estão disponíveis.
- 4 Selecione o **Endereço** e configure o endereço IP para os NICs.

Tabela 1-43. Exemplo de configuração do NIC

| Configuração | Valor |
|-----------------------|---------------|
| Tipo de endereço IPv4 | Estático |
| Endereço IPv4 | 172.22.0.2 |
| Máscara da Rede | 255.255.255.0 |

- 5 Verifique se todos os nós de vRealize Automation podem resolver uns aos outros pelo nome DNS.
- 6 Verifique se todos os nós de vRealize Automation podem acessar qualquer FQDNs de balanceamento de carga para componentes do vRealize Automation.

- 7 Se você estiver usando o Split-Brain DNS, verifique se todos os VIPs e nós de vRealize Automation têm o mesmo FQDN no DNS para cada nó IP e VIP.
- 8 No vCenter, adicione NICs aos servidores Windows do IaaS.
 - a Clique com o botão direito do mouse no servidor do IaaS e selecione **Editar Configurações**.
 - b Adicione NICs à máquina virtual do servidor do IaaS.
- 9 No Windows, configure os NICs do servidor do IaaS e seus endereços IP adicionados. Consulte a documentação da Microsoft, se necessário.

Próximo passo

(Opcional) Se você precisar de rotas estáticas, consulte [Configurar rotas estáticas](#).

Configurar rotas estáticas

Ao adicionar NICs a uma instalação do vRealize Automation, se você precisar de rotas estáticas, abra uma sessão de prompt de comando para configurá-las.

Pré-requisitos

Adicione vários NICs a appliances do vRealize Automation ou a servidores Windows do IaaS.

Procedimentos

- 1 Faça login na linha de comando do appliance do vRealize Automation como raiz.
- 2 Abra o arquivo de rotas em um editor de texto.

```
/etc/sysconfig/network/routes
```
- 3 Localize a linha do default para o gateway padrão, mas não a modifique.

Observação Nos casos em que o gateway padrão precisa ser alterado, use a interface de gerenciamento do vRealize Automation em vez disso.

- 4 Abaixo da linha do default, adicione novas linhas para rotas estáticas. Por exemplo:

```
default 10.10.10.1 --
172.30.30.0 192.168.100.1 255.255.255.0 eth0
192.168.210.0 192.168.230.1 255.255.255.0 eth2
```

- 5 Salve e feche o arquivo de rotas.
- 6 Reinicie o appliance.
- 7 Nos clusters de alta disponibilidade, repita o processo para cada appliance.
- 8 Faça login no servidor Windows do IaaS como um administrador.
- 9 Abra um prompt de comando como administrador.

- 10 Para configurar uma rota estática, digite o comando do route `-p add`, onde o `-p` persiste a rota estática nas reinicializações. Por exemplo:

```
C:\Windows\system32> route -p add 172.30.30.0 mask 255.255.255.0 192.168.100.1 metric 1
OK!
```

Para obter mais informações sobre como configurar rotas estáticas no Windows, consulte a documentação da Microsoft.

Gerenciamento de patches de acesso

O suporte técnico para sua instalação do vRealize Automation pode envolver um patch de software que você instala ou remove usando a interface de gerenciamento do appliance do vRealize Automation.

A interface de patch não pode corrigir os seguintes componentes do vRealize Automation.

- O agente de gerenciamento
- Não agentes do vSphere, como XenServer, VDI ou Hyper-V

Pré-requisitos

- Tire snapshots de todos os nós na instalação do vRealize Automation.
- Verifique se todos os nós na instalação do vRealize Automation estão em execução.

Se você tentar instalar ou remover um patch sem todos os nós em execução, a interface de gerenciamento do appliance do vRealize Automation poderá não responder. Se isso acontecer, entre em contato com o suporte técnico. Não tente gerenciar patches por outros meios ou usar o vRealize Automation até resolver o problema.

- Se o seu ambiente usa balanceadores de carga para alta disponibilidade, desative o tráfego para nós secundários até depois da instalação ou da remoção de patches.
- Se estiver instalando um novo patch, obtenha o arquivo de patch e copie-o no sistema de arquivos disponível para o navegador que você usa para a interface de gerenciamento do appliance do vRealize Automation.
- Verifique o [Base de Conhecimento da VMware](#) para obter as informações recentes ou recém-lançadas sobre os patches.

Abra a Base de conhecimento e insira *Aplicação de patches do vRealize Automation* na caixa de pesquisa. Por exemplo, [artigo 51708 da Base de dados de conhecimento da VMware](#) é monitorado e atualizado com as últimas informações sobre o patch 7.4 do vRealize Automation.

Procedimentos

- 1 Faça login na interface de gerenciamento de appliance do vRealize Automation como raiz.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Clique em **Configurações do vRA > Patches**.

3 Em Gerenciamento de patches, clique na opção que você precisa e siga os prompts.

| Opção | Descrição |
|---------------------------|--|
| Novo patch | Instale um novo patch que você baixou. |
| Patches instalados | Adicione o patch instalado mais recentemente aos nós de cluster recém-adicionados. |
| Reverter | Remova o patch instalado mais recentemente e reverta o vRealize Automation para o nível de patch anterior. |
| Histórico | Inspecione a lista de patches instalados e removidos. |

Para ativar ou desativar o Gerenciamento de patches, faça login no prompt de comando do appliance do vRealize Automation como raiz e digite um dos seguintes comandos.

```
/opt/vmware/share/htdocs/service/hotfix/scripts/hotfix.sh enable
/opt/vmware/share/htdocs/service/hotfix/scripts/hotfix.sh disable
```

Instalar um novo patch

Você instala novos patches do vRealize Automation por meio da interface de gerenciamento do appliance do vRealize Automation.

Pré-requisitos

Verifique os pré-requisitos e vá até a interface de gerenciamento de patches. Consulte [Gerenciamento de patches de acesso](#).

Procedimentos

- 1 Clique em **Novo Patch**.
- 2 Clique em **Carregar Patch**.
- 3 Encontre e selecione o arquivo de patch.
- 4 Depois que o patch for carregado, revise os detalhes do patch.
- 5 Se você tiver o patch incorreto, cancele clicando em **Remover**. Caso contrário, clique em **Instalar**.
- 6 Verifique se você seguiu os pré-requisitos e clique em **Instalar**.

A instalação do patch pode levar alguns minutos.

- 7 Clique em **Concluído**.

Se a instalação do patch falhar, você poderá clicar em **Repetir** para tentar novamente ou **Remover** para cancelar. O cancelamento reverte o vRealize Automation para o estado em que se encontrava antes de iniciar a instalação do patch.

Instalar o patch atual em novos nós

Você pode adicionar o patch vRealize Automation instalado mais recentemente aos nós de cluster recém-adicionados.

Pré-requisitos

Verifique os pré-requisitos e vá até a interface de gerenciamento de patches. Consulte [Gerenciamento de patches de acesso](#).

Procedimentos

- 1 Clique em **Patches Instalados**.
- 2 Selecione o patch mais recente.
- 3 Clique em **Instalar**.
- 4 Siga os prompts.

Remover o patch atual

Você pode remover o patch do vRealize Automation instalado mais recentemente e reverter para o patch anterior.

Pré-requisitos

Vá para a interface de gerenciamento de patches. Consulte [Gerenciamento de patches de acesso](#).

Procedimentos

- 1 Clique em **Reverter**.
- 2 Selecione o patch mais recente.
- 3 Clique em **Reverter**.
- 4 Siga os prompts.

Configurar o acesso ao tenant padrão

Você deve conceder a sua equipe direitos de acesso ao tenant padrão antes que eles possam começar a configuração do vRealize Automation

O tenant padrão é automaticamente criado quando você configura o Single Sign-On no assistente de instalação. Você não pode editar os detalhes do tenant, como token da URL ou nome, mas pode criar novos usuários locais e designar administradores adicionais de tenant ou de IaaS a qualquer momento.

Procedimentos

- 1 Faça login no vRealize Automation como administrador do tenant padrão.
 - a Navegue até a interface do produto vRealize Automation.
`https://vrealize-automation-FQDN/vcac`
 - b Faça login com o nome de usuário **administrator** e a senha que você definiu para esse usuário quando configurou o SSO.
- 2 Selecione **Administração > Tenants**.
- 3 Clique no nome do tenant padrão, **vsphere.local**.

4 Clique na guia **Usuários locais**.

5 Crie contas de usuário local para o tenant padrão do vRealize Automation.

Os usuários locais são específicos do tenant e só podem acessar o tenant no qual você os criou.

a Clique no ícone Adicionar (+).

b Insira os detalhes do usuário responsável pela administração da sua infraestrutura.

c Clique em **Adicionar**.

d Repita essa etapa para adicionar um ou mais usuários responsáveis pela configuração do tenant padrão.

6 Clique na guia **Administradores**.

7 Atribua seus usuários locais ao administrador de tenant e às funções de administrador do IaaS.

a Insira um nome de usuário na caixa de pesquisa **Administradores de tenant** e pressione Enter.

b Insira um nome de usuário na caixa de pesquisa **Administradores do IaaS** e pressione Enter.

O administrador do IaaS é responsável pela criação e gerenciamento dos seus endpoints de infraestrutura no vRealize Automation. Somente o administrador do sistema pode conceder essa função.

8 Clique em **Atualizar**.

Próximo passo

Forneça à sua equipe a URL de acesso e as informações de login das contas de usuário que você criou para que possam começar a configuração do vRealize Automation.

- Os administradores de tenant configuram definições, como a autenticação do usuário, incluindo a configuração de Gerenciamento de diretórios para alta disponibilidade. Consulte [Configurando as definições de tenant](#).
- Os administradores do IaaS preparam recursos externos para o provisionamento. Consulte [Preparações externas para o provisionamento](#).
- Se você tiver configurado a Criação de conteúdo inicial durante a instalação, o administrador de configuração poderá solicitar o item de catálogo Conteúdo inicial para preencher rapidamente uma prova de conceito. Para um exemplo sobre como solicitar o item e concluir a ação manual do usuário, consulte [Cenário: Solicitar conteúdo inicial para uma implementação de prova de conceito Rainpole](#).

Solucionando problemas com uma instalação do vRealize Automation

A solução de problemas do vRealize Automation oferece procedimentos para resolver os problemas que podem ser encontrados durante a instalação ou a configuração do vRealize Automation.

Localidades do log padrão

Consulte os arquivos de registro do sistema e do produto para obter informações sobre uma falha na instalação.

Observação Para a coleta de logs, considere tirar proveito dos vRealize Automation e vRealize Orchestrator Content Packs para o vRealize Log Insight. Os Content Packs e o Log Insight fornecem um resumo consolidado de eventos de log para componentes no vRealize Suite. Para obter mais informações, acesse o [VMware Solution Exchange](#).

Para obter a lista de localização de log mais recente, consulte [Artigo da Base de Conhecimento da VMware 2141175](#).

Registros do Windows

Use o seguinte para encontrar arquivos de log para eventos do Windows.

| Registro | Localização |
|---|--|
| Registros do visualizador de eventos do Windows | Iniciar > Painel de Controle > Ferramentas Administrativas > Visualizador de Eventos |

Registros de instalação

Os registros de instalação estão nas localizações a seguir.

| Registro | Localização padrão |
|---------------------------------|---|
| Registros de instalação | C:\Arquivos de programas (x86)\vCAC\InstallLogs C:\Arquivos de programas (x86)\VMware\vCAC\Server\ConfigTool\Log |
| Registros de instalação do WAPI | C:\Arquivos de programas (x86)\VMware\vCAC\Web API\ConfigTool\Logfilename WapiConfiguration-<XXX> |

Registros do IaaS

Os registros do IaaS estão nas localizações a seguir.

| Registro | Localização padrão |
|-------------------------------|---|
| Registros de site | C:\Arquivos de programas (x86)\VMware\vCAC\Server\Website\Logs |
| Registro do repositório | C:\Arquivos de programas (x86)\VMware\vCAC\Server\Model Manager Web\Logs |
| Registros do Manager Service | C:\Arquivos de programas (x86)\VMware\vCAC\Server\Logs |
| Registros do DEM Orchestrator | C:\Users\<nome do usuário>\AppData\Local\Temp\VMware\vCAC\Distributed Execution Manager\<nome do sistema> DEO \Logs |
| Registros do agente | C:\Users\<nome do usuário>\AppData\Local\Temp\VMware\vCAC\Agents\<nome do agente>\logs |

Registros de estrutura do vRealize Automation

As entradas de registro para Estruturas do vRealize Automation encontram-se na localização a seguir.

| Registro | Localização padrão |
|------------------------|--------------------|
| Registros de estrutura | /var/log/vmware |

Registros de provisionamento de componentes de software

Registros de provisionamento de componentes de software encontram-se na localização a seguir.

| Registro | Localização padrão |
|--|--|
| Registro de bootstrap do agente do software | /opt/vmware-appdirector (para Linux) ou \opt\vmware-appdirector (para Windows) |
| Registros de script do ciclo de vida do software | /tmp/taskId (para Linux) \Users\darwin\AppData\Local\Temp\taskId (para Windows) |

Coleção de registros para implantações distribuídas

Você pode criar um arquivo zip que agrupa todos os registros dos componentes de uma implantação distribuída. .

Revertendo uma instalação com falha

Quando uma instalação falha e reverte, o administrador de sistema deve verificar se todos os arquivos necessários foram desinstalados antes de iniciar outra instalação. Alguns arquivos devem ser desinstalados manualmente.

Reverter uma instalação mínima

Um administrador de sistema deve remover manualmente alguns arquivos e reverter o banco de dados para desinstalar completamente uma instalação do IaaS do vRealize Automation com falha.

Procedimentos

- Se os seguintes componentes estão presentes, desinstale-os com o desinstalador do Windows.
 - Agentes do vRealize Automation
 - vRealize Automation DEM-Worker
 - vRealize Automation DEM-Orchestrator
 - Servidor do vRealize Automation
 - WAPI do vRealize Automation

Observação Se você vir a seguinte mensagem, reinicie a máquina e, em seguida, siga as etapas neste procedimento: Erro ao abrir o arquivo de registro de instalação. Verifique se a localização do arquivo de registro especificado existe e é gravável

Observação Se o sistema Windows foi revertido ou o IaaS foi desinstalado, você deve executar o comando `iisreset` antes de reinstalar o IaaS do vRealize Automation.

- 2 Reverta o seu banco de dados para o estado em que estava antes da instalação ser iniciada. O método usado depende do modo de instalação do banco de dados original.
- 3 No IIS (Internet Information Services Manager), selecione o Site padrão (no site personalizado) e clique em **Associações**. Remova a associação de https (padrões para 443).
- 4 Verifique se o Repositório de aplicativos, vRealize Automation e WAPI foram excluídos e se os pools do aplicativo RepositoryAppPool, vCACAppPool, WapiAppPool também foram excluídos.

A instalação é completamente removida.

Reverter uma instalação distribuída

Um administrador de sistema deve remover manualmente alguns arquivos e reverter o banco de dados para desinstalar completamente uma instalação do IaaS com falha.

Procedimentos

- 1 Se os seguintes componentes estão presentes, desinstale-os com o desinstalador do Windows.
 - Servidor do vRealize Automation
 - WAPI do vRealize Automation

Observação Se você vir a seguinte mensagem, reinicie a máquina e, em seguida, siga este procedimento: Erro ao abrir o arquivo de registro de instalação. Verifique se a localização do arquivo de registro especificado existe e é gravável.

Observação Se o sistema Windows foi revertido ou o IaaS foi desinstalado, você deve executar o comando `iisreset` antes de reinstalar o IaaS do vRealize Automation.

- 2 Reverta o seu banco de dados para o estado em que estava antes da instalação ser iniciada. O método usado depende do modo de instalação do banco de dados original.
- 3 No IIS (Internet Information Services Manager), selecione o Site padrão (no site personalizado) e clique em **Associações**. Remova a associação de https (padrões para 443).
- 4 Verifique se o Repositório de aplicativos, vCAC e WAPI foram excluídos e se os pools de aplicativos RepositoryAppPool, vCACAppPool, WapiAppPool também foram excluídos.

Tabela 1-44. Pontos de falha de reversão

| Ponto de falha | Ação |
|-------------------------------|---|
| Instalando o Manager Service | Se estiver presente, desinstale o vCloud Automation Center Server. |
| Instalando o DEM-Orchestrator | Se estiver presente, desinstale o DEM Orchestrator. |
| Instalando o DEM-Worker | Se estiver presente, desinstale todos os DEM Workers. |
| Instalando um agente | Se estiver presente, desinstale todos os agentes vRealize Automation. |

Criar um pacote de suporte do vRealize Automation

Você pode criar um pacote de suporte do vRealize Automation usando a interface de gerenciamento do appliance do vRealize Automation. Os pacotes de suporte coletam logs e ajudam a você ou o suporte técnico do VMware a resolver problemas do vRealize Automation.

Procedimentos

- 1 Abra um navegador da Web para a URL da interface de gerenciamento do appliance do vRealize Automation.

`https://vrealize-automation-appliance-FQDN:5480`

- 2 Faça login como raiz e clique em **Configurações do vRA > Cluster**.
- 3 Clique em **Criar Pacote de Suporte**.
- 4 Clique em **Download** e salve o arquivo de pacote de suporte no seu sistema.

Os pacotes de suporte incluem informações do appliance do vRealize Automation e dos servidores Windows do IaaS. Se você perder a conectividade entre os componentes do IaaS e appliance do vRealize Automation, o pacote de suporte poderá não ter os logs do componente do IaaS.

Para ver quais arquivos de log foram coletados, descompacte o pacote de suporte e abra o arquivo `Environment.html` em um navegador da Web. Sem conectividade, os componentes do IaaS podem aparecer em vermelho na tabela Nós. Outra razão pela qual os logs do IaaS estão ausentes pode ser que o serviço do agente de gerenciamento do vRealize Automation foi interrompido nos servidores Windows IaaS que aparecem em vermelho.

Solução de problemas gerais com a instalação

Os tópicos de solução de problemas para appliances do vRealize Automation fornecem soluções para os possíveis problemas relacionados com a instalação, os quais você pode encontrar ao usar o vRealize Automation.

A instalação ou a atualização falha com um erro de tempo limite do balanceador de carga

Uma instalação ou atualização do vRealize Automation para um ambiente distribuído com um balanceador de carga falha com um erro 503, serviço indisponível.

Problema

A instalação ou atualização falha porque a configuração de tempo limite balanceador de carga não permite tempo suficiente para que a tarefa seja concluída.

Causa

Uma configuração insuficiente de tempo limite do balanceador de carga pode causar falhas. Você pode corrigir o problema aumentando a configuração de tempo limite do balanceador de carga para 100 segundos ou mais e executando novamente a tarefa.

Solução

- 1 Aumente o valor do tempo limite do balanceador de carga para pelo menos 100 segundos.
- 2 Execute novamente a instalação ou atualização.

Os horários do servidor não estão sincronizados

Uma instalação pode não ser bem-sucedida quando os servidores de hora do IaaS não são sincronizados com o appliance do vRealize Automation.

Problema

Você não pode fazer login após a instalação ou ela falha durante a conclusão.

Causa

Os servidores de hora em todos os servidores podem não ser sincronizados.

Solução

Sincronize todos os appliances do vRealize Automation e servidores Windows do IaaS para a mesma fonte de horário. Não misture fontes de horário em uma implantação do vRealize Automation.

- Defina uma fonte de horário do appliance do vRealize Automation:
 - a Faça login na interface de gerenciamento de appliance do vRealize Automation como raiz.
`https://vrealize-automation-appliance-FQDN:5480`
 - b Selecione **Administração > Configurações de Hora** e defina a fonte de sincronização da hora.

| Opção | Descrição |
|---------------------|--|
| Hora do host | Sincronize com o host ESXi do appliance do vRealize Automation. |
| Servidor de horário | Sincronize com um servidor NTP (Protocolo de tempo de rede) externo. Insira o endereço IP ou o FQDN do servidor NTP. |

- Para servidores Windows do IaaS, consulte [Ativar a sincronização de horário no servidor Windows](#).

Podem aparecer páginas em branco ao usar o Internet Explorer 9 ou 10 no Windows 7

Quando você usa o Internet Explorer 9 ou 10 no Windows 7 e o modo de compatibilidade está habilitado, aparecem algumas páginas sem conteúdo.

Problema

Ao usar o Internet Explorer 9 ou 10 no Windows 7, as seguintes páginas não têm conteúdo:

- Infraestrutura
- Página da pasta de tenant padrão no Orchestrator
- Página de configuração do servidor no Orchestrator

Causa

O problema pode estar relacionado ao fato de o modo de compatibilidade estar habilitado. Você pode desabilitar o modo de compatibilidade para o Internet Explorer seguindo as etapas abaixo.

Solução

Pré-requisitos

Certifique-se de que a barra de menus seja exibida. Se você estiver usando o Internet Explorer 9 ou 10, pressione Alt para exibir a barra de menus (ou clique com o botão direito do mouse na barra de endereços e selecione **Barra de menus**).

Procedimentos

- 1 Selecione **Ferramentas > Configurações do Modo de Exibição de Compatibilidade**.
- 2 Desmarque **Exibir sites da intranet no Modo de Exibição de Compatibilidade**.
- 3 Clique em **Fechar**.

Não é possível estabelecer uma relação confiável para o canal seguro de SSL/TLS

Talvez você receba a mensagem "Não é possível estabelecer uma relação confiável para o canal seguro de SSL/TLS ao atualizar certificados de segurança para o vCloud Automation Center".

Problema

Se ocorrer um problema de certificado com o arquivo vcac-config.exe ao atualizar um certificado de segurança, talvez apareça a seguinte mensagem:

```
A conexão subjacente foi fechada: não foi possível estabelecer uma relação confiável para o canal seguro de SSL/TLS.
```

Você pode obter mais informações sobre a causa do problema seguindo o procedimento abaixo.

Solução

- 1 Abra vcac-config.exe.config em um editor de texto e localize o endereço do repositório:

```
<add key="repositoryAddress" value="https://IaaS-address:443/repository/" />
```
- 2 Abra o Internet Explorer no endereço.
- 3 Prossiga pelas mensagens de erro sobre problemas com certificados não confiáveis.
- 4 Obtenha um relatório de segurança do Internet Explorer e use-o para solucionar os problemas com certificados não confiáveis.

Se os problemas persistirem, repita o procedimento navegando com o endereço que precisa ser registrado, o endereço de Endpoint que você usou para registrar o vcac-config.exe.

Conectar-se à rede por meio de um servidor proxy

Alguns sites podem se conectar à Internet por meio de um servidor proxy.

Problema

Sua implantação não pode se conectar à Internet aberta. Por exemplo, não é possível acessar sites, nuvens públicas que você gerencia ou endereços de fornecedores dos qual você baixa softwares ou atualizações.

Causa

Seu site se conecta à Internet por meio de um servidor proxy.

Solução

Pré-requisitos

Obtenha nomes de servidor proxy, números de porta e credenciais do administrador para o seu site.

Procedimentos

- 1 Abra um navegador da Web para a URL da interface de gerenciamento do appliance do vRealize Automation.

`https://vrealize-automation-appliance-FQDN:5480`

- 2 Faça login como raiz e clique em **Rede**.
- 3 Insira o FQDN ou endereço IP do servidor proxy local e o número da porta.
- 4 Se o servidor proxy exigir credenciais, insira o nome do usuário e a senha.
- 5 Clique em **Salvar Configurações**.

Próximo passo

A configuração para usar um proxy pode afetar o acesso do usuário do VMware Identity Manager. Para corrigir o problema, consulte [O proxy impede que os usuários do VMware Identity Manager façam login](#).

Etapas do console para a configuração de conteúdo inicial

Há uma alternativa para usar a interface de instalação do vRealize Automation para criar a conta do administrador de configuração e o conteúdo inicial.

Problema

Como última parte da instalação do vRealize Automation, você segue o processo para inserir uma nova senha, criar a conta de usuário local configurationadmin e criar o conteúdo inicial. Ocorre um erro, e a interface entra em um estado irrecuperável.

Solução

Em vez de usar a interface, insira comandos de console para criar o usuário configurationadmin e o conteúdo inicial. Observe que a interface pode falhar após a conclusão bem-sucedida de uma parte do processo e que, portanto, talvez você apenas precise de alguns dos comandos.

Por exemplo, você pode inspecionar os registros e a execução de fluxos de trabalho do vRealize Orchestrator e determinar que a configuração baseada em interface criou o usuário configurationadmin, mas não o conteúdo inicial. Nesse caso, basta inserir os dois últimos comandos de console para concluir o processo.

Procedimentos

- 1 Faça login no console do appliance do vRealize Automation como raiz.

- 2 Importe o fluxo de trabalho do vRealize Orchestrator inserindo o seguinte comando:

```
/usr/sbin/vcac-config -e content-import --
workflow /usr/lib/vcac/tools/initial-config/vra-initial-config-bundle-
workflow.package --user $SSO_ADMIN_USERNAME --password $SSO_ADMIN_PASSWORD --
tenant $TENANT
```

- 3 Execute o fluxo de trabalho para criar o usuário configurationadmin:

```
/usr/bin/python /opt/vmware/share/htdocs/service/wizard/initialcontent/workfl
owexecutor.py --host $CURRENT_VA_HOSTNAME --username $SSO_ADMIN_USERNAME --
password $SSO_ADMIN_PASSWORD --workflowid f2b3064a-75ca-4199-
a824-1958d9c1efed --configurationAdminPassword $CONFIGURATIONADMIN_PASSWORD
--tenant $TENANT
```

- 4 Importe o blueprint ASD inserindo o seguinte comando:

```
/usr/sbin/vcac-config -e content-import --
blueprint /usr/lib/vcac/tools/initial-config/vra-initial-config-bundle-
asd.zip --user $CONFIGURATIONADMIN_USERNAME --password
$CONFIGURATIONADMIN_PASSWORD --tenant $TENANT
```

- 5 Execute o fluxo de trabalho para configurar o conteúdo inicial:

```
/usr/bin/python /opt/vmware/share/htdocs/service/wizard/initialcontent/workfl
owexecutor.py --host $CURRENT_VA_HOSTNAME --username $SSO_ADMIN_USERNAME --
password $SSO_ADMIN_PASSWORD --workflowid ef00fce2-80ef-4b48-96b5-
fdee36981770 --configurationAdminPassword $CONFIGURATIONADMIN_PASSWORD
```

Não é possível fazer downgrade de licenças do vRealize Automation

Ocorre um erro quando você envia a chave de licença de uma edição de produto inferior.

Problema

Você verá a seguinte mensagem ao usar a página de Licenciamento da interface de administração do vRealize Automation para enviar a chave para uma edição de produto inferior à versão atual. Por exemplo, você inicia com uma licença Enterprise e tenta inserir uma licença Avançada.

```
Unable to downgrade existing license edition
```

Causa

Esta versão do vRealize Automation não permite o downgrade de licenças. Você só pode adicionar licenças de uma edição igual ou superior.

Solução

Para mudar para uma edição inferior, reinstale o vRealize Automation.

Solucionando problemas com o appliance do vRealize Automation

Os tópicos de solução de problemas para appliances do vRealize Automation fornecem soluções para os possíveis problemas relacionados à instalação, os quais você pode encontrar ao usar appliances do vRealize Automation.

Falha no download dos instaladores

Ocorre falha no download dos instaladores do appliance do vRealize Automation.

Problema

Instaladores não baixam ao executar `setup__vrealize-automation-appliance-FQDN@5480.exe`.

Causa

- Ocorrem problemas de conectividade de rede durante a conexão com a máquina do appliance do vRealize Automation.
- Impossível conectar-se à máquina do appliance do vRealize Automation porque não se consegue acessá-la, ou ela não consegue responder antes que a conexão expire.

Solução

- 1 Verifique se você consegue se conectar à URL do vRealize Automation em um navegador Web.
`https://vrealize-automation-appliance-FQDN`
- 2 Confira os outros tópicos de solução de problemas do appliance do vRealize Automation.
- 3 Faça download do arquivo de instalação e reconecte-se ao appliance do vRealize Automation.

O arquivo Encryption.key tem permissões incorretas

Um erro do sistema pode ocorrer quando permissões incorretas são atribuídas ao arquivo Encryption.key de um appliance virtual.

Problema

Faça login no Appliance do vRealize Automation e a página Tenants será exibida. Depois que a página tiver começado a carregar, você verá a mensagem Erro do Sistema.

Causa

O arquivo Encryption.key tem permissões incorretas ou o grupo ou o nível do usuário do proprietário foi atribuído incorretamente.

Solução

Pré-requisitos

Faça login no appliance virtual que exibe o erro.

Observação Se os appliances virtuais estiverem sendo executados sob um balanceador de carga, você deverá verificar cada appliance virtual.

Procedimentos

- 1 Exiba o arquivo de log `/var/log/vcac/catalina.out` e procure a mensagem Não é possível gravar em `/etc/vcac/Encryption.key`.
- 2 Vá até o diretório `/etc/vcac/` e verifique as permissões e a propriedade do arquivo `Encryption.key`. Você deverá ver uma linha semelhante à seguinte:

```
-rw----- 1 vcac vcac 48 Dec 4 06:48 encryption.key
```

A permissão de leitura e gravação é necessária, e o proprietário e grupo do arquivo devem ser `vcac`.

- 3 Se a saída que você vir for diferente, altere as permissões ou a propriedade do arquivo, conforme necessário.

Próximo passo

Faça login na página Tenant para verificar se você pode fazer login sem erros.

O Gerenciamento de Diretórios do Identity Manager não é iniciado após o reinício do espaço de trabalho do Horizon

Em um ambiente de alta disponibilidade vRealize Automation, o Gerenciamento de Diretórios do Identity Manager pode não ser iniciado após o reinício do serviço do espaço de trabalho do Horizon.

Problema

O serviço do espaço de trabalho do Horizon não inicia devido a um erro semelhante a este:

```
Error creating bean with name
'liquibase' defined in class path resource [spring/datastore-wireup.xml]:
Invocation of init method failed; nested exception is
liquibase.exception.LockException: Could not acquire change log lock. Currently
locked by fe80:0:0:0:250:56ff:fea8:7d0c%eth0
(fe80:0:0:0:250:56ff:fea8:7d0c%eth0) since 10/29/15
```

Causa

O Identity Manager pode não ser iniciado em um ambiente de alta disponibilidade devido a problemas com o utilitário de gerenciamento de dados liquibase usado por vRealize Automation.

Solução

- 1 Faça login como raiz em uma sessão de console no appliance do vRealize Automation.
- 2 Interrompa o serviço do espaço de trabalho do Horizon inserindo o seguinte comando.

```
#service horizon-workspace stop
```
- 3 Abra o shell do Postgres como um superusuário.

```
su postgres
```

- 4 Navegue até o diretório bin correto.

```
cd /opt/vmware/vpostgres/current/bin
```

- 5 Conecte-se ao banco de dados.

```
psql vcac
```

- 6 A partir de `saas.databasechangelock`, execute a seguinte Consulta SQL.

```
select * from databasechangelock;
```

Se a saída exibir um valor de "t" para verdadeiro, o bloqueio deve ser liberado manualmente.

- 7 Se for necessário liberar o bloqueio manualmente, execute a seguinte Consulta SQL.

```
update saas.databasechangelock set locked=FALSE, lockgranted=NULL,  
lockedby=NULL where id=1;
```

- 8 A partir de `saas.databasechangelock`, execute a seguinte Consulta SQL.

```
select * from databasechangelock;
```

A saída deve exibir um valor de "f" para falso, significando que está desbloqueada.

- 9 Saída do banco de dados vcac do Postgres.

```
vcac=# \q
```

- 10 Feche o shell do Postgres.

```
exit
```

- 11 Inicie o serviço do espaço de trabalho do Horizon.

```
#service horizon-workspace start
```

Atribuições de funções de appliance incorretas após o failover

Após um failover, os nós mestre e de réplica do appliance do vRealize Automation podem não ter a atribuição de função correta, o que afeta todos os serviços que exigem acesso de gravação ao banco de dados.

Problema

Em um cluster de alta disponibilidade de appliances do vRealize Automation, você encerra o nó do banco de dados mestre ou o torna inacessível. Você pode usar o console de gerenciamento em outro nó para promover esse nó como o novo mestre, o que restaura o acesso de gravação ao banco de dados do vRealize Automation.

Mais tarde, você recoloca o velho nó mestre online, mas a guia Banco de Dados em seu console de gerenciamento ainda lista o nó como o nó mestre, mesmo ele não sendo. Há falhas nas tentativas de usar qualquer console de gerenciamento de nós para resolver o problema promovendo oficialmente o nó antigo de volta como mestre.

Solução

Quando o failover ocorrer, siga estas diretrizes ao configurar os nós mestres antigos versus novos.

- Antes de promover outro nó como mestre, remova o nó mestre anterior do pool de balanceadores de carga de nós do appliance do vRealize Automation.
- Para ter o vRealize Automation recoloque um nó mestre antigo no cluster, deixe a máquina antiga ficar online. Em seguida, abra o console de gerenciamento do novo mestre. Olhe para o nó antigo listado como `invalid` na guia Banco de Dados e clique em seu botão **Redefinir**.

Após uma restauração bem-sucedida, você pode restaurar o nó antigo para o pool de balanceadores de carga dos nós do appliance do vRealize Automation.

- Para recolocar um nó mestre antigo no cluster, coloque a máquina online e faça com que ela se una ao cluster como se fosse um novo nó. Durante a união, especifique o nó recém-promovido como nó primário.

Após a união bem-sucedida, você pode restaurar o nó antigo para o pool de balanceadores de carga de nós do appliance do vRealize Automation.

- Até que você faça a redefinição ou a nova união do nó mestre antigo corretamente no cluster, não use seu console de gerenciamento para operações de gerenciamento de cluster, mesmo se o nó tiver voltado a ficar online.
- Depois de realizar a redefinição ou a nova união corretamente, você poderá promover um nó antigo de volta como mestre.

Falhas após promoção de nós mestres e réplicas

Um problema de espaço em disco, junto com a promoção de nós do banco de dados de appliance mestres e de réplica do vRealize Automation, pode causar problemas de provisionamento.

Problema

O nó mestre excede o espaço em disco. Você faz login na página do Banco de Dados da interface de gerenciamento e promove um nó de réplica com espaço suficiente para se tornar o novo mestre. A promoção parece bem-sucedida quando você atualiza a página da interface de gerenciamento, apesar da exibição de uma mensagem de erro.

Posteriormente, no nó que era o antigo mestre, você libera espaço em disco. Após você promover o nó para mestre novamente, entretanto, as operações de provisionamento falham travando em `IN_PROGRESS`.

Causa

vRealize Automation não pode atualizar a configuração do nó mestre antigo adequadamente quando o problema é a falta de espaço.

Solução

Se a interface de gerenciamento exibir erros durante a promoção, exclua temporariamente o nó do balanceador de carga. Corrija o problema do nó (por exemplo, adicionando um disco), antes de incluí-lo novamente no balanceador de carga. Depois, atualize a página do Banco de Dados da interface de gerenciamento e verifique se os nós mestres e réplicas estão corretos.

Registros de serviço incorretos do componente vRealize Automation

A interface de gerenciamento do appliance do vRealize Automation pode ajudar você a resolver problemas de registro com os serviços do componente do vRealize Automation.

Problema

Em operação normal, todos os serviços do componente vRealize Automation devem ser únicos e estar em um estado REGISTRADO. Qualquer outro conjunto de condições pode fazer com que o vRealize Automation se comporte de forma imprevisível.

Causa

A seguir, estão exemplos de problemas que podem ocorrer com serviços do componente vRealize Automation.

- Um serviço se tornou inativo.
- As configurações do servidor fizeram com que um serviço esteja em um estado diferente de REGISTRADO.
- Uma dependência em outro serviço fez com que um serviço esteja em um estado diferente de REGISTRADO.

Solução

Registre novamente os serviços do componente que aparentam ter problemas.

- 1 Obtenha um snapshot do appliance do vRealize Automation.

Poderá ser preciso reverter ao snapshot se você tentar diferentes mudanças de serviço, e o aparelho chegar em um estado imprevisível.

- 2 Faça login na interface de gerenciamento de appliance do vRealize Automation como raiz.

`https://vrealize-automation-appliance-FQDN:5480`

- 3 Clique em **Serviços**.

- 4 Na lista de serviços, procure por um serviço que não esteja no estado correto ou tenha outros problemas.

- 5 Se um serviço com defeito for o `iaas-service`, vá para a próxima etapa.

Caso contrário, para fazer com que o vRealize Automation registre novamente o serviço, faça login em uma sessão do console no appliance do vRealize Automation como raiz e reinicie o vRealize Automation inserindo o comando a seguir.

```
service vcac-server restart
```

Se houver serviços associados à instância incorporada do vRealize Orchestrator, insira o comando adicional a seguir.

```
service vco-restart restart
```

- 6 Se o serviço com falha for o `iaas-service`, execute as seguintes etapas para registrá-lo novamente.

- a Não cancele o registro do serviço.
- b No servidor Web principal do IaaS, faça login com uma conta que possua direitos de Administrador.
- c Abra um prompt de comando como administrador.
- d Execute o seguinte comando.

```
"C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe" RegisterSolutionUser -url https://appliance-or-load-balancer-IP-or-FQDN/ -t vsphere.local -cu administrator -cp password -f "C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.data" -v
```

A senha é a senha de `administrator@vsphere.local`.

- e Execute um comando para atualizar as informações de registro no banco de dados IaaS.

SQL Server com autenticação do Windows:

```
"C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe" MoveRegistrationDataToDb -s IaaS-SQL-server-IP-or-FQDN -d SQL-database-name -f "C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.data" -v
```

SQL Server com autenticação do SQL nativo:

```
"C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe" MoveRegistrationDataToDb -s SQL-server-IP-or-FQDN -d SQL-database-name -su SQL-user -sp SQL-user-password -f "C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.data" -v
```

Para encontrar o nome do servidor ou do banco de dados, verifique o seguinte arquivo em um editor de texto e procure por `repository`. Os valores da Fonte de dados e do Catálogo inicial exibem o endereço do servidor e o nome do banco de dados, respectivamente.

```
C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Web\Web.config
```

O usuário do SQL deve ter os privilégios DBO no banco de dados.

- f Registre os endpoints executando os seguintes comandos:

```
"C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe" RegisterEndpoint --EndpointAddress https://IaaS-Web-server-or-load-balancer-IP-or-FQDN /vcac --Endpoint ui -v
"C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
```

```
RegisterEndpoint --EndpointAddress https://IaaS-Web-server-or-load-balancer-IP-or-FQDN /WAPI --  
Endpoint wapi -v  
"C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"  
RegisterEndpoint --EndpointAddress https://IaaS-Web-server-or-load-balancer-IP-or-  
FQDN /repository --Endpoint repo -v  
"C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"  
RegisterEndpoint --EndpointAddress https://IaaS-Web-server-or-load-balancer-IP-or-  
FQDN /WAPI/api/status --Endpoint status -v
```

- g Registre os itens do catálogo executando o seguinte comando:

```
"C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-  
Config.exe" RegisterCatalogTypesAsync -v
```

- h Reinicie o IIS.

```
iisreset
```

- i Faça login no host do Serviço de Gerenciador IaaS primário.

- j Reinicie o serviço Windows do vRealize Automation.

```
VMware vCloud Automation Center Service
```

- 7 Para registrar novamente qualquer serviço associado a um sistema externo, como uma instância externa do vRealize Orchestrator, faça login no sistema externo e reinicie os serviços nele.

NIC adicional provoca erros na interface de gerenciamento

Após adicionar um segundo cartão de interface de rede (NIC) a um appliance do vRealize Automation algumas páginas da interface de gerenciamento do vRealize Automation não são carregadas adequadamente.

Problema

Você adiciona um segundo NIC com êxito utilizando o vCenter e as seguintes páginas da interface de gerenciamento do vRealize Automation apresentam erros ao invés de carregarem.

- A página **Status da > rede** exibe um erro sobre um script que não está respondendo.
- A página **Endereço da > rede** exibe um erro sobre a falha ao ler informações da interface de rede.

Causa

A partir da versão 7.3, o appliance do vRealize Automation pode suportar NICs duplos. No entanto, o modelo de engenharia no qual o appliance é baseado evita que a interface de gerenciamento funcione adequadamente até você aplicar a solução.

Solução

Após acrescentar um NIC adicional, reinicie o appliance do vRealize Automation.

Não é possível promover um appliance virtual secundário a um mestre

No vRealize Automation, a memória do appliance virtual baixa pode impedir promoções de appliance virtual no cluster.

Problema

O nó mestre é executado com pouca memória. Você faz login na página do Banco de Dados da interface de gerenciamento e tenta promover um nó secundário para que ele se torne o novo mestre. O seguinte erro ocorre.

```
Fail to execute on Node node-name, host is master-FQDN  
because of: Could not read remote lock command result for node: node-name  
on address: master-FQDN, reason is: 500 Internal Server Error
```

Causa

A promoção ocorrerá somente quando todos os nós puderem confirmar a reconfiguração para um mestre recém-promovido. A pouca memória impedirá que o antigo mestre seja confirmado, mesmo que todos os nós estejam acessíveis.

Solução

Desligue o nó mestre que tem pouca memória. Faça login na página do Banco de Dados da interface de gerenciamento do nó secundário e promova o nó secundário.

Tempo de retenção do log de sincronização do Active Directory é muito curto

No vRealize Automation, os logs de sincronização do Active Directory remetem a apenas alguns dias.

Problema

Depois de dois dias, os logs de sincronização do Active Directory desaparecem da interface de gerenciamento. As pastas para os logs também desaparecem do diretório do appliance do vRealize Automation a seguir.

```
/db/elasticsearch/horizon/nodes/0/indices
```

Causa

Para economizar espaço, o vRealize Automation define o tempo máximo de retenção de logs de sincronização do Active Directory para três dias.

Solução

- 1 Faça login em uma sessão de console no appliance do vRealize Automation como raiz.
- 2 Abra o seguinte arquivo no editor de texto.

```
/usr/local/horizon/conf/runtime-config.properties
```
- 3 Aumente a propriedade `analytics.maxQueryDays`.
- 4 Salve e feche `runtime-config.properties`.
- 5 Reinicie o Identity Manager e os serviços de pesquisa elástica.

```
service horizon-workspace restart  
service elasticsearch restart
```

O RabbitMQ não pode resolver os nomes de host

O RabbitMQ usa nomes de host curtos para appliances do vRealize Automation por padrão, o que pode impedir que os nós resolvam uns aos outros.

Problema

Tente ingressar em outro appliance do vRealize Automation no cluster e ocorrerá um erro semelhante ao abaixo.

```
Clustering node 'rabbit@sc2-rdops-vm01-dhcp-62-2' with rabbit@company ...
Error: unable to connect to nodes [rabbit@company]: nodedown

DIAGNOSTICS
=====

attempted to contact: [rabbit@company]

rabbit@company:
  * unable to connect to epmd (port 4369) on company: nxdomain (non-existing domain)

current node details:
- node name: 'rabbitmq-cli-11@sc2-rdops-vm01-dhcp-62-2'
- home dir: /var/lib/rabbitmq
- cookie hash: 4+kP1tKnxGYaGjrPL2C8bQ==

[2017-09-01 14:58:04] [root] [INFO] RabbitMQ join failed with exit code: 69, see RabbitMQ logs for
details.
```

Causa

Sua configuração de rede não permite que os appliances do vRealize Automation resolvam uns aos outros pelo nome de host curto.

Solução

- 1 Para todos os appliances do vRealize Automation na implantação, faça login como raiz em uma sessão de console.
- 2 Pare o serviço RabbitMQ.
`service rabbitmq-server stop`
- 3 Abra o seguinte arquivo no editor de texto.
`/etc/rabbitmq/rabbitmq-env.conf`
- 4 Defina a propriedade a seguir como true.
`USE_LONGNAME=true`
- 5 Salve e feche `rabbitmq-env.conf`.

6 Redefina o RabbitMQ.

```
vcac-vami rabbitmq-cluster-config reset-rabbitmq-node
```

7 Em apenas um nó de appliance do vRealize Automation, execute o seguinte script.

```
vcac-config cluster-config-ping-nodes --services rabbitmq-server
```

8 Em todos os nós, verifique se o serviço RabbitMQ foi iniciado.

```
vcac-vami rabbitmq-cluster-config get-rabbitmq-status
```

Solucionando problemas de componentes do IaaS

Os tópicos de solução de problemas para componentes do IaaS do vRealize Automation fornecem soluções para possíveis problemas relacionados com a instalação que você pode encontrar ao usar o vRealize Automation.

Corretor de pré-requisito não pode instalar os recursos .NET

A opção **Corrigir** do Verificador de pré-requisitos do vRealize Automation falha e exibe mensagens sobre não encontrar a origem da instalação para o .NET 3.5.1.

Problema

O Verificador de pré-requisitos precisa verificar se o .NET 3.5.1 está instalado para satisfazer os requisitos dos sistemas do Windows Server 2008 R2 com o IIS 7.5 e dos sistemas do Windows Server 2012 R2 com o IIS 8.

Causa

Para o Windows Server 2012 R2, a incapacidade de se conectar à Internet pode impedir a instalação automática do .NET. Algumas atualizações do Windows 2012 R2 também podem evitar a instalação. O problema ocorre porque a versão do Windows não tem uma cópia local da origem da instalação do .NET Framework 3.5.

Solução

Forneça manualmente uma origem da instalação do .NET Framework 3.5.

- 1 No host do Windows, insira um ISO da mídia de instalação do Windows Server 2012 R2.
- 2 No Gerenciador do servidor, ative o .NET Framework 3.5 utilizando o assistente Adicionar Funções e Recursos.
- 3 Durante o assistente, navegue até o caminho de instalação .NET Framework 3.5 na mídia ISO.
- 4 Após adicionar o .NET Framework 3.5, execute o Verificador de pré-requisitos do vRealize Automation novamente.

Validando certificados de servidor do IaaS

Você também pode usar o comando `vcac-Config.exe` para verificar se um servidor IaaS aceita os certificados de appliance do vRealize Automation e do appliance SSO.

Problema

Você vê erros de autorização ao usar os recursos do IaaS.

Causa

Os erros de autorização podem ocorrer quando o IaaS não reconhece os certificados de segurança de outros componentes.

Solução

- 1 Abra um prompt de comando como um administrador e navegue até o diretório Cafe em `vra-installation-dir\Server\Model Manager Data\Cafe`, geralmente `C:\Arquivos de Programas (x86)\VMware\vCAC\Server\Model Manager Data\Cafe`.
- 2 Digite um comando no formato `Vcac-Config.exe CheckServerCertificates -d [vra-database] -s [vRA SQL server] -v`. Os parâmetros opcionais são `-su [SQL user name]` e `-sp [password]`.

Se o comando for bem-sucedido, você verá a seguinte mensagem:

```
Certificates validated successfully.  
Command succeeded.
```

Se o comando falhar, você verá uma mensagem de erro detalhada.

Observação Esse comando só está disponível no nó do componente de Dados do Model Manager.

Erro de credenciais ao executar o instalador do IaaS

Quando você instala os componentes de IaaS, recebe um erro quando insere as credenciais de appliance virtual.

Problema

Depois de fornecer as credenciais no instalador do IaaS, um erro do `org.xml.sax.SAXParseException` é exibido.

Causa

Você usou credenciais incorretas ou um formato incorreto de credencial.

Solução

- ◆ Certifique-se de usar os valores corretos de tenant e nome de usuário.

Por exemplo, o tenant padrão do SSO usa nomes de domínio, como `vsphere.local`, e não `administrator@vsphere.local`.

O aviso "Salvar Configurações" é exibido durante a instalação do IaaS

A mensagem é exibida durante a instalação do IaaS. Aviso: não foi possível salvar as configurações do appliance virtual durante a instalação do IaaS.

Problema

Uma mensagem de erro imprecisa indicando que as configurações do usuário não foram salvas é exibida durante a instalação do IaaS.

Causa

Problemas de comunicação ou de rede podem fazer com que essa mensagem seja exibida erroneamente.

Solução

Ignore a mensagem de erro e continue a instalação. Essa mensagem não deve fazer com que a instalação falhe.

Falha na instalação do servidor de site e dos Distributed Execution Managers

A instalação do servidor de site de infraestrutura e dos Distributed Execution Managers do appliance do vRealize Automation não pode continuar porque a senha da conta do serviço IaaS contém aspas duplas.

Problema

Você vê uma mensagem informando que a instalação dos Distributed Execution Managers (DEMs) e do servidor de site do appliance do vRealize Automation falhou devido a parâmetros msisexec inválidos.

Causa

A senha da conta do serviço IaaS usa um caractere de aspas duplas.

Solução

- 1 Verifique se a sua senha da conta do serviço IaaS não inclui aspas duplas como parte da senha.
- 2 Se a senha incluir aspas duplas, crie uma nova senha.
- 3 Reinicie a instalação.

A autenticação do IaaS falha durante Instalação do IaaS Web e do Gerenciamento de Modelos

Durante a execução do Verificador de Pré-requisitos, você vê uma mensagem indicando que a verificação de autenticação do IIS falhou.

Problema

A mensagem informa que a autenticação não está ativada, mas a caixa de seleção de autenticação do IIS está marcada.

Solução

- 1 Desmarque a caixa de seleção de autenticação do Windows.
- 2 Clique em **Salvar**.
- 3 Marque a caixa de seleção de autenticação do Windows.
- 4 Clique em **Salvar**.

5 Execute novamente o Verificador de Pré-requisitos.

Falha ao instalar os dados e os componentes da Web do Model Manager

A instalação do vRealize Automation poderá falhar se o instalador do IaaS não salvar o componente de dados e o componente da Web do Model Manager.

Problema

A instalação falha com a seguinte mensagem:

```
O instalador do IaaS não conseguiu salvar os componentes de dados da Web do Model Manager.
```

Causa

A falha pode ter algumas causas possíveis.

- Problemas de conectividade com o appliance do vRealize Automation ou problemas de conectividade entre os appliances. Falha em uma tentativa de conexão porque não houve resposta ou a conexão não pôde ser realizada.
- Problemas com certificados confiáveis em IaaS usando-se uma configuração distribuída.
- Uma incompatibilidade entre nomes de certificado em uma configuração distribuída.
- O certificado pode ser inválido ou um erro pode ter ocorrido na cadeia de certificados.
- Falha na inicialização do Serviço de Repositório.
- Configuração incorreta do balanceador de carga em um ambiente distribuído.

Solução

- Conectividade

Verifique se você consegue se conectar à URL do vRealize Automation em um navegador Web.

`https://vrealize-automation-appliance-FQDN`

- Problemas com certificados confiáveis

- No IaaS, abra o Console de Gerenciamento da Microsoft com o comando `mmc.exe` e verifique se o certificado usado na instalação foi adicionado ao Armazenamento de Certificados de Raiz Confiável na máquina.
- Em um navegador Web, verifique o status do serviço MetaModel e confirme se nenhum erro de certificado aparece:

`https://FQDN-or-IP/repository/data/MetaModel.svc`

- Incompatibilidade entre nomes de certificado

Esse erro pode ocorrer quando o certificado é emitido com um nome específico, sendo usado um nome ou um endereço IP diferente. Você pode impedir a incompatibilidade entre nomes de certificado selecionando **Impedir incompatibilidade entre certificados**.

Você também pode usar a opção Impedir incompatibilidade entre certificados para ignorar erros remotos de compatibilidade na lista de certificados revogados.

- Certificado inválido

Abra o Console de Gerenciamento da Microsoft com o comando `mmc.exe`. Verifique se o certificado está expirado e se o status está correto. Faça isso para todos os certificados na cadeia de certificados. Talvez você precise importar outros certificados na cadeia para o Armazenamento de Certificados de Raiz Confiável quando estiver usando uma Hierarquia de certificado.

- Serviço de Repositório

Use as seguintes ações para verificar o status do serviço de repositório.

- Em um navegador Web, verifique o status do serviço MetaModel:

`https://FQDN-or-IP/repository/data/MetaModel.svc`

- Verifique se há erros no arquivo `Repository.log`.

- Reinicie o IIS (`iisreset`) caso tenha problemas com os aplicativos hospedados no site da Web (Repositório, vRealize Automation ou WAPI).

- Verifique os logs do site da Web acessando `%SystemDrive%\inetpub\logs\LogFiles` para obter mais informações de registro.

- Confira se o Verificador de Pré-requisitos foi executado durante a verificação de requisitos.

- No Windows 2012, verifique se os Serviços de WCF no .NET Framework estão instalados e se a ativação HTTP está instalada.

Servidores Windows IaaS não oferecem suporte ao FIPS

Uma instalação não tem êxito quando o Federal Information Processing Standard (FIPS) está habilitado.

Problema

A instalação falha com o seguinte erro durante a instalação do componente Web IaaS.

Esta implementação não faz parte dos algoritmos criptográficos validados por FIPS da Plataforma Windows.

Causa

O vRealize Automation IaaS se baseia no Microsoft Windows Communication Foundation (WCF), que não oferece suporte ao FIPS.

Solução

No servidor Windows IaaS, desative a política FIPS.

- 1 Acesse **Iniciar > Painel de Controle > Ferramentas administrativas > Política de Segurança Local**.
- 2 Na caixa de diálogo Política de Grupo, em **Diretivas Locais**, selecione **Opções de Segurança**.
- 3 Localize e desative a seguinte entrada.

Criptografia do sistema: use algoritmos compatíveis com o FIPS para criptografia, hash e assinatura.

A adição de um endpoint do XaaS causa um erro interno

Quando você tenta criar um endpoint do XaaS, aparece uma mensagem de erro interno.

Problema

Ocorre falha na criação de um endpoint com a seguinte mensagem de erro interno: Ocorreu um erro interno. Se o problema persistir, entre em contato com o administrador do sistema. Ao contatar o administrador do sistema, use esta referência: `c0DD0C01`. Os códigos de referência são gerados aleatoriamente e não estão associados a uma determinada mensagem de erro.

Solução

- 1 Abra o arquivo de log do aplicativo vRealize Automation.
`/var/log/vcac/catalina.out`
- 2 Localize o código de referência na mensagem de erro.
Por exemplo, `c0DD0C01`.
- 3 Procure o código de referência no arquivo de log para localizar a entrada associada.
- 4 Revise as entradas que aparecem acima e abaixo da entrada associada para solucionar o problema.
A entrada do log associado não indica especificamente a causa do problema.

A desinstalação de um agente de proxy falha

A remoção de um agente de proxy pode falhar se o Log do Windows Installer estiver habilitado.

Problema

Quando você tenta desinstalar um agente de proxy no Painel de controle do Windows, a desinstalação falha e você vê o seguinte erro:

```
Error opening installation log file. Verify that the
specified log file location exists and is writable
```

Causa

Isso poderá ocorrer se o Log do Windows Installer estiver habilitado, mas o mecanismo do Windows Installer não pode gravar corretamente no arquivo de log da desinstalação. Para obter mais informações, consulte [Artigo da Base de Conhecimento da Microsoft 2564571](#).

Solução

- 1 Reinicie a máquina ou o explorer.exe no Gerenciador de tarefas.
- 2 Desinstale o agente.

Falha nas solicitações de máquina quando as transações remotas estão desativadas

As solicitações de máquina falham quando as transações remotas do Coordenador de Transações Distribuídas da Microsoft (DTC) estão desativadas nas máquinas de servidores Windows.

Problema

Se você provisionar uma máquina quando as transações remotas estão desativadas no portal Model Manager ou no SQL Server, a solicitação não será concluída. A coleta de dados falha e a solicitação de máquina permanece em um estado de CloneWorkflow.

Causa

As Transações Remotas do DTC estão desativadas na Instância SQL do IaaS usada pelo sistema do vRealize Automation.

Solução

- 1 Inicie o Windows Server Manager para ativar o DTC em todos os servidores do vRealize e SQL associados.

No Windows 7, navegue até **Iniciar > Ferramentas Administrativas > Serviços de Componentes**.

Observação Certifique-se de que todos os servidores Windows tenham SIDs exclusivos para a configuração do MSDTC.

Além disso, o host do Serviço de Gerenciador IaaS deve ser capaz de resolver o nome NETBIOS do host do banco de dados do SQL Server IaaS. Se não for possível resolver o nome NETBIOS, adicione o nome NETBIOS do SQL Server no arquivo /etc/hosts da máquina do Serviço de Gerenciador e reinicie o Serviço de Gerenciador.

- 2 Abra todos os nós para localizar o DTC local ou o DTC em cluster se você estiver usando um sistema em cluster.

Navegue até **Serviços de Componentes > Computadores > Meu Computador > Coordenador de Transações Distribuídas**.

- 3 Clique com o botão direito do mouse no DTC local ou em cluster e selecione **Propriedades**.
- 4 Clique na guia **Segurança**.
- 5 Selecione a opção **Acesso DTC de Rede**.

- 6 Selecione as opções **Permitir Computadores Cliente Remotos** e **Permitir Administração Remota**.
- 7 Selecione as opções **Permitir Entrada** e **Permitir Saída**.
- 8 Insira ou selecione o NT AUTHORITY\Network Service no campo **Conta** da Conta de Logon DTC.
- 9 Clique em **OK**.
- 10 Remova as máquinas que estão presas no estado Fluxo de Trabalho de Clone.
 - a Faça login na interface do produto do vRealize Automation.
`https://vrealize-automation-appliance-FQDN/vcac/org/tenant-name`
 - b Navegue até **Infraestrutura > Máquinas Gerenciadas**.
 - c Clique com o botão direito do mouse na máquina de destino.
 - d Selecione **Excluir** para remover a máquina.

Erro na comunicação do serviço de gerenciador

Servidores do IaaS clonados de um modelo onde o DTC já estava instalado contêm identificadores duplicados para DTC, o que previne a comunicação entre nós.

Problema

O Manager Service de IaaS falha e registra o seguinte erro no log do serviço de gerenciador.

```
A comunicação com o gerenciador de transação subjacente falhou. --->
System.Runtime.InteropServices.COMException: O gerenciador de transação MSDTC não pôde puxar a
transação do gerenciador de transação de origem devido a problemas de comunicação. As possíveis causas
são: a firewall está presente e não tem uma exceção para o processo MSDTC, as duas máquinas não se
encontram pelos seus nomes NetBIOS ou o suporte às operações de rede não está habilitado para um dos
dois gerenciadores de transação.
```

Causa

Ao clonar um servidor de IaaS que já tenha o DTC instalado, o clone conterá o mesmo identificador único para o DTC que o servidor principal. A comunicação entre as duas máquinas falha.

Solução

- 1 No clone, abra um prompt de comando como Administrador.
- 2 Execute o seguinte comando.
`msdtc -uninstall`
- 3 Reinicie o clone.
- 4 Abra outro prompt de comando, e execute o seguinte comando.
`msdtc -install manager-service-host-FQDN`

O comportamento de personalização de e-mails foi alterado

No vRealize Automation 6.0 ou versão posterior, apenas as notificações geradas pelo componente IaaS podem ser personalizadas com o uso da funcionalidade de modelos de e-mail de versões anteriores.

Solução

Você pode usar os seguintes modelos de XSLT:

- ArchivePeriodExpired
- EpiRegister
- EpiUnregister
- LeaseAboutToExpire
- LeaseExpired
- LeaseExpiredPowerOff
- ManagerLeaseAboutToExpire
- ManagerLeaseExpired
- ManagerReclamationExpiredLeaseModified
- ManagerReclamationForcedLeaseModified
- ReclamationExpiredLeaseModified
- ReclamationForcedLeaseModified
- VdiRegister
- VdiUnregister

Os modelos de e-mail estão localizados no diretório `\Templates` sob o diretório de instalação do servidor, geralmente `%SystemDrive%\Program Files x86\VMware\VCAC\Server`. O diretório `\Templates` também inclui modelos XSLT que não são mais aceitos e não podem ser modificados.

Solução de erros de login

Os tópicos de solução de problemas para erros de login do vRealize Automation fornecem soluções para os possíveis problemas relacionados com a instalação, os quais você pode encontrar ao usar o vRealize Automation.

As tentativas de fazer login como o administrador do IaaS com credenciais incorretas no formato UPN apresentam falhas sem explicação

Você tenta fazer login no vRealize Automation como um administrador do IaaS e é redirecionado para a página de login sem nenhuma explicação.

Problema

Se tentar fazer login no vRealize Automation como um administrador do IaaS usando credenciais UPN que não incluem a parte *@seudomínio* do nome do usuário, você será desconectado do SSO imediatamente e redirecionado à página de login sem explicação.

Causa

O UPN inserido deve seguir um formato *seunome.admin@seudomínio*. Por exemplo, se você fizer login usando *jsmith.admin@sqa.local* como o nome de usuário, mas o UPN no Active Directory estiver definido somente como *jsmith.admin*, o login falhará.

Solução

Para corrigir o problema, altere o valor `userPrincipalName` para incluir o conteúdo *@seudomínio* necessário e tentar fazer login novamente. Neste exemplo, o nome UPN deve ser *jsmith.admin@sqa.local*. Essas informações são fornecidas no arquivo de log na pasta `log/vcac`.

O login falha com alta disponibilidade

Quando você tem mais de um appliance do vRealize Automation, os appliances devem ser capazes de se identificar uns aos outros com um nome de host curto. Caso contrário, você não poderá fazer login.

Problema

Você configura o vRealize Automation para alta disponibilidade instalando um appliance adicional do vRealize Automation. Ao tentar fazer login no vRealize Automation, é exibida uma mensagem sobre uma licença inválida. Essa mensagem está incorreta, pois você determinou que sua licença é válida.

Causa

Os nós do appliance do vRealize Automation não formarão corretamente um cluster de alta disponibilidade até poderem resolver os nomes de host curtos dos nós no cluster.

Solução

Para permitir que um cluster de appliances de alta disponibilidade do vRealize Automation resolva nomes de host curtos, siga qualquer uma destas abordagens. Você deve modificar todos os appliances do cluster.

Procedimentos

- Edite ou crie uma linha de pesquisa em `/etc/resolv.conf`. A linha deve conter domínios que contenham appliances do vRealize Automation. Separe vários domínios com espaços. Por exemplo:

```
search sales.mycompany.com support.mycompany.com
```

- Edite ou crie linhas de domínio em `/etc/resolv.conf`. Cada linha deve conter um domínio que contenham appliances do vRealize Automation. Por exemplo:

```
domain support.mycompany.com
```

- Adicione linhas ao arquivo `/etc/hosts` para que cada nome curto do appliance do vRealize Automation seja mapeado para seu nome de domínio totalmente qualificado. Por exemplo:

```
node1    node1.support.mycompany.com
node2    node2.support.mycompany.com
```

O proxy impede que os usuários do VMware Identity Manager façam login

A configuração para usar um proxy pode impedir que os usuários do VMware Identity Manager façam login.

Problema

Você configura o vRealize Automation para acessar a rede por meio de um servidor proxy, e os usuários do VMware Identity Manager visualizam o seguinte erro quando tentam fazer login.

```
Error Unable to get metadata
```

Solução

Pré-requisitos

Configure o vRealize Automation para acessar a rede por meio de um servidor proxy. Consulte [Conectar-se à rede por meio de um servidor proxy](#).

Procedimentos

- 1 Faça login no console do appliance do vRealize Automation como root.
- 2 Abra o seguinte arquivo no editor de texto.
`/etc/sysconfig/proxy`
- 3 Atualize a linha `NO_PROXY` para ignorar o servidor proxy para logins do VMware Identity Manager.
`NO_PROXY=vrealize-automation-hostname`
Por exemplo: `NO_PROXY="localhost, 127.0.0.1, automation.mycompany.com"`
- 4 Salve e feche proxy.
- 5 Reinicie o serviço de espaço de trabalho Horizon inserindo o seguinte comando.
`service horizon-workspace restart`

Atualizando o vRealize Automation

Você pode atualizar o seu ambiente atual do vRealize Automation para a versão mais recente.

Dependendo do seu ambiente atual do vRealize Automation, você pode atualizar para a versão mais recente realizando uma atualização no local ou uma atualização lado a lado. Revise as informações desta página para determinar o melhor método de atualização para o seu ambiente.

Uma atualização in-loco é um processo de várias etapas. Deve-se realizar os procedimentos em uma ordem específica para atualizar os vários componentes em seu ambiente atual. Você deve atualizar todos os componentes do produto para a mesma versão. Você pode executar somente uma atualização in-loco para esses caminhos.

- vRealize Automation 6.2.5 para o 7.4
- vRealize Automation 7.1 para o 7.4
- vRealize Automation 7.2 para o 7.4
- vRealize Automation 7.3.x para o 7.4

Uma atualização lado a lado migra os dados em seu ambiente atual do vRealize Automation para um ambiente de destino implantado com a versão mais recente do vRealize Automation. Você pode executar uma atualização lado a lado para esses caminhos.

- vRealize Automation 6.2.0 até o 6.2.5 para o 7.4
- vRealize Automation 7.0 e 7.0.1 para o 7.4
- vRealize Automation 7.1, 7.2 e 7.3.x para o 7.4

A migração não altera seu ambiente atual. Se o seu ambiente atual estiver integrado com o vCloud Director, o vCloud Air ou tiver endpoints físicos, será necessário usar a migração para atualizar. A migração remove todos os endpoints sem suporte e todos os itens associados a eles no ambiente de destino.

Localize sua versão atual do vRealize Automation nesta tabela. Use os documentos à direita para realizar uma atualização do seu ambiente do vRealize Automation para a versão mais recente.

Tabela 1-45. Caminhos de atualização com suporte para o vRealize Automation 7.4

| Sua versão instalada atualmente | Documentação para atualizações incrementais |
|---|---|
| vRealize Automation 7.1, 7.2 ou 7.3.x | Consulte um dos tópicos a seguir. <ul style="list-style-type: none"> ■ Atualizando do vRealize Automation 7.1 ou superior para a versão 7.4 ■ Migrando para o vRealize Automation 7.4 |
| vRealize Automation 7.0 ou 7.0.1 | Consulte Migrando para o vRealize Automation 7.4 . |
| vRealize Automation 6.2.5 | Consulte um dos tópicos a seguir. <ul style="list-style-type: none"> ■ Atualizando o vRealize Automation 6.2.5 para o 7.4 ■ Migrando para o vRealize Automation 7.4 |
| vRealize Automation 6.2.0, 6.2.1, 6.2.2, 6.2.3, 6.2.4 | Consulte Migrando para o vRealize Automation 7.4 |

Esta tabela fornece informações sobre atualização a partir de uma versão anterior do vCloud Automation Center. Você deve atualizar para o vRealize Automation 6.2.5 antes de atualizar para a versão mais recente do vRealize Automation. Você pode encontrar links para a documentação das versões 5.x e 6.x do vCloud Automation Center e do vRealize Automation em <https://www.vmware.com/support/pubs/vcac-pubs.html>.

Tabela 1-46. Caminhos de atualização compatíveis para o vRealize Automation 6.2.5

| Sua versão instalada atualmente | Documentação para atualizações incrementais |
|---------------------------------|--|
| vCloud Automation Center 6.0 | <p>Realize as atualizações na seguinte ordem:</p> <ol style="list-style-type: none"> 1 <i>Fazendo upgrade para o vCloud Automation Center 6.0 para 6.0.1</i> 2 <i>Fazendo upgrade para o vCloud Automation Center 6.1</i> 3 <i>Fazendo upgrade para o vRealize Automation 6.2.x</i> |
| vCloud Automation Center 6.0.1 | <p>Realize as atualizações na seguinte ordem:</p> <ol style="list-style-type: none"> 1 <i>Fazendo upgrade para o vCloud Automation Center 6.1</i> 2 <i>Fazendo upgrade para o vRealize Automation 6.2.x</i> |
| vCloud Automation Center 6.1.x | <i>Fazendo upgrade para o vRealize Automation 6.2.x</i> |
| vRealize Automation 6.2.x | Atualize diretamente para a versão 6.2.5, conforme descrito em <i>Fazendo upgrade para o vRealize Automation 6.2.x</i> |

Observação vCloud Automation Center renomeado para vRealize Automation na versão 6.2.0. Somente a interface do usuário e os nomes do serviço foram alterados. Os nomes de diretório e os nomes de programa que contêm vcac não são afetados.

Se você estiver atualizando de um ambiente 6.2.x, reveja estes itens.

- A VMware vRealize Production Test Upgrade Assessment Tool analisa seu ambiente do vRealize Automation 6.2.x em busca de qualquer configuração de recurso que possa causar problemas de atualização e verifica se o seu ambiente está pronto para atualização. Para baixar essa ferramenta e a documentação relacionada, acesse a página de download do produto [VMware vRealize Production Test Tool](#).
- A atualização de um ambiente 6.2.x para a versão mais recente do vRealize Automation introduz muitas alterações funcionais. Para obter mais informações, consulte [Considerações sobre a atualização para esta versão do vRealize Automation](#).
- Se você tiver personalizado a implantação do vRealize Automation 6.2.x, entre em contato com a equipe de suporte CCE para obter mais informações sobre a atualização.
- Os controles do dicionário de propriedade que não são suportados após a upgrade podem ser restaurados usando o vRealize Orchestrator e os relacionamentos de dicionário de propriedade.
- Se você tiver fluxos de trabalho em seu ambiente de origem que contenham um código obsoleto, consulte o [Guia de Migração de Extensibilidade do vRealize Automation](#) para obter informações sobre as mudanças de código necessárias para a conversão de inscrições de agentes de eventos.

Para evitar um problema conhecido durante a atualização do vRealize Automation 6.2.0, execute as seguintes etapas em cada nó do site do IaaS, antes de atualizar. Esse problema afeta apenas a versão 6.2.0. As outras versões 6.2.x não são afetadas.

- 1 Abra o bloco de notas com direitos de administrador. Em Iniciar, clique com o botão direito no ícone do Bloco de notas e selecione **Executar como administrador**.

- 2 Abra o seguinte arquivo:

C:\Arquivos de programas (x86)\VMware\vCAC\Server\Model Manager Web\web.config

- 3 Localize a seguinte instrução no arquivo:

```
<!-- add key="DisableMessageSignatureCheck" value="false"-->
```

- 4 Remova o comentário da instrução e altere o valor de false para true.

```
<add key="DisableMessageSignatureCheck" value="true" />
```

- 5 Salve o arquivo.

Se o bloco de notas solicitar o Salvar como, você não abriu o bloco de notas como Administrador e deve voltar à etapa 1.

- 6 Abra um Prompt de comando com direitos administrativos. Em Iniciar, clique com o botão direito no ícone do Prompt de comando e selecione **Executar como administrador**.

- 7 Reinicialize.

- 8 Repita as etapas de 1 a 7 para todos os nós do site.

Atualizando do vRealize Automation 7.1 ou superior para a versão 7.4

Ao atualizar seu ambiente do vRealize Automation 7.1 ou superior para a versão mais recente, você usa os procedimentos de atualização específicos ao seu ambiente da versão 7.1 ou superior.

Essas informações são específicas para atualizar o vRealize Automation 7.1 ou superior para o 7.4. Para obter informações sobre outros caminhos de atualização aceitos, consulte [Atualizando o vRealize Automation](#).

Atualizando o vRealize Automation 7.1, 7.2 ou 7.3.x para 7.4

É possível atualizar o seu ambiente atual do vRealize Automation 7.1, 7.2 ou 7.3.x para 7.4. Você usa os procedimentos específicos de atualização para essa versão para atualizar seu ambiente.

Uma atualização in-loco é um processo de três etapas. Você atualiza os componentes no seu ambiente atual nesta ordem.

- 1 Appliance do vRealize Automation
- 2 Servidor Web do IaaS
- 3 vRealize Orchestrator

Você deve atualizar todos os componentes do produto para a mesma versão.

Começando com o vRealize Automation 7.2, o JFrog Artifactory Pro não vem mais no pacote com o appliance vRealize Automation. Se você tiver atualizado de versão mais antiga do vRealize Automation, o processo de atualização remove o JFrog Artifactory Pro. Para obter mais informações, consulte o [artigo 2147237 da base de dados de conhecimento](#).

Pré-requisitos para atualizar o vRealize Automation

Antes de executar a atualização do ambiente do vRealize Automation 7.1, 7.2 ou 7.3.x para 7.4, revise estes pré-requisitos.

Requisitos de configuração do sistema

Certifique-se de cumprir os seguintes pré-requisitos antes de iniciar uma atualização.

- Verifique se todos os dispositivos e servidores que fazem parte de sua implantação satisfazem os requisitos do sistema para a versão mais recente. Consulte a *Matriz de suporte do vRealize Automation* na [Documentação do VMware vRealize Automation](#).
- Consulte a *Matriz de Interoperabilidade de Produtos VMware* no site do VMware para obter informações sobre a compatibilidade com outros produtos VMware.
- Verifique se o vRealize Automation a partir do qual você está atualizando está em uma condição de trabalho estável. Corrija quaisquer problemas antes de atualizar.
- Verifique se você alterou as configurações de tempo limite do balanceador de carga do padrão para pelo menos 10 minutos.

Requisitos de configuração de hardware

Verifique se o hardware no seu ambiente é adequado para o vRealize Automation 7.4.

Consulte [Especificações de hardware do vRealize Automation e máximos de capacidade](#)

Certifique-se de cumprir os seguintes pré-requisitos antes de iniciar uma atualização.

- Você deve ter pelo menos 18 GB de RAM, 4 CPUs, Disco 1 = 50 GB, Disco 3 = 25 GB e Disco 4 = 50 GB antes de executar a atualização.

Se a máquina virtual estiver no vCloud Networking and Security, talvez seja necessário alocar mais espaço em RAM.

Embora o suporte geral para vCloud Networking and Security tenha terminado, as propriedades personalizadas de VCNS continuam válidas para fins de NSX. Consulte o [artigo 2144733 da Base de Conhecimento](#).

- Estes nós devem ter pelo menos 5 GB de espaço livre em disco:
 - Sites do IaaS primário
 - Banco de dados Microsoft SQL
 - Model Manager
- O nó de Site do IaaS primário no qual os dados do Model Manager estão instalados deve ter o JAVA SE Runtime Environment 8, 64 bits, atualização 161 ou posterior, instalado. Depois de instalar o Java, você deve definir a variável do ambiente JAVA_HOME como a nova versão.
- Para baixar e executar a atualização, você deve ter os seguintes recursos:
 - Pelo menos 5 GB na partição raiz
 - 5 GB na partição /storage/db para o mestre Appliance do vRealize Automation

- 5 GB na partição raiz para cada appliance virtual de réplica
- Verifique a subpasta `/storage/log` e remova arquivos ZIP arquivados mais antigos para liberar espaço.

Pré-requisitos gerais

Certifique-se de cumprir os seguintes pré-requisitos antes de iniciar uma atualização.

- Você deve instalar o PowerShell 3.0 ou superior em seus sistemas do Windows IaaS antes da atualização. A atualização falhará se o PowerShell 3.0 ou superior não estiver instalado.
- Execute um IISRESET em suas máquinas IaaS Web e Manager Service se o Microsoft IIS estiver instalado. Executar o IISRESET verifica se não há um serviço dependente do IIS desativado no modo de inicialização.
- Você tem acesso a todos os bancos de dados e todos os balanceadores de carga são impactados ou participam da atualização do vRealize Automation.
- Você torna o sistema indisponível para os usuários enquanto realiza a atualização.
- Você desabilita todos os aplicativos que consultam o vRealize Automation.
- Verifique se o MSDTC (Microsoft Distributed Transaction Coordinator) está ativado em todos os vRealize Automation e servidores SQL associados. Para obter mais informações, consulte o [artigo 2089503 da Base de Conhecimento](#).
- Conclua estas etapas se estiver atualizando um ambiente distribuído configurado com um banco de dados PostgreSQL integrado.
 - a Examine os arquivos no diretório `pgdata` do host mestre antes de atualizar os hosts de réplica.
 - b Navegue até a pasta de dados PostgreSQL no host mestre em `/var/vmware/vpostgres/current/pgdata/`.
 - c Feche todos os arquivos abertos no diretório `pgdata` e remova todos os arquivos com um sufixo `.swp`.
 - d Verifique se todos os arquivos neste diretório possuem a posse correta: `postgres:users`.

Além disso, verifique se as propriedades personalizadas não têm espaços nos nomes. Antes da atualização para esta versão do vRealize Automation, remova os caracteres de espaço dos nomes da sua propriedade personalizada, por exemplo, substitua o espaço por um caractere de sublinhado para permitir que a propriedade personalizada seja reconhecida na instalação do vRealize Automation atualizada. Os nomes da propriedade personalizada do vRealize Automation não podem conter espaços. Esse problema pode ter impacto sobre o uso de uma instalação do vRealize Orchestrator atualizada que usa as propriedades personalizadas que continham espaços nas versões anteriores do vRealize Automation ou do vRealize Orchestrator, ou em ambos.

Lista de verificação para atualizar o vRealize Automation

Ao atualizar o vRealize Automation 7.1, 7.2 ou 7.3.x para 7.4, você atualiza todos os componentes do vRealize Automation em uma ordem específica.

A ordem de atualização varia dependendo do fato de você estar atualizando um ambiente mínimo ou distribuído com vários appliances do vRealize Automation.

Use as listas de verificação para acompanhar seu trabalho enquanto conclui a atualização. Conclua as tarefas na ordem em que elas são apresentadas.

Tabela 1-47. Lista de verificação para atualizar um ambiente mínimo do vRealize Automation

| Tarefa | Instruções |
|---|--|
| <input type="checkbox"/> Execute a coleta de dados do Inventário de Segurança e Rede do NSX antes de fazer a atualização do vRealize Automation 7.1, 7.2 ou 7.3.x para 7.4. Isso só é necessário quando o vRealize Automation está integrado com o NSX. | Consulte Executar a coleta de dados do Inventário de Segurança e Rede do NSX antes da atualização do vRealize Automation . |
| <input type="checkbox"/> Faça backup da instalação atual. Essa é uma etapa crítica. | Para obter mais informações sobre como fazer backup e restaurar o sistema, consulte Fazer backup do ambiente existente do vRealize Automation . Para obter informações gerais, consulte <i>Configurando o backup e a restauração usando o Symantec Netbackup</i> em http://www.vmware.com/pdf/vrealize-backup-and-restore-netbackup.pdf . |
| <input type="checkbox"/> Baixe a atualização no appliance do vRealize Automation. | Consulte Fazendo download de atualizações do appliance vRealize Automation . |
| <input type="checkbox"/> Instale a atualização nos componentes do IaaS e do appliance vRealize Automation. | Consulte Instalar a atualização nos componentes do IaaS e do appliance do vRealize Automation |

Tabela 1-48. Lista de verificação para atualizar um ambiente distribuído do vRealize Automation

| Tarefa | Instruções |
|---|--|
| <input type="checkbox"/> Execute a coleta de dados do Inventário de Segurança e Rede do NSX antes de fazer a atualização do vRealize Automation 7.1, 7.2 ou 7.3.x para 7.4. Isso só é necessário quando o vRealize Automation está integrado com o NSX. | Consulte Executar a coleta de dados do Inventário de Segurança e Rede do NSX antes da atualização do vRealize Automation . |
| <input type="checkbox"/> Faça backup de sua instalação atual. Essa é uma etapa crítica. | Para obter mais informações sobre como fazer backup e restaurar o sistema, consulte Fazer backup do ambiente existente do vRealize Automation . Para obter informações detalhadas, consulte <i>Configurando o backup e a restauração usando o Symantec Netbackup</i> em http://www.vmware.com/pdf/vrealize-backup-and-restore-netbackup.pdf |
| <input type="checkbox"/> Se você estiver fazendo a atualização do vRealize Automation 7.3.x, desative o failover automático do PostgreSQL. | Consulte Definir o modo de replicação do PostgreSQL vRealize Automation como assíncrono . |
| <input type="checkbox"/> Baixe as atualizações no appliance do vRealize Automation. | Consulte Fazendo download de atualizações do appliance vRealize Automation . |
| <input type="checkbox"/> Desative seu balanceador de carga. | Consulte a documentação do balanceador de carga. |

Tabela 1-48. Lista de verificação para atualizar um ambiente distribuído do vRealize Automation (Continuação)

| Tarefa | Instruções |
|--|---|
| <input type="checkbox"/> Instale a atualização nos componentes mestres do IaaS e do appliance vRealize Automation. | Consulte Instalar a atualização nos componentes do IaaS e do appliance do vRealize Automation . |
| Observação Você deve instalar a atualização no appliance mestre em um ambiente distribuído. | |
| <input type="checkbox"/> Ative o balanceador de carga. | Ativar os balanceadores de carga |

Interfaces de usuário do ambiente do vRealize Automation

Você usa e gerencia seu ambiente do vRealize Automation com várias interfaces.

Interfaces do Usuário

Estas tabelas descrevem as interfaces que você usa para gerenciar seu ambiente do vRealize Automation.

Tabela 1-49. vRealize Automation Console administrativo

| Finalidade | Acesso | Credenciais necessárias |
|--|--|--|
| Use o console do vRealize Automation para estas tarefas de administrador do sistema. <ul style="list-style-type: none"> ■ Adicionar tenants. ■ Personalizar a interface do usuário do vRealize Automation. ■ Configurar servidores de e-mail. ■ Exibir logs de evento. ■ Configure o vRealize Orchestrator. | <ol style="list-style-type: none"> 1 Inicie um navegador e abra a tela inicial do appliance do vRealize Automation usando o nome de domínio totalmente qualificado do appliance virtual: <code>https://vra-va-hostname.domain.name</code>. 2 Clique em Console do vRealize Automation. Você também pode usar esta URL para abrir o console do vRealize Automation: <code>https://vra-va-hostname.domain.name/vcac</code> 3 Faça login. | Você deve ser um usuário com a função de administrador de sistema. |

Tabela 1-50. Console do tenant do vRealize Automation . Essa interface é a interface de usuário principal que você pode usar para criar e gerenciar seus serviços e recursos.

| Finalidade | Acesso | Credenciais necessárias |
|---|---|---|
| <p>Use o vRealize Automation para estas tarefas.</p> <ul style="list-style-type: none"> ■ Solicite novos blueprints de serviço de TI. ■ Criar e gerenciar recursos de TI e da nuvem. ■ Criar e gerenciar grupos personalizados. ■ Crie e gerencie grupos de negócios. ■ Atribuir funções a usuários. | <p>1 Inicie um navegador e insira a URL da sua locação usando o nome de domínio totalmente qualificado do appliance virtual e o nome da URL do tenant:</p> <p><code>https://vra-va-hostname.domain.name/vcac/org/nome_URL_tenant.</code></p> <p>2 Faça login.</p> | <p>Você deve ser um usuário com uma ou mais destas funções:</p> <ul style="list-style-type: none"> ■ Arquiteto de aplicativos ■ Administrador de aprovação ■ Administrador do catálogo ■ Administrador do contentor ■ Arquiteto do contentor ■ Consumidor de integridade ■ Arquiteto de infraestrutura ■ Consumidor de Exportação Segura ■ Arquiteto de software ■ Administrador de tenant ■ Arquiteto do XaaS |

Tabela 1-51. Gerenciamento do Appliance do vRealize Automation . Às vezes, esta interface é chamada de Interface de Gerenciamento do Appliance Virtual (VAMI).

| Finalidade | Acesso | Credenciais necessárias |
|--|---|---|
| <p>Use o Gerenciamento do Appliance do vRealize Automation para estas tarefas.</p> <ul style="list-style-type: none"> ■ Visualizar o status de serviços registrados. ■ Visualizar informações do sistema e reinicializar ou desligar o appliance. ■ Gerenciar a participação no Programa de Aperfeiçoamento da Experiência do Cliente. ■ Visualizar o status da rede. ■ Visualizar o status da atualização e instalar atualizações. ■ Gerenciar configurações de administração. ■ Gerenciar configurações do host vRealize Automation. ■ Gerenciar configurações de SSO. ■ Gerenciar licenças de produto. ■ Configurar o banco de dados Postgres do vRealize Automation. ■ Configurar mensagens do vRealize Automation. ■ Configurar o registro em log do vRealize Automation. ■ Instalar componentes do IaaS. ■ Migrar de uma instalação existente do vRealize Automation. ■ Gerenciar certificados de componentes do IaaS. ■ Configurar o serviço Xenon. | <ol style="list-style-type: none"> 1 Inicie um navegador e abra a tela inicial do appliance do vRealize Automation usando o nome de domínio totalmente qualificado do appliance virtual: <code>https://vra-va-hostname.domain.name.</code> 2 Clique em Gerenciamento do Appliance do vRealize Automation. Você também pode usar esta URL para abrir o Gerenciamento do Appliance do vRealize Automation: <code>https://vra-va-hostname.domain.name:5480.</code> 3 Faça login. | <ul style="list-style-type: none"> ■ Nome de usuário: root ■ Senha: senha que você inseriu quando implantou o appliance do vRealize Automation. |

Tabela 1-52. Cliente vRealize Orchestrator

| Finalidade | Acesso | Credenciais necessárias |
|--|--|--|
| <p>Use o Cliente vRealize Orchestrator para estas tarefas.</p> <ul style="list-style-type: none"> ■ Desenvolver ações. ■ Desenvolver fluxos de trabalho. ■ Gerenciar políticas. ■ Instalar pacotes. ■ Gerenciar usuários e permissões de grupos de usuários. ■ Anexar marcas a objetos de URI. ■ Visualizar o inventário. | <ol style="list-style-type: none"> 1 Inicie um navegador e abra a tela inicial do appliance vRealize Automation usando o nome de domínio totalmente qualificado do appliance virtual: <code>https://vra-va-hostname.domain.name.</code> 2 Para baixar o arquivo <code>client.jnlp</code> no seu computador local, clique em Cliente vRealize Orchestrator. 3 Clique com o botão direito do mouse no arquivo <code>client.jnlp</code> e selecione Iniciar. 4 Na caixa de diálogo Deseja Continuar?, clique em Continuar. 5 Faça login. | <p>Você deve ser um usuário com a função de administrador de sistema ou parte do grupo <code>vcoadmins</code> definido nas configurações do Provedor de Autenticação do Centro de Controle do vRealize Orchestrator.</p> |

Tabela 1-53. Centro de Controle do vRealize Orchestrator

| Finalidade | Acesso | Credenciais necessárias |
|---|---|--|
| <p>Use o Centro de Controle do vRealize Orchestrator para editar a configuração da instância do vRealize Orchestrator padrão que está incorporada no vRealize Automation.</p> | <ol style="list-style-type: none"> 1 Inicie um navegador e abra a tela inicial do appliance do vRealize Automation usando o nome de domínio totalmente qualificado do appliance virtual: <code>https://vra-va-hostname.domain.name.</code> 2 Clique em Gerenciamento do Appliance do vRealize Automation. Você também pode usar esta URL para abrir o Gerenciamento do Appliance do vRealize Automation: <code>https://vra-va-hostname.domain.name:5480.</code> 3 Faça login. 4 Clique em Configurações do vRA > Orchestrator. 5 Selecione a interface de usuário do Orchestrator. 6 Clique em Iniciar. 7 Clique na URL da interface de usuário do Orchestrator. 8 Faça login. | <p>Nome do usuário</p> <ul style="list-style-type: none"> ■ Insira a raiz se a autenticação com base na função não estiver configurada. ■ Insira seu nome de usuário vRealize Automation se ele estiver configurado para autenticação com base na função. <p>Senha</p> <ul style="list-style-type: none"> ■ Insira a senha que você inseriu quando implantou o appliance do vRealize Automation se a autenticação com base na função não estiver configurada. ■ Insira a senha para o seu nome de usuário, se o seu nome de usuário estiver configurado para autenticação com base na função. |

Tabela 1-54. Prompt de Comando do Linux

| Finalidade | Acesso | Credenciais necessárias |
|--|--|---|
| <p>Você pode usar o prompt de comando do Linux em um host, como o host do appliance do vRealize Automation, para estas tarefas.</p> <ul style="list-style-type: none"> ■ Parar ou iniciar serviços ■ Editar arquivos de configuração ■ Executar comandos ■ Recuperar dados | <p>1 No host do appliance do vRealize Automation, abra um prompt de comando.</p> <p>Uma maneira de abrir o prompt de comando no computador local é iniciar uma sessão no host usando um aplicativo, como o PuTTY.</p> <p>2 Faça login.</p> | <ul style="list-style-type: none"> ■ Nome de usuário: root ■ Senha: senha que você criou quando implantou o appliance do vRealize Automation. |

Tabela 1-55. Prompt de Comando do Windows

| Finalidade | Acesso | Credenciais necessárias |
|--|--|---|
| <p>Você pode usar um prompt de comando do Windows em um host, como o host laaS, para executar scripts.</p> | <p>1 No host do laaS, faça login no Windows.</p> <p>Uma maneira de fazer logon no seu computador local é iniciar uma sessão de área de trabalho remota.</p> <p>2 Abra o prompt de comando do Windows.</p> <p>Uma maneira de abrir o prompt de comando é clicar com o botão direito no ícone Iniciar no host e selecionar Prompt de Comando ou Prompt de Comando (Admin).</p> | <ul style="list-style-type: none"> ■ Nome de usuário: usuário com privilégios administrativos. ■ Senha: Senha do usuário. |

Atualizando produtos VMware integrados com o vRealize Automation

É necessário gerenciar produtos VMware integrados com seu ambiente do vRealize Automation ao atualizar o vRealize Automation.

Se seu ambiente do vRealize Automation estiver integrado com um ou mais produtos adicionais, você deverá atualizar o vRealize Automation antes de atualizar os outros produtos. Se o vRealize Business for Cloud estiver integrado com o vRealize Automation, você deverá cancelar o registro do vRealize Business for Cloud antes de atualizar o vRealize Automation.

Siga o fluxo de trabalho sugerido para gerenciar produtos integrados quando atualizar o vRealize Automation.

- 1 Atualize o vRealize Automation.
- 2 Atualize o VMware vRealize Operations Manager.
- 3 Atualize o VMware vRealize Log Insight.
- 4 Atualize o VMware vRealize Business for Cloud.

Esta seção fornece orientação adicional para gerenciar o vRealize Business for Cloud quando é integrado com seu ambiente do vRealize Automation.

Atualizando o vRealize Operations Manager integrado com o vRealize Automation

Atualize o vRealize Operations Manager depois de atualizar o vRealize Automation.

Procedimentos

- 1 Atualize o vRealize Automation.
- 2 Atualize o vRealize Operations Manager. Para obter informações, consulte *Atualizando seu software* na [Documentação do VMware vRealize Operations Manager](#).

Atualizando o vRealize Log Insight integrado com o vRealize Automation

Atualize o vRealize Log Insight depois de atualizar o vRealize Automation.

Procedimentos

- 1 Atualize o vRealize Automation.
- 2 Atualize o vRealize Log Insight. Para obter informações, consulte *Atualizando o vRealize Log Insight* na [Documentação do VMware vRealize Log Insight](#).

Atualizando o vRealize Business for Cloud integrado com o vRealize Automation

Ao atualizar o ambiente do vRealize Automation, é necessário cancelar o registro e registrar sua conexão no vRealize Business for Cloud.

Execute este procedimento para garantir a continuidade do vRealize Business for Cloud quando atualizar o ambiente do vRealize Automation.

Procedimentos

- 1 Cancele o registro do vRealize Business for Cloud do vRealize Automation. Consulte *Cancelar o registro do vRealize Business for Cloud do vRealize Automation* na [Documentação do VMware vRealize Business for Cloud](#).
- 2 Atualize o vRealize Automation.
- 3 Se necessário, atualize o vRealize Business for Cloud. Consulte *Atualizando o vRealize Business for Cloud* na [Documentação do VMware vRealize Business for Cloud](#).
- 4 Registre o vRealize Business for Cloud com o vRealize Automation. Consulte *Registrar o vRealize Business for Cloud no vRealize Automation* na [Documentação do VMware vRealize Business for Cloud](#).

Preparando para atualizar o vRealize Automation

Conclua essas tarefas antes de atualizar o vRealize Automation 7.1, 7.2 ou 7.3.x para 7.4.

Conclua essas tarefas na ordem em que aparecem na lista de verificação. Consulte [Lista de verificação para atualizar o vRealize Automation](#).

Executar a coleta de dados do Inventário de Segurança e Rede do NSX antes da atualização do vRealize Automation

Antes de atualizar o vRealize Automation 7.1, 7.2 ou 7.3.x para 7.4, você deve executar a coleta de dados do Inventário de Segurança e Rede do NSX no ambiente do vRealize Automation 7.1, 7.2 ou 7.3.x.

Essa coleta de dados é necessária para que a ação de reconfiguração do balanceador de carga funcione no vRealize Automation 7.4 para implantações das versões 7.1, 7.2 ou 7.3.x.

Procedimentos

- ◆ Execute a coleta de dados do Inventário de Segurança e Rede do NSX no vRealize Automation 7.1, 7.2 ou 7.3.x antes de atualizar para o 7.4. Consulte [Iniciar a coleta de dados do endpoint manualmente](#).

Próximo passo

[Pré-requisitos de backup para atualizar o vRealize Automation 7.1, 7.2 ou 7.3 para a versão 7.4.](#)

Pré-requisitos de backup para atualizar o vRealize Automation 7.1, 7.2 ou 7.3 para a versão 7.4

Conclua os pré-requisitos de backup antes de começar a atualização.

Pré-requisitos

- Verifique se o ambiente de origem foi totalmente instalado e configurado.
- Faça login no seu cliente do vSphere e, para cada appliance no ambiente de origem, faça backup de todos os arquivos de configuração do appliance do vRealize Automation nos diretórios a seguir:
 - `/etc/vcac/`
 - `/etc/vco/`
 - `/etc/apache2/`
 - `/etc/rabbitmq/`
- Faça backup do banco de dados do Microsoft SQL Server do IaaS. Para mais informações, consulte artigos na [Microsoft Developer Network](#) sobre como criar um backup completo do banco de dados SQL Server.
- Faça backup de todos os arquivos que você tenha personalizado, como o `DataCenterLocations.xml`.
- Crie um snapshot de cada servidor de IaaS e de cada appliance virtual. Siga as diretrizes comuns para fazer backup de todo o sistema caso ocorra falha na atualização do vRealize Automation. Consulte [Backup e Recuperação para Instalações do vRealize Automation](#).

Fazer backup do ambiente existente do vRealize Automation

Antes de fazer a atualização do vRealize Automation 7.1, 7.2 ou 7.3.x para o 7.4, desligue e obtenha um snapshot de cada servidor IaaS do vRealize Automation em cada nó do Windows e de cada appliance do vRealize Automation em cada nó do Linux. Se a atualização for malsucedida, use o snapshot para voltar para a última configuração válida e tente outra atualização.

Para obter informações sobre como iniciar o vRealize Automation, consulte [Inicializar o vRealize Automation](#).

Pré-requisitos

- [Pré-requisitos de backup para atualizar o vRealize Automation 7.1, 7.2 ou 7.3 para a versão 7.4.](#)
- A partir do vRealize Automation 7.0, o banco de dados PostgreSQL é sempre configurado no modo de alta disponibilidade. Faça login no console de gerenciamento do appliance do vRealize Automation e selecione **Configurações do vRA > Banco de Dados** para localizar o nó Mestre atual. Se a configuração do banco de dados estiver listada como um banco de dados externo, crie um backup manual desse banco de dados externo.
- Se o banco de dados Microsoft SQL do vRealize Automation não estiver hospedado no servidor IaaS, crie um arquivo de backup de banco de dados.
- Verifique se os pré-requisitos de backup foram cumpridos para atualização.
- Lembre-se de criar um snapshot do seu sistema enquanto ele estiver desligado. Este é o método preferencial para obter um snapshot. Consulte a *Documentação do vSphere 6.0*.

Observação Quando você fizer backup do appliance do vRealize Automation e de componentes do IaaS, desative snapshots na memória e snapshots inativos.

- Se você tiver modificado o arquivo `app.config`, faça um backup desse arquivo. Consulte [Restaurar alterações de registro no arquivo app.config](#).
- Faça um backup dos arquivos de configuração de fluxo de trabalho externo (xmlldb). Consulte [Restaurar arquivos de limite de fluxo de trabalho externo](#).
- Verifique que você tenha um local fora da sua pasta atual onde você possa armazenar o seu arquivo de backup. Consulte [Cópias de backup de arquivos .xml fazem com que o sistema atinja o tempo limite](#).

Procedimentos

- 1 Faça login no seu cliente do vSphere.
- 2 Localize cada máquina Windows de IaaS do vRealize Automation e cada nó de appliance do vRealize Automation.
- 3 Em cada máquina, clique em **Desligar guest** nesta ordem.
 - a Máquina do IaaS Windows Server
 - b Appliance do vRealize Automation.
- 4 Obtenha um snapshot de cada máquina do vRealize Automation.
- 5 Utilize o seu método de backup preferido para criar um backup completo de cada nó de appliance.
- 6 Ligue o sistema. Confira a Inicializar vRealize Automation em *Gerenciando o vRealize Automation*.

Se você tiver um ambiente de alta disponibilidade, conclua essas etapas para ligar seus appliances virtuais.

 - a Inicie o appliance do vRealize Automation mestre.

- b Faça login no Gerenciamento de Appliance do vRealize Automation, clique em **Serviços** e aguarde até que o status do serviço de licenciamento seja REGISTRADO.
- c Inicie os appliances restantes do vRealize Automation ao mesmo tempo.
- d Inicie o nó primário da Web e aguarde o término da inicialização.
- e Inicie a máquina primária do Manager Service e aguarde de 2 a 5 minutos.

O tempo real depende da configuração do seu site.

Observação Em máquinas secundárias, não inicie ou execute o serviço do Windows, a menos que tenha feito a configuração para failover automático do Serviço de Gerenciador.

- f Inicie os trabalhadores e o Orchestrator do Distributed Execution Manager e todos os agentes proxy do vRealize Automation.

Observação É possível iniciar esses componentes em qualquer ordem. Você não precisa esperar que um componente seja concluído antes de iniciar outro.

- 7 Faça login em cada console de gerenciamento do appliance vRealize Automation e verifique se o sistema está completamente funcional.
 - a Clique em **Serviços**.
 - b Confira se cada serviço está REGISTRADO.

Próximo passo

[Definir o modo de replicação do PostgreSQL vRealize Automation como assíncrono.](#)

Definir o modo de replicação do PostgreSQL vRealize Automation como assíncrono

Se atualizar um ambiente distribuído do vRealize Automation que opera em modo de replicação síncrono do PostgreSQL, você deverá alterá-lo para assíncrono antes da atualização.

Pré-requisitos

- Você tem um ambiente distribuído do vRealize Automation que deseja atualizar.
- Você está conectado como **raiz** ao Gerenciamento de appliance do vRealize Automation em `https://vra-va-hostname.domain.name:5480`.

Procedimentos

- 1 Clique em **Configurações vRA > Banco de dados**.
- 2 Clique em **Modo Assíncrono** e espere a conclusão da ação.
- 3 Verifique se todos os nós na coluna Estado de Sincronização exibem o status Assíncrono.

Próximo passo

[Fazendo download de atualizações do appliance vRealize Automation](#)

Fazendo download de atualizações do appliance vRealize Automation

Você pode verificar se há atualizações no console de gerenciamento de seu appliance e baixar as atualizações usando um dos seguintes métodos.

Para obter o melhor desempenho de atualização, use o método de arquivo ISO.

Para evitar possíveis problemas ao atualizar seu appliance ou se surgirem problemas durante a atualização do appliance, consulte o [artigo da Base de dados de conhecimento da VMware Falha na atualização do vRealize Automation devido a duplicatas no banco de dados do vRealize Orchestrator \(54987\)](#).

Fazer download de atualizações do appliance virtual para uso com uma unidade de CD-ROM

Você pode atualizar seu appliance virtual de um arquivo ISO que ele lê na unidade de CD-ROM virtual. Este é o método preferencial.

Baixe o arquivo ISO e configure o appliance primário para usar esse arquivo para atualizar seu appliance.

Pré-requisitos

- Faça backup do ambiente vRealize Automation existente.
- Verifique se todas as unidades de CD-ROM usadas na atualização estão ativadas antes de atualizar um appliance do vRealize Automation. Consulte a documentação do vSphere para obter informações sobre como adicionar uma unidade de CD-ROM a uma máquina virtual no cliente do vSphere.

Procedimentos

- 1 Baixe o arquivo ISO do repositório de atualização.
 - a Inicie um navegador e acesse a [página de produto do vRealize Automation](#) em www.vmware.com.
 - b Clique em **Recursos de download do vRealize Automation** para acessar a página de downloads da VMware.
 - c Baixe o arquivo apropriado.
- 2 Localize o arquivo baixado no sistema para verificar se o tamanho dele corresponde ao do arquivo na página de downloads da VMware. Use os checksums fornecidos na página de downloads para validar a integridade do arquivo que você baixou. Para obter informações, consulte os links na parte inferior da página de downloads do VMware.
- 3 Certifique-se de que o appliance virtual primário esteja ligado.
- 4 Conecte a unidade de CD-ROM do appliance virtual primário ao arquivo ISO que você fez download.
- 5 No appliance do vRealize Automation primário, faça login no Gerenciamento do Appliance do vRealize Automation como **root** usando a senha que você inseriu quando implantou o appliance do vRealize Automation.
- 6 Clique na guia **Atualizar**.
- 7 Clique em **Configurações**.

- 8 Em Repositório de Atualização, selecione **Usar Atualizações de CDROM**.
- 9 Clique em **Salvar Configurações**.

Fazer download de atualizações do appliance do vRealize Automation a partir de um repositório da VMware

Você pode baixar a atualização do seu appliance do vRealize Automation de um repositório público no site vmware.com.

Pré-requisitos

- Faça backup do ambiente existente do vRealize Automation .
- Verifique se o appliance do vRealize Automation está ligado.

Procedimentos

- 1 No appliance do vRealize Automation primário, faça login no Gerenciamento do Appliance do vRealize Automation como **root** usando a senha que você inseriu quando implantou o appliance do vRealize Automation.
- 2 Clique na guia **Atualizar**.
- 3 Clique em **Configurações**.
- 4 (Opcional) Definir a frequência de verificação de atualizações no painel Atualizações Automáticas.
- 5 Selecione **Usar Repositório Padrão** no painel Repositório de Atualização.
O repositório padrão é definido como a URL VMware.com correta.
- 6 Clique em **Salvar Configurações**.

Atualizando os componentes do IaaS e do appliance do vRealize Automation

Depois de concluir os pré-requisitos de atualização e baixar a atualização do appliance virtual, você instala a atualização no appliance do vRealize Automation 7.1, 7.2 ou 7.3.x para atualizar para a versão 7.4.

Para obter um ambiente mínimo, você instala a atualização no appliance do vRealize Automation. Para um ambiente distribuído, você instala a atualização no nó do appliance mestre. O tempo necessário para a atualização terminar varia de acordo com o seu ambiente e rede. Quando a atualização terminar, o sistema exibirá as alterações feitas na página Status da Atualização do Gerenciamento do appliance do vRealize Automation. Quando a atualização do appliance terminar, você deverá reiniciá-lo. Quando você reinicializa o appliance mestre em um ambiente distribuído, o sistema reinicializa cada nó de réplica.

Após a reinicialização, a mensagem *Aguardando a inicialização dos serviços de VA* é exibida na página Status da Atualização. A atualização do IaaS será iniciada quando o sistema estiver totalmente inicializado e todos os serviços estiverem em execução. É possível observar o progresso da atualização do IaaS na página Status da Atualização. O primeiro componente do servidor IaaS pode demorar cerca de 30 minutos para ser finalizado. Durante a atualização, você verá uma mensagem semelhante a *Atualizando componentes do servidor para o nó web1-vra.mycompany.com*.

No final do processo de atualização para cada nó do Manager Service, você verá uma mensagem semelhante a Ativando modo de failover automático do Manager Service para o nó mgr-vra.mycompany.com. Começando com o vRealize Automation 7.3, o nó ativo do Manager Service muda de uma seleção manual para uma decisão do sistema sobre qual nó deve se tornar o servidor de failover. O sistema ativa esse recurso durante a atualização. Se tiver problemas com esse recurso, consulte [Falha na atualização do Agente de Gerenciamento](#).

Instalar a atualização nos componentes do IaaS e do appliance do vRealize Automation

Você instala a atualização no appliance virtual do vRealize Automation 7.1, 7.2 ou 7.3.x para atualizar o vRealize Automation e os componentes do IaaS para o 7.4.

Não feche o console de gerenciamento enquanto você instala a atualização.

Se você encontrar problemas durante o processo de atualização, consulte [Solucionando problemas de atualização do vRealize Automation](#).

Observação Ao atualizar o Agente de Gerenciamento nas máquinas virtuais de IaaS, um certificado público da VMware é temporariamente instalado no repositório de certificados de Editores Confiáveis. O processo de atualização do Agente de Gerenciamento usa um script do PowerShell que é assinado com esse certificado. Quando a atualização terminar, esse certificado será removido do seu repositório de certificados.

Pré-requisitos

- Verifique se você selecionou um método de download e concluiu o procedimento para o método. Consulte [Fazendo download de atualizações do appliance vRealize Automation](#).
- Para todos os ambientes de alta disponibilidade, consulte [Fazer backup do ambiente existente do vRealize Automation](#).
- Para ambientes com balanceadores de carga, verifique se você desativou todos os nós redundantes e removeu os monitores de integridade. Para mais informações, confira a documentação do balanceador de carga.
 - Appliance do vRealize Automation
 - Website do IaaS
 - Serviço de gerenciador do IaaS
- Para ambientes com balanceadores de carga, verifique se o tráfego está direcionado apenas ao nó primário.
- Realizando as seguintes etapas, verifique se o serviço de IaaS hospedado no Microsoft Internet Information Services (IIS) está em execução:
 - a Inicie um navegador e insira a URL **https://webhostname/Repository/Data/MetaModel.svc** para verificar se o Repositório da Web está em execução. No caso de êxito, nenhum erro será retornado e você verá uma lista de modelos no formato XML.

- b Faça login no Site IaaS e verifique se o status registrado nos relatórios do arquivo `Repository.log` está OK. O arquivo está localizado na pasta inicial do VCAC, em `/Server/Model Manager Web/Logs/Repository.log`.

Observação Para um site IaaS distribuído, faça login no site secundário, sem o MMD, e pare o Microsoft IIS temporariamente. Para garantir que o tráfego do balanceador de carga esteja apenas passando pelo nó da Web primário, verifique a conectividade de `MetaModel.svc` e reinicie o Microsoft IIS.

- Verifique se todos os nós IaaS estão em um estado íntegro, realizando as seguintes etapas:
 - a No appliance virtual primário, faça login no Gerenciamento do Appliance do vRealize Automation como **root** usando a senha que você inseriu quando implementou o appliance do vRealize Automation.
 - b Selecione **Configurações do vRA > Cluster**.
 - c Em **Última Conexão**, verifique o seguinte.
 - Os nós IaaS na tabela têm um horário de última conexão inferior a 30 segundos.
 - Os nós do appliance virtual têm um horário de última conexão de menos de 10 minutos.

Se os nós de IaaS estiverem em comunicação com o appliance do vRealize Automation, a atualização falhará.

Para diagnosticar problemas de conectividade entre o Management Agent e o appliance virtual, realize estas etapas.

 - 1 Faça logon em cada nó IaaS que não esteja listado ou que tenha um horário de **Última Conexão** maior que 30 segundos.
 - 2 Verifique os logs do Management Agent para ver há erros registrados.
 - 3 Se o Management Agent não estiver em execução, reinicie o agente no console de Serviços.
 - d Observe todos os nós órfãos listados na tabela. Um nó órfão é um nó duplicado que está relatado no host, mas que não existe no host. Você deve excluir todos eles. Para obter mais informações, consulte [Excluir nós órfãos no vRealize Automation](#).
- Se você tiver um appliance virtual de réplica que não faça mais parte do cluster, você deverá excluí-la da tabela do cluster. Se você não excluir esse appliance, o processo de atualização exibirá uma mensagem de aviso de que a atualização da réplica não foi bem-sucedida.
- Verifique se todas as solicitações salvas e em andamento foram finalizadas com êxito antes da atualização.
- Se você atualizar os componentes do IaaS manualmente depois de atualizar o appliance do vRealize Automation 7.1, 7.2 ou 7.3.x, consulte [Excluir a atualização do IaaS](#). Se você planeja atualizar o IaaS manualmente, também deve parar todos os serviços IaaS, exceto o Management Agent, em cada nó IaaS.

Procedimentos

- 1 No appliance do vRealize Automation primário, faça login no Gerenciamento do Appliance do vRealize Automation como **root** usando a senha que você inseriu quando implantou o appliance do vRealize Automation.

Para um ambiente distribuído, abra o console de gerenciamento no appliance mestre.

- 2 Clique em **Serviços** e verifique se todos os serviços estão registrados.
- 3 Selecione **Configurações do vRA > Banco de Dados** e verifique se esse appliance é o appliance vRealize Automation mestre.

Você instala a atualização somente no appliance mestre do vRealize Automation. Cada appliance vRealize Automation de réplica é atualizado com o appliance mestre.

- 4 Selecione **Atualizar > Status**.
- 5 Clique em **Verificar atualizações** para verificar se uma atualização pode ser acessada.
- 6 (Opcional) Para instâncias do appliance do vRealize Automation, clique em **Detalhes** na área Versão do appliance para ver informações sobre o local das notas de versão.
- 7 Clique em **Instalar Atualizações**.
- 8 Clique em **OK**.

É exibida uma mensagem informando que a atualização está em andamento. O sistema mostra as alterações feitas durante uma atualização na página Resumo da Atualização. O tempo necessário para a atualização terminar varia de acordo com o seu ambiente e rede.

- 9 (Opcional) Para controlar a atualização com maiores detalhes, use um emulador de terminal para fazer login no appliance primário. Visualize o arquivo `updatecli.log` em `/opt/vmware/var/log/vami/updatecli.log`.

Informações de progresso da atualização adicional também podem ser vistas nestes arquivos.

- `/opt/vmware/var/log/vami/vami.log`
- `/var/log/vmware/horizon/horizon.log`
- `/var/log/bootstrap/*.log`

Se você fizer logoff durante o processo de atualização, poderá continuar acompanhando o progresso da atualização no arquivo de log. O arquivo `updatecli.log` pode exibir informações sobre a versão do vRealize Automation da qual você está atualizando. Essa versão exibida mudará para a versão adequada mais tarde no processo de atualização.

- 10 Quando a atualização do appliance vRealize Automation terminar, clique em **Sistema > Reinicializar** no console de gerenciamento.

Em um ambiente distribuído, todos os nós do appliance de réplica atualizados com êxito serão reinicializados quando você reinicializar o appliance mestre.

A atualização do IaaS será iniciada quando o sistema é inicializado e todos os serviços estiverem funcionando. Clique em **Atualizar > Status** para observar o progresso de atualização do IaaS.

- 11 Quando a atualização do IaaS terminar, clique em **Cluster** no console de gerenciamento do appliance e verifique se o número da versão é a versão atual para todos os nós e componentes do IaaS.
- 12 Clique em **Telemetria** no console de gerenciamento do appliance. Leia a observação sobre a participação no Programa de Aperfeiçoamento da Experiência do Cliente (CEIP) e escolha se deseja participar do programa.

Os detalhes sobre os dados recolhidos pelo CEIP e os fins para os quais eles são utilizados pelo VMware são estabelecidos pelo Centro de Confiança e Garantia, em <http://www.vmware.com/trustvmware/ceip.html>.

Para obter mais informações sobre o Programa de Aperfeiçoamento da Experiência do Cliente, consulte [Participar ou sair do Programa de Aperfeiçoamento da Experiência do Cliente para o vRealize Automation](#).

Próximo passo

Se a sua implantação usa um balanceador de carga, realize essas etapas.

- 1 Ative as verificações de integridade do vRealize Automation do balanceador de carga.
- 2 Reative o tráfego do balanceador de carga para todos os nós de vRealize Automation.

Se a atualização dos componentes do IaaS falhar, consulte [Atualizando os componentes do servidor IaaS separadamente quando o processo de atualização falha](#).

Atualizando os componentes do servidor IaaS separadamente quando o processo de atualização falha

Se o processo de atualização automático falhar, você poderá atualizar os componentes do IaaS separadamente.

Se o site do IaaS do vRealize Automation e o Manager Service forem atualizados com êxito, você poderá executar o script do shell de atualização do IaaS novamente sem reverter para os snapshots que você tirou antes da atualização. Às vezes, um evento de reinicialização pendente gerado durante a atualização de vários componentes do IaaS instalados na mesma máquina virtual pode falhar na atualização. Nesse caso, tente reinicializar manualmente o nó do IaaS e executar novamente a atualização para corrigir o problema. Se a atualização falhar de forma consistente, entre em contato com o suporte da VMware ou tente realizar uma atualização manual, seguindo estas etapas.

- 1 Reverta seu appliance do vRealize Automation para o estado anterior à atualização.
- 2 Execute um comando para excluir os componentes do IaaS do processo de atualização. Consulte [Excluir a atualização do IaaS](#).
- 3 Execute o processo de atualização no appliance vRealize Automation.
- 4 Atualize os componentes do IaaS separadamente usando o Script do Shell de Atualização ou o pacote MSI do instalador do IaaS do vRealize Automation 7.4.

Atualizar os componentes do IaaS usando o script do shell de atualização após atualizar o appliance do vRealize Automation

Use o script do shell de atualização para atualizar os componentes do IaaS após atualizar cada appliance do vRealize Automation 7.1, 7.2 ou 7.3.x para o 7.4.

O Appliance do vRealize Automation atualizado contém um script shell que você usa para atualizar cada nó e componente do IaaS.

Você pode executar o script de atualização usando o console do vSphere para a máquina virtual ou usando uma sessão do console de SSH. Se você usar o console do vSphere, poderá evitar problemas intermitentes de conectividade de rede que podem interromper a execução do script.

Se você interromper o script enquanto ele estiver atualizando um componente, esse script será interrompido quando terminar de atualizar o componente. Se outros componentes no nó ainda precisarem ser atualizados, você poderá executar o script novamente.

Quando a atualização estiver concluída, você poderá revisar o resultado da atualização abrindo o arquivo de log de atualização em `/opt/vmware/var/log/vami/upgrade-iaas.log`.

Pré-requisitos

- Revise [Solucionando problemas de atualização do vRealize Automation](#).
- Verifique a atualização bem-sucedida de todos os appliances do vRealize Automation.
- Se você reinicializar um servidor IaaS depois de atualizar todos os appliances do vRealize Automation, mas antes de atualizar os componentes IaaS, interrompa todos os serviços IaaS no Windows, exceto o serviço Management Agent.
- Antes de executar o script do shell de atualização no nó de appliance do vRealize Automation mestre, clique em **Serviços** no console de gerenciamento do appliance. Verifique se cada serviço, exceto `iaas-service`, está REGISTRADO.
- Para instalar manualmente o Agente de Gerenciamento do IaaS em cada nó do IaaS, siga estas etapas.
 - a Na página Abra um navegador e navegue até a instalação IaaS do VMware vRealize Automation no appliance em `https://virtual_appliance_host_FQDN:5480/installer`.
 - b Baixe o instalador do Management Agent, `vCAC-iaasManagementAgent-Setup.msi`.
 - c Faça login em cada máquina IaaS do vRealize Automation e atualize o Management Agent com o instalador do Management Agent. Reinicie o serviço Management Agent do Windows.
- Verifique se o nó de site IaaS primário e o nó do Model Manager têm o JAVA SE Runtime Environment 8, 64 bits, atualização 161 ou versão posterior, instalado. Depois de instalar o Java, você deverá definir a variável de ambiente `JAVA_HOME` como a nova versão em cada nó de servidor.
- Faça login em cada nó do site de IaaS e verifique se a data de criação é anterior à data de modificação no arquivo `web.config`. Se a data de criação do arquivo `web.config` for igual ou posterior à data de modificação, realize o procedimento descrito em [Falha na atualização para o componente do site do IaaS](#)

- Para verificar se todos os nós de IaaS possuem um Agente de Gerenciamento de IaaS atualizado, siga estas etapas em cada nó:
 - a Faça login no vRealize Automation console de gerenciamento do appliance.
 - b Selecione **Configurações do vRA > Cluster**.
 - c Expanda a lista de todos os componentes instalados em cada nó de IaaS e localize o Agente de Gerenciamento de IaaS.
 - d Verifique se a versão do Agente de Gerenciamento é a atual.
- [Excluir a atualização do IaaS](#).
- Verifique se o backup do banco de dados Microsoft SQL Server IaaS está acessível caso você precise fazer uma reversão.
- Verifique se os snapshots dos servidores do IaaS na sua implantação estão disponíveis.

Se a atualização não for concluída com sucesso, volte ao snapshot e backup do banco de dados e tente atualizar novamente.

Procedimentos

- 1 Abra uma nova sessão de console no host Appliance do vRealize Automation. Faça login com a conta raiz.
- 2 Altere os diretórios para `/usr/lib/vcac/tools/upgrade/`.

É importante que todas as instâncias do IaaS Management Agent sejam atualizadas e estejam íntegras antes da execução do script de shell do `./upgrade`. Se algum Agente de Gerenciamento de IaaS apresentar um problema quando você executar o shell script de atualização, consulte [Falha na atualização do Agente de Gerenciamento](#).
- 3 Execute o script de atualização.
 - a No prompt de comando, insira `./upgrade`.
 - b Pressione Enter.

Para obter uma descrição do processo de atualização do IaaS, consulte [Atualizando os componentes do IaaS e do appliance do vRealize Automation](#).

Se o Script do Shell de Atualização falhar, revise o arquivo `upgrade-iaas.log`.

Você poderá executar o script de atualização novamente depois de corrigir os problemas.

Próximo passo

- 1 [Restaurar o acesso ao centro de controle integrado do vRealize Orchestrator](#).
- 2 Se a implantação usa um balanceador de carga, reative os monitores de integridade do vRealize Automation e o tráfego para todos os nós.

Para obter mais informações, consulte *Balanceamento de carga do vRealize Automation*.

Atualizando os componentes do IaaS usando o arquivo executável do instalador do IaaS depois de atualizar o appliance do vRealize Automation

Você pode usar esse método alternativo para atualizar os componentes do IaaS depois de atualizar o appliance do vRealize Automation 7.1, 7.2 ou 7.3.x para 7.4.

Baixar o instalador do IaaS para atualizar os componentes do IaaS depois de atualizar o appliance do vRealize Automation

Depois de atualizar o appliance do vRealize Automation para 7.4, baixe o instalador do IaaS para a máquina onde estão instalados os componentes do IaaS a serem atualizados.

Se receber avisos de certificado durante tal procedimento, você poderá ignorá-los.

Observação Exceto por uma instância de backup passiva do Serviço de Gerenciador, o tipo de inicialização para todos os serviços deve ser definido como Automático durante o processo de atualização. O processo de atualização falhará se você definir a opção Manual para serviços.

Pré-requisitos

- Verifique se o Microsoft .NET Framework 4.5.2 ou posterior está instalado na máquina de instalação do IaaS. Você pode baixar o instalador do .NET na página da Web do instalador do vRealize Automation. Se você atualizar o .NET para a versão 4.5.2 depois de desligar os serviços e a máquina for reiniciada como parte da instalação, será necessário interromper manualmente todos os serviços do IaaS, exceto o agente de Gerenciamento.
- Se você estiver usando o Internet Explorer para fazer o download, verifique se a Configuração de Segurança Reforçada está ativada. Insira `res://iesetup.dll/SoftAdmin.htm` na barra de pesquisa e pressione Enter.
- Faça login como administrador local no servidor Windows no qual um ou mais componentes do IaaS que você deseja atualizar estão instalados.

Procedimentos

1 Inicie um navegador da Web.

2 Insira a URL da página de download do instalador do Windows.

Por exemplo, `https://vcac-va-hostname.domain.name:5480/installer`, em que `vcac-va-hostname.domain.name` é o nome do nó primário (mestre) do Appliance do vRealize Automation.

3 Clique no link **Instalador do IaaS**.

4 Quando solicitado, salve o arquivo de instalação `setup__vcac-va-nomedohost.domínio.nome@5480.exe` na área de trabalho.

Não altere o nome do arquivo. Ele é utilizado para conectar a instalação com o Appliance do vRealize Automation.

Próximo passo

[Atualizar os componentes do IaaS após a atualização do vRealize Automation 7.1 ou 7.2 para a versão 7.3.](#)

Atualizar os componentes do IaaS após a atualização do vRealize Automation 7.1 ou 7.2 para a versão 7.3

É preciso atualizar o banco de dados SQL e configurar todos os sistemas que têm componentes de IaaS instalados. Você pode usar estas etapas para instalações mínimas e distribuídas.

Observação O instalador do IaaS deve estar na máquina que contém os componentes de IaaS que você deseja atualizar. Você não pode executar o instalador de uma localização externa, exceto para o banco de dados do Microsoft SQL que também pode ser atualizado remotamente por meio do nó da Web.

Verifique se os snapshots dos servidores do IaaS na sua implantação estão disponíveis. Se ocorrer falha na atualização, você poderá voltar para o snapshot e tentar outra atualização.

Execute a atualização para que os serviços sejam atualizados na seguinte ordem:

1 Sites de IaaS

Se você estiver usando um balanceador de carga, desative o tráfego para todos os nós não primários.

Conclua a atualização em um servidor antes de atualizar o próximo servidor que está executando um serviço de site. Comece com um servidor que tenha componente Model Manager Data instalado.

Se você estiver realizando uma atualização externa manual do banco de dados do Microsoft SQL, deverá atualizar o SQL externo antes de atualizar o nó da Web. Você pode atualizar um SQL externo remotamente no nó da Web.

2 Manager Services

Atualize o Manager Service ativo antes de atualizar o Manager Service passivo.

Se você não tiver a criptografia SSL habilitada em sua instância do SQL, desmarque a caixa de seleção Criptografia SSL na caixa de diálogo de configuração da atualização do IaaS ao lado da definição de SQL.

3 Orchestrator e trabalhadores do DEM

Atualize todos os orchestrators e trabalhadores do DEM. Conclua a atualização em um servidor antes de atualizar o próximo.

4 Agentes

Conclua a atualização em um servidor antes de atualizar o próximo que está executando um agente.

5 Agente de gerenciamento

É atualizado automaticamente como parte do processo de atualização.

Se você estiver usando diferentes serviços em um servidor, a atualização atualiza os serviços na ordem correta. Por exemplo, se o site tiver serviços de site e de gerente no mesmo servidor, selecione ambos para a atualização. O instalador da atualização aplica as atualizações na ordem correta. É possível concluir a atualização em um servidor antes de iniciar uma atualização em outro.

Observação Se a implantação usa um balanceador de carga, o appliance primário deve estar conectado ao balanceador de carga. Todas as outras instâncias de appliances do Appliance do vRealize Automation devem ser desativadas para o tráfego do balanceador de carga antes de se aplicar a atualização para evitar erros de cache.

Pré-requisitos

- Faça backup do seu ambiente existente do vRealize Automation.
- Se você reiniciar um servidor de IaaS após atualizar todos os appliances do vRealize Automation, mas antes de atualizar os componentes de IaaS, interrompa todos os serviços do Windows de IaaS, exceto o serviço do Agente de Gerenciamento, no servidor.
- [Baixar o instalador do IaaS para atualizar os componentes do IaaS depois de atualizar o appliance do vRealize Automation.](#)
- Verifique se o site IaaS primário, o banco de dados Microsoft SQL e o nó do Model Manager têm o JAVA SE Runtime Environment 8, 64 bits, atualização 111 ou versão posterior, instalado. Depois de instalar o Java, você deve configurar a variável de ambiente, JAVA_HOME, como a nova versão em cada nó do servidor.
- Verifique se a data de criação é anterior à data de modificação no arquivo web.config. Se a data de criação do arquivo web.config for igual ou posterior à data de modificação, realize o procedimento descrito em [Falha na atualização para o componente do site do IaaS](#)
- Conclua estas etapas para reconfigurar o Microsoft Distributed Transaction Coordinator (DTC).

Observação Mesmo com o Distributed Transaction Coordinator ativado, a transação distribuída a transação distribuída poderá falhar se o firewall estiver ativado.

- a No appliance vRealize Automation, selecione **Iniciar > Ferramentas Administrativas > Serviços de Componentes**.
- b Expanda **Serviços de Componentes > Computadores > Meu Computador > Distributed Transaction Coordinator**.
- c Selecione a tarefa apropriada.
 - Para um DTC local autônomo, clique com o botão direito do mouse em **DTC Local** e selecione **Propriedades**
 - Para um DTC em cluster, expanda **DTCs em Cluster** e clique com o botão direito no DTC em cluster nomeado e selecione **Propriedades**.
- d Clique em **Segurança**.

- e Selecione todas estas opções:
 - **Acesso DTC à Rede**
 - **Permitir Clientes Remotos**
 - **Permitir Entrada**
 - **Permitir Saída**
 - **Autenticação Mútua Obrigatória**
- f Clique em **OK**.

Procedimentos

- 1 Se você estiver usando um balanceador de carga, prepare o ambiente.
 - a Verifique se o nó do site de IaaS que contém os dados do Model Manager está ativado para tráfego do balanceador de carga.

É possível identificar este nó pela presença da pasta `vCAC Folder\Server\ConfigTool`.
 - b Desabilite todos os outros sites de IaaS e Manager Services não primários para o tráfego do balanceador de carga.
- 2 Clique com o botão direito do mouse no arquivo de configuração `setup__vrealize-automation-appliance-FQDN@5480.exe` e selecione **Executar como administrador**.
- 3 Clique em **Avançar**.
- 4 Aceite o contrato de licença e clique em **Avançar**.
- 5 Digite as credenciais de administrador para a implantação atual na página Login.

O nome de usuário é **root**, e a senha é aquela que você especificou durante a implantação do appliance.
- 6 Selecione **Aceitar Certificado**.
- 7 Na página **Tipo de instalação**, confirme que **Atualizar** está marcada.

Se **Atualizar** não estiver selecionada, os componentes deste sistema já foram atualizados para esta versão.
- 8 Clique em **Avançar**.

9 Defina as configurações de atualização.

| Opção | Ação |
|--|---|
| Se você estiver atualizando o Model Manager Data | <p>Marque a caixa de seleção Model Manager Data na seção Servidor vCAC.</p> <p>A caixa de seleção aparece selecionada por padrão. Atualize o Model Manager Data apenas uma vez. Se você estiver executando o arquivo de instalação em várias máquinas para atualizar uma instalação distribuída, os servidores da Web param de funcionar enquanto houver uma incompatibilidade de versão entre os servidores da Web e o Model Manager Data. Quando você tiver atualizado os dados do Model Manager e todos os servidores da Web, todos os servidores da Web devem funcionar.</p> |
| Se você estiver atualizando dados do Model Manager | <p>Desmarque a caixa de seleção Dados do Model Manager na seção Servidor vCAC.</p> |
| Para preservar fluxos de trabalho personalizados como a versão mais recente no Model Manager Data | <p>Se você estiver atualizando o Model Manager Data, marque a caixa de seleção Preservar as versões mais recentes do fluxo de trabalho na seção Fluxos de trabalho de extensibilidade.</p> <p>A caixa de seleção aparece selecionada por padrão. Os fluxos de trabalho personalizados são sempre preservados. A caixa de seleção determina apenas a ordem da versão. Se você usou o vRealize Automation Designer para personalizar fluxos de trabalho no Model Manager, selecione essa opção para a versão mais recente de cada fluxo de trabalho personalizado antes de a atualização ser mantida como a versão mais recente após a atualização.</p> <p>Se você não selecionar essa opção, a versão de cada fluxo de trabalho fornecido com o vRealize Automation Designer torna-se a mais recente após a atualização, e a versão mais recente antes da atualização torna-se a segunda mais recente.</p> <p>Para obter informações sobre o vRealize Automation Designer, consulte Estender ciclos de vida de máquina usando o vRealize Automation Designer.</p> |
| Se você estiver atualizando um Distributed Execution Manager ou um agente proxy | <p>Digite as credenciais da conta de administrador na seção Conta de serviço.</p> <p>Todos os serviços que você atualiza são executados sob esta conta.</p> |
| Para especificar seu banco de dados do Microsoft SQL Server | <p>Se você estiver atualizando o Model Manager Data, digite os nomes do servidor e da instância do banco de dados na caixa de seleção Servidor na seção Informações sobre a instalação do banco de dados do Microsoft SQL Server.</p> <p>Digite um nome de domínio totalmente qualificado (FQDN) para o nome do servidor de banco de dados na caixa de seleção Nome do banco de dados.</p> <p>Se a instância do banco de dados estiver em uma porta SQL não padrão, inclua o número da porta na especificação de instância do servidor. O número de porta padrão do Microsoft SQL é 1433.</p> <p>Ao atualizar os nós do gerenciador, a opção MSSQL SSL é selecionada por padrão. Se o seu banco de dados não usar SSL, desmarque a opção Usar SSL para conexão do banco de dados.</p> |

10 Clique em **Avançar**.

11 Confirme que todos os serviços a serem atualizados aparecem na página Pronto para Atualizar e clique em **Atualizar**.

A página Atualizar e um indicador de progresso aparecem. Quando o processo de atualização terminar, o botão **Avançar** é ativado.

12 Clique em **Avançar**.

- 13 Clique em **Concluir**.
- 14 Confirme que todos os serviços reiniciaram.
- 15 Repita essas etapas para cada servidor do IaaS da implantação na ordem recomendada.
- 16 Após a instalação de todos os componentes, faça login no console de gerenciamento do appliance e confirme que todos os serviços, incluindo o IaaS, estão registrados agora.
- 17 (Opcional) Ative o failover automático do Manager Service. Consulte [Ativar o Failover automático do Manager Service após a atualização](#).

Todos os componentes selecionados são atualizados para a nova versão.

Próximo passo

- 1 [Restaurar o acesso ao centro de controle integrado do vRealize Orchestrator](#).
- 2 Se a sua implantação usa um balanceador de carga, atualize todos os nós desse balanceador para que eles utilizem verificações de integridade do vRealize Automation e reabilite o tráfego do balanceador de carga para todos os nós desconectados.

Para obter mais informações, consulte *Balanceamento de carga do vRealize Automation*.

Restaurar o acesso ao centro de controle integrado do vRealize Orchestrator

Depois de atualizar os componentes do servidor IaaS, você deve restaurar o acesso para o vRealize Orchestrator.

Ao atualizar do vRealize Automation 7.3 e anterior para 7.4, você precisa executar este procedimento para acomodar o novo recurso de Controle de Acesso Baseado em Função. Esse procedimento é escrito para um ambiente de alta disponibilidade.

Pré-requisitos

Faça um snapshot do seu ambiente do vRealize Automation.

Procedimentos

- 1 Faça login no console de gerenciamento do Appliance do vRealize Automation como raiz usando o nome de domínio totalmente qualificado do host do appliance, `https://va-hostname.domain.name:5480`.
- 2 Selecione **Configurações do vRA > Banco de Dados**.
- 3 Identifique os nós mestre e de réplica.
- 4 Em cada nó de réplica, abra uma sessão SSH, faça login como administrador e execute este comando:

```
service vco-server stop && service vco-configurator stop
```
- 5 No nó mestre, abra uma sessão SSH, faça login como administrador e execute este comando:

```
rm /etc/vco/app-server/vco-registration-id
```
- 6 No nó mestre, altere os diretórios para `/etc/vco/app-server/`.

- 7 Abra o arquivo `sso.properties`.
- 8 Se o nome da propriedade `com.vmware.o11n.sso.admin.group.name` contiver espaços ou quaisquer outros caracteres relacionados à Bash que possam ser aceitos como um caractere especial em um comando de Bash, como um hífen (-) ou um sinal de dinheiro (\$), conclua estas etapas.
 - a Copie a linha com a propriedade `com.vmware.o11n.sso.admin.group.name` e insira `AdminGroup` para o valor.
 - b Adicione `#` ao início da linha original com a propriedade `com.vmware.o11n.sso.admin.group.name` para comentar na linha.
 - c Salve e feche o arquivo `sso.properties`.
- 9 Execute este comando:

```
vcac-vami vco-service-reconfigure
```
- 10 Abra o arquivo `sso.properties`. Se o arquivo foi alterado, conclua estas etapas.
 - a Remova o `#` do começo da linha original com a propriedade `com.vmware.o11n.sso.admin.group.name` para retirar o comentário da linha.
 - b Remova a cópia da linha com a propriedade `com.vmware.o11n.sso.admin.group.name`.
 - c Salve e feche o arquivo `sso.properties`.
- 11 Execute este comando para reiniciar o serviço `vco-server`:

```
reiniciar o serviço vco-server
```
- 12 Execute este comando para reiniciar o serviço `vco-configurator`:

```
reiniciar o serviço vco-configurator
```
- 13 No console de gerenciamento do Appliance do vRealize Automation, clique em **Serviços** e espere até que todos os serviços no nó mestre estejam registrados.
- 14 Quando todos os serviços estiverem registrados, ingresse os nós de réplica vRealize Automation ao cluster do vRealize Automation para sincronizar a configuração do vRealize Orchestrator. Para obter informações, consulte [Reconfigurar o vRealize Orchestrator integrado para dar suporte à alta disponibilidade](#).

Próximo passo

[Atualizando o vRealize Orchestrator após a atualização do vRealize Automation.](#)

Atualizando o vRealize Orchestrator após a atualização do vRealize Automation

Você deve atualizar sua instância do vRealize Orchestrator ao atualizar do vRealize Automation 7.1, 7.2 ou 7.3.x para o 7.4.

Com o lançamento do vRealize Orchestrator 7.4, você tem duas opções para atualizar o vRealize Orchestrator após uma atualização para o vRealize Automation 7.4.

- Você pode migrar seu servidor vRealize Orchestrator externo existente para um vRealize Orchestrator incluído no vRealize Automation 7.4.
- Você pode atualizar o seu servidor vRealize Orchestrator autônomo ou em cluster existente para funcionar com o vRealize Automation 7.4.

Migrando um servidor externo do vRealize Orchestrator para o vRealize Automation

Você pode migrar o servidor externo existente do vRealize Orchestrator para uma instância do vRealize Orchestrator incorporada no vRealize Automation 7.4.

Você pode implantar o vRealize Orchestrator como uma instância do servidor externo e configurar o vRealize Automation para funcionar com essa instância externa, ou você pode configurar e usar o servidor vRealize Orchestrator que está incluído no Appliance do vRealize Automation.

A VMware recomenda que você migre o vRealize Orchestrator externo para o servidor Orchestrator que está incorporado no vRealize Automation. A migração de um Orchestrator externo para um incorporado fornece os seguintes benefícios:

- Reduz o custo total de propriedade.
- Simplifica o modelo de implantação.
- Melhora a eficiência operacional.

Observação Considere utilizar o vRealize Orchestrator externo nos seguintes casos:

- Múltiplos tenants no ambiente vRealize Automation
 - Ambiente geográfico disperso
 - Manipulação da carga de trabalho
 - Utilização de plug-ins específicos, como o plug-in Site Recovery Manager das versões antigas
-

As diferenças do Centro de Controle entre o Orchestrator externo e integrado

Alguns dos itens de menu que estão disponíveis no Centro de Controle de um vRealize Orchestrator externo não estão incluídos na exibição padrão do Centro de Controle de uma instância integrada do Orchestrator.

No centro de controle do servidor do Orchestrator integrado, algumas opções estão ocultas por padrão.

| Item de Menu | Detalhes |
|---------------------------------------|--|
| Licenciamento | O Orchestrator integrado está pré-configurado para usar o vRealize Automation como um provedor de licença. |
| Configuração de Exportação/Importação | A configuração do Orchestrator integrada está incluída nos componentes exportados do vRealize Automation. |

| Item de Menu | Detalhes |
|--|--|
| Configurar banco de dados | O Orchestrator integrado usa o banco de dados que é usado pelo vRealize Automation. |
| Programa de Aperfeiçoamento da Experiência do Cliente | Você pode se associar ao Programa de Aperfeiçoamento da Experiência do Cliente (PAEC) na interface de gerenciamento do appliance vRealize Automation. Consulte o <i>Programa de Aperfeiçoamento da Experiência do Cliente em Gerenciando o vRealize Automation</i> . |

Outras opções que estão ocultas na exibição padrão do Centro de Controle são a caixa de texto do **endereço do host** e o botão **CANCELAR REGISTRO** na página **Configurar Provedor de Autenticação**.

Observação Para consultar todo o conjunto de opções do Centro de Controle no vRealize Orchestrator que está integrado em vRealize Automation, você deve acessar a página avançada de Gerenciamento do Orchestrator em https://vra-va-hostname.domain.name_or_load_balancer_address:8283/vco-controlcenter/#!/?advanced e clicar no botão F5, no teclado para atualizar a página.

Migrar um vRealize Orchestrator 7.x externo para o vRealize Automation 7.4

Você pode exportar a configuração da instância externa do Orchestrator existente e importá-la para o servidor do Orchestrator que está integrado em vRealize Automation.

Observação Se você tem diversos nós do Appliance do vRealize Automation, execute o procedimento de migração apenas no nó primário vRealize Automation.

Pré-requisitos

- Faça o upgrade ou migre o seu vRealize Automation para a versão 7.4. Para obter mais informações, consulte *Upgrade do vRealize Automation em Instalação ou Upgrade do vRealize Automation*.
- Pare o serviço do servidor Orchestrator do Orchestrator externo.
- Faça backup do banco de dados, incluindo o esquema do banco de dados do servidor Orchestrator externo.

Procedimentos

- 1 Exporte a configuração do servidor Orchestrator externo.
 - a Faça login no Centro de Controle do servidor Orchestrator externo como **raiz** ou como um **administrador**, dependendo da visão de origem.
 - b Pare o serviço do servidor do Orchestrator na página de **Opções de Inicialização** para prevenir alterações não desejadas ao banco de dados.
 - c Vá para a página **Configuração de Exportação/Importação**.
 - d Na página de **Configuração de Exportação**, selecione **Configuração do servidor de exportação**, **Plug-ins de pacote** e **Configurações do plug-in de exportação**.

2 Migre a configuração exportada para a instância integrada do Orchestrator.

- a Carregue o arquivo de configuração exportado para o diretório `/usr/lib/vco/tools/configuration-cli/bin` do Appliance do vRealize Automation.
- b Faça login para o Appliance do vRealize Automation pelo SSH como **raiz**.
- c Pare o serviço do servidor Orchestrator e o serviço do Centro de Controle do servidor vRealize Orchestrator integrado.

```
service vco-server stop && service vco-configurator stop
```

- d Importe o arquivo de configuração do Orchestrator para o servidor integrado vRealize Orchestrator, ao executar o script `vro-configure` com o comando `import`.

```
./vro-configure.sh import --type embedded --path orchestrator-config-export-orchestrator_appliance_ip-date_hour.zip
```

3 Se o servidor Orchestrator externo do qual você deseja migrar usar o banco de dados PostgreSQL integrado, edite os arquivos de configuração do banco de dados.

- a No arquivo `/var/vmware/vpostgres/current/pgdata/postgresql.conf`, remova o comentário da linha `listen_addresses`.
- b Defina os valores de `listen_addresses` para um caractere universal (*).

```
listen_addresses = '*'
```

- c Anexe a linha ao arquivo `/var/vmware/vpostgres/current/pgdata/pg_hba.conf`.

```
host all all vra-va-ip-address/32 md5
```

Observação O arquivo `pg_hba.conf` exige o uso de um prefixo do formato CIDR em vez de um endereço IP e de uma máscara de sub-rede.

- d Reinicia o serviço de servidor do PostgreSQL.

```
service vpostgres restart
```

- 4 Migre o banco de dados para o banco de dados PostgreSQL interno, executando o script vro-configure com o comando db-migrate.

```
./vro-configure.sh db-migrate --sourceJdbcUrl JDBC_connection_URL --sourceDbUsername database_user
--sourceDbPassword database_user_password
```

Observação Coloque entre aspas simples as senhas que contenham caracteres especiais.

O *JDBC_connection_URL* depende do tipo de banco de dados que você usa.

```
PostgreSQL: jdbc:postgresql://host:port/database_name
```

```
MSSQL: jdbc:jtds:sqlserver://host:port/database_name\; if using SQL authentication and MSSQL:
jdbc:jtds:sqlserver://host:port/database_name\;domain=domain\;useNTLMv2=TRUE if using Windows
authentication.
```

```
Oracle: jdbc:oracle:thin:@host:port:database_name
```

As informações de login do banco de dados padrão são:

| | |
|-------------------------------|--------|
| <i>database_name</i> | vmware |
| <i>database_user</i> | vmware |
| <i>database_user_password</i> | vmware |

- 5 Remova todos os certificados do armazenamento de chaves do banco de dados.

```
./vro-configuration.sh untrust --reset-db
```

- 6 Reinstalar os plug-ins do Orchestrator.
 - a Faça login no Control Center como **root**.
 - b Clique em **Solução de Problemas**.
 - c Clique em **Forçar reinstalação de plug-ins**.
- 7 Inicie o serviço do servidor Orchestrator.
- 8 Reverte para a configuração padrão dos arquivos postgresql.conf e pg_hba.conf.
 - a Reinicia o serviço de servidor do PostgreSQL.

Você migrou com êxito uma instância do servidor Orchestrator externo para uma instância vRealize Orchestrator integrada ao vRealize Automation.

Próximo passo

Definir o servidor integrado do vRealize Orchestrator. Consulte [Configure o Servidor vRealize Orchestrator integrado](#).

Configure o Servidor vRealize Orchestrator integrado

Depois de exportar a configuração de um servidor Orchestrator externo e importá-la para o vRealize Automation 7.4, você deve configurar o servidor Orchestrator integrado ao vRealize Automation.

Pré-requisitos

Migre a configuração do vRealize Orchestrator externo para o interno.

Procedimentos

- 1 Faça login para o Appliance do vRealize Automation pelo SSH como **raiz**.
- 2 Inicie o serviço do Centro de Controle e o serviço do servidor Orchestrator do servidor vRealize Orchestrator integrado.

```
service vco-configurator start && service vco-server start
```

- 3 Faça login no Centro de Controle do servidor Orchestrator integrado como um **administrador**.

Observação Se você migrar de uma instância externa do vRealize Orchestrator 7.4, pule para a etapa 5.

- 4 Verifique se o Orchestrator está configurado adequadamente na página **Validar Configuração** no Centro de controle.
- 5 Se o Orchestrator externo foi configurado para funcionar em modo cluster, reconfigure o cluster do Orchestrator em vRealize Automation.

- a Vá para a página avançada do **Gerenciamento do Cluster do Orchestrator** em https://vra-vr-hostname.domain.name_or_load_balancer_address:8283/vco-controlcenter/#!/control-app/ha?remove-nodes.

Observação Se as caixas de seleção **Remove** ao lado dos nós existentes no cluster não aparecerem, você deve atualizar a página do navegador clicando no botão F5, no teclado.

- b Selecione as caixas de seleção ao lados dos nós do Orchestrator externo e clique em **Remove** para removê-los do cluster.
 - c Para sair da página de gerenciamento avançada do cluster, exclua a cadeia de caracteres `remove-nodes` do URL e atualize a página do navegador clicando no botão F5, no teclado.
 - d Na página **Validar Configuração** no Centro de Controle, verifique se o Orchestrator está configurado adequadamente.
- 6 (Opcional) Na guia **Certificado de Assinatura do Pacote** na página de **Certificados**, gere um novo certificado de assinatura do pacote.
 - 7 (Opcional) Altere os valores para **Tenant padrão** e **Grupo de Admin** na página **Configura Provedor de Autenticação**.
 - 8 Verifique se o serviço `vco-server` aparece como REGISTRADO na guia **Serviços** no console de gerenciamento do Appliance do vRealize Automation.

- 9 Selecione os serviços do vco do servidor externo do Orchestrator e clique em **Cancelar o registro**.

Próximo passo

- Importe quaisquer certificados que eram confiáveis no servidor externo do Orchestrator para o armazenamento de confiança do Orchestrator integrado.
- Associe os nós de réplica do vRealize Automation ao cluster vRealize Automation para sincronizar a configuração do Orchestrator.

Para mais informações, consulte *Reconfigurar o vRealize Orchestrator integrado para suportar alta disponibilidade* em *Instalando ou Atualizando o vRealize Automation*.

Observação As instâncias vRealize Orchestrator são automaticamente clusterizadas e disponibilizadas para uso.

- Reinicie o serviço vco-configurator em todos os nós do cluster.
- Atualize o endpoint vRealize Orchestrator para apontar para o servidor Orchestrator integrado migrado.
- Adicione o host vRealize Automation e o host laaS ao inventário do plug-in vRealize Automation ao executar Adicionar um host vRA e Adicionar o host laaS de fluxos de trabalho de um host vRA.

Atualizando um appliance autônomo do vRealize Orchestrator para uso com o vRealize Automation

Se você mantiver uma instância externa e autônoma do vRealize Orchestrator para uso com o vRealize Automation, será preciso atualizar o vRealize Orchestrator ao fazer a atualização do vRealize Automation 7.1, 7.2 ou 7.3.x para o 7.4.

As instâncias incorporadas do vRealize Orchestrator são atualizadas como parte da atualização do appliance do vRealize Automation. Nenhuma ação extra é necessária para instâncias integradas.

Se você estiver fazendo a atualização de um cluster de appliance do vRealize Orchestrator, veja [Atualizar o cluster do vRealize Orchestrator Appliance para uso com o vRealize Automation 7.4](#).

Pré-requisitos

- [Instalar a atualização nos componentes do laaS e do appliance do vRealize Automation](#).
- Desmonte todos os sistemas do arquivo de rede. Consulte *Administração da Máquina virtual do vSphere* na documentação do vSphere.
- Aumente a memória do Orchestrator Appliance do vSphere para pelo menos 6 GB. Consulte *Administração da Máquina virtual do vSphere* na documentação do vSphere.
- Tire um snapshot da máquina virtual Orchestrator do vSphere. Consulte *Administração da Máquina virtual do vSphere* na documentação do vSphere.
- Se utilizar um banco de dados externo, faça backup dele.

- Se você usar o banco de dados PostgreSQL pré-configurado no Orchestrator vSphere, faça backup do banco de dados usando o menu **Exportar banco de dados** menu no Centro de controle do vSphere.

Procedimentos

- ◆ Use um dos métodos documentados para atualizar o seu vRealize Orchestrator independente.
 - [Atualizar o Orchestrator Appliance usando o Repositório VMware padrão.](#)
 - [Atualizado o Orchestrator Appliance usando uma imagem ISO.](#)
 - [Atualizar o Orchestrator Appliance usando um Repositório Específico.](#)

Atualizar o Orchestrator Appliance usando o Repositório VMware padrão

Você pode configurar o Orchestrator para baixar o pacote de atualização do repositório VMware padrão.

Pré-requisitos

- Desmonte todos os sistemas do arquivo de rede. Para obter mais informações, consulte a documentação *Administração da Máquina Virtual vSphere*.
- Aumente a memória do Orchestrator Appliance para pelo menos 6 GB. Para obter mais informações, consulte a documentação *Administração da Máquina Virtual vSphere*.
- Aumente o tamanho do disco da máquina virtual do vRealize Orchestrator: Disco 1 = 7 GB, Disco 2 = 10 GB.
- Certifique-se de que a partição raiz do Orchestrator Appliance tenha pelo menos de 3 GB de espaço livre disponível. Para obter mais informações sobre como aumentar o tamanho de uma partição de disco, consulte KB 1004071: <http://kb.vmware.com/kb/1004071>.
- Tire um snapshot da máquina virtual Orchestrator. Para obter mais informações, consulte a documentação *Administração da Máquina Virtual vSphere*.
- Se utilizar um banco de dados externo, faça backup dele.
- Se você usar o pré-configurado no banco de dados Orchestrator PostgreSQL, faça backup do banco de dados usando o menu **Exportar banco de dados** menu no Centro de controle.

Procedimentos

- 1 Vá para a Interface de Gerenciamento do Appliance Virtual (VAMI) em https://orchestrator_server:5480 e faça login como **raiz**.
- 2 Na guia **Atualizar**, clique em **Configurações**.
O botão de seleção próximo da opção **Use o Repositório Especificado** está selecionado.
- 3 Na página **Status**, clique em **Verificar Atualizações**.
- 4 Se houver alguma atualização disponível, clique em **Instalar Atualizações**.
- 5 Aceite o acordo de licença do usuário final VMware e confirme que você deseja instalar a atualização.

- 6 Para concluir a atualização, reinicie o Orchestrator Appliance.
 - a Faça login novamente na Interface de Gerenciamento do Appliance Virtual (VAMI) como **raiz**.
- 7 (Opcional) Na guia **Atualizar**, verifique se a última versão do Orchestrator Appliance está instalada com sucesso.
- 8 Faça login no Control Center como **root**.
- 9 Se você planeja criar um cluster de instâncias do Orchestrator, redefina as configurações dos hosts.
 - a Na página **Configurações do Host** do Centro de Controle, clique em **CHANGE**.
 - b Insira o nome do host do servidor do balanceador de carga em vez de inserir o nome do appliance do vRealize Orchestrator.
- 10 Reconfigure a autenticação.
 - a Se, antes da atualização, o servidor Orchestrator foi configurado para usar **LDAP** ou **SSO (legado)** como o método de autenticação, configure o **vSphere** ou o **vRealize Automation** como um provedor de autenticação.
 - b Se a autenticação já estiver definida como **vSphere** ou **vRealize Automation**, remova as configurações e registre-as novamente.

Observação Se, antes da atualização, o Orchestrator tiver usado o **vSphere** como um provedor de autenticação e tiver sido configurado para se conectar ao nome de domínio totalmente qualificado ou endereço IP do vCenter Server, caso você tenha um Platform Services Controller externo, após a atualização, você deverá configurar o Orchestrator para conectar-se ao nome de domínio totalmente qualificado ou endereço IP da instância do Controlador de Serviços de Plataforma que contém o vCenter Single Sign-On. Você também deve importar para o Orchestrator manualmente os certificados de todos os Platform Services Controllers que compartilham o mesmo domínio do vCenter Single Sign-On.

Você atualizou com êxito o Orchestrator Appliance.

Próximo passo

Verifique se o Orchestrator está configurado adequadamente na página **Validar Configuração** no Centro de controle.

Atualizado o Orchestrator Appliance usando uma imagem ISO

Você pode configurar o Orchestrator para baixar o pacote de atualização de um arquivo de imagem ISO montado na unidade de CD-ROM do appliance.

Pré-requisitos

- Desmonte todos os sistemas do arquivo de rede. Para obter mais informações, consulte a documentação *Administração da Máquina Virtual vSphere*.
- Aumente a memória do Orchestrator Appliance para pelo menos 6 GB. Para obter mais informações, consulte a documentação *Administração da Máquina Virtual vSphere*.

- Aumente o tamanho do disco da máquina virtual do vRealize Orchestrator: Disco 1 = 7 GB, Disco 2 = 10 GB.
- Certifique-se de que a partição raiz do Orchestrator Appliance tenha pelo menos de 3 GB de espaço livre disponível. Para obter mais informações sobre como aumentar o tamanho de uma partição de disco, consulte KB 1004071: <http://kb.vmware.com/kb/1004071>.
- Tire um snapshot da máquina virtual Orchestrator. Para obter mais informações, consulte a documentação *Administração da Máquina Virtual vSphere*.
- Se utilizar um banco de dados externo, faça backup dele.
- Se você usar o pré-configurado no banco de dados Orchestrator PostgreSQL, faça backup do banco de dados usando o menu **Exportar banco de dados** menu no Centro de controle.

Procedimentos

- 1 Baixe o arquivo VMware-vRO-Appliance-version-build_number-updaterepo.iso do site de download oficial da VMware.
- 2 Conecte a unidade de CD-ROM da máquina virtual Orchestrator Appliance. Para obter mais informações, consulte a documentação *Administração da Máquina Virtual vSphere*.
- 3 Monte o arquivo de imagem ISO para a unidade CD-ROM do appliance. Para obter mais informações, consulte a documentação *Administração da Máquina Virtual vSphere*.
- 4 Vá para a Interface de Gerenciamento do Appliance Virtual (VAMI) em https://orchestrator_server:5480 e faça login como **raiz**.
- 5 Na guia **Atualizar**, clique em **Configurações**.
- 6 Selecione o botão de seleção próximo da opção **Use as atualizações do CD-ROM**.
- 7 Retorne para página de **Status**.
A versão da atualização disponível é exibida.
- 8 Clique em **Instalar Atualizações**.
- 9 Aceite o acordo de licença do usuário final VMware e confirme que você deseja instalar a atualização.
- 10 Para concluir a atualização, reinicie o Orchestrator Appliance.
 - a Faça login novamente na Interface de Gerenciamento do Appliance Virtual (VAMI) como **raiz**.
- 11 (Opcional) Na guia **Atualizar**, verifique se a última versão do Orchestrator Appliance está instalada com sucesso.
- 12 Faça login no Control Center como **root**.
- 13 Se você planeja criar um cluster de instâncias do Orchestrator, redefina as configurações dos hosts.
 - a Na página **Configurações do Host** do Centro de Controle, clique em **CHANGE**.
 - b Insira o nome do host do servidor do balanceador de carga em vez de inserir o nome do appliance do vRealize Orchestrator.

14 Reconfigure a autenticação.

- a Se, antes da atualização, o servidor Orchestrator foi configurado para usar **LDAP** ou **SSO (legado)** como o método de autenticação, configure o **vSphere** ou o **vRealize Automation** como um provedor de autenticação.
- b Se a autenticação já estiver definida como **vSphere** ou **vRealize Automation**, remova as configurações e registre-as novamente.

Observação Se, antes da atualização, o Orchestrator tiver usado o **vSphere** como um provedor de autenticação e tiver sido configurado para se conectar ao nome de domínio totalmente qualificado ou endereço IP do vCenter Server, caso você tenha um Platform Services Controller externo, após a atualização, você deverá configurar o Orchestrator para conectar-se ao nome de domínio totalmente qualificado ou endereço IP da instância do Controlador de Serviços de Plataforma que contém o vCenter Single Sign-On. Você também deve importar para o Orchestrator manualmente os certificados de todos os Platform Services Controllers que compartilham o mesmo domínio do vCenter Single Sign-On.

Você atualizou com êxito o Orchestrator Appliance.

Próximo passo

Verifique se o Orchestrator está configurado adequadamente na página **Validar Configuração** no Centro de controle.

Atualizar o Orchestrator Appliance usando um Repositório Específico

Você pode configurar o Orchestrator para usar um repositório local no qual você carrega o arquivo de atualização.

Pré-requisitos

- Desmonte todos os sistemas do arquivo de rede. Para obter mais informações, consulte a documentação *Administração da Máquina Virtual vSphere*.
- Aumente a memória do Orchestrator Appliance para pelo menos 6 GB. Para obter mais informações, consulte a documentação *Administração da Máquina Virtual vSphere*.
- Aumente o tamanho do disco da máquina virtual do vRealize Orchestrator: Disco 1 = 7 GB, Disco 2 = 10 GB.
- Certifique-se de que a partição raiz do Orchestrator Appliance tenha pelo menos de 3 GB de espaço livre disponível. Para obter mais informações sobre como aumentar o tamanho de uma partição de disco, consulte KB 1004071: <http://kb.vmware.com/kb/1004071>.
- Tire um snapshot da máquina virtual Orchestrator. Para obter mais informações, consulte a documentação *Administração da Máquina Virtual vSphere*.
- Se utilizar um banco de dados externo, faça backup dele.
- Se você usar o pré-configurado no banco de dados Orchestrator PostgreSQL, faça backup do banco de dados usando o menu **Exportar banco de dados** menu no Centro de controle.

Procedimentos

- 1 Preparar o repositório local para atualizações.
 - a Instalar e configurar um servidor web local.
 - b Baixe o arquivo `VMware-vR0-Appliance-version-build_number-updaterepo.zip` do site de download oficial da VMware.
 - c Extraia o arquivo .ZIP para o repositório local.
- 2 Vá para a Interface de Gerenciamento do Appliance Virtual (VAMI) em `https://orchestrator_server:5480` e faça login como **raiz**.
- 3 Na guia **Atualizar**, clique em **Configurações**.
- 4 Selecione o botão de seleção próximo da opção **Use o Repositório Especificado**.
- 5 Insira o endereço do URL do repositório local apontando para o diretório `Update_Repo`.
`http://local_web_server:port/build/mts/release/bora-build_number/publish/exports/Update_Repo`
- 6 Caso o repositório local necessite de autenticação, insira o nome de usuário e senha.
- 7 Clique em **Salvar Configurações**.
- 8 Na página **Status**, clique em **Verificar Atualizações**.
- 9 Se houver alguma atualização disponível, clique em **Instalar Atualizações**.
- 10 Aceite o acordo de licença do usuário final VMware e confirme que você deseja instalar a atualização.
- 11 Para concluir a atualização, reinicie o Orchestrator Appliance.
 - a Faça login novamente na Interface de Gerenciamento do Appliance Virtual (VAMI) como **raiz**.
- 12 (Opcional) Na guia **Atualizar**, verifique se a última versão do Orchestrator Appliance está instalada com sucesso.
- 13 Faça login no Control Center como **root**.
- 14 Se você planeja criar um cluster de instâncias do Orchestrator, redefina as configurações dos hosts.
 - a Na página **Configurações do Host** do Centro de Controle, clique em **CHANGE**.
 - b Insira o nome do host do servidor do balanceador de carga em vez de inserir o nome do appliance do vRealize Orchestrator.

15 Reconfigure a autenticação.

- a Se, antes da atualização, o servidor Orchestrator foi configurado para usar **LDAP** ou **SSO (legado)** como o método de autenticação, configure o **vSphere** ou o **vRealize Automation** como um provedor de autenticação.
- b Se a autenticação já estiver definida como **vSphere** ou **vRealize Automation**, remova as configurações e registre-as novamente.

Observação Se, antes da atualização, o Orchestrator tiver usado o **vSphere** como um provedor de autenticação e tiver sido configurado para se conectar ao nome de domínio totalmente qualificado ou endereço IP do vCenter Server, caso você tenha um Platform Services Controller externo, após a atualização, você deverá configurar o Orchestrator para conectar-se ao nome de domínio totalmente qualificado ou endereço IP da instância do Controlador de Serviços de Plataforma que contém o vCenter Single Sign-On. Você também deve importar para o Orchestrator manualmente os certificados de todos os Platform Services Controllers que compartilham o mesmo domínio do vCenter Single Sign-On.

Você atualizou com êxito o Orchestrator Appliance.

Próximo passo

Verifique se o Orchestrator está configurado adequadamente na página **Validar Configuração** no Centro de controle.

Atualizar o cluster do vRealize Orchestrator Appliance para uso com o vRealize Automation 7.4

Se você usar um cluster do vRealize Orchestrator Appliance com o vRealize Automation, deverá atualizar o cluster do Orchestrator Appliance para a versão 7.4, atualizando uma única instância e associando os nós recém-instalados da versão 7.4 à instância atualizada.

Para atualizar uma única instância de vRealize Orchestrator, consulte [Atualizando um appliance autônomo do vRealize Orchestrator para uso com o vRealize Automation](#).

Pré-requisitos

- [Instalar a atualização nos componentes do IaaS e do appliance do vRealize Automation](#).
- Configure um balanceador de carga para distribuir o tráfego entre as várias instâncias do vRealize Orchestrator. Consulte o [Guia de Configuração do Balanceador de Carga do vRealize Orchestrator](#).
- Faça um snapshot de todos os nós do servidor vRealize Orchestrator.
- Faça backup do banco de dados compartilhado vRealize Orchestrator.

Procedimentos

- 1 Pare os serviços do Orchestrator `vco-server` e `vco-configurator` em todos os nós do cluster.
- 2 Atualize apenas uma das instâncias do servidor do Orchestrator no seu cluster usando um dos procedimentos documentados.

- 3 Instale um novo Orchestrator Appliance na versão 7.3.
 - a Configure o novo nó com as configurações de rede de uma instância existente não atualizada que seja parte do cluster.
- 4 Acesse o Centro de Controle do segundo nó para iniciar o assistente de configuração.
 - a Navegue para `https://your_orchestrator_server_IP_or_DNS_name:8283/vco-controlcenter`.
 - b Faça login como **raiz** com a senha que você inseriu durante a implantação OVA.
- 5 Selecione o tipo de implantação **Orchestrator Clusterizado**.

Ao escolher este tipo, você seleciona associar o nó a um cluster existente do Orchestrator.
- 6 Na caixa de texto **Hostname** insira o nome do host ou o endereço IP da primeira instância do servidor do Orchestrator.

Observação Deve ser o IP local ou nome do host da instância do Orchestrator para a qual você está associando o segundo nó. Você não deve utilizar o endereço do balanceador de carga.

- 7 Nas caixas de texto **Nome de Usuário** e **Senha**, insira as credenciais raiz da primeira instância do servidor Orchestrator.
- 8 Clique em **Associar**. A instância do Orchestrator clona a configuração do nó ao qual ela se associa. O serviço do servidor Orchestrator de ambos os nós reinicia automaticamente.
- 9 Acesse o Centro de Controle do cluster do Orchestrator atualizado através do endereço do balanceador de carga e faça login como **administrador**.
- 10 Na página **Gerenciamento de Cluster do Orchestrator**, verifique se as cadeias de caracteres **Configuração de Impressão Digital Ativa** e **Configuração de Impressão Digital Pendente** em todos os nós do cluster são correspondentes.

Observação Talvez seja preciso atualizar a página diversas vezes até que as duas cadeias de caracteres correspondam-se.

- 11 Verifique se o cluster do vRealize Orchestrator está configurado adequadamente abrindo a página **Validar Configuração** no Centro de controle.
- 12 (Opcional) Repita os passos de 3 a 8 para cada nó adicional no cluster.

Você atualizou com êxito o cluster do Orchestrator.

Próximo passo

[Ativar os balanceadores de carga.](#)

Ativar os balanceadores de carga

Se a sua implantação usar balanceadores de carga, reative os nós secundários e as verificações de integridade e reverta as configurações de tempo limite do balanceador de carga.

As checagens de integridade para vRealize Automation variam de acordo com a versão. Para obter informações, consulte o *Guia de Configuração de Balanceamento de Carga do vRealize Automation* na [Documentação do VMware vRealize Automation](#).

Altere as configurações de tempo limite do balanceador de carga de 10 minutos de volta para as configurações padrão.

Tarefas de pós-atualização para atualizar o vRealize Automation

Após a atualização do vRealize Automation 7.1, 7.2 ou 7.3.x para 7.4, você deve realizar as tarefas de pós-atualização necessárias.

Atualizando os agentes de software para o TLS 1.2

Após a atualização para o vRealize Automation 7.4, você deve realizar várias tarefas para atualizar os Agentes de Software do ambiente do vRealize Automation 7.1, 7.2, 7.3 ou 7.3.1 para o TLS 1.2.

Começando com o vRealize Automation 7.4, o Transport Layer Security (TLS) 1.2 é o único protocolo TLS suportado para comunicação de dados entre o vRealize Automation e seu navegador.

Após a migração, você deve atualizar os modelos da máquina virtual existentes do ambiente do vRealize Automation 7.1, 7.2, 7.3 ou 7.3.1 bem como quaisquer máquinas virtuais existentes.

Atualizar modelos da máquina virtual do vRealize Automation

Você deve atualizar os modelos existentes após concluir a atualização para o vRealize Automation 7.4 para que os Agentes de Software usem o protocolo TLS 1.2.

O agente guest e o código de bootstrap do agente devem ser atualizados nos modelos do vRealize Automation 7.1, 7.2, 7.3 ou 7.3.1. Se você estiver usando uma opção de clone vinculado, talvez você precise mapear novamente os modelos com as máquinas virtuais recém-criadas e os snapshots.

Para atualizar seus modelos, você deve concluir estas tarefas.

- 1 Faça login no vSphere.
- 2 Converta cada modelo do vRealize Automation 7.1, 7.2, 7.3 ou 7.3.1 em uma máquina virtual e ligue a máquina.
- 3 Importe o instalador de software adequado e execute o instalador de software em cada máquina virtual.
- 4 Converta cada máquina virtual em um modelo novamente.

Use esse procedimento para localizar o instalador de software para Linux ou Windows.

Pré-requisitos

Atualização bem-sucedida para o vRealize Automation 7.4.

Procedimentos

- 1 Inicie um navegador e abra a tela inicial do appliance do vRealize Automation 7.4 usando o nome de domínio completo do appliance virtual: `https://vra-va-hostname.domain.name`.

- 2 Clique na **página de agentes guest e de software**.
- 3 Siga as instruções para o instalador de software Linux ou Windows.

Próximo passo

[Identificar máquinas virtuais que precisam de atualização do Agente de Software.](#)

Identificar máquinas virtuais que precisam de atualização do Agente de Software

Você pode usar o Serviço de Integridade no vRealize Automation para identificar máquinas virtuais que precisam de uma atualização do Agente de Software para o TLS 1.2.

Você pode usar o Serviço de Integridade para identificar as máquinas virtuais que precisam de uma atualização do Agente de Software para o TLS 1.2. Todos os Agentes de Software no ambiente do vRealize Automation 7.4 precisam ser atualizados para que você possa realizar os procedimentos de pós-provisionamento, que exigem uma comunicação segura entre o navegador e o vRealize Automation.

Pré-requisitos

- Você atualizou com êxito para o vRealize Automation 7.4.
- Você está conectado ao vRealize Automation 7.4 no appliance virtual primário como administrador de locatário.

Procedimentos

- 1 Clique em **Administração > Integridade**.
- 2 Clique em **Nova Configuração**.
- 3 Na página Detalhes da Configuração, forneça as informações solicitadas.

| Opção | Comentário |
|-------------|---|
| Nome | Insira a verificação do Agente de SW . |
| Descrição | Adicione uma descrição opcional, por exemplo, Localizar os agentes de software para atualizar para o TLS 1.2 . |
| Produto | Selecione vRealize Automation 7.4.0. |
| Programação | Selecione Nenhum(a) . |

- 4 Clique em **Avançar**.
- 5 Na página Selecionar Pacotes de Teste, selecione **Testes do Sistema para o vRealize Automation** e **Testes de Tenant para o vRealize Automation**.
- 6 Clique em **Avançar**.

- Na página Parâmetros da Configuração, forneça as informações solicitadas.

Tabela 1-56. Appliance virtual vRealize Automation

| Opção | Descrição |
|--|---|
| Endereço do Servidor Web Público | <ul style="list-style-type: none"> Para uma implantação mínima, a URL base para o host do appliance do vRealize Automation. Por exemplo, <code>https://va-host.domain/</code>. Para uma implantação de alta disponibilidade, a URL base para o balanceador de carga do vRealize Automation. Por exemplo, <code>https://load-balancer-host.domain/</code>. |
| Endereço do Console SSH | Nome do domínio totalmente qualificado do appliance vRealize Automation. Por exemplo, <code>va-host.domain</code> . |
| Usuário do Console SSH | raiz |
| Senha do Console SSH | Senha para a raiz. |
| Tempo Máximo de Resposta do Serviço (ms) | Aceitar o padrão: 2000 |

Tabela 1-57. Tenant do Sistema vRealize Automation

| Opção | Descrição |
|-------------------------------------|-----------------------------|
| Administrador de Tenants do Sistema | administrador |
| Senha do Tenant do Sistema | Senha para o administrador. |

Tabela 1-58. Monitoramento do Espaço em Disco do vRealize Automation

| Opção | Descrição |
|--------------------------------|---------------------|
| Porcentagem de Limite de Aviso | Aceite o padrão: 75 |
| Porcentagem de Limite Crítico | Aceite o padrão: 90 |

Tabela 1-59. Tenant do vRealize Automation

| Opção | Descrição |
|---|---|
| Tenant em Teste | Tenant selecionado para teste. |
| Nome de Usuário do Administrador da Estrutura | Nome de usuário do administrador da estrutura. Por exemplo, <code>admin@va-host.local</code> . Observação O administrador da estrutura também deve ter um administrador de locatário e uma função de administrador de IaaS para que todos os testes sejam executados. |
| Senha do Administrador da Estrutura | Senha para o administrador da estrutura. |

- Clique em **Avançar**.
- Na página Resumo, revise as informações e clique em **Concluir**.
A configuração de verificação do agente de software está concluída.
- No cartão de verificação do Agente de SW, clique em **Executar**.

- 11 Quando o teste estiver concluído, clique no centro do cartão de verificação do Agente de SW.
- 12 Na página de resultados da verificação do Agente de SW, acesse os resultados do teste e encontre o teste Verificar a versão do Agente de Software na coluna Nome. Se ocorrer um erro no resultado do teste, clique no link **Causa** na coluna Causa para ver as máquinas virtuais com um agente de software desatualizado.

Próximo passo

Se você tiver máquinas virtuais com um agente de software desatualizado, consulte [Atualizar os Agentes de Software no vSphere](#).

Atualizar os Agentes de Software no vSphere

Você pode atualizar os Agentes de Software desatualizados no vSphere para o TLS 1.2 após a atualização usando o Gerenciamento de Appliance do vRealize Automation.

Esse procedimento atualiza os Agentes de Software desatualizados para o TLS 1.2 nas máquinas virtuais em seu ambiente atualizado. Ele é necessário para a atualização para o vRealize Automation 7.4.

Pré-requisitos

- Atualização bem-sucedida para o vRealize Automation 7.4.
- Você usou o Serviço de Integridade para identificar os appliances virtuais com os Agentes de Software desatualizados.

Procedimentos

- 1 No appliance do vRealize Automation primário, faça login no Gerenciamento do Appliance do vRealize Automation como **root** usando a senha que você inseriu quando implantou o appliance do vRealize Automation.

Para um ambiente de alta disponibilidade, abra o Gerenciamento do Appliance no appliance mestre.

- 2 Clique em **Configurações do vRA > Agentes de SW**.

- 3 Clique em **Alternar TLS 1.0, 1.1**.

O Status do TLS v1.0, v1.1 está HABILITADO.

- 4 Quanto às credenciais de Locatário, insira as informações solicitadas para o appliance do vRealize Automation 7.4.

| Opção | Descrição |
|-----------------|---|
| Nome do tenant | Nome do locatário no appliance do vRealize Automation atualizado. Observação O usuário do locatário deve ter a função de Arquiteto de Software atribuída. |
| Nome de usuário | Nome de usuário de administrador do locatário no appliance do vRealize Automation. |
| Senha | Senha do administrador do locatário. |

- 5 Clique em **Testar conexão**.

Se uma conexão é estabelecida, uma mensagem de êxito é exibida.

- 6 Clique em **Listar lotes**.

A tabela Lista de opções de lote é exibida.

- 7 Clique em **Mostrar**.

Uma tabela é exibida com uma lista de máquinas virtuais com os Agentes de Software desatualizados.

- 8 Atualize o Agente de Software para as máquinas virtuais que estão no estado ATUALIZÁVEL.

- Para atualizar o Agente de Software em uma máquina virtual individual, clique em **Mostrar** em um grupo de máquinas virtuais, identifique a máquina virtual que você deseja atualizar e clique em **Executar** para iniciar o processo de atualização.
- Para atualizar o Agente de Software em um lote de máquinas virtuais, identifique o grupo que você deseja atualizar e clique em **Executar** para iniciar o processo de atualização.

Se você tiver mais de 200 máquinas virtuais para atualizar, será possível controlar a velocidade do processo de atualização em lote, inserindo valores para esses parâmetros.

| Opção | Descrição |
|----------------------|---|
| Tamanho do lote | O número de máquinas virtuais selecionadas para a atualização em lote. Você pode variar esse número para ajustar a velocidade de atualização. |
| Profundidade da Fila | O número de execuções de atualização paralelas que ocorrem ao mesmo tempo. Por exemplo, 20. Você pode variar esse número para ajustar a velocidade de atualização. |
| Erros em Lote | A contagem de erros REST está fazendo com que a atualização em lote seja reduzida. Por exemplo, se você quiser parar a atualização em lote atual após 5 falhas para melhorar a estabilidade da atualização, insira 5 no campo de texto. |

| Opção | Descrição |
|------------------|---|
| Falhas em Lote | O número de atualizações do Agente de Software com falha está fazendo com que o processamento em lote seja reduzido. Por exemplo, se você quiser parar a atualização em lote atual após 5 falhas para melhorar a estabilidade da atualização, insira 5 no campo de texto. |
| Sondagem em Lote | Com que frequência o processo de atualização é monitorado para verificar o processo de atualização. Você pode variar esse número para ajustar a velocidade de atualização. |

Se o processo de atualização é muito lento ou produz muitas atualizações bem-sucedidas, você pode ajustar esses parâmetros para melhorar o desempenho da atualização.

Observação A lista de lotes é limpa ao clicar em **Atualizar**. Isso não afeta o processo de atualização. Ele também atualiza as informações no que se refere à definição ou não do TLS 1.2. Além disso, ao clicar em **Atualizar**, uma verificação de integridade dos serviços do vRealize Automation também é realizada. Se os serviços não estão em execução, o sistema exibe uma mensagem de erro e desativa todos os outros botões de ação.

9 Clique em **Alternar TLS 1.0, 1.1**.

O Status do TLS v1.0, v1.1 está DESABILITADO.

Atualizar os Agentes de Software no Amazon Web Services ou Azure

Você pode atualizar qualquer Agente de Software desatualizado nas máquinas virtuais no Amazon Web Service (AWS) ou Azure manualmente.

Pré-requisitos

- Atualização bem-sucedida para o vRealize Automation 7.4.
- Um túnel de software está presente e o endereço IP da máquina virtual de túnel é conhecido.

Procedimentos

- 1 Crie um arquivo de nó para cada nó que você precisa atualizar.

```
/usr/lib/vcac/server/webapps/ROOT/software/initializeUpdateSoftwareAgents.py -a <
$DestinationVRAServer> -t <$Tenant> -tu <$TenantUser> -S <$SourceVRAServer>
```

Observação Para uma atualização no local, o \$DestinationVRAServer é igual ao \$SourceVRAServer.

2 Crie um arquivo de plano para atualizar o Agente de Software em uma máquina virtual do Linux ou Windows.

- Modifique o arquivo de parâmetros de migração em `/var/log/vcac/agentupdate/{tenant}/{subtenant-UUID}` para conter o valor do endereço IP privado correspondente ao endpoint do AWS ou Azure.

```
"key": "ipAddress",
  "value": {
    "type": "string",
    "value": "<$PrivateIp:$PrivatePort>"
  }
}
```

- Utilize este comando para atualizar uma máquina Linux.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer>
-t <$Tenant> -S <$SourceVRAServer> -tu <$TenantUser> -CL Software.LinuxAgentUpdate74 --
source_cloud_provider azure
```

- Utilize este comando para atualizar uma máquina Windows.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer>
-t <$Tenant> -S <$SourceVRAServer> -tu <$TenantUser> -CW Software.WindowsAgentUpdate74 --
source_cloud_provider azure
```

- Este comando executa o arquivo de plano.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer>
-t <$Tenant> -tu <$TenantUser> --plan_file /usr/lib/vcac/server/webapps/ROOT/software/plan
```

- 3 Use este comando para atualizar o Agente de Software usando o arquivo de nó da etapa 1 e o arquivo de plano da etapa 2.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer> -t <$tenant> -tu <$TenantUser> --component_windows Software.WindowsAgentUpdate74 --component_linux Software.LinuxAgentUpdate74 --plan_file /usr/lib/vcac/server/webapps/ROOT/software/plan --plan_index 0 --node_file /usr/lib/vcac/server/webapps/ROOT/software/node --source_cloud_provider azure --action plan_batch -S <$SourceVRAServer>
```

Como alternativa, você pode usar este comando para executar um nó de cada vez do arquivo de nó, fornecendo um índice de nó.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer> -t <$tenant> -tu <$TenantUser> --component_windows Software.WindowsAgentUpdate74 --component_linux Software.LinuxAgentUpdate74 --plan_file /usr/lib/vcac/server/webapps/ROOT/software/plan --plan_index 0 --node_file /usr/lib/vcac/server/webapps/ROOT/software/node --source_cloud_provider azure --action execute_node -S <$SourceVRAServer> --node_index <0 through n-1>
```

Ao realizar esse procedimento, é possível seguir os logs do appliance virtual do vRealize Automation e a máquina do host para ver o processo de atualização do Agente do Servidor.

Após a atualização, o processo de atualização importa um script de atualização de software para Windows ou Linux para o appliance virtual do vRealize Automation 7.4. Você pode fazer login no host do appliance virtual do vRealize Automation para garantir que o componente de software seja importado com êxito. Após a importação do componente, uma atualização de software é enviada para o antigo Serviço de Agente de Eventos (Event Broker Service, EBS) a fim de transmitir os scripts de atualização de software para as máquinas virtuais identificadas. Quando a atualização é concluída e os novos Agentes de Software tornam-se operativos, eles se associam ao novo appliance virtual do vRealize Automation, enviando uma solicitação de ping.

Observação Arquivos de log úteis

- Saída Catalina para a origem vRealize Automation: `/var/log/vcac/catalina.out`. Neste arquivo, você vê as solicitações de atualização que estão sendo feitas quando as migrações do agente são efetuadas. Essa atividade é igual à execução de uma solicitação de provisionamento de software.
- Saída Catalina para o destino vRealize Automation: `/var/log/vcac/catalina.out`. Neste arquivo, você vê as máquinas virtuais migradas, relatando suas solicitações ping aqui para incluir os números da versão 7.4.0-SNAPSHOT. Você pode reunir esses conjuntos comparando os nomes dos tópicos EBS, por exemplo, `sw-agent-UUID`.
- Pasta de atualização do agente no arquivo de log de atualização mestre da máquina vRealize Automation de destino: `/var/log/vmware/vcac/agentupdate/updateSoftwareAgents.log`. É possível seguir este arquivo para ver qual operação de atualização está em andamento.
- Registros individuais disponíveis nas pastas de localitório: `/var/log/vcac/agentupdate/{tenant}/{subtenant-UUID}`. Os nós individuais estão listados aqui como arquivos com falhas e extensões em andamento.

- Máquinas Virtuais (VMs) migradas: /opt/vmware-appdirector/agent/logs/darwin*.log. Você pode verificar essa localização que deve listar as solicitações de atualização de software recebidas, bem como a reinicialização eventual do agent_bootstrap + agente de software.

Definir o modo de replicação do PostgreSQL vRealize Automation como síncrono

Se você definir o modo de replicação do PostgreSQL como assíncrono antes da atualização, poderá definir o modo de replicação do PostgreSQL como síncrono depois de atualizar um ambiente distribuído do vRealize Automation.

Pré-requisitos

- Você atualizou um ambiente distribuído do vRealize Automation.
- Você está conectado como **raiz** ao Gerenciamento de appliance do vRealize Automation apropriado em <https://vra-va-hostname.domain.name:5480>.

Procedimentos

- 1 Clique em **Configurações vRA > Banco de dados**.
- 2 Clique em **Modo de Sincronização** e espere a conclusão da ação.
- 3 Verifique se todos os nós na coluna Estado de Sincronização exibem o status Síncrono.

Próximo passo

[Executar a Conexão de Teste e verificar endpoints atualizados.](#)

Executar a Conexão de Teste e verificar endpoints atualizados

Atualizar do vRealize Automation 7.3 ou anterior para o 7.4 faz alterações nos endpoints no ambiente de destino.

Depois de atualizar para o vRealize Automation 7.4, você deve usar a ação **Testar Conexão** para todos os endpoints aplicáveis. Você pode precisar também de fazer ajustes a alguns endpoints atualizados. Para mais informações, consulte [Considerações ao trabalhar com endpoints atualizados ou migrados](#).

A configuração de segurança padrão para endpoints atualizados ou migrados é não aceitar certificados não confiáveis.

Após a atualização ou migração de uma instalação anterior do vRealize Automation, se você estiver usando certificados não confiáveis, execute as seguintes etapas para todos os endpoints vSphere e NSX para ativar a validação do certificado. Caso contrário, as operações de endpoint falharão com erros de certificado. Para obter mais informações, consulte os artigos da Base de conhecimento da VMware *A comunicação do endpoint está interrompida após a atualização para o vRA 7.3 (2150230)* em <http://kb.vmware.com/kb/2150230> e *Como baixar e instalar os certificados raiz do vCenter Server para evitar avisos de certificado do navegador da Web (2108294)* em <http://kb.vmware.com/kb/2108294>.

- 1 Após a atualização ou migração, faça login na máquina do agente do vRealize Automation vSphere e reinicie seus agentes do vSphere usando a guia **Serviços**.

A migração pode não reiniciar todos os agentes. Portanto, reinicialize-os manualmente, se necessário.

2 Aguarde a conclusão de pelo menos um relatório ping. O relatório leva de um a dois minutos para ser concluído.

3 Quando os agentes do vSphere terminarem a coleta de dados, faça login no vRealize Automation como administrador de IaaS.

4 Clique em **Infraestrutura > Endpoints > Endpoints**.

5 Edite um endpoint do vSphere e clique em **Testar Conexão**.

6 Se aparecer um prompt de certificado, clique em **OK** para aceitar o certificado.

Se não aparecer um prompt de certificado, o certificado pode estar armazenado corretamente no momento em uma autoridade raiz confiável do serviço de hospedagem de máquina do Windows para o endpoint, por exemplo como uma máquina de agente de proxy ou máquina do DEM.

7 Clique em **OK** para aplicar a aceitação do certificado e salvar o endpoint.

8 Repita este procedimento para cada endpoint do vSphere.

9 Repita este procedimento para cada endpoint do NSX.

Se a ação **Testar Conexão** for bem-sucedida, mas algumas operações de coleta ou provisionamento de dados falharem, você pode instalar o mesmo certificado em todas as máquinas do agente que sirvam o endpoint e em todas as máquinas do DEM. Como alternativa, você pode desinstalar o certificado das máquinas existentes e repetir o procedimento anterior para o endpoint com falha.

Executar a coleta de dados do Inventário de Segurança e Rede do NSX depois de atualizar o vRealize Automation

Após atualizar o vRealize Automation 7.1, 7.2 ou 7.3.x para 7.4, você deve executar a coleta de dados do Inventário de Segurança e Rede do NSX no ambiente do vRealize Automation 7.4.

Essa coleta de dados é necessária para que a ação de reconfiguração do balanceador de carga funcione no vRealize Automation 7.4 para implantações das versões 7.1, 7.2 ou 7.3.x.

Pré-requisitos

- [Executar a coleta de dados do Inventário de Segurança e Rede do NSX antes da atualização do vRealize Automation.](#)
- Atualização bem-sucedida para o vRealize Automation 7.4.

Procedimentos

- ◆ Execute a coleta de dados de Inventário de Segurança e Rede do NSX no vRealize Automation 7.4 após a atualização. Consulte [Iniciar a coleta de dados do endpoint manualmente](#).

Ingressar appliance de réplica no cluster

Após concluir a atualização do appliance mestre do vRealize Automation, cada nó de réplica atualizado será ingressado automaticamente no nó mestre. Caso um nó de réplica tenha que ser atualizado separadamente, use estas etapas para ingressar manualmente o nó de réplica no cluster.

Acesse o console de gerenciamento do appliance do nó de réplica que não está ingressado no cluster e realize as etapas a seguir.

Procedimentos

- 1 Selecione **Configurações do vRA > Cluster**.
- 2 Clique em **Unir cluster**.

Configuração de porta para implantações de alta disponibilidade

Depois de terminar um upgrade em uma implantação de alta disponibilidade, você deve configurar o balanceador de carga para passar o tráfego na porta 8444 para o appliance do vRealize Automation, a fim de oferecer suporte a recursos de console remoto.

Para obter mais informações, consulte o *Guia de Configuração de Balanceamento de Carga do vRealize Automation* na [Documentação do vRealize Automation](#).

Reconfigurar o vRealize Orchestrator integrado para dar suporte à alta disponibilidade

Para uma implantação de alta disponibilidade, você deve reassociar manualmente cada appliance vRealize Automation de réplica de destino ao cluster para ativar o suporte à alta disponibilidade para o vRealize Orchestrator incorporado.

Pré-requisitos

Faça login no console de gerenciamento do appliance vRealize Automation de réplica de destino.

- 1 Inicie um navegador e abra o console de gerenciamento do vRealize Automation de réplica de destino usando o nome de domínio totalmente qualificado (FQDN) do appliance virtual de réplica de destino: `//vra-va-hostname.domain.name:5480`.
- 2 Faça login com o nome de usuário **root** e a senha que você inseriu quando implantou o appliance vRealize Automation de réplica de destino.

Procedimentos

- 1 Selecione **Configurações do vRA > Cluster**.
- 2 Na caixa de texto **Nó de Cluster Principal**, insira o FQDN do appliance vRealize Automation mestre de destino.
- 3 Insira a senha root na caixa de texto **Senha**.
- 4 Clique em **Unir cluster**.
Ignore todos os avisos de certificado para continuar. O sistema reinicia serviços para o cluster.
- 5 Verifique se os serviços estão em execução.
 - a Na barra de guias superior, clique em **Serviços**.
 - b Clique em **Atualizar** para monitorar o progresso da inicialização dos serviços.

Restaurar arquivos de limite de fluxo de trabalho externo.

Você deve reconfigurar os arquivos de tempo limite de fluxo de trabalho externo do vRealize Automation, pois o processo de atualização substituiu os arquivos xmldb.

Procedimentos

- 1 Abra os arquivos de configuração de fluxo de trabalho externo (xmldb) no sistema do diretório a seguir.

`\VMware\VCAC\Server\ExternalWorkflows\xmldb\.`

- 2 Substitua os arquivos xmldb pelos arquivos que você fez backup antes da migração. Caso não tenha os arquivos de backup, redefina as configurações de tempo limite de fluxo de trabalho externo.
- 3 Salve as configurações.

Ativando a ação Conectar-se ao console remoto para consumidores

A ação do console remoto para consumidores tem suporte para appliances provisionados pelo vSphere no vRealize Automation.

Edite o blueprint depois de atualizar a versão e selecione a ação **Conectar-se ao console remoto** na guia **Ação**.

Para obter mais informações, consulte o [artigo 2109706 da base de dados de conhecimento](#).

Restaurar alterações de registro no arquivo app.config

O processo de atualização substitui as alterações feitas no processo de registro nos arquivos de configuração. Depois de concluir uma atualização, você deve restaurar todas as alterações feitas ao arquivo `app.config` antes da atualização.

Ativar o Failover automático do Manager Service após a atualização

O failover automático do Manager Service está desativado por padrão com a atualização do vRealize Automation.

Conclua essas etapas para ativar o failover automático do Manager Service após a atualização.

Procedimentos

- 1 Abra um prompt de comando como root no appliance vRealize Automation.
- 2 Mude para o diretório `/usr/lib/vcac/tools/vami/commands`.
- 3 Para ativar o failover automático do Manager Service, execute o seguinte comando.

```
python ./manager-service-automatic-failover ENABLE
```

Para desativar o failover automático em toda uma implantação do IaaS, execute o seguinte comando.

```
python ./manager-service-automatic-failover DISABLE
```

Sobre o failover automático do Serviço de Gerenciador

Você pode configurar o Serviço de Gerenciador do IaaS para realizar um failover de um backup vRealize Automation automaticamente se o Serviço de Gerenciador primário parar.

A partir do vRealize Automation 7.3, não será mais necessário iniciar ou interromper manualmente o Serviço de Gerenciador em cada servidor Windows para controlar qual servirá como primário ou backup. O failover automático do Manager Service está desativado por padrão quando você atualiza o IaaS com o Script de shell de upgrade ou usa o arquivo executável do instalador do Installer.

Quando o failover automático está ativado, o Serviço de Gerenciador é iniciado automaticamente em todos os hosts do Serviço de Gerenciador, incluindo backups. O recurso de failover automático permite aos hosts monitorar uns aos outros de maneira transparente e realizar o failover quando necessário, mas o serviço Windows deve estar sendo executado em todos os hosts.

Observação Não é obrigatório utilizar o failover automático. É possível desativá-lo e continuar a iniciar e parar manualmente o serviço Windows para controlar qual host servirá como primário ou backup. Se você optar pela abordagem de failover, será necessário iniciar o serviço em um host por vez. Com o failover automático desativado, executar o serviço simultaneamente em vários servidores IaaS torna o vRealize Automation inutilizável.

Não tente ativar ou desativar seletivamente o failover automático. O failover automático deve estar sempre sincronizado como ligado ou desligado, em todos os hosts do Serviço de Gerenciador em uma implantação do IaaS.

Solucionando problemas de atualização do vRealize Automation

Os tópicos de solução de problemas de atualização fornecem soluções para problemas que você pode enfrentar ao atualizar o vRealize Automation 7.1, 7.2 ou 7.3.x para 7.4.

O failover automático do Manager Service não é ativado

Sugestões para a solução de problema com o comando `manager-service-automatic-failover`.

Solução

- O comando `manager-service-automatic-failover` falha ou exibe esta mensagem por mais de dois minutos: Ativando o modo de failover automático do Service Manager no nó: `IAAS_MANAGER_SERVICE_NODEID`.
 - a Faça login no gerenciamento do appliance do vRealize Automation em `https://va-hostname.domain.name:5480` com o nome de usuário **host** e a senha que você inseriu quando implantou o appliance.
 - b Selecione **Configurações do vRA > Cluster**.
 - c Verifique se o serviço Management Agent está em execução em todos os hosts do Manager Service.
 - d Verifique se o horário da última conexão para todos os nós do IaaS Manager Service é inferior a 30 segundos.

Se você se deparar com problemas de conectividade do Management Agent, resolva-os manualmente e repita o comando para ativar o failover automático do Manager Service.

- O comando `manager-service-automatic-failover` falha ao ativar o failover em um nó do Manager Service. É seguro executar novamente o comando para corrigir isso.

- Alguns hosts do Manager Service na implantação IaaS tem o failover ativado, enquanto outros não. Todos os hosts do Manager Service na implantação IaaS devem ter o recurso ativado, ou ele não funcionará. Para corrigir esse problema, execute um destes procedimentos:
 - Desative o failover em todos os nós do Manager Service e use a abordagem de failover manual. Somente execute o failover em um host de cada vez.
 - Se várias tentativas falharem ao ativar o recurso em um nó do Manager Service, pare o Serviço VMware vCloud Automation Center do Windows nesse nó e defina o tipo de inicialização do nó como Manual até resolver o problema.
- Use o Python para validar que o failover está ativado em cada nó do Manager Service.
 - a Faça login no nós do appliance do vRealize Automation mestre como **raiz** usando o SSH.
 - b Execute o `python /usr/lib/vcac/tools/vami/commands/manager-service-automatic-failover ENABLE`.
 - c Verifique se o sistema retorna esta mensagem: Ativando modo de failover automático do Manager Service no nó: `IAAS_MANAGER_SERVICE_NODEID` concluído.
- Verifique se o failover está ativado em cada nó do Manager Service, inspecionando o arquivo de configuração do Manager Service.
 - a Abra um prompt de comando em um nó do Manager Service.
 - b Navegue até a pasta de instalação do vRealize Automation e abra o arquivo de configuração do Manager Service em `VMware\VCAC\Server\ManagerService.exe.config`.
 - c Verifique se os seguintes elementos estão presentes na seção `<appSettings>`.
 - `<add key="FailoverModeEnabled" value="True" />`
 - `<add key="FailoverPingIntervalMilliseconds" value="30000" />`
 - `<add key="FailoverNodeState" value="active" />`
 - `<add key="FailoverMaxFailedDatabasePingAttempts" value="5" />`
 - `<add key="FailoverMaxFailedRepositoryPingAttempts" value="5" />`
- Verifique se o status do serviço VMware vCloud Automation Center do Windows é Iniciado e se o tipo de inicialização é Automático.
- Use o Python para validar que o failover está desativado em cada nó do Manager Service.
 - a Faça login no nós do appliance do vRealize Automation mestre como **raiz** usando o SSH.
 - b Execute o `python /usr/lib/vcac/tools/vami/commands/manager-service-automatic-failover DISABLE`.
 - c Verifique se o sistema retorna esta mensagem: Desativando modo de failover automático do Manager Service no nó: `IAAS_MANAGER_SERVICE_NODEID` concluído.

- Verifique se o failover está desativado em cada nó do Manager Service, inspecionando o arquivo de configuração do Manager Service.
 - a Abra um prompt de comando em um nó do Manager Service.
 - b Navegue até a pasta de instalação do vRealize Automation e abra o arquivo de configuração do Manager Service em `VMware\vCAC\Server\ManagerService.exe.config`.
 - c Verifique se o seguinte elemento está presente na seção `<appSettings>`.
 - `<add key="FailoverModeEnabled" value="False" />`
- Para criar um nó de espera passiva do Manager Service, defina o status do Serviço VMware vCloud Automation Center do Windows desse nó como Parado e o seu tipo de inicialização como Manual.
- Para um nó ativo do Manager Service, o status do Serviço VMware vCloud Automation Center do Windows deve ser Iniciado e seu tipo de inicialização deve ser Automático.
- O comando `manager-service-automatic-failover` usa o ID interno do nó do Manager Service - `IAAS_MANAGER_SERVICE_NODEID`. Para localizar o nome de host correspondente a esse ID interno, execute o comando `vra-command list-nodes` e procure o host do Manager Service com o ID de Nó: `IAAS_MANAGER_SERVICE_NODEID`.
- Para localizar o Manager Service que o sistema escolheu automaticamente para ser o serviço ativo no momento, realize estas etapas.
 - a Faça login no nós do appliance do vRealize Automation mestre como **raiz** usando o SSH.
 - b Execute o `vra-command list-nodes --components`.
 - Se o failover estiver ativado, localize o nó do Manager Service com Estado: Ativo.
 - Se o failover estiver desativado, localize o nó do Manager Service com Estado: Iniciado.

A instalação ou a atualização falha com um erro de tempo limite do balanceador de carga

Uma instalação ou atualização do vRealize Automation para um ambiente distribuído com um balanceador de carga falha com um erro 503, serviço indisponível.

Problema

A instalação ou atualização falha porque a configuração de tempo limite balanceador de carga não permite tempo suficiente para que a tarefa seja concluída.

Causa

Uma configuração insuficiente de tempo limite do balanceador de carga pode causar falhas. Você pode corrigir o problema aumentando a configuração de tempo limite do balanceador de carga para 100 segundos ou mais e executando novamente a tarefa.

Solução

- 1 Aumente o valor do tempo limite do balanceador de carga para pelo menos 100 segundos.
- 2 Execute novamente a instalação ou atualização.

Falha na atualização para o componente do site do IaaS

A atualização do IaaS falha e você não pode continuá-la.

Problema

A atualização do IaaS falha para o componente do site. As seguintes mensagens de erro aparecem no arquivo de log do instalador.

- System.Data.Services.Client.DataServiceQueryException:
An error occurred while processing this request. --->
System.Data.Services.Client.DataServiceClientException: <!DOCTYPE html>
- Description: An application error
occurred on the server. The current custom error settings for this application
prevent the details of the application error from being viewed remotely (for
security reasons). It could, however, be viewed by browsers running on the
local server machine.
- Warning: Non-zero return code. Command failed.
- Done Building Project "C:\Program Files
(x86)\VMware\VMware\Server\Model Manager Data\DeployRepository.xml"
(InstallRepoModel target(s)) -- FAILED.

As seguintes mensagens de erro aparecem no arquivo de log do repositório.

- [Error]: [sub-thread-Id="20"
context="" token=""] Failed to start repository service. Reason:
System.InvalidOperationException: Configuration section encryptionKey is not
protected
at
DynamicOps.Common.Utils.EncryptionHelpers.ReadKeyFromConfiguration(Configuration
config)
at DynamicOps.Common.Utils.EncryptionHelpers.Decrypt(String value)
at DynamicOps.Repository.Runtime.CoreModel.GlobalPropertyItem.Decrypt(Func`2
decryptFunc)
at
DynamicOps.Common.Entity.ContextHelpers.OnObjectMaterializedCallbackEncryptable(Object
sender, ObjectMaterializedEventArgs e)
at

```
System.Data.Common.Internal.Materialization.Shaper.RaiseMaterializedEvents()  
at  
System.Data.Common.Internal.Materialization.Shaper`1.SimpleEnumerator.MoveNext()  
at System.Linq.Enumerable.FirstOrDefault[TSource](IEnumerable`1 source)  
at System.Linq.Queryable.FirstOrDefault[TSource](IQueryable`1 source)  
at  
DynamicOps.Repository.Runtime.Common.GlobalPropertyHelper.GetGlobalPropertyItemValue(Core  
ModelEntities  
coreModelContext, String propertyName, Boolean throwIfPropertyNotFound)  
at  
DynamicOps.Repository.Runtime.CafeClientAbstractFactory.LoadSolutionUserCertificate()  
at  
DynamicOps.Repository.Runtime.CafeClientAbstractFactory.InitializeFromDb(String  
coreModelConnectionString)  
at DynamicOps.Repository.Runtime.Common.RepositoryRuntime.Initialize().
```

Causa

A atualização do IaaS falha quando a data de criação do arquivo `web.config` é igual ou posterior à data de modificação.

Solução

- 1 No host do IaaS, faça login no Windows.
- 2 Abra o prompt de comando do Windows.
- 3 Mude de diretório para a pasta de instalação do vRealize Automation.
- 4 Inicie seu editor de texto preferencial com a opção **Executar como administrador**.
- 5 Localize e selecione o arquivo `web.config` e salve-o para alterar a data de modificação do arquivo.
- 6 Examine as propriedades do arquivo `web.config` para confirmar se a data de modificação do arquivo é posterior à data de criação.
- 7 Atualizar IaaS.

Falha de execução do Manager Service devido a erros de validação de SSL durante o tempo de execução

Ocorre uma falha na execução do Manager Service devido a erros de validação de SSL.

Problema

Ocorre falha do Manager Service com a seguinte mensagem de erro no log:

```
[Info]: Thread-Id="6" - context="" token="" Failed to connect to the core database, will retry in 00:00:05, error details: A connection was successfully established with the server, but then an error occurred during the login process. (provider: SSL Provider, error: 0 - The certificate chain was issued by an authority that is not trusted.)
```

Causa

Durante o tempo de execução, ocorre uma falha na execução do Manager Service devido a erros de validação de SSL.

Solução

- 1 Abra o arquivo de configuração `ManagerService.config`.
- 2 Atualize **Encrypt=False** na seguinte linha:

```
<add name="vcac-repository" providerName="System.Data.SqlClient"
connectionString="Data Source=ias-db.sqa.local;Initial Catalog=vcac;Integrated
Security=True;Pooling=True;Max Pool
Size=200;MultipleActiveResultSets=True;Connect Timeout=200, Encrypt=True" />
```

Falha de login após a atualização

Você deve sair do navegador e repetir o login após uma atualização para sessões que usam contas de usuário não sincronizadas.

Problema

Após a atualização do vRealize Automation, o sistema bloqueia o acesso a contas de usuário não sincronizadas no login.

Solução

Saia do navegador e reinicie o vRealize Automation.

Excluir nós órfãos no vRealize Automation

Um nó órfão é um nó duplicado que está relatado no host, mas que não existe no host.

Problema

Ao verificar que todos os nós IaaS e do appliance virtual estão em estado íntegro, você pode descobrir que um host tem um ou mais nós órfãos. Você deve excluir todos eles.

Solução

- 1 No appliance do vRealize Automation primário, faça login no Gerenciamento do Appliance do vRealize Automation como **root** usando a senha que você inseriu quando implantou o appliance do vRealize Automation.
- 2 Selecione **Configurações do vRA > Cluster**.
- 3 Para cada nó órfão na tabela, clique em **Excluir**.

O comando Unir Cluster parece falhar após a atualização de um ambiente de alta disponibilidade

Depois de clicar em **Unir Cluster** no console de gerenciamento em um nó de cluster secundário, o indicador de progresso desaparece.

Problema

Quando você usa o console de gerenciamento do appliance do vRealize Automation após a atualização para unir um nó de cluster secundário ao nó primário, o indicador de progresso desaparece e nenhuma mensagem de erro ou êxito é exibida. Esse comportamento é um problema intermitente.

Causa

O indicador de progresso desaparece porque alguns navegadores param de aguardar uma resposta do servidor. Esse comportamento não interrompe o processo de união ao cluster. Você pode confirmar se o processo de união ao cluster foi bem-sucedido visualizando o arquivo de registro em `/var/log/vmware/vcac/vcac-config.log`.

A Mesclagem do Banco de Dados PostgreSQL Não é Bem-Sucedida

A mesclagem do banco de dados PostgreSQL externo com o banco de dados PostgreSQL incorporado não é bem-sucedida.

Problema

Se a mesclagem de atualização do banco de dados PostgreSQL não for bem-sucedida, você poderá realizar uma mesclagem manual.

Solução

- 1 Reverta o appliance virtual do vRealize Automation para o snapshot criado antes da atualização.
- 2 Faça login no appliance virtual do vRealize Automation e execute esse comando para permitir a conclusão da atualização se a mesclagem do banco de dados não for bem-sucedida.

```
touch /tmp/allow-external-db
```

O comando não desativa a mesclagem automática.

- 3 No host do banco de dados PostgreSQL remoto, conecte-se ao banco de dados PostgreSQL usando a ferramenta `psql` e execute estes comandos.

```
CREATE EXTENSION IF NOT EXISTS "hstore";
```

```
CREATE EXTENSION IF NOT EXISTS "uuid-osspl";
```

```
CREATE SCHEMA saas AUTHORIZATION vcac;
```

O usuário neste comando é vcac. Se o vRealize Automation se conectar ao banco de dados externo com um usuário diferente, substitua vcac neste comando pelo nome do usuário.

```
CREATE EXTENSION IF NOT EXISTS "citext" SCHEMA saas;
```

4 Execute a atualização.

Se a atualização for bem-sucedida, o sistema funcionará conforme esperado com o banco de dados PostgreSQL externo. Certifique-se de que o banco de dados PostgreSQL externo esteja sendo executado corretamente.

5 Faça login no appliance virtual do vRealize Automation e execute estes comandos

```
/etc/bootstrap/postupdate.d/00-20-db-merge-external
```

```
/etc/bootstrap/postupdate.d/11-db-merge-external
```

O appliance de réplica do vRealize Automation falha ao atualizar

O appliance de réplica do vRealize Automation falha ao atualizar durante a atualização do appliance mestre.

Causa

A atualização de um appliance de réplica pode falhar devido a problemas de conectividade ou outros erros. Quando isso acontecer, você verá uma mensagem de aviso na guia Atualizar do appliance mestre do vRealize Automation, destacando a réplica que falhou ao atualizar.

Solução

- 1 Reverta o snapshot do appliance virtual de réplica ou faça backup para o estado pré-atualização e ligue-o.
- 2 Faça login como raiz na interface de gerenciamento do appliance do vRealize Automation de réplica.
<https://vrealize-automation-appliance-FQDN:5480>
- 3 Clique em **Atualizar > Configurações**.
- 4 Selecione para baixar as atualizações de um repositório VMware ou de um CDROM na seção Repositório de Atualizações.
- 5 Clique em **Status**.
- 6 Clique em **Verificar atualizações** para verificar se uma atualização pode ser acessada.
- 7 Clique em **Instalar Atualizações**.
- 8 Clique em **OK**.
É exibida uma mensagem informando que a atualização está em andamento.
- 9 Abra os arquivos de log para confirmar que o upgrade está progredindo com sucesso.
 - `/opt/vmware/var/log/vami/vami.log`

- `/var/log/vmware/horizon/horizon.log`

Se você fizer logoff durante o processo de atualização e voltar a fazer login antes do término da atualização, poderá continuar acompanhando o progresso da atualização no arquivo de registro. O arquivo `updatecli.log` pode exibir informações sobre a versão do vRealize Automation da qual você está atualizando. Essa versão exibida mudará para a versão adequada mais tarde no processo de atualização.

O tempo necessário para a atualização terminar varia de acordo com o seu ambiente.

10 Quando a atualização for finalizada, reinicie o appliance virtual.

- a Clique em **Sistema**.
- b Clique em **Reiniciar** e confirme a seleção.

11 Selecione **Configurações do vRA > Cluster**.

12 Insira o FQDN da instância mestre do appliance do vRealize Automation e clique em **Ingressar no Cluster**.

Cópias de backup de arquivos .xml fazem com que o sistema atinja o tempo limite

O vRealize Automation registra qualquer arquivo com uma extensão `.xml` no diretório `\VMware\VMware\Server\ExternalWorkflows\xml\`. Se esse diretório contiver arquivos de backup com extensão `.xml`, o sistema executará fluxos de trabalho duplicados que farão com que ele atinja o tempo limite.

Solução

Solução alternativa: quando você fizer o backup de arquivos nesse diretório, mova os backups para outro diretório ou altere a extensão do nome do arquivo de backup para algo diferente de `.xml`.

Excluir a atualização do IaaS

Você pode atualizar o appliance do vRealize Automation sem atualizar os componentes do IaaS.

Use esse procedimento quando quiser atualizar o appliance vRealize Automation sem atualizar os componentes IaaS. Esse procedimento

- Não para os serviços do IaaS.
- Ignora a atualização dos Agentes de Gerenciamento.
- Impede a atualização automática dos componentes do IaaS após as atualizações do appliance do vRealize Automation.

Procedimentos

- 1 Abra uma conexão de shell seguro para o nó do appliance primário do vRealize Automation.
- 2 No prompt de comando, execute este comando para criar o arquivo de toggle:

```
touch /tmp/disable-iaas-upgrade
```

- 3 Pare manualmente os serviços do IaaS.
 - a Faça login no seu servidor Windows do IaaS.
 - b Selecione **Iniciar > Ferramentas administrativas > Serviços**.
 - c Para os serviços na seguinte ordem.

Observação Não encerre o servidor Windows do IaaS.

- 1 Cada Agente de Proxy do VMware vRealize Automation.
 - 2 Cada trabalhador do VMware DEM.
 - 3 O orchestrator do VMware DEM.
 - 4 O serviço do VMware vCloud Automation Center.
- 4 Acesse o console de gerenciamento do appliance primário do vRealize Automation e atualize o appliance primário do vRealize Automation.

Não foi possível criar um novo diretório em vRealize Automation

Tentando adicionar um novo diretório com a falha do conector de sincronização.

Problema

Este problema ocorre em função de um arquivo `config-state.json` localizado em `usr/local/horizon/conf/states/VSPHERE.LOCAL/3001/`.

Para obter informações sobre como reparar esse erro, consulte o [Artigo 2145438 da Base de Conhecimento](#).

Expiração da atualização do appliance virtual de réplica do vRealize Automation

A atualização do appliance virtual de réplica do vRealize Automation expira quando você atualiza o appliance virtual mestre.

Problema

Quando você atualiza o appliance virtual mestre, a guia de atualização do console de gerenciamento mestre do vRealize Automation mostra um appliance virtual de réplica destacado que atingiu o limite do tempo limite da atualização.

Causa

A atualização expira devido a um problema de desempenho ou de infraestrutura.

Solução

- 1 Verifique o progresso da atualização de réplica do appliance virtual.
 - a Vá para o console de gerenciamento do appliance virtual de réplica usando o nome de domínio totalmente qualificado (FQDN), `https://va-hostname.domain.name:5480`.
 - b Faça login usando o nome de usuário **raiz** e a senha que você inseriu quando o appliance foi implantado.
 - c Selecione **Atualizar > Status** e verifique o progresso da atualização.
Faça um dos seguintes:
 - Se a atualização falhar, siga as etapas no tópico de solução de problemas [O appliance de réplica do vRealize Automation falha ao atualizar](#).
 - Se a atualização de appliance virtual de réplica estiver em andamento, aguarde até que a atualização seja concluída e prossiga para a etapa 2.
- 2 Reinicie o appliance virtual.
 - a Clique em **Sistema**.
 - b Clique em **Reiniciar** e confirme a seleção.
- 3 Selecione **Configurações do vRA > Cluster**.
- 4 Insira o FQDN da instância mestre do appliance virtual do vRealize Automation e clique em **Ingressar no Cluster**.

Algumas máquinas virtuais não possuem uma implantação criada durante a atualização

As máquinas virtuais que se encontram no estado ausente no momento da atualização não possuem uma implantação correspondente criada no ambiente de destino.

Problema

Se uma máquina virtual estiver no estado ausente no ambiente de origem durante a migração, não será criada uma atualização correspondente no ambiente de destino. Se uma máquina virtual sair do estado ausente após a atualização, você poderá importar a máquina para a implantação de destino com a importação em massa.

Erro de certificado não confiável

Ao visualizar a página Visualizador de Registros da infraestrutura no console do Appliance do vRealize Automation, você pode ver um relatório de falha de conexão com o endpoint contendo as seguintes palavras: `Certificate is not trusted`.

Problema

No console Appliance do vRealize Automation, selecione **Infraestrutura > Monitoramento > Registro**. Na página Visualizador de Registros, você pode ver um relatório semelhante a este:

Falha ao se conectar ao endpoint. Para verificar se uma conexão segura pode ser estabelecida com esse endpoint, acesse o endpoint do vSphere na página Endpoints e clique no botão Testar Conexão.

Exceção interna: o certificado não é confiável (RemoteCertificateChainErrors). Assunto: C=US, CN=vc6.mycompany.com Impressão digital: DC5A8816231698F4C9013C42692B0AF93D7E35F1

Causa

Atualizar do vRealize Automation 7.3 ou anterior para o 7.4 faz alterações nos endpoints do seu ambiente original. Para ambientes recentemente atualizados para o vRealize Automation 7.4, o administrador do IaaS deve rever cada endpoint existente que utiliza uma conexão https segura. Se um endpoint tiver um erro `Certificate is not trusted`, ele não funcionará corretamente.

Solução

- 1 Faça login no console do vRealize Automation como administrador de infraestrutura.
- 2 Selecione **Infraestrutura > Pontos de extremidade > Pontos de extremidade**.
- 3 Conclua essas etapas para cada endpoint com uma conexão segura.
 - a Clique em **Editar**.
 - b Clique em **Testar Conexão**.
 - c Reveja os detalhes do certificado e clique em **OK** se confiar nesse certificado.
 - d Reinicie os serviços Windows para todos os Agentes Proxy IaaS usados por esse endpoint.
- 4 Verifique se erros `Certificate is not trusted` deixaram de aparecer na página Visualizador de Registros da infraestrutura.

Falha na instalação ou no upgrade para vRealize Automation

A instalação ou a atualização do vRealize Automation apresenta uma falha e uma mensagem de erro aparece no arquivo de log.

Problema

Quando você instala ou atualiza o vRealize Automation, o procedimento falha. Normalmente, isso ocorre quando uma correção aplicada durante a instalação ou a atualização não é bem-sucedida. Uma mensagem de erro, parecida com a seguinte, aparece no arquivo de registro: `Security error. Applying automatic fix for FIREWALL prerequisite failed. RPM Status 1: Pre install script failed, package test and installation skipped.`

Causa

O ambiente Windows tem uma política de grupo para a execução de script PowerShell definida como ativado.

Solução

- 1 Na máquina host do Windows, execute o `gpedit.msc` para abrir o Editor de Política de Grupo Local.
- 2 No painel esquerdo em **Configuração do Computador**, clique o botão de expansão para abrir os **Modelos Administrativos > Componentes do Windows > PowerShell do Windows**.

3 Para **Ligar Execução de Script**, altere o estado de Enabled para Not Configured.

Não é possível atualizar os componentes DEM e DEO

Não é possível atualizar os componentes DEM e DEO durante a atualização do vRealize Automation 7.2 para 7.3.x

Problema

Após a atualização do vRealize Automation 7.2 para 7.3.x, os componentes DEM e DEO instalados no caminho personalizado, como a unidade D:, não serão atualizados.

Consulte o [artigo 2150517 da Base de Conhecimento](#).

Falha na atualização do Agente de Gerenciamento

Aparece uma mensagem de erro sobre o agente de gerenciamento quando se clica em **Instalar Atualizações** na página Status de Atualização do console de gerenciamento do Appliance do vRealize Automation.

Problema

O processo de atualização não foi bem-sucedido. Mensagem aparece: Não é possível atualizar o agente de gerenciamento no nó x. Às vezes a mensagem lista mais de um nó.

Causa

Muitas circunstâncias podem causar esse problema. A mensagem de erro identifica apenas a ID de nó da máquina afetada. Mais informações podem ser encontradas no arquivo ALL.log do Agente de Gerenciamento na máquina na qual o comando falhou.

Realize estas tarefas nos nós afetados de acordo com a sua situação:

Solução

- Se o serviço do Agente de Gerenciamento não estiver em execução, inicie o serviço e reinicie a atualização no appliance virtual.
- Se o serviço do Agente de Gerenciamento estiver em execução e o Agente de Gerenciamento for atualizado, reinicie a atualização no appliance virtual.
- Se o serviço do Agente de Gerenciamento estiver em execução, mas o Agente de Gerenciamento não estiver atualizado, realize uma atualização manual.
 - a Abra um navegador e navegue até a página de instalação do IaaS vRealize Automation no appliance do vRealize Automation em `https:// va-hostname.domain.name:5480/install`.
 - b Baixe e execute o instalador do agente de gerenciamento.
 - c Reinicialize a máquina do Agente de Gerenciamento.
 - d Reinicie a atualização no appliance virtual.

A atualização do Agente de Gerenciamento não é bem-sucedida

A atualização do Agente de Gerenciamento não é bem-sucedida durante a atualização do vRealize Automation para a versão 7.2. - 7.3.x.

Problema

Se um incidente de failover tiver trocado os hosts primário e secundário do Agente de Gerenciamento, a atualização não será bem-sucedida, pois o processo de atualização automatizado não conseguirá encontrar o host esperado. Realize esse procedimento em cada nó IaaS em que o Agente de gerenciamento não está atualizado.

Solução

- 1 Abra o arquivo All.log na pasta de registros do Agente de Gerenciamento, localizada em C:\Program Files (x86)\VMware\VCAC\Management Agent\Logs\.

A localização da pasta de instalação pode ser diferente da localização padrão.

- 2 Pesquise o arquivo de registro em busca de uma mensagem sobre um appliance virtual desatualizado ou desligado.

Por exemplo, EXCEÇÃO INTERNA: System.Net.WebException: Não é possível conectar-se ao servidor remoto ---> System.Net.Sockets.SocketException: Uma tentativa de conexão falhou porque a parte conectada não respondeu corretamente após um período de tempo, ou a conexão estabelecida falhou porque o host conectado não conseguiu responder *Endereço_IP:5480*

- 3 Edite o arquivo de configuração do Agente de Gerenciamento em C:\Program Files (x86)\VMware\VCAC\Management Agent\VMware.IaaS.Management.Agent.exe.config para substituir o valor existente de alternativeEndpointaddress pela URL do endpoint do appliance virtual primário.

A localização da pasta de instalação pode ser diferente da localização padrão.

Exemplo de alternativeEndpointaddress em VMware.IaaS.Management.Agent.exe.config.

```
<alternativeEndpoint address="https://FQDN:5480/" thumbprint="número da impressão digital" />
```

- 4 Reinicie o serviço do Windows do Agente de Gerenciamento e consulte o arquivo All.log para verificar se ele está funcionando.
- 5 Execute o procedimento de atualização no appliance primário do vRealize Automation.

Falha na atualização do vRealize Automation devido às configurações de tempo limite padrão

Você poderá aumentar a configuração de tempo para atualização se a configuração padrão para a sincronização dos bancos de dados for muito curta para o seu ambiente.

Problema

A configuração de tempo limite para o comando Vcac-Config SynchronizeDatabases não é suficiente para alguns ambientes nos quais a sincronização dos bancos de dados demora mais do que o valor padrão de 3600 segundos.

Os valores de propriedade `cafeTimeoutInSeconds` e `cafeRequestPageSize` no arquivo `Vcac-Config.exe.config` controlam a comunicação entre a API e a ferramenta do utilitário `Vcac-config.exe`. O arquivo está no *local de instalação do IaaS\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe.config*.

Você pode substituir o valor de tempo limite padrão apenas para o comando `SynchronizeDatabases`, fornecendo um valor para esses parâmetros opcionais.

| Parâmetro | Nome abreviado | Descrição |
|-------------------------------------|--------------------|--|
| <code>--DatabaseSyncTimeout</code> | <code>-dstm</code> | Define o valor de tempo limite de solicitação http apenas para <code>SynchronizeDatabases</code> em segundos. |
| <code>--DatabaseSyncPageSize</code> | <code>-dsps</code> | Define o tamanho de página de solicitação de sincronização apenas para a sincronização de Reserva ou Política de Reserva. O padrão é 10. |

Se esses parâmetros não estiverem definidos no arquivo `Vcac-Config.exe.config`, o sistema usará o valor de tempo limite padrão.

Falha na atualização do IaaS em um ambiente de alta disponibilidade

Falha na execução do processo de atualização do IaaS no nó do servidor da Web primário com balanceamento de carga ativado. Você poderá ver essas mensagens de erro:

"System.Net.WebException: A operação expirou" ou "401 - Não autorizado: acesso negado devido a credenciais inválidas".

Problema

Atualizar o IaaS com o balanceamento de carga ativado pode causar uma falha intermitente. Quando isso acontece, você deve executar a atualização do vRealize Automation novamente com o balanceamento de carga desativado.

Solução

- 1 Reverta seu ambiente para os snapshots anteriores à atualização.
- 2 Abra uma conexão de área de trabalho remota para o nó primário do servidor de Web do IaaS.
- 3 Navegue até o arquivo dos hosts do Windows em `c:\windows\system32\drivers\etc`.

- Abra o arquivo dos hosts e adicione esta linha para ignorar o balanceador de carga do servidor da Web.

IP_address_of_primary_iaas_website_node vrealizeautomation_iaas_website_lb_fqdn

Exemplo:

10.10.10.5 vra-iaas-web-lb.domain.com

- Salve o arquivo dos hosts e tente atualizar o vRealize Automation novamente.
- Quando a atualização do vRealize Automation for concluída, abra o arquivo dos hosts e remova a linha que você adicionou na etapa 4.

Solucionar problemas de atualização

Você pode modificar o processo de atualização para solucionar problemas de atualização.

Solução

Quando você tiver problemas de atualização do ambiente do vRealize Automation, use esse procedimento para modificar o processo de atualização selecionando um dos sinalizadores disponíveis.

Procedimentos

- Abra uma conexão de shell seguro para o nó do appliance primário do vRealize Automation.
- No prompt de comando, execute este comando para criar o arquivo de toggle:

touch available_flag

Por exemplo: ***touch /tmp/disable-iaas-upgrade***

Tabela 1-60. Sinalizadores disponíveis

| Sinalizador | Descrição |
|----------------------------------|--|
| <i>/tmp/disable-iaas-upgrade</i> | <ul style="list-style-type: none"> ■ Impede o processo de atualização do IaaS depois do reinício do appliance virtual. ■ Impede a atualização do Agente de Gerenciamento. ■ Impede as verificações e correções de pré-requisito automáticas. ■ Impede a parada dos serviços do IaaS. |
| <i>/tmp/do-not-upgrade-ma</i> | Impede a atualização do Agente de Gerenciamento. Este sinalizador é adequado quando o Agente de Gerenciamento é atualizado manualmente. |
| <i>/tmp/skip-prereq-checks</i> | Impede as verificações e correções de pré-requisito automáticas. Este sinalizador é adequado quando há um problema com as correções de pré-requisito automáticas e as correções foram aplicadas manualmente. |
| <i>/tmp/do-not-stop-services</i> | Impede a parada dos serviços do IaaS. A atualização não interrompe os serviços do IaaS Windows como o Serviço de Gerenciador, DEMs e agentes. |

Tabela 1-60. Sinalizadores disponíveis (Continuação)

| Sinalizador | Descrição |
|-----------------------------|--|
| /tmp/do-not-upgrade-servers | <p>Impede a atualização automática de todos os componentes do IaaS do servidor como o banco de dados, site da web, WAPI, repositório, os dados do Modelo Mfrontanager e o Manager Service.</p> <hr/> <p>Observação Este sinalizador também impede a ativação do modo de failover automático do Manager Service.</p> |
| /tmp/do-not-upgrade-dems | Impede a atualização do DEM. |
| /tmp/do-not-upgrade-agents | Impede a atualização do agente de proxy do IaaS. |

3 Conclua as tarefas para o sinalizador escolhido.

Tabela 1-61. Tarefas adicionais

| Sinalizador | Tarefas |
|---------------------------|--|
| /tmp/disable-iaas-upgrade | <ul style="list-style-type: none"> ■ Atualize o Agente de Gerenciamento manualmente. ■ Aplique quaisquer pré-requisitos do IaaS manualmente. ■ Pare manualmente os serviços do IaaS. <ol style="list-style-type: none"> a Faça login no seu servidor Windows do IaaS. b Selecione Iniciar > Ferramentas administrativas > Serviços. c Para os serviços na seguinte ordem. <hr/> <p>Observação Não encerre o servidor Windows do IaaS.</p> <hr/> <ol style="list-style-type: none"> a Cada Agente de Proxy do VMware vRealize Automation. b Cada trabalhador do VMware DEM. c O orchestrator do VMware DEM. d O serviço do VMware vCloud Automation Center. ■ Inicie a atualização do IaaS manualmente depois que a atualização do appliance virtual estiver concluída. |
| /tmp/do-not-upgrade-ma | Atualize o Agente de Gerenciamento manualmente. |
| /tmp/skip-prereq-checks | Aplique quaisquer pré-requisitos do IaaS manualmente. |

Tabela 1-61. Tarefas adicionais (Continuação)

| Sinalizador | Tarefas |
|-----------------------------|---|
| /tmp/do-not-stop-services | <p>Pare manualmente os serviços do IaaS.</p> <ol style="list-style-type: none"> 1 Faça login no seu servidor Windows do IaaS. 2 Selecione Iniciar > Ferramentas administrativas > Serviços. 3 Para os serviços na seguinte ordem. <p>Observação Não encerre o servidor Windows do IaaS.</p> <ol style="list-style-type: none"> a Cada Agente de Proxy do VMware vRealize Automation. b Cada trabalhador do VMware DEM. c O orchestrator do VMware DEM. d O serviço do VMware vCloud Automation Center. |
| /tmp/do-not-upgrade-servers | |
| /tmp/do-not-upgrade-dems | |
| /tmp/do-not-upgrade-agents | |

- 4 Acesse o console de gerenciamento do appliance primário do vRealize Automation e atualize o appliance primário do vRealize Automation.

Observação Como cada sinalizador permanece ativo até que ele seja removido, execute este comando para remover o sinalizador escolhido após a atualização: `rm /flag_path/flag_name`. Por exemplo, `rm /tmp/disable-iaas-upgrade`.

Atualizando o vRealize Automation 6.2.5 para o 7.4

Ao atualizar seu ambiente do vRealize Automation 6.2.5 para a versão mais recente, você usa os procedimentos específicos ao seu ambiente da versão 6.2.5.

Essas informações são específicas para atualizar o vRealize Automation 6.2.5 para o 7.4. Para obter informações sobre outros caminhos de atualização aceitos, consulte [Atualizando o vRealize Automation](#).

Atualizando o vRealize Automation 6.2.5 para o 7.4

Você pode realizar uma atualização in-loco do seu ambiente atual do vRealize Automation 6.2.5 para o 7.4. Você usa os procedimentos específicos para essa versão para atualizar o ambiente.

Uma atualização in-loco é um processo de três etapas. Você atualiza os componentes no ambiente atual nesta ordem.

- 1 Appliance do vRealize Automation
- 2 Servidor Web do IaaS
- 3 vRealize Orchestrator

Você deve atualizar todos os componentes do produto para a mesma versão.

A vRealize Production Test Upgrade Assist Tool analisa seu ambiente do vRealize Automation 6.2.x em busca de qualquer configuração de recurso que possa causar problemas de atualização e verifica se o seu ambiente está pronto para atualização. Para baixar essa ferramenta e a documentação relacionada, acesse a página de download do produto [VMware vRealize Production Test Tool](#).

Os controles do dicionário de propriedade que não são suportados após a upgrade podem ser restaurados usando o vRealize Orchestrator e os relacionamentos de dicionário de propriedade.

Se você tiver fluxos de trabalho em seu ambiente de origem que contenham um código obsoleto, consulte o [Guia de Migração de Extensibilidade do vRealize Automation](#) para obter informações sobre as mudanças de código necessárias para a conversão de inscrições de agentes de eventos.

A partir do vRealize Automation 7.2, o JFrog Artifactory Pro não é mais fornecido com o Appliance do vRealize Automation. Se você tiver atualizado de versão mais antiga do vRealize Automation, o processo de atualização remove o JFrog Artifactory Pro. Para obter mais informações, consulte o [artigo 2147237 da base de dados de conhecimento](#).

Observação Se você tiver personalizado o ambiente atual do vRealize Automation 6.2.5, entre em contato com a equipe de suporte CCE para obter mais informações sobre a atualização.

Pré-requisitos para atualizar o vRealize Automation

Antes de atualizar o vRealize Automation 6.2.5, revise os seguintes pré-requisitos.

Requisitos de configuração do sistema

Certifique-se de atender aos seguintes requisitos do sistema antes de iniciar uma atualização.

- Verifique se todos os dispositivos e servidores que fazem parte de sua implantação satisfazem os requisitos do sistema para a versão mais recente. Consulte a *Matriz de suporte do vRealize Automation* na [Documentação do VMware vRealize Automation](#).
- Consulte a *Matriz de Interoperabilidade de Produtos VMware* no site do VMware para obter informações sobre a compatibilidade com outros produtos VMware.
- Verifique se o vRealize Automation a partir do qual você está atualizando está em uma condição de trabalho estável. Corrija quaisquer problemas antes de atualizar.
- Se você estiver atualizando do vRealize Automation 6.2.5, registre a chave de licença do vCloud Suite usada para o ambiente atual do vRealize Automation. Durante a atualização, as chaves de licença existentes são removidas do banco de dados.
- Verifique se você alterou as configurações de tempo limite do balanceador de carga do padrão para pelo menos 10 minutos.

Requisitos de configuração de hardware

Verifique se o hardware no seu ambiente é adequado para a versão de destino do vRealize Automation.

Consulte [Especificações de hardware do vRealize Automation e máximos de capacidade](#)

Certifique-se de atender aos seguintes requisitos do sistema antes de iniciar uma atualização.

- Você deve configurar o seu hardware atual antes de baixar a atualização. Consulte [Aumentar os recursos de hardware do vCenter Server para o vRealize Automation 6.2.5](#).
- Você deve ter pelo menos 18 GB de RAM, 4 CPUs, Disco 1 = 50 GB, Disco 3 = 25 GB e Disco 4 = 50 GB antes de executar a atualização.

Se a máquina virtual estiver no vCloud Networking and Security, talvez seja necessário alocar mais espaço em RAM.

Embora o suporte geral para vCloud Networking and Security tenha terminado, as propriedades personalizadas de VCNS continuam válidas para fins de NSX. Consulte o [artigo 2144733 da Base de Conhecimento](#).

- Estes nós devem ter pelo menos 5 GB de espaço livre em disco:
 - Sites do IaaS primário
 - Banco de dados Microsoft SQL
 - Model Manager
- O nó de Site do IaaS primário no qual os dados do Model Manager estão instalados deve ter o JAVA SE Runtime Environment 8, 64 bits, atualização 161 ou posterior, instalado. Depois de instalar o Java, você deve definir a variável do ambiente JAVA_HOME como a nova versão.
- Para baixar e executar a atualização, você deve ter os seguintes recursos:
 - Pelo menos 5 GB na partição raiz
 - 5 GB na partição /storage/db para o mestre Appliance do vRealize Automation
 - 5 GB na partição raiz para cada appliance virtual de réplica
- Verifique a subpasta /storage/log e remova arquivos ZIP arquivados mais antigos para liberar espaço.

Pré-requisitos gerais

Certifique-se de atender aos seguintes requisitos do sistema antes de iniciar uma atualização.

- Você tem acesso a uma conta do Active Directory com formato nomedeusuario@dominio e permissões de associação ao diretório.
- Você atende às seguintes condições:
 - Você tem acesso a uma conta com formato SAMAccountName.
 - Você tem privilégios suficientes para associar o sistema ao domínio por meio da criação de um objeto de computador dinamicamente ou para mesclagem em um objeto pré-criado.
- Você tem acesso a todos os bancos de dados e todos os balanceadores de carga são impactados ou participam da atualização do vRealize Automation.
- Você torna o sistema indisponível para os usuários enquanto realiza a atualização.

- Você desabilita todos os aplicativos que consultam o vRealize Automation.
- Verifique se o MSDTC (Microsoft Distributed Transaction Coordinator) está ativado em todos os vRealize Automation e servidores SQL associados. Para obter mais informações, consulte o [artigo 2089503 da Base de Conhecimento](#).
- Se o seu ambiente tiver um appliance vRealize Orchestrator externo e um appliance vRealize Orchestrator externo que esteja conectado ao Identity Appliance, atualize o vRealize Orchestrator antes de fazer a atualização do vRealize Automation.
- É necessário concluir tarefas adicionais para preparar suas máquinas virtuais do vRealize Automation antes do upgrade. Antes de fazer a atualização, veja o [artigo 51531 da Base de Conhecimento](#).
- Verifique se você alterou as configurações de tempo limite do balanceador de carga do padrão para pelo menos 10 minutos.
- Se você estiver usando o plug-in DynamicTypes, deverá exportar as configurações de plug-in DynamicType do vRealize Orchestrator como um fluxo de trabalho de pacote.
`/Library/Dynamic Types/Configuration/Export Configuration As Package`
- Conclua estas etapas se estiver atualizando um ambiente distribuído configurado com um banco de dados PostgreSQL integrado.
 - a Examine os arquivos no diretório pgdata do host mestre antes de atualizar os hosts de réplica.
 - b Navegue até a pasta de dados PostgreSQL no host mestre em `/var/vmware/vpostgres/current/pgdata/`.
 - c Feche todos os arquivos abertos no diretório pgdata e remova todos os arquivos com um sufixo `.swp`.
 - d Verifique se todos os arquivos neste diretório possuem a posse correta: `postgres:users`.

Considerações sobre a atualização para esta versão do vRealize Automation

O vRealize Automation 7 e versões posteriores introduzem várias mudanças funcionais durante e após o processo de atualização. Você deve revisar as alterações antes de atualizar a implantação do vRealize Automation 6.2.5 para a nova versão.

Avalie estas considerações antes de atualizar.

Especificações de atualização e do Identity Appliance

Durante o processo de atualização do vRealize Automation, você responde a prompts para atualizar o appliance de identidade.

A implantação de destino usa o VMware Identity Manager.

Atualização e licenciamento

Durante a atualização, as licenças existentes do vRealize Automation 6.2.5 e quaisquer licenças do vCloud Suite 6.x que você tiver são removidas. Você deve reinserir as licenças no console de gerenciamento do appliance do vRealize Automation do vRealize Automation 7.4.

Agora, você usa o licenciamento do vRealize Automation para appliances virtuais e o IaaS digitando as informações de chave de licença no appliance do vRealize Automation. As informações de licenciamento já não estão mais disponíveis na interface do usuário do IaaS e o IaaS não realiza mais verificações de licenciamento. Endpoints e cotas são aplicados de acordo com os contratos de licença do usuário final (EULAs).

Observação Anote a chave de licença do vCloud Suite 6.x se você a usou para o vRealize Automation 6.2.5 antes da atualização. Durante a atualização, as chaves de licença existentes são removidas do banco de dados.

Para obter mais informações sobre como reinserir as informações de licença durante ou após a atualização, consulte [Atualizar a chave de licença](#).

Noções básicas sobre como as funções são atualizadas

Quando você atualiza o vRealize Automation, as atribuições de função existentes em sua organização são mantidas. A atualização também cria algumas atribuições de função para oferecer suporte às funções de arquiteto de blueprint adicionais.

As seguintes funções de arquiteto são usadas para oferecer suporte à definição de blueprint na tela de criação:

- Arquiteto de aplicativo: monta os componentes e blueprints existentes para criar blueprints compostos.
- Arquiteto de infraestrutura. Cria e gerencia blueprints de máquinas virtuais.
- Arquiteto do XaaS. Cria e gerencia blueprints do XaaS.
- Arquiteto de software: cria e gerencia componentes do Software.

Por padrão, no vRealize Automation 7, os administradores de tenant e os gerentes de grupo de negócios não podem projetar blueprints. A função de arquiteto de infraestrutura é atribuída aos administradores de tenant e aos gerentes de grupo de negócios atualizados.

Os usuários que puderem reconfigurar uma máquina virtual na versão de origem do vRealize Automation 6.2.x poderão alterar a propriedade da máquina virtual após a atualização para a nova versão.

As atribuições de função a seguir são feitas durante a atualização. As funções que não estão listadas na tabela são atualizadas para o mesmo nome de função na implantação de destino.

Tabela 1-62. Funções atribuídas durante a atualização

| Função na implantação de origem | Função na implantação de destino |
|---------------------------------|---|
| Administrador de tenant | Administrador de tenants e arquiteto de infraestrutura |
| Gerente de grupos de negócios | Gerente de grupos de negócios e arquiteto de infraestrutura |
| Arquiteto de serviços | Arquiteto do XaaS |
| Arquiteto de aplicativos | Arquiteto de software |

Para mais informações sobre funções, consulte [Funções e Responsabilidades de Tenant no vRealize Automation](#).

Noções básicas de como os blueprints são atualizados

Via de regra, os blueprints publicados são atualizados como blueprints publicados.

No entanto, há exceções a essa regra. Os blueprints de várias máquinas são atualizados como blueprints compostos que contêm componentes de blueprint. Os blueprints de várias máquinas, os quais contêm configurações não suportadas, são atualizados como não publicados.

Observação O vRealize Automation 7.x tira um snapshot do blueprint na implantação. Se você encontrar problemas de reconfiguração ao atualizar as propriedades da máquina, como CPU e RAM em uma implantação, consulte o artigo da Base de conhecimento [2150829 Tirando um snapshot do blueprint do vRA 7.x](#).

Para obter mais informações sobre como atualizar blueprints, consulte [Atualização e blueprints do vApp, endpoints do vCloud e reservas do vCloud](#) e [Noções básicas de como os blueprints de várias máquinas são atualizados](#).

Atualização e blueprints do vApp, endpoints do vCloud e reservas do vCloud

Não é possível atualizar uma implantação que contém endpoints do vApp (vCloud). A presença de endpoints do vApp (vCloud) impede a atualização para esta versão do vRealize Automation.

A atualização falhará no appliance virtual mestre se houver um endpoint do vApp (vCloud) na implantação de origem. Uma mensagem aparece no log e na interface do usuário. Para determinar se a sua implantação de origem contém um endpoint do vApp (vCloud), faça login no console do vRealize Automation como usuário administrador do IaaS. Selecione **Infraestrutura > Endpoints**. Se a lista de endpoints contiver endpoints do vApp (vCloud), não será possível atualizar para esta versão do vRealize Automation.

VApps gerenciados para recursos do vCloud Air ou vCloud Director não têm suporte no ambiente vRealize Automation de destino.

Observação Os seguintes tipos de política de aprovação estão obsoletos. Se aparecerem na lista de tipos de política de aprovação disponíveis após a conclusão da atualização, eles não terão utilidade.

- Catálogo de serviços - Solicitação de item do catálogo - vApp
 - Catálogo de serviços - Solicitação de item do catálogo - Componente do vApp
-

É possível criar endpoints e reservas do vCloud Air e do vCloud Director na implantação de destino. Você também pode criar blueprints com componentes de máquina virtual do vCloud Air ou do vCloud Director.

Noções básicas de como os blueprints de várias máquinas são atualizados

Você pode atualizar blueprints de várias máquinas e de serviço gerenciado na implantação da versão do vRealize Automation 6.2.x.

Quando você atualiza um blueprint de várias máquinas, os blueprints de componente são atualizados como blueprints de máquina única separados. O blueprint de várias máquinas é atualizado como um blueprint composto em que seus blueprints filhos anteriores são aninhados como componentes de blueprint separados.

A atualização cria um único blueprint composto único na implantação de destino que contém um componente de máquina virtual para cada blueprint de componente no blueprint de várias máquinas de origem. Se um blueprint tiver uma configuração sem suporte na nova versão, ele será atualizado e definido para o status de rascunho. Por exemplo, se o blueprint de várias máquinas contiver um perfil de rede privado, a atualização ignorará a configuração do perfil, e o blueprint será atualizado em um estado de rascunho. É possível editar o blueprint de rascunho para inserir informações de perfil de rede com suporte e publicá-las.

Observação Se um blueprint publicado na implantação de origem for atualizado para um blueprint com status de rascunho, ele não fará mais parte de um serviço ou direito. Depois de atualizar e publicar o blueprint na versão atualizada do vRealize Automation, você deve recriar suas políticas e direitos de aprovação necessários.

Algumas configurações de blueprint de várias máquinas não são suportadas na implantação de destino do vRealize Automation, incluindo perfis de rede privada e perfis de rede roteada com configurações de borda PLR associadas. Se você tiver usado uma propriedade personalizada para especificar as configurações de borda PLR (`VCNS.LoadBalancerEdgePool.Names`), a propriedade personalizada será atualizada.

Você pode atualizar um blueprint de várias máquinas com endpoints do vSphere e configurações de segurança e rede do NSX. O blueprint atualizado contém componentes de rede e segurança do NSX na tela de criação.

Observação As especificações de gateway roteadas para blueprints de várias máquinas, conforme definido nas reservas, são atualizadas. No entanto, a implantação de destino do vRealize Automation não oferece suporte a reservas de perfis roteados que contêm configurações de borda PLR associadas. Se a reserva de origem contiver um valor de gateway roteado para uma borda PLR, a reserva é atualizada, mas a configuração do gateway roteado é ignorada. Como resultado, a atualização gera uma mensagem de erro no arquivo de log e a reserva é desabilitada.

Durante a atualização, espaços e caracteres especiais são removidos dos nomes de componente de segurança e rede referenciados.

Observação O vRealize Automation 7.x tira um snapshot do blueprint na implantação. Se você encontrar problemas de reconfiguração ao atualizar as propriedades da máquina, como CPU e RAM em uma implantação, consulte o artigo da Base de conhecimento [2150829 Tirando um snapshot do blueprint do vRA 7.x](#).

Dependendo do tipo de configuração, as informações de rede e de segurança são capturadas como várias configurações diferentes no novo blueprint.

- Configurações para o blueprint geral em sua página de propriedades. Isso inclui o isolamento de aplicativo, a zona de transporte e o gateway roteado ou as informações de políticas de reserva de borda do NSX.
- Configurações disponíveis para componentes de máquina virtual do vSphere nos componentes de rede e de segurança do NSX na tela de criação.
- Configurações nas guias de rede e de segurança de componentes de máquina virtual individuais do vSphere na tela de criação.

Atualização e endpoints, reservas e blueprints físicos

Você não pode atualizar uma implantação que contém endpoints físicos. Se endpoints físicos estiverem presentes, o processo de atualização do vRealize Automation falhará.

A atualização falha no appliance virtual mestre quando a implantação do vRealize Automation 6.2.x tem um endpoint físico. Uma mensagem de falha aparece no log e na interface de migração. Para determinar se a sua implantação do vRealize Automation 6.2.x tem um endpoint físico, faça login no vRealize Automation como um usuário administrador do IaaS. Selecione **Infraestrutura > Endpoints** e examine a lista de endpoints. Se a lista tiver um endpoint Platform Type Physical, não será possível atualizar para o vRealize Automation 7,0 e versões posteriores.

Não há suporte para endpoints, reservas e componentes de máquinas virtuais em blueprints no vRealize Automation 7,0 e versões posteriores.

Atualização e configurações de perfil de rede

Perfis de rede particulares não têm suporte no vRealize Automation 7 e versões posteriores. Esses perfis são ignorados durante a atualização. Perfis de rede roteada com configurações de borda PLR associadas também não têm suporte no vRealize Automation 7 e versões posteriores. Os balanceadores de carga que fazem referência a essas redes privadas são ignorados durante a atualização.

O tipo de perfil de rede privada não tem suporte no vRealize Automation 7 e versões posteriores. Quando o processo de atualização do vRealize Automation encontra um perfil de rede privada na implementação de origem, ele ignora o perfil de rede. Balanceadores de carga que fazem referência a essas redes privadas também são ignorados durante a atualização. As mesmas condições de atualização são verdadeiras para um perfil de rede roteada com configurações de borda PLR associadas. Nenhuma configuração de perfil de rede é atualizada.

Se uma reserva contiver um perfil de rede privada, a configuração do perfil de rede privada será ignorada durante a atualização. A reserva será atualizada como desativada na implantação de destino.

Se uma reserva contiver um perfil de rede roteada com configurações de borda PLR associadas, a especificação do perfil de rede roteada será ignorada durante a atualização. A reserva será atualizada como desativada na implantação de destino.

Para obter informações sobre como atualizar um blueprint de várias máquinas que contém configurações de rede, consulte [Noções básicas de como os blueprints de várias máquinas são atualizados](#).

Atualização de ações e ações autorizadas

Não é possível atualizar ações da máquina virtual.

As ações que você pode executar em máquinas virtuais provisionadas, com base nas especificações do blueprint, não são atualizadas. Para recriar as ações que você pode realizar em uma máquina virtual, personalize os direitos de blueprints para ativar somente algumas ações.

Para informações relacionadas, consulte [Ações em Autorizações](#).

Atualização e propriedades de personalização

Todas as propriedades personalizadas que o vRealize Automation fornece estão disponíveis na implantação atualizada. Propriedades personalizadas e grupos de propriedades são atualizados.

Terminologia e alterações relacionadas

Todos os perfis de compilação que você criou na implementação de origem são atualizados como grupos de propriedades. O termo *perfil de compilação* não é mais utilizado.

O termo *conjunto de propriedades* não é mais utilizado e os arquivos de conjunto de propriedades de CSV não estão mais disponíveis.

Distinção entre maiúsculas e minúsculas em nomes de propriedade personalizadas

Antes do vRealize Automation 7.0, nomes de propriedade personalizadas não faziam distinção entre maiúsculas e minúsculas. No vRealize Automation 7.0 e versões posteriores, nomes de propriedades personalizadas fazem distinção entre maiúsculas e minúsculas. Durante a atualização, os nomes das propriedades personalizadas devem ser uma correspondência exata. Isso garante que os valores de propriedades não substituam uns aos outros e que eles correspondam às definições do dicionário de propriedades. Por exemplo, uma propriedade personalizada `hostname` e outra propriedade personalizada `HOSTNAME` são consideradas propriedades personalizadas diferentes pelo vRealize Automation 7.0 e versões posteriores. A propriedade personalizada `hostname` e a propriedade personalizada `HOSTNAME` não substituem uma à outra durante a atualização.

Espaços nos nomes de propriedade personalizada

Antes da atualização para esta versão do vRealize Automation, remova os caracteres de espaço dos nomes da sua propriedade personalizada, por exemplo, substitua o espaço por um caractere de sublinhado para permitir que a propriedade personalizada seja reconhecida na instalação do vRealize Automation atualizada. Os nomes da propriedade personalizada do vRealize Automation não podem conter espaços. Esse problema também pode ter impacto sobre o uso de uma instalação do vRealize Orchestrator atualizada que usa as propriedades personalizadas que continham espaços nas versões anteriores do vRealize Automation ou do vRealize Orchestrator, ou em ambos.

Nomes de propriedade reservados

Como várias palavras-chave estão agora reservadas, algumas propriedades atualizadas podem ser afetadas. Algumas palavras-chave usadas pelo código de blueprint podem ser importadas, por exemplo, utilizando-se funções de importação de blueprint do vRealize CloudClient. Essas palavras-chave são consideradas reservadas e não estão disponíveis para as propriedades que estão sendo atualizadas. As palavras-chave incluem `cpu`, `storage` e `memory`, mas não se limitam a esses.

Atualização e Application Services

A atualização do Application Services tem suporte no vRealize Automation 7 e versões posteriores.

Após a migração bem-sucedida para o vRealize Automation 7.4, você pode usar a Ferramenta de Migração de Serviços de Aplicativo do vRealize Automation para atualizar seus serviços de aplicativo. Conclua estas etapas para baixar a ferramenta.

- 1 Clique em [Baixar VMware vRealize Automation](#).
- 2 Selecione **Drivers e Ferramentas > VMware vRealize Application Services Migration Tool**.

Atualização e Advanced Service Design

Quando você atualizar para o vRealize Automation 7 e versões posteriores, os itens de Design de Serviços Avançados serão atualizados para elementos XaaS.

Os componentes do XaaS estão disponíveis para uso na tela de design.

Informações sobre preços de blueprint e atualização

A partir da versão 7.0, não há mais suporte para perfis de preço do vRealize Automation, e eles não serão migrados na implantação de destino durante a atualização. No entanto, você pode usar a integração avançada com o vRealize Business for Cloud para gerenciar suas despesas com recursos do vRealize Automation.

Agora, o vRealize Business for Cloud está totalmente integrado ao vRealize Automation e oferece suporte aos seguintes recursos de precificação aprimorados.

- Localização unificada no vRealize Business for Cloud para definir políticas de preço flexíveis para:
 - Blueprints de recurso de infraestrutura, de máquina e de aplicativo
 - Máquinas virtuais provisionadas no vRealize Automation para endpoints com suporte, como o vCenter Server, o vCloud Director, o Amazon Web Services, o Azure e o OpenStack.
 - Qualquer preço operacional, preço único e preço para propriedades personalizadas de máquinas virtuais provisionadas
 - Implantações, que incluem o preço de máquinas virtuais nas implantações
- Relatórios showback baseados em funções no vRealize Business for Cloud
- Aproveite ao máximo os novos recursos no vRealize Business for Cloud

Antes de atualizar, você pode exportar seus relatórios de despesas existentes da sua instância do vRealize Automation de origem para referência. Ao terminar a atualização, você pode instalar e configurar o vRealize Business for Cloud para lidar com preços.

Observação O vRealize Automation 7.4 é compatível apenas com o vRealize Business for Cloud 7.4 e versões posteriores.

Atualização e itens de catálogo

Após atualizar do vRealize Automation 6.2.x para a versão mais recente, alguns itens de catálogo aparecem no catálogo de serviços, mas não estão disponíveis para solicitação.

Após migrar para a versão mais recente do vRealize Automation, os itens de catálogo que utilizam essas definições de propriedades aparecem no catálogo de serviços, mas não estão disponíveis para solicitação.

- Tipos de controle: caixa de seleção ou link.
- Atributos: Relacionamento, expressões regulares ou layouts de propriedades.

No vRealize Automation 7.x, as definições de propriedades não usam mais estes elementos. Você deverá recriar a definição de propriedade ou configurá-la para utilizar uma ação de script do vRealize Orchestrator em vez dos tipos de controle ou atributos incorporados. Para obter mais informações, consulte [Itens de catálogo aparecem no catálogo de serviços após atualização, mas não estão disponíveis para solicitação](#).

Lista de verificação para atualizar o vRealize Automation

Ao atualizar o vRealize Automation 6.2.5 para 7.4, você atualiza todos os componentes do vRealize Automation em uma ordem específica.

Use as listas de verificação para acompanhar seu trabalho enquanto conclui a atualização. Conclua as tarefas na ordem em que elas são apresentadas.

Observação Você deve atualizar os componentes na ordem prescrita e atualizar todos os componentes. Usar uma ordem diferente pode resultar em um comportamento inesperado após a atualização ou falha na conclusão da atualização.

A ordem de atualização varia dependendo do fato de você estar atualizando um ambiente mínimo ou distribuído com vários appliances do vRealize Automation.

Tabela 1-63. Lista de verificação para atualizar um ambiente vRealize Automation mínimo

| Tarefa | Instruções |
|--|--|
| <p><input type="checkbox"/> Faça backup de sua instalação atual. A criação desse backup é uma tarefa crítica.</p> | <p>Para obter mais informações sobre como fazer backup e restaurar o sistema, consulte Fazer backup do ambiente do vRealize Automation 6.2.5 existente.</p> <p>Para obter informações gerais, consulte <i>Configurando o backup e a restauração usando o Symantec Netbackup</i> em http://www.vmware.com/pdf/vrealize-backup-and-restore-netbackup.pdf</p> |
| <p><input type="checkbox"/> Prepare as máquinas virtuais do vRealize Automation 6.2.x para atualização.</p> | <p>Veja o artigo 51531 da Base de conhecimento e realize as correções relevantes nos seus ambientes antes da atualização.</p> |
| <p><input type="checkbox"/> Desligue os serviços Windows do vRealize Automation no servidor IaaS.</p> | <p>Consulte Pare os serviços do vRealize Automation no servidor Windows do IaaS.</p> |
| <p><input type="checkbox"/> Se o catálogo de componentes comuns estiver instalado, será preciso desinstalá-lo antes da atualização.</p> | <p>Para obter informações sobre como desinstalar componentes comuns do Catálogo de Componentes, consulte o <i>Common Components Catalog Installation Guide</i>.</p> <p>Se esse guia não estiver disponível, execute estas etapas em cada nó IaaS.</p> <ol style="list-style-type: none"> 1 Faça login no nó do IaaS. 2 Clique em Iniciar. 3 Insira serviços na caixa de texto Pesquisar programas e arquivos. 4 Clique em Serviços. 5 No painel direito da janela Serviços, clique com o botão direito em cada serviço de IaaS e selecione Parar para pará-lo. 6 Clique em Iniciar > Painel de Controle > Programas e Recursos. 7 Clique com o botão direito em cada componente do Catálogo de Componentes Comuns instalado e selecione Desinstalar. 8 Clique em Iniciar > Prompt de Comando. 9 No prompt de comando, execute iisreset. |
| <p><input type="checkbox"/> Consulte Considerações de atualização para esta versão do vRealize Automation, para saber o que pode e não pode ser atualizado e como os itens atualizados podem apresentar comportamentos diferentes.</p> <p>Nem todos os itens, incluindo blueprints, reservas e endpoints, podem ser atualizados. A atualização é bloqueada pela presença de algumas configurações sem suporte.</p> | <p>Consulte Considerações sobre a atualização para esta versão do vRealize Automation.</p> |
| <p><input type="checkbox"/> Configure seus recursos de hardware.</p> | <p>Consulte Aumentar os recursos de hardware do vCenter Server para o vRealize Automation 6.2.5.</p> |
| <p><input type="checkbox"/> Baixe as atualizações no appliance do vRealize Automation.</p> | <p>Consulte Fazendo download de atualizações do appliance vRealize Automation.</p> |

Tabela 1-63. Lista de verificação para atualizar um ambiente vRealize Automation mínimo (Continuação)

| Tarefa | Instruções |
|--|--|
| <input type="checkbox"/> Instale a atualização no appliance do vRealize Automation. | Consulte Instalar a atualização no appliance do vRealize Automation . |
| <input type="checkbox"/> Atualize o utilitário de Single-Sign On para o utilitário do VMware Identity Manager. | Consulte Atualizar a senha do Single Sign-On para o VMware Identity Manager . |
| <input type="checkbox"/> Atualize a chave de licença. | Consulte Atualizar a chave de licença . |
| <input type="checkbox"/> Migre o Repositório de identidades para o VMware Identity Manager. | Migrar repositórios de identidades para VMware Identity Manager |
| <input type="checkbox"/> Atualize os componentes do IaaS. | Consulte Atualizar os componentes do servidor de IaaS após atualizar o vRealize Automation . |
| <input type="checkbox"/> Atualize o vRealize Orchestrator externo. | Consulte Atualizando o appliance autônomo do vRealize Orchestrator para uso com o vRealize Automation . Consulte Atualizando o cluster do appliance externo do vRealize Orchestrator para uso com o vRealize Automation |
| <input type="checkbox"/> Adicionar usuários ou grupos a uma conexão do Active Directory. | Consulte Adicionar usuários ou grupos a uma conexão do Active Directory . |

Tabela 1-64. Lista de verificação para atualizar um ambiente vRealize Automation distribuído

| Tarefa | Instruções |
|--|--|
| <input type="checkbox"/> Faça backup de sua instalação atual. A criação desse backup é uma tarefa crítica. | Para obter mais informações sobre como fazer backup e restaurar o sistema, consulte Fazer backup do ambiente do vRealize Automation 6.2.5 existente . Para obter informações detalhadas, consulte <i>Configurando o backup e a restauração usando o Symantec Netbackup</i> em http://www.vmware.com/pdf/vrealize-backup-and-restore-netbackup.pdf |
| <input type="checkbox"/> Prepare as máquinas virtuais do vRealize Automation 6.2.x para atualização. | Veja o artigo 51531 da Base de conhecimento e realize as correções relevantes nos seus ambientes antes da atualização. |
| <input type="checkbox"/> Desligue os serviços do vRealize Automation nos Windows Servers de IaaS. | Consulte Pare os serviços do vRealize Automation no servidor Windows do IaaS . |

Tabela 1-64. Lista de verificação para atualizar um ambiente vRealize Automation distribuído (Continuação)

| Tarefa | Instruções |
|--|---|
| <p><input type="checkbox"/> Se o catálogo de componentes comuns estiver instalado, será preciso desinstalá-lo antes da atualização.</p> | <p>Para obter informações sobre como desinstalar componentes comuns do Catálogo de Componentes, consulte o <i>Common Components Catalog Installation Guide</i>.</p> <p>Se esse guia não estiver disponível, execute estas etapas em cada nó IaaS.</p> <ol style="list-style-type: none"> 1 Faça login no nó do IaaS. 2 Clique em Iniciar. 3 Insira serviços na caixa de texto Pesquisar programas e arquivos. 4 Clique em Serviços. 5 No painel direito da janela Serviços, clique com o botão direito em cada serviço de IaaS e selecione Parar para pará-lo. 6 Clique em Iniciar > Painel de Controle > Programas e Recursos. 7 Clique com o botão direito em cada componente do Catálogo de Componentes Comuns instalado e selecione Desinstalar. 8 Clique em Iniciar > Prompt de Comando. 9 No prompt de comando, execute isreset. |
| <p><input type="checkbox"/> Configure os recursos de hardware para a atualização.</p> | <p>Consulte Aumentar os recursos de hardware do vCenter Server para o vRealize Automation 6.2.5.</p> |
| <p><input type="checkbox"/> Desative seus balanceadores de carga.</p> | <p>Desative cada nó secundário e remova os monitores de integridade do vRealize Automation para os seguintes itens.</p> <ul style="list-style-type: none"> ■ Appliance do vRealize Automation ■ Site do IaaS ■ IaaS Manager Service <p>Para uma atualização bem-sucedida, verifique o seguinte:</p> <ul style="list-style-type: none"> ■ O tráfego do balanceador de carga está direcionado somente ao nó primário. ■ Os monitores de integridade do vRealize Automation estão removidos para o appliance, o site e o Manager Service. |
| <p><input type="checkbox"/> Baixe as atualizações no appliance do vRealize Automation.</p> | <p>Consulte Fazendo download de atualizações do appliance vRealize Automation.</p> |
| <p><input type="checkbox"/> Instale a atualização no primeiro appliance do vRealize Automation da instalação. Se você tiver designado um appliance como mestre, atualize o appliance primeiro.</p> | <p>Consulte Instalar a atualização no appliance do vRealize Automation.</p> |
| <p><input type="checkbox"/> Atualize o utilitário de Single-Sign On para o utilitário do VMware Identity Manager.</p> | <p>Consulte Atualizar a senha do Single Sign-On para o VMware Identity Manager.</p> |
| <p><input type="checkbox"/> Atualize a chave de licença.</p> | <p>Consulte Atualizar a chave de licença.</p> |

Tabela 1-64. Lista de verificação para atualizar um ambiente vRealize Automation distribuído (Continuação)

| Tarefa | Instruções |
|---|--|
| <input type="checkbox"/> Migre o Repositório de identidades para o utilitário do VMware Identity Manager. | Migrar repositórios de identidades para VMware Identity Manager |
| <input type="checkbox"/> Instale a atualização nos appliances restantes do vRealize Automation. | Instalar a atualização em appliances adicionais do vRealize Automation |
| <input type="checkbox"/> Atualize os componentes do IaaS. | Consulte Atualizar os componentes do servidor de IaaS após atualizar o vRealize Automation . |
| <input type="checkbox"/> Atualize o vRealize Orchestrator externo. | Consulte Atualizando o appliance autônomo do vRealize Orchestrator para uso com o vRealize Automation . Consulte Atualizando o cluster do appliance externo do vRealize Orchestrator para uso com o vRealize Automation |
| <input type="checkbox"/> Ative os balanceadores de carga. | Ativar os balanceadores de carga |

Interfaces de usuário do ambiente do vRealize Automation

Você usa e gerencia seu ambiente do vRealize Automation com várias interfaces.

Interfaces do Usuário

Estas tabelas descrevem as interfaces que você usa para gerenciar seu ambiente do vRealize Automation.

Tabela 1-65. vRealize Automation Console administrativo

| Finalidade | Acesso | Credenciais necessárias |
|--|--|--|
| Use o console do vRealize Automation para estas tarefas de administrador do sistema. <ul style="list-style-type: none"> ■ Adicionar tenants. ■ Personalizar a interface do usuário do vRealize Automation. ■ Configurar servidores de e-mail. ■ Exibir logs de evento. ■ Configure o vRealize Orchestrator. | <ol style="list-style-type: none"> 1 Inicie um navegador e abra a tela inicial do appliance do vRealize Automation usando o nome de domínio totalmente qualificado do appliance virtual: https://vra-va-hostname.domain.name. 2 Clique em Console do vRealize Automation. Você também pode usar esta URL para abrir o console do vRealize Automation: https://vra-va-hostname.domain.name/vcac 3 Faça login. | Você deve ser um usuário com a função de administrador de sistema. |

Tabela 1-66. Console do tenant do vRealize Automation . Essa interface é a interface de usuário principal que você pode usar para criar e gerenciar seus serviços e recursos.

| Finalidade | Acesso | Credenciais necessárias |
|---|---|---|
| <p>Use o vRealize Automation para estas tarefas.</p> <ul style="list-style-type: none"> ■ Solicite novos blueprints de serviço de TI. ■ Criar e gerenciar recursos de TI e da nuvem. ■ Criar e gerenciar grupos personalizados. ■ Crie e gerencie grupos de negócios. ■ Atribuir funções a usuários. | <p>1 Inicie um navegador e insira a URL da sua locação usando o nome de domínio totalmente qualificado do appliance virtual e o nome da URL do tenant:</p> <p><code>https://vra-va-hostname.domain.name/vcac/org/nome_URL_tenant.</code></p> <p>2 Faça login.</p> | <p>Você deve ser um usuário com uma ou mais destas funções:</p> <ul style="list-style-type: none"> ■ Arquiteto de aplicativos ■ Administrador de aprovação ■ Administrador do catálogo ■ Administrador do contentor ■ Arquiteto do contentor ■ Consumidor de integridade ■ Arquiteto de infraestrutura ■ Consumidor de Exportação Segura ■ Arquiteto de software ■ Administrador de tenant ■ Arquiteto do XaaS |

Tabela 1-67. Gerenciamento do Appliance do vRealize Automation . Às vezes, esta interface é chamada de Interface de Gerenciamento do Appliance Virtual (VAMI).

| Finalidade | Acesso | Credenciais necessárias |
|--|---|---|
| <p>Use o Gerenciamento do Appliance do vRealize Automation para estas tarefas.</p> <ul style="list-style-type: none"> ■ Visualizar o status de serviços registrados. ■ Visualizar informações do sistema e reinicializar ou desligar o appliance. ■ Gerenciar a participação no Programa de Aperfeiçoamento da Experiência do Cliente. ■ Visualizar o status da rede. ■ Visualizar o status da atualização e instalar atualizações. ■ Gerenciar configurações de administração. ■ Gerenciar configurações do host vRealize Automation. ■ Gerenciar configurações de SSO. ■ Gerenciar licenças de produto. ■ Configurar o banco de dados Postgres do vRealize Automation. ■ Configurar mensagens do vRealize Automation. ■ Configurar o registro em log do vRealize Automation. ■ Instalar componentes do IaaS. ■ Migrar de uma instalação existente do vRealize Automation. ■ Gerenciar certificados de componentes do IaaS. ■ Configurar o serviço Xenon. | <ol style="list-style-type: none"> 1 Inicie um navegador e abra a tela inicial do appliance do vRealize Automation usando o nome de domínio totalmente qualificado do appliance virtual: <code>https://vra-va-hostname.domain.name.</code> 2 Clique em Gerenciamento do Appliance do vRealize Automation. Você também pode usar esta URL para abrir o Gerenciamento do Appliance do vRealize Automation: <code>https://vra-va-hostname.domain.name:5480.</code> 3 Faça login. | <ul style="list-style-type: none"> ■ Nome de usuário: root ■ Senha: senha que você inseriu quando implantou o appliance do vRealize Automation. |

Tabela 1-68. Cliente vRealize Orchestrator

| Finalidade | Acesso | Credenciais necessárias |
|--|--|--|
| <p>Use o Cliente vRealize Orchestrator para estas tarefas.</p> <ul style="list-style-type: none"> ■ Desenvolver ações. ■ Desenvolver fluxos de trabalho. ■ Gerenciar políticas. ■ Instalar pacotes. ■ Gerenciar usuários e permissões de grupos de usuários. ■ Anexar marcas a objetos de URI. ■ Visualizar o inventário. | <ol style="list-style-type: none"> 1 Inicie um navegador e abra a tela inicial do appliance vRealize Automation usando o nome de domínio totalmente qualificado do appliance virtual: <code>https://vra-va-hostname.domain.name.</code> 2 Para baixar o arquivo <code>client.jnlp</code> no seu computador local, clique em Cliente vRealize Orchestrator. 3 Clique com o botão direito do mouse no arquivo <code>client.jnlp</code> e selecione Iniciar. 4 Na caixa de diálogo Deseja Continuar?, clique em Continuar. 5 Faça login. | <p>Você deve ser um usuário com a função de administrador de sistema ou parte do grupo <code>vcoadmins</code> definido nas configurações do Provedor de Autenticação do Centro de Controle do vRealize Orchestrator.</p> |

Tabela 1-69. Centro de Controle do vRealize Orchestrator

| Finalidade | Acesso | Credenciais necessárias |
|---|---|--|
| <p>Use o Centro de Controle do vRealize Orchestrator para editar a configuração da instância do vRealize Orchestrator padrão que está incorporada no vRealize Automation.</p> | <ol style="list-style-type: none"> 1 Inicie um navegador e abra a tela inicial do appliance do vRealize Automation usando o nome de domínio totalmente qualificado do appliance virtual: <code>https://vra-va-hostname.domain.name.</code> 2 Clique em Gerenciamento do Appliance do vRealize Automation. Você também pode usar esta URL para abrir o Gerenciamento do Appliance do vRealize Automation: <code>https://vra-va-hostname.domain.name:5480.</code> 3 Faça login. 4 Clique em Configurações do vRA > Orchestrator. 5 Selecione a interface de usuário do Orchestrator. 6 Clique em Iniciar. 7 Clique na URL da interface de usuário do Orchestrator. 8 Faça login. | <p>Nome do usuário</p> <ul style="list-style-type: none"> ■ Insira a raiz se a autenticação com base na função não estiver configurada. ■ Insira seu nome de usuário vRealize Automation se ele estiver configurado para autenticação com base na função. <p>Senha</p> <ul style="list-style-type: none"> ■ Insira a senha que você inseriu quando implantou o appliance do vRealize Automation se a autenticação com base na função não estiver configurada. ■ Insira a senha para o seu nome de usuário, se o seu nome de usuário estiver configurado para autenticação com base na função. |

Tabela 1-70. Prompt de Comando do Linux

| Finalidade | Acesso | Credenciais necessárias |
|--|--|---|
| <p>Você pode usar o prompt de comando do Linux em um host, como o host do appliance do vRealize Automation, para estas tarefas.</p> <ul style="list-style-type: none"> ■ Parar ou iniciar serviços ■ Editar arquivos de configuração ■ Executar comandos ■ Recuperar dados | <p>1 No host do appliance do vRealize Automation, abra um prompt de comando.</p> <p>Uma maneira de abrir o prompt de comando no computador local é iniciar uma sessão no host usando um aplicativo, como o PuTTY.</p> <p>2 Faça login.</p> | <ul style="list-style-type: none"> ■ Nome de usuário: root ■ Senha: senha que você criou quando implantou o appliance do vRealize Automation. |

Tabela 1-71. Prompt de Comando do Windows

| Finalidade | Acesso | Credenciais necessárias |
|--|--|---|
| <p>Você pode usar um prompt de comando do Windows em um host, como o host laaS, para executar scripts.</p> | <p>1 No host do laaS, faça login no Windows.</p> <p>Uma maneira de fazer logon no seu computador local é iniciar uma sessão de área de trabalho remota.</p> <p>2 Abra o prompt de comando do Windows.</p> <p>Uma maneira de abrir o prompt de comando é clicar com o botão direito no ícone Iniciar no host e selecionar Prompt de Comando ou Prompt de Comando (Admin).</p> | <ul style="list-style-type: none"> ■ Nome de usuário: usuário com privilégios administrativos. ■ Senha: Senha do usuário. |

Atualizando produtos VMware integrados com o vRealize Automation

É necessário gerenciar produtos VMware integrados com seu ambiente do vRealize Automation ao atualizar o vRealize Automation.

Se seu ambiente do vRealize Automation estiver integrado com um ou mais produtos adicionais, você deverá atualizar o vRealize Automation antes de atualizar os outros produtos. Se o vRealize Business for Cloud estiver integrado com o vRealize Automation, você deverá cancelar o registro do vRealize Business for Cloud antes de atualizar o vRealize Automation.

Siga o fluxo de trabalho sugerido para gerenciar produtos integrados quando atualizar o vRealize Automation.

- 1 Atualize o vRealize Automation.
- 2 Atualize o VMware vRealize Operations Manager.
- 3 Atualize o VMware vRealize Log Insight.
- 4 Atualize o VMware vRealize Business for Cloud.

Esta seção fornece orientação adicional para gerenciar o vRealize Business for Cloud quando é integrado com seu ambiente do vRealize Automation.

Atualizando o vRealize Operations Manager integrado com o vRealize Automation

Atualize o vRealize Operations Manager depois de atualizar o vRealize Automation.

Procedimentos

- 1 Atualize o vRealize Automation.
- 2 Atualize o vRealize Operations Manager. Para obter informações, consulte *Atualizando seu software* na [Documentação do VMware vRealize Operations Manager](#).

Atualizando o vRealize Log Insight integrado com o vRealize Automation

Atualize o vRealize Log Insight depois de atualizar o vRealize Automation.

Procedimentos

- 1 Atualize o vRealize Automation.
- 2 Atualize o vRealize Log Insight. Para obter informações, consulte *Atualizando o vRealize Log Insight* na [Documentação do VMware vRealize Log Insight](#).

Atualizando o vRealize Business for Cloud integrado com o vRealize Automation

Ao atualizar o ambiente do vRealize Automation, é necessário cancelar o registro e registrar sua conexão no vRealize Business for Cloud.

Execute este procedimento para garantir a continuidade do vRealize Business for Cloud quando atualizar o ambiente do vRealize Automation.

Procedimentos

- 1 Cancele o registro do vRealize Business for Cloud do vRealize Automation. Consulte *Cancelar o registro do vRealize Business for Cloud do vRealize Automation* na [Documentação do VMware vRealize Business for Cloud](#).
- 2 Atualize o vRealize Automation.
- 3 Se necessário, atualize o vRealize Business for Cloud. Consulte *Atualizando o vRealize Business for Cloud* na [Documentação do VMware vRealize Business for Cloud](#).
- 4 Registre o vRealize Business for Cloud com o vRealize Automation. Consulte *Registrar o vRealize Business for Cloud no vRealize Automation* na [Documentação do VMware vRealize Business for Cloud](#).

Preparando para atualizar o vRealize Automation

Você deve realizar várias tarefas e procedimentos antes de atualizar o vRealize Automation do 6.2.5 para 7.4.

Realize as tarefas na ordem em que aparecem na lista de verificação de atualização. Consulte [Lista de verificação para atualizar o vRealize Automation](#).

Pré-requisitos de backup para atualizar o vRealize Automation

Conclua os pré-requisitos de backup antes de atualizar o vRealize Automation 6.2.5 para o 7.4.

Pré-requisitos

- Verifique se o ambiente de origem foi totalmente instalado e configurado.

- Para cada appliance no ambiente de origem, faça backup de todos os arquivos de configuração do appliance do vRealize Automation nos diretórios a seguir.
 - `/etc/vcac/`
 - `/etc/vco/`
 - `/etc/apache2/`
 - `/etc/rabbitmq/`
- Faça backup dos arquivos de configuração de fluxo de trabalho externo (xmldb) do vRealize Automation no seu sistema. Armazene os arquivos de backup em um diretório temporário. Esses arquivos estão localizados em `VMware\VC\Server\ExternalWorkflows\xmldb\`. Você restaura os arquivos xmldb no seu novo sistema após a migração. Consulte [Restaurar arquivos de limite de fluxo de trabalho externo..](#)

Para um problema relacionado, consulte [Cópias de backup de arquivos .xml fazem com que o sistema atinja o tempo limite.](#)
- Faça backup do banco de dados externo PostgreSQL do vRealize Automation. Para ver se o seu banco de dados PostgreSQL é externo, conclua estas etapas.
 - a Faça login no console de gerenciamento do appliance vRealize Automation usando seu nome de domínio totalmente qualificado `https://va-hostname.domain.name:5480`.

Para um ambiente distribuído, faça login no console de gerenciamento do appliance vRealize Automation primário.
 - b Selecione **Configurações do vRA > Banco de Dados**.
 - c Se o host do nó do banco de dados PostgreSQL do vRealize Automation for diferente do host do appliance vRealize Automation, faça backup do banco de dados. Se o host do nó do banco de dados for idêntico ao host do appliance, você não precisará fazer backup do banco de dados.

Para obter mais informações sobre o backup do banco de dados PostgreSQL, consulte <https://www.postgresql.org/>.
- Crie um snapshot da configuração do seu tenant e dos usuários atribuídos.
- Faça backup de todos os arquivos que você tenha personalizado, como o `DataCenterLocations.xml`.
- Obtenha um snapshot de cada appliance virtual e servidor de IaaS. Siga as diretrizes comuns para fazer backup de todo o sistema caso ocorra falha na atualização do vRealize Automation. Consulte [Backup e Recuperação para Instalações do vRealize Automation](#).

Fazer backup do ambiente do vRealize Automation 6.2.5 existente

Antes de atualizar, desligue os componentes do seu ambiente do vRealize Automation 6.2.5 e tire um snapshot deles.

Antes de atualizar, obtenha um snapshot desses componentes enquanto desliga o sistema.

- Servidores de IaaS do vRealize Automation (nós Windows)

- Appliances do vRealize Automation (nós Linux)
- Nó de identidade (SSO) do vRealize Automation

Se houver falha na atualização, use o snapshot para voltar para a última configuração válida e tente outra atualização.

Pré-requisitos

- Verifique se o banco de dados PostgreSQL incorporado está no modo de alta disponibilidade. Em caso afirmativo, localize o nó mestre atual. Veja o artigo da base de conhecimento <http://kb.vmware.com/kb/2105809>.
- Se o seu ambiente tiver um banco de dados PostgreSQL externo, crie um arquivo de backup do banco de dados.
- Se o banco de dados Microsoft SQL do vRealize Automation não estiver hospedado no servidor IaaS, crie um arquivo de backup de banco de dados. Para obter informações, encontre o artigo na [Microsoft Developer Network](#) sobre como criar um backup completo do banco de dados do SQL Server.
- Verifique se os pré-requisitos de backup foram cumpridos para atualização.
- Lembre-se de criar um snapshot do seu sistema enquanto ele estiver desligado. Este é o método preferencial para obter um snapshot. Consulte a *Documentação do vSphere 6.0*.

Observação Quando você fizer backup do appliance do vRealize Automation e de componentes do IaaS, desative snapshots na memória e snapshots inativos.

- Se você tiver modificado o arquivo `app.config`, faça um backup desse arquivo. Consulte [Restaurar alterações de registro no arquivo app.config](#).
- Faça um backup dos arquivos de configuração de fluxo de trabalho externo (xmlldb). Consulte [Restaurar arquivos de limite de fluxo de trabalho externo](#).
- Verifique que você tenha um local fora da sua pasta atual onde você possa armazenar o seu arquivo de backup. Consulte [Cópias de backup de arquivos .xml fazem com que o sistema atinja o tempo limite](#).

Procedimentos

- 1 Faça login no seu vCenter Server.
- 2 Localize estes componentes do vRealize Automation 6.2.5.
 - Servidores de IaaS do vRealize Automation (nós Windows)
 - Appliances do vRealize Automation (nós Linux)
 - Nó de identidade (SSO) do vRealize Automation
- 3 Para cada uma das máquinas virtuais, selecione a máquina virtual, clique em **Desligar guest** e aguarde que a máquina virtual pare. Desligue essas máquinas virtuais na seguinte ordem.
 - a Máquinas virtuais de agentes de proxy IaaS

- b Máquinas virtuais de Trabalhador do DEM
 - c Máquina virtual do DEM Orchestrator
 - d Máquina virtual do Manager Service
 - e Máquinas virtuais de Serviços Web
 - f Appliances virtuais do vRealize Automation secundários
 - g Appliance virtual do vRealize Automation primário
 - h Máquinas virtuais do Manager (se disponíveis)
 - i Identity Appliance
- 4 Tire um snapshot de cada máquina virtual 6.2.5 do vRealize Automation.
 - 5 Clone cada nó de appliance vRealize Automation.
Execute a atualização nas máquinas virtuais clonadas.
 - 6 Desligue cada máquina virtual do appliance vRealize Automation original antes de atualizar as máquinas virtuais clonadas.

Mantenha as máquinas virtuais originais desligadas e use-as apenas se precisar de restaurar o sistema.

Próximo passo

[Aumentar os recursos de hardware do vCenter Server para o vRealize Automation 6.2.5.](#)

Aumentar os recursos de hardware do vCenter Server para o vRealize Automation 6.2.5

Antes de atualizar do vRealize Automation 6.2.5, é preciso aumentar os recursos de hardware para cada appliance vRealize Automation.

Este procedimento supõe que você esteja usando o cliente vCenter Server para Windows.

Pré-requisitos

- Verifique se você tem um clone de cada appliance vRealize Automation.
- Certifique-se de ter pelo menos 140 GB de espaço livre no vCenter Server para cada clone do appliance.
- Verifique se os aparelhos originais estão desligados.

Procedimentos

- 1 Faça login no vCenter Server.
- 2 Clique com o botão direito do mouse no ícone de um appliance clonado do vRealize Automation e selecione **Editar configurações**.
- 3 Selecione **Memória** e defina o valor para 18 GB.
- 4 Selecione **CPU** e defina o valor da **Quantidade de soquetes virtuais** para 4.

- 5 Estenda o tamanho do Disco virtual 1 para 50 GB.
 - a Selecione o Disco 1.
 - b Mude o tamanho para 50 GB.
 - c Clique em **OK**.
- 6 Se você não tiver o Disco 3, conclua estas etapas para adicionar um Disco 3 com um tamanho de 25 GB
 - a Clique em **Adicionar** acima da tabela Recursos para adicionar um disco virtual.
 - b Selecione **Hard Disk** para o **Tipo de Dispositivo**, e clique em **Próximo**.
 - c Selecione **Criar um novo disco virtual**, e clique em **Próximo**.
 - d Defina o **tamanho do disco** para 25 GB.
 - e Selecione **Armazenar com a máquina virtual** e clique em **Próximo**.
 - f Verifique se a opção **Independente** está desmarcada para **Modo** e **SCSI (0:2)** está marcada para **Modo de Dispositivo Virtual** e clique em **Próximo**.

Se for solicitado para aceitar as configurações recomendadas, faça isso.
 - g Clique em **Concluir**.
 - h Clique em **OK**.
- 7 Se houver um Disco 4 virtual existente de uma versão anterior do vRealize Automation, conclua essas etapas.
 - a Ligue o clone do appliance virtual primário e aguarde 1 minuto.
 - b Ligue o clone do appliance virtual secundário.
 - c No clone do appliance virtual primário, abra um novo prompt de comando e navegue até `/etc/fstab`.
 - d No clone do appliance virtual primário, abra o arquivo `fstab` e remova as linhas que começam com `/dev/sdd` e contêm os registros `write ahead Wal_Archive`.
 - e No clone do appliance virtual primário, salve o arquivo.
 - f No clone do appliance virtual secundário, abra um novo prompt de comando e navegue até `/etc/fstab`.
 - g No clone do appliance virtual secundário, abra o arquivo `fstab` e remova as linhas que começam com `/dev/sdd` e contêm os registros `write ahead Wal_Archive`.
 - h No clone do appliance virtual secundário, salve o arquivo.
 - i Desligue o clone do appliance virtual secundário e aguarde 1 minuto.
 - j Desligue o clone do appliance virtual primário.
 - k Clique com o botão direito do mouse no ícone do appliance vRealize Automation primário clonado e selecione **Editar Configurações**.

- l Excluir o Disco 4 na máquina do appliance virtual primário clonado.
 - m Clique com o botão direito do mouse no ícone do appliance vRealize Automation secundário clonado e selecione **Editar Configurações**.
 - n Excluir o Disco 4 na máquina do appliance virtual secundário clonado.
- 8 Conclua essas etapas para adicionar um Disco 4 com um tamanho de disco de 50 GB às máquinas do appliance virtual primário e secundário clonado.
- a Clique em **Adicionar** acima da tabela Recursos para adicionar um disco virtual.
 - b Selecione **Hard Disk** para o **Tipo de Dispositivo**, e clique em **Próximo**.
 - c Selecione **Criar um novo disco virtual**, e clique em **Próximo**.
 - d Defina o **tamanho do disco** para 50 GB.
 - e Selecione **Armazenar com a máquina virtual** e clique em **Próximo**.
 - f Verifique se a opção **Independente** está desmarcada para **Modo** e **SCSI (0:3)** está marcada para **Modo de Dispositivo Virtual** e clique em **Próximo**.
- Se for solicitado para aceitar as configurações recomendadas, faça isso.
- g Clique em **Concluir**.
 - h Clique em **OK**.
- 9 Crie um snapshot da máquina do appliance virtual primário clonado e da máquina do appliance virtual secundário clonado.

Próximo passo

[Ligar todo o sistema.](#)

Ligar todo o sistema

Depois de aumentar os recursos de hardware do vCenter para a atualização, ligue o sistema antes de realizar a atualização.

Pré-requisitos

- [Fazer backup do ambiente do vRealize Automation 6.2.5 existente.](#)
- [Aumentar os recursos de hardware do vCenter Server para o vRealize Automation 6.2.5.](#)

Procedimentos

1 Ligue todo o sistema.

Para obter instruções, consulte a versão 6.2 do vRealize Automation do tópico [Inicializar o vRealize Automation](#).

Observação Se você tiver um ambiente de alta disponibilidade, use esse procedimento para ligar seus appliances virtuais.

- a Ligue o appliance virtual que você desligou por último.
- b Aguarde um minuto.
- c Ligue os appliances virtuais restantes.

2 Verifique se o sistema está totalmente funcional.

Próximo passo

[Pare os serviços do vRealize Automation no servidor Windows do IaaS.](#)

Pare os serviços do vRealize Automation no servidor Windows do IaaS

Quando necessário, você pode usar os seguintes procedimentos para parar os serviços do vRealize Automation em cada servidor que está executando os serviços do IaaS.

Antes de iniciar a atualização, pare os serviços do vRealize Automation em cada servidor Windows IaaS.

Observação Exceto por uma instância de backup passiva do Serviço de Gerenciador, o tipo de inicialização para todos os serviços deve ser definido como Automático durante o processo de atualização. Se você definir os serviços para Manual, o processo de atualização falha.

Procedimentos

1 Faça login no seu servidor Windows do IaaS.

2 Selecione **Iniciar > Ferramentas administrativas > Serviços**.

3 Pare os serviços na seguinte ordem. Tome cuidado para não desligar a máquina virtual.

Cada máquina virtual tem um agente de Gerenciamento que deve ser interrompido com cada conjunto de serviços.

- a Cada agente do VMware vCloud Automation Center
- b Cada VMware DEM-Worker
- c O VMware DEM-Orchestrator
- d O serviço do VMware vCloud Automation Center

- 4 Para implantações distribuídas com balanceadores de carga, desative cada nó secundário e remova os monitores de integridade do vRealize Automation para os seguintes itens.
 - a Appliance do vRealize Automation
 - b Website do IaaS
 - c Serviço de gerenciador do IaaS

Verifique se o tráfego do balanceador de carga está direcionado apenas para os nós primários e se os monitores de integridade do vRealize Automation foram excluídos do appliance, do site e do Manager Service, caso contrário a atualização falha.

- 5 Verifique se o serviço IaaS hospedado no Microsoft Internet Information Services (IIS) está em execução, realizando as seguintes etapas.
 - a No seu navegador, insira a URL `https://webhostname/Repository/Data/MetaModel.svc` para verificar se o Repositório da Web está funcionando. No caso de êxito, nenhum erro será retornado e você verá uma lista de modelos no formato XML.
 - b Verifique o status registrado no arquivo `Repository.log` no nó Web da máquina virtual do IaaS para ver se ele indica OK. O arquivo está localizado na pasta inicial do VCAC, em `/Server/Model Manager Web/Logs/Repository.log`.

Para um site IaaS distribuído, faça login no site secundário, sem o MMD, e pare o servidor Microsoft IIS temporariamente. Confira a conectividade do `MetaModel.svc`. Para verificar se o tráfego do balanceador de carga está passando apenas pelo nó web primário, inicie o servidor Microsoft IIS.

Próximo passo

[Fazendo download de atualizações do appliance vRealize Automation.](#)

Fazendo download de atualizações do appliance vRealize Automation

Você pode verificar se há atualizações no console de gerenciamento de seu appliance e baixar as atualizações usando um dos seguintes métodos.

Para obter o melhor desempenho de atualização, use o método de arquivo ISO.

Para evitar possíveis problemas ao atualizar seu appliance ou se surgirem problemas durante a atualização do appliance, consulte o [artigo da Base de dados de conhecimento da VMware Falha na atualização do vRealize Automation devido a duplicatas no banco de dados do vRealize Orchestrator \(54987\)](#).

- [Fazer download de atualizações do appliance do vRealize Automation a partir de um repositório da VMware](#)

Você pode baixar a atualização do seu appliance do vRealize Automation de um repositório público no site vmware.com.
- [Fazer download de atualizações do appliance virtual para uso com uma unidade de CD-ROM](#)

Você pode atualizar seu appliance virtual de um arquivo ISO que ele lê na unidade de CD-ROM virtual. Este é o método preferencial.

Fazer download de atualizações do appliance do vRealize Automation a partir de um repositório da VMware

Você pode baixar a atualização do seu appliance do vRealize Automation de um repositório público no site vmware.com.

Pré-requisitos

- Faça backup do ambiente existente do vRealize Automation .
- Verifique se o appliance do vRealize Automation está ligado.

Procedimentos

- 1 No appliance do vRealize Automation primário, faça login no Gerenciamento do Appliance do vRealize Automation como **root** usando a senha que você inseriu quando implantou o appliance do vRealize Automation.
- 2 Clique na guia **Atualizar**.
- 3 Clique em **Configurações**.
- 4 (Opcional) Definir a frequência de verificação de atualizações no painel Atualizações Automáticas.
- 5 Selecione **Usar Repositório Padrão** no painel Repositório de Atualização.
O repositório padrão é definido como a URL VMware.com correta.
- 6 Clique em **Salvar Configurações**.

Fazer download de atualizações do appliance virtual para uso com uma unidade de CD-ROM

Você pode atualizar seu appliance virtual de um arquivo ISO que ele lê na unidade de CD-ROM virtual. Este é o método preferencial.

Baixe o arquivo ISO e configure o appliance primário para usar esse arquivo para atualizar seu appliance.

Pré-requisitos

- Faça backup do ambiente vRealize Automation existente.
- Verifique se todas as unidades de CD-ROM usadas na atualização estão ativadas antes de atualizar um appliance do vRealize Automation. Consulte a documentação do vSphere para obter informações sobre como adicionar uma unidade de CD-ROM a uma máquina virtual no cliente do vSphere.

Procedimentos

- 1 Baixe o arquivo ISO do repositório de atualização.
 - a Inicie um navegador e acesse a [página de produto do vRealize Automation](#) em www.vmware.com.
 - b Clique em **Recursos de download do vRealize Automation** para acessar a página de downloads da VMware.
 - c Baixe o arquivo apropriado.

- 2 Localize o arquivo baixado no sistema para verificar se o tamanho dele corresponde ao do arquivo na página de downloads da VMware. Use os checksums fornecidos na página de downloads para validar a integridade do arquivo que você baixou. Para obter informações, consulte os links na parte inferior da página de downloads do VMware.
- 3 Certifique-se de que o appliance virtual primário esteja ligado.
- 4 Conecte a unidade de CD-ROM do appliance virtual primário ao arquivo ISO que você fez download.
- 5 No appliance do vRealize Automation primário, faça login no Gerenciamento do Appliance do vRealize Automation como **root** usando a senha que você inseriu quando implantou o appliance do vRealize Automation.
- 6 Clique na guia **Atualizar**.
- 7 Clique em **Configurações**.
- 8 Em Repositório de Atualização, selecione **Usar Atualizações de CDRom**.
- 9 Clique em **Salvar Configurações**.

Atualizando o appliance do vRealize Automation

Depois de concluir os pré-requisitos de atualização e baixar a atualização do appliance virtual, você atualiza o appliance do vRealize Automation 6.2.5 para 7.4. Você também reconfigura algumas configurações do appliance do vRealize Automation principal.

Depois de atualizar o appliance primário do vRealize Automation, você atualiza os outros nós no seu ambiente na seguinte ordem:

- 1 Todos os appliances secundários do vRealize Automation
- 2 Site do IaaS
- 3 Serviço de gerenciador do IaaS
- 4 IaaS DEM
- 5 Agente de IaaS
- 6 Atualize ou migre cada instância externa do vRealize Orchestrator

Instalar a atualização no appliance do vRealize Automation

Instale a atualização do vRealize Automation no appliance do vRealize Automation 6.2.5 e defina as configurações desse appliance.

O suporte para um banco de dados externo PostgreSQL está descontinuado a partir do vRealize Automation 7.1. O processo de atualização combina os dados de um banco de dados externo PostgreSQL existente com o banco de dados interno PostgreSQL que faz parte do Appliance do vRealize Automation

Os detalhes sobre os dados recolhidos pelo CEIP e os fins para os quais eles são utilizados pelo VMware são estabelecidos pelo Centro de Confiança e Garantia, em

<http://www.vmware.com/trustvmware/ceip.html>.

Não feche o console de gerenciamento enquanto você instala a atualização.

Se você encontrar problemas durante o processo de atualização, consulte [Solucionando problemas de atualização do vRealize Automation](#).

Pré-requisitos

- Verifique se você selecionou um método de download e baixou a atualização. Consulte [Fazendo download de atualizações do appliance vRealize Automation](#).
- Para implantações de alta disponibilidade distribuídas, consulte [Fazer backup do ambiente do vRealize Automation 6.2.5 existente](#).
- Para implantações com balanceamento de carga, verifique se o tráfego está direcionado apenas para o nó primário e que os monitores de integridade estão desativados.
- Se você tiver um componente de Catálogo de Componentes Comuns instalado no seu ambiente, desinstale-o antes da atualização. Para obter informações, consulte o *Guia de Instalação do Catálogo de Componentes Comuns*. Se este guia não estiver disponível, use o procedimento alternativo na [Lista de verificação para atualizar o vRealize Automation](#).
- Verifique se a conexão do banco de dados jdbc:postgresql aponta para o endereço IP externo do nó PostgreSQL mestre.
 - a Em cada appliance do vRealize Automation, abra um novo prompt de comando.
 - b Navegue até `/etc/vcac/server.xml` e faça backup do `server.xml`.
 - c Abra o `server.xml`.
 - d Se necessário, edite a entrada `jdbc:postgresql` do arquivo `server.xml` que aponta para o banco de dados Postgres e direcione-a ao endereço IP externo do nó PostgreSQL mestre para o PostgreSQL externo ou ao appliance virtual primário para o PostgreSQL incorporado.

Por exemplo, `jdbc:postgresql://198.15.100.60:5432/vcac`
- Verifique se todas as solicitações salvas e em andamento foram finalizadas com êxito antes da atualização.

Procedimentos

- 1 Abra o console de gerenciamento do appliance do vRealize Automation.
 - a No appliance do vRealize Automation primário, faça login no Gerenciamento do Appliance do vRealize Automation como **root** usando a senha que você inseriu quando implantou o appliance do vRealize Automation.
 - b Faça login com o nome de usuário **root** e a senha que você inseriu quando implantou o appliance.
- 2 Clique em **Serviços** e verifique se cada serviço, exceto `iaas-service`, está listado como REGISTRADO.
- 3 Selecione **Atualizar > Configurações**.

- 4 Selecione uma das opções a seguir:
 - **Usar repositório padrão.**
 - **Usar atualizações do CDROM**
- 5 Clique em **Salvar Configurações**.
- 6 Selecione **Status**
- 7 Clique em **Verificar atualizações** para verificar se uma atualização pode ser acessada.
- 8 (Opcional) Para instâncias do appliance do vRealize Automation, clique em **Detalhes** na área Versão do appliance para ver informações sobre o local das notas de versão.
- 9 Clique em **Instalar Atualizações**.
- 10 Clique em **OK**.

É exibida uma mensagem informando que a atualização está em andamento.

- 11 (Opcional) Se você não tiver redimensionado o Disco 1 para 50 GB manualmente, execute as seguintes etapas.
 - a Quando o sistema solicitar que você reinicialize o appliance virtual, clique na guia **Sistema** e clique em **Reinicializar**.

Durante a reinicialização, o sistema ajusta o espaço necessário para a atualização.
 - b Após o sistema ser reiniciado, faça o login novamente no console de gerenciamento do appliance do vRealize Automation, confira se cada serviço, exceto iaas-service, está listado com o REGISTRADO e selecione **Status > Atualizar**.
 - c Clique em **Verificar Atualizações** e **Instalar Atualizações**.
- 12 Para visualizar o progresso da atualização, abra os seguintes arquivos de log.
 - `/opt/vmware/var/log/vami/updatecli.log`
 - `/opt/vmware/var/log/vami/vami.log`
 - `/var/log/vmware/horizon/horizon.log`
 - `/var/log/bootstrap/*.log`

Se você fizer logoff durante o processo de atualização e voltar a fazer login antes do término da atualização, poderá continuar acompanhando o progresso da atualização no arquivo de registro. O arquivo `updatecli.log` pode exibir informações sobre a versão do vRealize Automation da qual você está atualizando. Essa versão exibida mudará para a versão adequada mais tarde no processo de atualização.

O tempo necessário para a atualização terminar varia de acordo com o seu ambiente.

- 13 Clique em **Telemetria** no console de gerenciamento do appliance. Leia a observação sobre a participação no Programa de Aperfeiçoamento da Experiência do Cliente (CEIP) e escolha se deseja participar do programa.

Os detalhes sobre os dados recolhidos pelo CEIP e os fins para os quais eles são utilizados pelo VMware são estabelecidos pelo Centro de Confiança e Garantia, em <http://www.vmware.com/trustvmware/ceip.html>.

Para obter mais informações sobre o Programa de Aperfeiçoamento da Experiência do Cliente, consulte [Participar ou sair do Programa de Aperfeiçoamento da Experiência do Cliente para o vRealize Automation](#).

Próximo passo

[Atualizar a senha do Single Sign-On para o VMware Identity Manager](#).

Atualizar a senha do Single Sign-On para o VMware Identity Manager

Depois de instalar as atualizações, você deve atualizar a senha de Single Sign-On para o VMware Identity Manager.

O VMware Identity Manager substitui os componentes de SSO do Identity Appliance e do vSphere.

Procedimentos

- 1 Faça logout do console de gerenciamento do appliance do vRealize Automation, feche o navegador, abra o navegador novamente e faça login novamente.
- 2 Selecione **Configurações do vRA > SSO**.
- 3 Insira uma nova senha do VMware Identity Manager e clique em **Salvar configurações**.

Não use senhas simples. Você pode ignorar sem receio a mensagem de erro Servidor SSO não conectado. Pode levar vários minutos para reiniciar os serviços.

A senha é aceita.

Para uma implantação de alta disponibilidade, a senha é aplicada ao primeiro nó do appliance do vRealize Automation e propagada para todos os nós secundários do appliance do vRealize Automation.

- 4 Reinicie o appliance virtual.
 - a Clique na guia **Sistema**.
 - b Clique em **Reiniciar** e confirme a seleção.
- 5 Verifique se todos os serviços estão em execução.
 - a Faça login no vRealize Automation console de gerenciamento do appliance.
 - b Clique na guia **Serviços** no console.
 - c Clique na guia **Atualizar** para monitorar o andamento da inicialização do serviço.
Você deve ver no mínimo 35 serviços.

- 6 Verifique se todos os serviços são registrados, exceto o serviço iaas.

O serviço de gerenciamento de versões não é iniciado sem uma chave de licença do vRealize Code Stream.

Próximo passo

[Atualizar a chave de licença.](#)

Atualizar a chave de licença

É necessário atualizar a chave de licença para usar a versão mais recente do appliance do vRealize Automation.

Procedimentos

- 1 Vá para o console de gerenciamento do appliance virtual usando o nome de domínio totalmente qualificado, `https://va-hostname.domain.name:5480`.
- 2 Faça login usando o nome de usuário **raiz** e a senha que você inseriu quando o appliance foi implantado.
- 3 Selecione **Configurações do vRA > Licenciamento**.
Se a guia **Licenciamento** não estiver disponível, realize estas etapas e repeta o procedimento.
 - a Faça logoff do console de gerenciamento.
 - b Limpe o cache do navegador.
- 4 Insira sua nova chave de licença na caixa de texto **Nova chave de licença**.
Endpoints e cotas são sinalizados de acordo com o seu contrato de licença de usuário final (EULA).
- 5 Clique em **Enviar chave**.

Próximo passo

[Migrar repositórios de identidades para VMware Identity Manager.](#)

Migrar repositórios de identidades para VMware Identity Manager

Ao atualizar do 6.2.5 para a versão atual do vRealize Automation, você deverá migrar os repositórios de identidades.

Conforme exigido pelos procedimentos a seguir, consulte o snapshot das informações de configuração do tenant do 6.2.5.

Observação Após migrar os armazenamentos de identidade, usuários do vRealize Code Stream devem reatribuir manualmente as funções do vRealize Code Stream.

Procedimentos

- 1 [Criar uma conta de usuário local para seus tenants](#)

Você deve configurar um tenant com uma conta de usuário local e atribuir privilégios de administrador de tenant à conta de usuário local.

2 Sincronizar usuários e grupos para um link do Active Directory

Para importar seus usuários e grupos no vRealize Automation usando a capacidade de Gerenciamento de Diretórios, você deve se conectar ao seu link do Active Directory.

3 Migrar os grupos personalizados para o VMware Identity Manager de destino

Você deve migrar todos os grupos personalizados do ambiente de origem para o VMware Identity Manager (vIDM) na implantação de destino.

4 Migrar vários administradores de tenant e IaaS

Para cada tenant do vRealize Automation com os administradores de tenants ou do IaaS, você deve excluir e restaurar cada administrador manualmente.

Criar uma conta de usuário local para seus tenants

Você deve configurar um tenant com uma conta de usuário local e atribuir privilégios de administrador de tenant à conta de usuário local.

Repita este procedimento para cada um dos seus tenants.

Pré-requisitos

Confirme que você definiu uma nova senha do VMware Identity Manager. Consulte [Atualizar a senha do Single Sign-On para o VMware Identity Manager](#).

Procedimentos

- 1 Faça login no console do vRealize Automation com a senha e o nome do usuário de **administrador** do sistema padrão.

A localização do console é `https://vra-appliance/vcac/`.

- 2 Clique no tenant.

Por exemplo, para o tenant padrão, clique em **vsphere.local**.

- 3 Selecione a guia **Usuários locais**.

- 4 Clique em **Novo**.

- 5 Criar uma conta local de usuário.

Você atribui a função de administrador tenant a este usuário. Verifique se o nome de usuário local é único no active directory do vsphere.local.

- 6 Clique em **OK**.

- 7 Clique em **Administradores**.

- 8 Insira o nome de usuário local na caixa de pesquisa **Administradores de tenant** e pressione Enter.

- 9 Clique em **Concluir**.

- 10 Faça logoff do console.

Próximo passo

[Sincronizar usuários e grupos para um link do Active Directory.](#)

Sincronizar usuários e grupos para um link do Active Directory

Para importar seus usuários e grupos no vRealize Automation usando a capacidade de Gerenciamento de Diretórios, você deve se conectar ao seu link do Active Directory.

Realize este procedimento para cada um dos tenants.

Pré-requisitos

Verifique se você tem privilégios de acesso ao Active Directory.

Procedimentos

- 1 Faça login no console do vRealize Automation em:
`https://vra-appliance/vcac/org/tenant_name`.
- 2 Selecione **Administração > Gerenciamento de Diretórios > Diretórios**.
- 3 Clique em **Acrescentar Diretório** e selecione **Acrescentar Active Directory sobre LDAP/IWA**.
- 4 Insira suas configurações de conta do Active Directory.

◆ Active Directory não nativo

| Opção | Entrada de amostra |
|--|---|
| Nome do diretório | Insira um nome de diretório exclusivo. Selecione Active Directory sobre LDAP ao usar o Active Directory não nativo. |
| Este diretório suporta serviços DNS | Desmarque esta opção. |
| DN base | Insira o nome diferenciado (DN) do ponto de início para as pesquisas do servidor de diretórios. Por exemplo, cn=users,dc=rainpole,dc=local . |
| Vincular DN | Insira todo o nome diferenciado (DN), incluindo o nome comum (CN), de uma conta de usuário do Active Directory que tenha privilégios para pesquisar os usuários. Por exemplo, cn=config_admin infra,cn=users,dc=rainpole,dc=local . |
| Vincular senha do DN | Insira a senha do Active Directory para a conta que pode pesquisar usuários. |

◆ Active Directory nativo

| Opção | Entrada de amostra |
|---|---|
| Nome do diretório | Insira um nome de diretório exclusivo. Selecione Active Directory (Autenticação integrada do Windows) ao usar Active Directory nativo. |
| Nome do domínio | Insira o nome do domínio ao qual deseja ingressar. |
| Nome de usuário Admin do domínio | Insira o nome do usuário para o administrador do domínio. |
| Senha Admin do domínio | Insira a senha para a conta Admin do domínio. |

| Opção | Entrada de amostra |
|-------------------------|---|
| Vincular UPN de usuário | Use o formato de endereço de e-mail para inserir o nome do usuário que pode autenticar o domínio. |
| Vincular senha do DN | Insira a senha da conta vinculada ao Active Directory para a conta que pode pesquisar usuários. |

- 5 Clique em **Testar Conexão** para testar a conexão com o diretório configurado.
- 6 Clique em **Salvar e Avançar**.
A página **Selecionar os Domínios** aparece e exibe a lista de domínios.
- 7 Aceite a configuração de domínio padrão e clique em **Avançar**.
- 8 Verifique se os nomes de atributo estão mapeados para os atributos corretos do Active Directory e clique em **Avançar**.
- 9 Selecione os grupos e usuários para sincronizar.
 - a Clique no ícone **Novo**.
 - b Insira o nome do domínio e clique em **Localizar Grupos**.
Por exemplo, insira **dc=vcac, dc=local**.
 - c Para selecionar os grupos para sincronizar, clique em **Selecionar** e depois em **Avançar**.
 - d Na página **Selecionar Usuários**, selecione os usuários para sincronizar e clique em **Avançar**.
- 10 Confirme os usuários e grupos que estão sendo sincronizados com o diretório e clique em **Sincronizar Diretório**.
A sincronização de diretórios demora um pouco e é executada em segundo plano.
- 11 Selecione **Administração > Gerenciamento de Diretórios > Provedores de Identidade** e clique no seu novo provedor de identidade.
Por exemplo, **WorkspacelDP__1**.
- 12 Role até o final da página e atualize o valor da propriedade IdP Hostname de forma que ela aponte para o FQDN para o balanceador de carga do vRealize Automation.
- 13 Clique em **Salvar**.
- 14 Repita as etapas de 11 a 13 para cada tenant e provedor de identidade.
- 15 Após atualizar todos os nós do vRealize Automation, faça login em cada tenant e selecione **Administração > Gerenciamento de Diretórios > Provedores de Identidade**.
Cada provedor de identidade tem todos os conectores do vRealize Automation adicionados a ele.
Por exemplo, se a sua implantação tiver dois appliances do vRealize Automation, o provedor de identidade terá dois conectores associados.

Migrar os grupos personalizados para o VMware Identity Manager de destino

Você deve migrar todos os grupos personalizados do ambiente de origem para o VMware Identity Manager (vIDM) na implantação de destino.

Conclua este procedimento para migrar os grupos personalizados.

Pré-requisitos

- [Criar uma conta de usuário local para seus tenants.](#)
- Certifique-se de que o serviço do espaço de trabalho do horizon esteja em execução no appliance virtual do vRealize Automation.

Procedimentos

- 1 Inicie uma sessão de SSH no appliance virtual do vRealize Automation.
- 2 No prompt de comando, faça login como **raiz** com a senha que você criou quando instalou o appliance virtual do vRealize Automation.
- 3 Execute este comando.

```
vcac-config migrate-custom-groups
```

- Essa mensagem aparece quando a migração é concluída: A migração de grupos personalizados foi concluída com êxito!
- Essa mensagem aparece se não há grupos personalizados no seu ambiente de origem: Não foram encontrados grupos personalizados no banco de dados do vRA. O processo de migração será ignorado.

Observação Se ocorrer falha na migração do grupo personalizado, visualize o arquivo de log em `/var/log/vmware/vcac/vcac-config.log` para obter detalhes.

Migrar vários administradores de tenant e IaaS

Para cada tenant do vRealize Automation com os administradores de tenants ou do IaaS, você deve excluir e restaurar cada administrador manualmente.

Realize o seguinte procedimento para cada tenant no console do vRealize Automation.

Pré-requisitos

Faça login no console do vRealize Automation no appliance virtual atualizado.

- 1 Abra o console do vRealize Automation no aparelho virtual atualizado usando seu nome de domínio totalmente qualificado, `https://va-hostname.domain_name/vcac`.
Para um ambiente distribuído, abra o console no appliance virtual mestre.
- 2 Selecione o domínio **vsphere.local**.
- 3 Faça login com o nome de usuário **administrator** e a senha que você definiu quando implantou o appliance virtual.

Procedimentos

- 1 Selecione **Administração > Tenants**.
- 2 Clique em um nome de tenant.
- 3 Clique em **Administradores**.
- 4 Faça uma lista de cada nome de usuário e nome de administrador de tenants e do IaaS.
- 5 Aponte para cada administrador e clique no ícone Excluir (✘) até excluir todos os administradores.
- 6 Clique em **Concluir**.
- 7 Na página Tenants, clique novamente no nome do tenant.
- 8 Clique em **Administradores**.
- 9 Insira o nome de cada usuário que você excluiu na caixa de pesquisa apropriada e pressione Enter.
- 10 Clique no nome do usuário apropriado resultado pela pesquisa para voltar a adicionar esse usuário como administrador.

Quando terminar, a lista de administradores de tenants e administradores do IaaS será igual à lista de administradores excluídos.

- 11 Clique em **Concluir**.

Próximo passo

Atualize os appliances secundários. Consulte [Instalar a atualização em appliances adicionais do vRealize Automation](#).

Instalar a atualização em appliances adicionais do vRealize Automation

Em um ambiente de alta disponibilidade, o appliance virtual mestre é o nó que executa o banco de dados PostgreSQL incorporado no modo Mestre. Os outros nós no ambiente executam o banco de dados PostgreSQL incorporado no modo Réplica. Durante a atualização, a réplica do appliance virtual 6.2.5 não requer alterações no banco de dados.

Não feche o console de gerenciamento enquanto você instala a atualização.

Pré-requisitos

- Confirme que você baixou as atualizações do appliance virtual. Consulte [Fazendo download de atualizações do appliance vRealize Automation](#).
- Verifique se a conexão do banco de dados jdbc:postgresql aponta para o endereço IP externo do nó PostgreSQL mestre.
 - a No appliance do vRealize Automation, abra um novo prompt de comando.
 - b Navegue até `/etc/vcac/server.xml` e faça backup do arquivo `server.xml`.
 - c Abra o arquivo `server.xml`.

- d Se necessário, edite a entrada do arquivo `server.xml` jdbc:postgresql para indicar o banco de dados PostgreSQL que você deseja usar.
 - Para um banco de dados externo do PostgreSQL, digite o endereço IP externo do nó mestre do PostgreSQL.
 - Para um banco de dados incorporado do PostgreSQL, digite o endereço IP do nó mestre do PostgreSQL.

Por exemplo, `jdbc:postgresql://198.15.100.60:5432/vcac`

Procedimentos

- 1 Abra o console de gerenciamento do appliance do vRealize Automation para o upgrade.
 - a Em cada appliance do vRealize Automation secundário, faça login no Gerenciamento do Appliance do vRealize Automation como **raiz** usando a senha que você inseriu quando implantou o appliance do vRealize Automation.
 - b Faça login com o nome de usuário **root** e a senha que você inseriu quando implantou o appliance.
 - c Clique em **Atualizar**.
- 2 Clique em **Configurações**.
- 3 Selecione para baixar as atualizações de um repositório VMware ou de um CDROM na seção Repositório de Atualizações.
- 4 Clique em **Status**.
- 5 Clique em **Verificar atualizações** para verificar se uma atualização pode ser acessada.
- 6 Clique em **Instalar Atualizações**.
- 7 Clique em **OK**.

É exibida uma mensagem informando que a atualização está em andamento.
- 8 (Opcional) Se você não tiver redimensionado manualmente o Disco de 1 GB para 50 GB, execute as seguintes etapas.
 - a Quando o sistema solicitar que você reinicialize o appliance virtual, clique na guia **Sistema** e clique em **Reinicializar**.

Durante a reinicialização, o sistema ajusta o espaço no Disco 1 necessário para a atualização.
 - b Após a reinicialização do sistema, faça logout e login novamente no console de gerenciamento do Appliance do vRealize Automation e selecione **Atualizar > Status**.
 - c Clique em **Verificar Atualizações** e **Instalar Atualizações**.
- 9 Para verificar se a atualização está progredindo com sucesso, abra os arquivos de registro.
 - `/opt/vmware/var/log/vami/vami.log`
 - `/opt/vmware/var/log/vami/updatecli.log`

- /var/log/vmware/horizon/horizon.log
- /var/log/bootstrap/*.log

Se você fizer logoff durante o processo de atualização e voltar a fazer login, poderá continuar acompanhando o progresso da atualização no arquivo de log /opt/vmware/var/log/vami/updatecli.log.

O tempo gasto até a conclusão da atualização depende do seu ambiente.

- 10 Quando concluída a atualização, faça logout do console de gerenciamento do Appliance do vRealize Automation, limpe o cache do navegador da Web e faça login no console de gerenciamento do Appliance do vRealize Automation.
- 11 Reinicie o appliance virtual.
 - a Clique em **Sistema**.
 - b Clique em **Reiniciar** e confirme a seleção.
- 12 Após a reinicialização do appliance virtual, efetue login no console de gerenciamento de réplica do Appliance do vRealize Automation.
- 13 Selecione **Configurações do vRA > Cluster**.
- 14 Digite seu nome de usuário e senha mestres do Appliance do vRealize Automation.
- 15 Clique em **Unir cluster**.
- 16 Clique em **Serviços** e verifique se cada serviço, exceto iaas-service, está listado como REGISTRADO.

Próximo passo

[Atualizar os componentes do servidor de IaaS após atualizar o vRealize Automation.](#)

Atualizar os componentes do servidor de IaaS após atualizar o vRealize Automation

Após atualizar o vRealize Automation 6.2.5 para 7.4, um administrador do sistema atualiza os componentes do servidor IaaS, incluindo o banco de dados Microsoft SQL Server.

Você tem duas opções para atualizar os componentes do servidor de IaaS.

- Utilizar a atualização IaaS automática do script shell.
- Use o arquivo executável do instalador do IaaS do vRealize Automation 7.4.

Se você tiver um componente de Catálogo de Componentes Comuns instalado, deverá desinstalar esse componente antes da atualização. Depois de concluir a atualização, será possível reinstalar o componente com a versão apropriada. Para obter mais informações, consulte o *Guia de Instalação do Catálogo de Componentes Comuns*. Se este guia não estiver disponível, use o procedimento alternativo na [Lista de verificação para atualizar o vRealize Automation](#).

Atualizar os componentes do IaaS usando o script do shell de atualização

Use o script do shell de atualização para atualizar os componentes do IaaS após atualizar cada appliance do vRealize Automation 6.2.5 para o 7.4.

A Appliance do vRealize Automation primária ou mestre atualizada contém um shell script que você usa para atualizar cada nó e componente de IaaS.

Você pode executar o script de atualização usando o console do vSphere para a máquina virtual ou usando uma sessão do console de SSH. Se você usar o console vSphere, poderá evitar problemas intermitentes de conectividade de rede que podem interromper a execução do script.

Se você interromper o script enquanto ele estiver atualizando um componente, o script é executado até que a atualização esteja terminada no componente. Se quaisquer componentes no nó não estiverem atualizados, você deverá executar o script novamente.

Quando a atualização estiver concluída, você poderá revisar o resultado da atualização abrindo o arquivo de log em `/usr/lib/vcac/tools/upgrade/upgrade.log`.

Pré-requisitos

- Verifique a atualização bem-sucedida de todos os appliances do vRealize Automation.
- Se você reiniciar um servidor IaaS após atualizar todos os appliances do vRealize Automation, você deve encerrar os serviços Windows IaaS. Antes de atualizar os componentes IaaS, encerre todos os serviços Windows IaaS, exceto o serviço do Management Agent, no servidor.
- Antes de executar o shell script de atualização no nó mestre ou primário Appliance do vRealize Automation, certifique-se que cada serviço esteja REGISTRADO.
 - a Vá para o appliance do console de gerenciamento do appliance virtual usando o nome de domínio totalmente qualificado, `https://va-hostname.domain.name:5480`.
 - b Faça login usando o nome de usuário **raiz** e a senha que você inseriu quando o appliance foi implantado.
 - c Clique em **Serviços**.
 - d Verifique se cada serviço, exceto o `iaas-service`, está REGISTRADO.
- Atualize o Management Agent em cada máquina virtual IaaS do vRealize Automation.
 - a Abra um navegador e vá até a página Instalação de IaaS do VMware vRealize Automation na appliance vRealize Automation usando o nome de domínio totalmente qualificado, `https://virtual_appliance_host:5480/installer`.
 - b Clique em **Instalador do Management Agent**.

Por padrão, o instalador é baixado para a pasta Downloads.
 - c Faça login em cada máquina virtual do IaaS do vRealize Automation e atualize o Agente de gerenciamento com o arquivo do **instalador do Agente de gerenciamento**.
- Verifique se o nó de site IaaS primário no qual os dados do Model Manager estão instalados tem o JAVA SE Runtime Environment 8, 64 bits, atualização 161 ou versão posterior, instalado. Depois de instalar o Java, você deve configurar a variável de ambiente, `JAVA_HOME`, como a nova versão.

- Faça login em cada nó do site de IaaS e verifique se a data de criação é anterior à data de modificação no arquivo `web.config`. Se a data de criação do arquivo `web.config` for igual ou posterior à data de modificação, realize o procedimento descrito em [Falha na atualização para o componente do site do IaaS](#)
 - Para verificar se todos os nós de IaaS possuem um Agente de Gerenciamento de IaaS atualizado, execute estas etapas em cada nó.
 - a Faça login no vRealize Automation console de gerenciamento do appliance.
 - b Selecione **Configurações do vRA > Cluster**.
 - c Expanda a lista de todos os componentes instalados em cada nó de IaaS e localize o Agente de Gerenciamento de IaaS.
 - d Verifique se a versão do Agente de Gerenciamento é a atual.
 - Verifique se o backup do banco de dados Microsoft SQL Server IaaS está acessível caso você precise fazer uma reversão.
 - Exclua todos os nós de IaaS órfãos. Consulte [Excluir nós órfãos no vRealize Automation](#).
 - Verifique se os snapshots dos servidores do IaaS na sua implantação estão disponíveis.
- Se a atualização não for concluída com sucesso, volte ao snapshot e backup do banco de dados e tente atualizar novamente.

Procedimentos

- 1 Abra uma nova sessão do console no nó da instância primária ou mestre do Appliance do vRealize Automation e faça login com a conta raiz.

Se planeja executar o script de atualização com o SSH, abra uma sessão do console de SSH.

- 2 Altere os diretórios para `/usr/lib/vcac/tools/upgrade/`.
- 3 No prompt, execute este comando para criar o arquivo `upgrade.properties`.

```
./generate_properties
```

- 4 Abra o arquivo `upgrade.properties` e insira todos os valores obrigatórios.

Esta tabela mostra os valores obrigatórios, que variam conforme o ambiente. Por exemplo, em um nó contendo um DEM Worker ou Orchestrator, as credenciais de DEM são obrigatórias.

| Valor obrigatório | Descrição | Formato da credencial | Valor de exemplo |
|---------------------------|--|-----------------------|---------------------------------|
| <code>web_username</code> | Nome de usuário do nó Web primário. Obrigatório somente uma vez. | Domínio\Usuário | <code>iaasDomain\webuser</code> |
| <code>web_password</code> | Senha do nó Web primário. Obrigatório somente uma vez. | Senha | <code>pa\$\$w0rd!</code> |

| Valor obrigatório | Descrição | Formato da credencial | Valor de exemplo |
|---------------------|--|-----------------------|-----------------------|
| dem_username | Nome de usuário do DEM Worker ou DEM Orchestrator. Obrigatório para todos os nós onde um componente de DEM está instalado. | Domínio\Usuário | iaasDomain\demuser |
| dem_password | Senha do DEM Worker ou DEM Orchestrator. Obrigatório para todos os nós onde um componente de DEM está instalado. | Senha | pa\$\$w0rd! |
| agent_username | Nome de usuário de um agente, como um agente vSphere. Obrigatório para todos os nós onde um componente de agente está instalado. | Domínio\Usuário | iaasDomain\agent_user |
| agent_password | Senha de um agente, como um agente vSphere. Obrigatório para todos os nós onde um componente de agente está instalado. | Senha | pa\$\$w0rd! |
| vidm_admin_password | A senha do administrador de VIDM. Necessário somente ao atualizar a partir do vRealize Automation 6.2.5. | vidm_password | pa\$\$w0rd! |

Por motivos de segurança, o arquivo `upgrade.properties` é removido quando você executa o shell script de atualização. As propriedades do arquivo são definidas usando as informações de cada componente de IaaS que vem através dos Agentes de Gerenciamento de IaaS. É importante que todas as instâncias do IaaS Management Agent sejam atualizadas e estejam íntegras antes da execução dos scripts de shell do `./generate_properties` ou `./upgrade_from_62x`. Se algum Agente de Gerenciamento de IaaS apresentar um problema quando você executar o shell script de atualização, consulte [Falha na atualização do Agente de Gerenciamento](#). Para recriar o arquivo `upgrade.properties`, repita as etapas 2 e 3.

5 Execute o script de atualização.

- a No prompt de comando, insira `./upgrade_from_62x`.
- b Pressione Enter.

O script exibe todos os nós de IaaS e todos os componentes instalados neles. O script valida todos os componentes antes de instalar a atualização. O script vai falhar caso existam valores incorretos no arquivo `upgrade.properties`.

O primeiro componente do servidor IaaS pode demorar 30 minutos ou mais para ser finalizado. Durante a atualização, você verá uma mensagem semelhante a `Upgrading server components for node web1-vra.mycompany.com`.

Se o Shell Script de Atualização falhar, revise o arquivo `upgrade.log`.

Você poderá executar o script de atualização novamente depois de corrigir os problemas. Antes de executar o script de atualização novamente, recrie o arquivo `upgrade.properties`, abra-o e insira todos os valores obrigatórios.

- 6 (Opcional) Ative o failover automático do Manager Service. Consulte [Ativar o Failover automático do Manager Service após a atualização](#).

Próximo passo

[Restaurar o acesso ao centro de controle integrado do vRealize Orchestrator](#).

Atualizando os componentes do laaS usando o instalador do laaS

Você pode usar esse método alternativo para atualizar os componentes do laaS depois de atualizar o vRealize Automation 6.2.5 para 7.4.

Baixar o instalador do laaS para atualizar os componentes do laaS

Após a atualização do vRealize Automation 6.2.5 para 7.4, baixe o instalador do laaS na máquina virtual onde estão instalados os componentes do laaS a serem atualizados.

Se receber avisos de certificado durante tal procedimento, você poderá ignorá-los.

Observação Exceto por uma instância de backup passiva do Serviço de Gerenciador, o tipo de inicialização para todos os serviços deve ser definido como Automático durante o processo de atualização. Se você definir os serviços para Manual, o processo de atualização falha.

Pré-requisitos

- Verifique se o Microsoft .NET Framework 4.5.2 ou posterior está instalado na máquina virtual de instalação do laaS. Você pode baixar o instalador do .NET da página de instalação laaS do VMware vRealize Automation. Se você atualizar o .NET para 4.5.2 após encerrar os serviços, a máquina virtual deve reiniciar como parte da instalação. Quando isso acontece, você deve parar manualmente todos os serviços do laaS na máquina virtual, exceto o Management Agent.
- Se você estiver usando o Internet Explorer para fazer o download, verifique se a Configuração de Segurança Reforçada está ativada. Insira `res://iesetup.dll/SoftAdmin.htm` na barra de pesquisa e pressione Enter.
- Faça login como administrador local no servidor Windows no qual um ou mais componentes do laaS que você deseja atualizar estão instalados.

Procedimentos

- 1 Abra um navegador da Web.
- 2 Insira o URL para a página de instalação do laaS VMware vRealize Automation.

Por exemplo, `https://vcac-va-hostname.domain.name:5480/installer`, em que `vcac-va-hostname.domain.name` é o nome do nó primário ou mestre do appliance do vRealize Automation.

- 3 Clique em **Instalador do laaS**.

- 4 O arquivo instalador, `setup__vcac-va-hostname.domain.name@5480.exe`, por padrão, é enviado para a pasta de Downloads.

Não altere o nome do arquivo. Ele é utilizado para conectar a instalação ao appliance do vRealize Automation.

Próximo passo

- Se tiver um vRealize Orchestrator autônomo, consulte [Atualizando o appliance autônomo do vRealize Orchestrator para uso com o vRealize Automation](#).
- Se você tiver um cluster de appliances vRealize Orchestrator externo, consulte [Atualizando o cluster do appliance externo do vRealize Orchestrator para uso com o vRealize Automation](#).
- Consulte [Atualizar os componentes do IaaS após atualizar o vRealize Automation](#).

Atualizar os componentes do IaaS após atualizar o vRealize Automation

Depois de atualizar o vRealize Automation 6.2.5 para 7.4, você deve atualizar o banco de dados PostgreSQL e configurar todos os sistemas com componentes do IaaS instalados. Você pode usar estas etapas para instalações mínimas e distribuídas.

Observação O instalador do IaaS deve estar na máquina virtual que contém os componentes IaaS que você deseja atualizar. Você não pode executar o instalador de uma localização externa, exceto para o banco de dados do Microsoft SQL que também pode ser atualizado remotamente por meio do nó da Web.

Verifique se os snapshots dos servidores do IaaS na sua implantação estão disponíveis. Se ocorrer falha na atualização, você poderá voltar para o snapshot e tentar outra atualização.

Execute a atualização para que os serviços sejam atualizados na seguinte ordem:

- 1 Sites do IaaS

Se você estiver usando um balanceador de carga, desative o tráfego para todos os nós não primários.

Conclua a atualização em um servidor antes de atualizar o próximo servidor que está executando um serviço de site. Comece com um que tenha o componente de dados do Model Manager instalado.

Se você estiver realizando uma atualização externa manual do banco de dados do Microsoft SQL, deverá atualizar o SQL externo antes de atualizar o nó da Web. Você pode atualizar um SQL externo remotamente no nó da Web.

- 2 Manager Services

Atualize o Manager Service ativo antes de atualizar o Manager Service passivo.

Se você não tem a criptografia SSL ativada na sua instância SQL, desmarque **Criptografia SSL** na caixa de diálogo de configuração da Atualização do IaaS.

- 3 Orchestrator e trabalhadores do DEM

Atualize todos os orchestrators e trabalhadores do DEM. Conclua a atualização em um servidor antes de atualizar o próximo.

4 Agentes

Conclua a atualização em um servidor antes de atualizar o próximo que está executando um agente.

5 Agente de gerenciamento

É atualizado como parte do processo de atualização.

Se você estiver usando diferentes serviços em um servidor, a atualização atualiza os serviços na ordem correta. Por exemplo, se o site tiver serviços de website e de gerente no mesmo servidor, selecione ambos para a atualização. O instalador da atualização aplica as atualizações na ordem correta. É possível concluir a atualização em um servidor antes de iniciar uma atualização em outro.

Observação Se a implantação usa um balanceador de carga, o primeiro appliance que você planeja atualizar deve ser conectado ao balanceador de carga. Todas as outras instâncias do Appliance do vRealize Automation devem ser desativadas para o tráfego do balanceador de carga antes de se aplicar a atualização para evitar erros de cache.

Pré-requisitos

- Faça backup do seu ambiente existente do vRealize Automation 6.2.5.
- Se você reiniciar um servidor IaaS após atualizar todas as appliances do vRealize Automation, você deve encerrar os serviços Windows IaaS. Antes de atualizar os componentes IaaS, encerre todos os serviços Windows IaaS, exceto o serviço do Management Agent, no servidor.
- [Baixar o instalador do IaaS para atualizar os componentes do IaaS.](#)
- Verifique se o nó primário do site IaaS no qual os dados do Model Manager estão instalados tem a versão Java adequada. É preciso ter o JAVA SE Runtime Environment 8, 64 bits, atualização 161 ou posterior, instalado. Após instalar o Java, configure a variável de ambiente, JAVA_HOME, como a nova versão.
- Verifique se a data de criação é anterior à data de modificação no arquivo `web.config`. Se a data de criação do arquivo `web.config` for igual ou posterior à data de modificação, realize o procedimento descrito em [Falha na atualização para o componente do site do IaaS](#)
- Se você estiver atualizando do vRealize Automation 6.2.5 e tem um banco de dados Microsoft SQL externo, você deve ter a versão adequada do Management Agent. O Management Agent no banco de dados externo deve ser da versão 7.0 ou superior antes de executar a atualização do site IaaS. Você pode verificar a versão do Management Agent no painel de controle da sua máquina virtual externa SQL. Se o Management Agent não for a versão 7.0 ou superior, faça os seguintes passos para atualizar o Management Agent.
 - a Abra um navegador e navegue até a página Instalação de IaaS do VMware vRealize Automation em Appliance do vRealize Automation usando o nome de domínio totalmente qualificado, `https://virtual_appliance_host:5480/installer`.
 - b Clique em **Instalador do Management Agent**.
Por padrão, o instalador é baixado para a pasta Downloads.

- c Faça login no banco de dados externo, atualize o Management Agent com o arquivo do **instalador do Management Agent** reinicie o serviço Management Agent do Windows.
- Se você tiver um componente de Catálogo de Componentes Comuns instalado, deverá desinstalar esse componente antes da atualização. Para obter mais informações, consulte o *Guia de Instalação do Catálogo de Componentes Comuns* ou siga as etapas fornecidas no [Lista de verificação para atualizar o vRealize Automation](#).

Procedimentos

- 1 Se você estiver usando um balanceador de carga, prepare o ambiente.
 - a Verifique se o nó do site de IaaS que contém os dados do Model Manager está ativado para tráfego do balanceador de carga.
É possível identificar este nó pela presença da pasta `vCAC Folder\Server\ConfigTool`.
 - b Desabilite todos os outros sites de IaaS e Manager Services não primários para o tráfego do balanceador de carga.
- 2 Clique com o botão direito do mouse no arquivo de configuração `setup__vrealize-automation-appliance-FQDN@5480.exe` e selecione **Executar como administrador**.
- 3 Clique em **Avançar**.
- 4 Aceite o contrato de licença e clique em **Avançar**.
- 5 Insira as credenciais de administrador para a implantação atual na página de Login.
O nome de usuário é **raiz**, e a senha é aquela que você especificou durante a implantação do appliance.
- 6 Selecione **Aceitar Certificado**.
- 7 Na página **Tipo de instalação**, confirme que **Atualizar** está marcada.
Se **Atualizar** não estiver selecionada, os componentes deste sistema já foram atualizados para esta versão.
- 8 Clique em **Avançar**.
- 9 Defina as configurações de atualização.

| Opção | Ação |
|---|--|
| Se você estiver atualizando o Model Manager Data | Marque a caixa de seleção Model Manager Data na seção Servidor vCAC. A caixa de seleção aparece selecionada por padrão. Atualize o Model Manager Data apenas uma vez. Quando você atualiza uma instalação distribuída, os servidores web param de funcionar enquanto há um desacordo de versão entre os servidores Web e os dados do Model Manager. Quando a atualização dos dados do Model Manager termina, o servidor Web volta a funcionar normalmente. |
| Se você estiver atualizando dados do Model Manager | Desmarque a caixa de seleção Dados do Model Manager na seção Servidor vCAC. |

| Opção | Ação |
|--|--|
| Para preservar fluxos de trabalho personalizados como a versão mais recente no Model Manager Data | <p>Se você estiver atualizando o Model Manager Data, marque a caixa de seleção Preservar as versões mais recentes do fluxo de trabalho na seção Fluxos de trabalho de extensibilidade.</p> <p>A caixa de seleção aparece selecionada por padrão. Os fluxos de trabalho personalizados são sempre preservados. Ao selecionar a caixa de seleção é determinada apenas a ordem da versão. Se você tiver fluxos de trabalho personalizados no Model Manager, selecione essa opção para que o fluxo de trabalho mais recente permaneça como a versão mais recente após a atualização.</p> <p>Se você não selecionar essa opção, a versão de cada fluxo de trabalho fornecido com o vRealize Automation Designer torna-se a mais recente após a atualização. A versão mais recente antes da atualização torna-se a segunda mais recente.</p> <p>Para obter mais informações sobre vRealize Automation Designer, consulte <i>Extensibilidade do ciclo de vida</i>.</p> |
| Se você estiver atualizando um Distributed Execution Manager ou um agente proxy | <p>Digite as credenciais da conta de administrador na seção Conta de serviço.</p> <p>Todos os serviços que você atualiza são executados nesta conta.</p> |
| Para especificar seu banco de dados do Microsoft SQL Server | <p>Se você atualizar os dados do Model Manager, insira os nomes dos servidores do banco de dados e da instância do banco de dados na caixa de texto Servidor. Digite um nome de domínio totalmente qualificado (FQDN) para o nome do servidor de banco de dados na caixa de seleção Nome do banco de dados.</p> <p>Se a instância do banco de dados estiver em uma porta SQL não padrão, inclua o número da porta na especificação de instância do servidor. O número de porta padrão do Microsoft SQL é 1433.</p> <p>Ao atualizar os nós do gerenciador, a opção MSSQL SSL é selecionada por padrão. Se o seu banco de dados não usar SSL, desmarque a opção Usar SSL para conexão do banco de dados.</p> |

10 Clique em **Avançar**.

11 Confirme que todos os serviços a serem atualizados aparecem na página Pronto para Atualizar e clique em **Atualizar**.

A página Atualizar e um indicador de progresso aparecem. Quando o processo de atualização terminar, o botão **Avançar** é ativado.

12 Clique em **Avançar**.

13 Clique em **Concluir**.

14 Confirme que todos os serviços reiniciaram.

15 Repita essas etapas para cada servidor do IaaS da implantação na ordem definida.

16 Após a instalação de todos os componentes, faça login no console de gerenciamento do appliance e confirme que todos os serviços, incluindo o IaaS, estão registrados agora.

Todos os componentes selecionados são atualizados para a nova versão.

Próximo passo

- [Restaurar o acesso ao centro de controle integrado do vRealize Orchestrator.](#)

- Se a sua implantação usa um balanceador de carga, atualize todos os nós desse balanceador para que eles utilizem verificações de integridade do vRealize Automation. Reabilite o tráfego do balanceador de carga para todos os nós desconectados. Se a sua implementação anterior usava um banco de dados PostgreSQL incorporado com balanceamento de carga, desative todos os nós no pool do PostgreSQL porque eles não são necessários. Exclua o pool quando for conveniente.

Para obter mais informações, consulte [Balanceamento de carga do vRealize Automation](#).

- (Opcional) Ative o failover automático do Manager Service. Consulte [Ativar o Failover automático do Manager Service após a atualização](#).

Restaurar o acesso ao centro de controle integrado do vRealize Orchestrator

Depois de atualizar os componentes do servidor IaaS, você deve restaurar o acesso para o vRealize Orchestrator.

Ao atualizar o vRealize Automation 6.2.5 para 7.4, você precisa executar este procedimento para acomodar o novo recurso de Controle de Acesso Baseado em Função. Esse procedimento é escrito para um ambiente de alta disponibilidade.

Pré-requisitos

Faça um snapshot do seu ambiente do vRealize Automation.

Procedimentos

- 1 Faça login no console de gerenciamento do Appliance do vRealize Automation como raiz usando o nome de domínio totalmente qualificado do host do appliance, `https://va-hostname.domain.name:5480`.
- 2 Selecione **Configurações do vRA > Banco de Dados**.
- 3 Identifique os nós mestre e de réplica.
- 4 Em cada nó de réplica, abra uma sessão SSH, faça login como administrador e execute este comando:

```
service vco-server stop && service vco-configurator stop
```
- 5 No nó mestre, abra uma sessão SSH, faça login como administrador e execute este comando:

```
rm /etc/vco/app-server/vco-registration-id
```
- 6 No nó mestre, altere os diretórios para `/etc/vco/app-server/`.
- 7 Abra o arquivo `sso.properties`.

8 Se o nome da propriedade `com.vmware.o11n.sso.admin.group.name` contiver espaços ou quaisquer outros caracteres relacionados à Bash que possam ser aceitos como um caractere especial em um comando de Bash, como um hífen (-) ou um sinal de dinheiro (\$), conclua estas etapas.

- a Copie a linha com a propriedade `com.vmware.o11n.sso.admin.group.name` e insira `AdminGroup` para o valor.
- b Adicione `#` ao início da linha original com a propriedade `com.vmware.o11n.sso.admin.group.name` para comentar na linha.
- c Salve e feche o arquivo `sso.properties`.

9 Execute este comando:

```
vcac-vami vco-service-reconfigure
```

10 Se você concluiu a etapa 8, abra o arquivo `sso.properties` e conclua estas etapas.

- a Remova o `#` do começo da linha original com a propriedade `com.vmware.o11n.sso.admin.group.name` para retirar o comentário da linha.
- b Remova a cópia da linha com a propriedade `com.vmware.o11n.sso.admin.group.name`.
- c Salve e feche o arquivo `sso.properties`.

11 Execute este comando para reiniciar o serviço `vco-server`:

```
reiniciar o serviço vco-server
```

12 Execute este comando para reiniciar o serviço `vco-configurator`:

```
reiniciar o serviço vco-configurator
```

13 No console de gerenciamento do Appliance do vRealize Automation, clique em **Serviços** e espere até que todos os serviços no nó mestre estejam registrados.

14 Quando todos os serviços estiverem registrados, ingresse os nós de réplica vRealize Automation ao cluster do vRealize Automation para sincronizar a configuração do vRealize Orchestrator. Para obter informações, consulte [Reconfigurar o vRealize Orchestrator integrado para dar suporte à alta disponibilidade](#).

Próximo passo

[Atualizando o vRealize Orchestrator após a atualização do vRealize Automation](#).

Atualizando o vRealize Orchestrator após a atualização do vRealize Automation

Você deve atualizar sua instância do vRealize Orchestrator após a atualização do vRealize Automation 6.2.5 para o 7.4.

Com o lançamento do vRealize Orchestrator 7.4, você tem duas opções para atualizar o vRealize Orchestrator após uma atualização bem-sucedida para o vRealize Automation 7.4.

- Você pode migrar seu servidor vRealize Orchestrator externo existente para um vRealize Orchestrator incluído no vRealize Automation 7.4.
- Você pode atualizar o seu servidor vRealize Orchestrator autônomo ou em cluster existente para funcionar com o vRealize Automation 7.4.

Migrando um servidor externo do vRealize Orchestrator para o vRealize Automation

Você pode migrar o servidor externo existente do vRealize Orchestrator para uma instância do vRealize Orchestrator incorporada no vRealize Automation 7.4.

Você pode implantar o vRealize Orchestrator como uma instância do servidor externo e configurar o vRealize Automation para funcionar com essa instância externa, ou você pode configurar e usar o servidor vRealize Orchestrator que está incluído no Appliance do vRealize Automation.

A VMware recomenda que você migre o vRealize Orchestrator externo para o servidor Orchestrator que está incorporado no vRealize Automation. A migração de um Orchestrator externo para um incorporado fornece os seguintes benefícios:

- Reduz o custo total de propriedade.
- Simplifica o modelo de implantação.
- Melhora a eficiência operacional.

Observação Considere utilizar o vRealize Orchestrator externo nos seguintes casos:

- Múltiplos tenants no ambiente vRealize Automation
 - Ambiente geográfico disperso
 - Manipulação da carga de trabalho
 - Utilização de plug-ins específicos, como o plug-in Site Recovery Manager das versões antigas
-

As diferenças do Centro de Controle entre o Orchestrator externo e integrado

Alguns dos itens de menu que estão disponíveis no Centro de Controle de um vRealize Orchestrator externo não estão incluídos na exibição padrão do Centro de Controle de uma instância integrada do Orchestrator.

No centro de controle do servidor do Orchestrator integrado, algumas opções estão ocultas por padrão.

| Item de Menu | Detalhes |
|---------------------------------------|--|
| Licenciamento | O Orchestrator integrado está pré-configurado para usar o vRealize Automation como um provedor de licença. |
| Configuração de Exportação/Importação | A configuração do Orchestrator integrada está incluída nos componentes exportados do vRealize Automation. |

| Item de Menu | Detalhes |
|--|--|
| Configurar banco de dados | O Orchestrator integrado usa o banco de dados que é usado pelo vRealize Automation. |
| Programa de Aperfeiçoamento da Experiência do Cliente | Você pode se associar ao Programa de Aperfeiçoamento da Experiência do Cliente (PAEC) na interface de gerenciamento do appliance vRealize Automation. Consulte o <i>Programa de Aperfeiçoamento da Experiência do Cliente em Gerenciando o vRealize Automation</i> . |

Outras opções que estão ocultas na exibição padrão do Centro de Controle são a caixa de texto do **endereço do host** e o botão **CANCELAR REGISTRO** na página **Configurar Provedor de Autenticação**.

Observação Para consultar todo o conjunto de opções do Centro de Controle no vRealize Orchestrator que está integrado em vRealize Automation, você deve acessar a página avançada de Gerenciamento do Orchestrator em https://vra-va-hostname.domain.name_or_load_balancer_address:8283/vco-controlcenter/#!/?advanced e clicar no botão F5, no teclado para atualizar a página.

Migrar um vRealize Orchestrator externo no Windows para o vRealize Automation

Depois de atualizar o vRealize Automation da versão 6.x para a versão 7.4, você pode migrar seu Orchestrator 6.x externo existente instalado no Windows para o servidor Orchestrator integrado ao vRealize Automation 7.4.

Observação Se você tem um ambiente vRealize Automation distribuído com múltiplos nós vRealize Automation, execute o procedimento de migração apenas no nó primário vRealize Automation.

Pré-requisitos

- Migração bem-sucedida para o vRealize Automation 7.4.
- Pare o serviço do servidor Orchestrator no Orchestrator externo.
- Faça backup do banco de dados, incluindo o esquema do banco de dados do servidor Orchestrator externo.

Procedimentos

- 1 Baixe a ferramenta de migração do servidor de destino do Orchestrator.
 - a Faça login no appliance do vRealize Automation pelo SSH como **raiz**.
 - b Baixe o arquivo `migration-tool.zip` que está localizado no diretório `/var/lib/vco/downloads`.
- 2 Exporte a configuração do Orchestrator do servidor do Orchestrator de origem.
 - a Defina a variável do ambiente `PATH` apontando-a para pasta `lixreira` do Java JRE instalado com o Orchestrator.
 - b Carregue a ferramenta de migração para o servidor Windows no qual o Orchestrator externo está instalado.

- c Extraia o arquivo baixado na pasta de instalação do Orchestrator.

O caminho padrão para a pasta de instalação do Orchestrator em uma instalação padrão do Windows é C:\Program Files\VMware\Orchestrator.

- d Execute o comando prompt do Windows como administrador e navegue para a pasta da lixeira na pasta de instalação do Orchestrator.

Por padrão, o caminho para a pasta de lixeira é C:\Program Files\VMware\Orchestrator\migration-cli\bin.

- e Execute o comando export da linha de comando.

```
C:\Program Files\VMware\Orchestrator\migration-cli\bin\vro-migrate.bat export
```

Esse comando combina os arquivos de configuração e plug-ins do vRealize Orchestrator em um arquivo de exportação.

O arquivo é criado na mesma pasta que a pasta migration-cli.

- 3 Migre a configuração exportada para o servidor Orchestrator incorporado no vRealize Automation 7.4.

- a Carregue o arquivo exportado de configuração para o diretório /usr/lib/vco/tools/configuration-cli/bin no Appliance do vRealize Automation.

- b No diretório /usr/lib/vco/tools/configuration-cli/bin, altere a propriedade do arquivo exportado de configuração do Orchestrator.

```
chown vco:vco orchestrator-config-export-orchestrator_ip_address-date_hour.zip
```

- c Importe o arquivo de configuração do Orchestrator para o servidor integrado vRealize Orchestrator, ao executar o script vro-configure com o comando import.

```
./vro-configure.sh import --skipDatabaseSettings --skipLicense --skipSettings --skipSslCertificate --notForceImportPlugins --notRemoveMissingPlugins --skipTrustStore --path orchestrator-config-export-orchestrator_appliance_ip-date_hour.zip
```

- 4 Migre o banco de dados para o banco de dados PostgreSQL interno, executando o script vro-configure com o comando db-migrate.

```
./vro-configure.sh db-migrate --sourceJdbcUrl JDBC_connection_URL --sourceDbUsername database_user
--sourceDbPassword database_user_password
```

Observação Coloque entre aspas simples as senhas que contenham caracteres especiais.

O *JDBC_connection_URL* depende do tipo de banco de dados que você usa.

PostgreSQL: `jdbc:postgresql://host:port/database_name`

MSSQL: `jdbc:jtds:sqlserver://host:port/database_name\;` if using SQL authentication and MSSQL:
`jdbc:jtds:sqlserver://host:port/database_name\;domain=domain\;useNTLMv2=TRUE` if using Windows authentication.

Oracle: `jdbc:oracle:thin:@host:port:database_name`

As informações de login do banco de dados padrão são:

| | |
|-------------------------------|--------|
| <i>database_name</i> | vmware |
| <i>database_user</i> | vmware |
| <i>database_user_password</i> | vmware |

- 5 Se você migrou o vRealize Automation em vez de atualizá-lo, exclua os certificados de Single Sign-On do banco de dados da instância integrada do Orchestrator.

```
sudo -u postgres -i -- /opt/vmware/vpostgres/current/bin/psql vcac -c "DELETE FROM vmo_keystore
WHERE id='cakeystore-id';"
```

Você migrou com sucesso um vRealize Orchestrator 6.x externo instalado no Windows para uma instância do vRealize Orchestrator incorporada no vRealize Automation 7.4.

Próximo passo

Definir o servidor integrado do vRealize Orchestrator. Consulte [Configure o Servidor vRealize Orchestrator integrado](#).

Migrar um appliance virtual do vRealize Orchestrator 6.x externo para o vRealize Automation 7.4

Depois de atualizar o vRealize Automation da versão 6.x para a versão 7.4, você pode migrar seu Appliance Virtual do Orchestrator 6.x externo existente para o servidor Orchestrator integrado ao vRealize Automation 7.4.

Observação Se você tem um ambiente vRealize Automation distribuído com múltiplos nós Appliance do vRealize Automation, execute o procedimento de migração apenas no nó primário vRealize Automation.

Pré-requisitos

- Migração bem-sucedida para o vRealize Automation 7.4.
- Pare o serviço do servidor Orchestrator no Orchestrator externo.
- Faça backup do banco de dados, incluindo o esquema do banco de dados do servidor Orchestrator externo.

Procedimentos

- 1 Baixe a ferramenta de migração do servidor de destino do Orchestrator para o Orchestrator de origem.
 - a Faça login para o Appliance Virtual 6.x vRealize Orchestrator pelo SSH como **raiz**.
 - b No diretório `/var/lib/vco`, execute o comando `scp` para baixar o arquivo `migration-tool.zip`.

```
scp root@vra-va-hostname.domain.name:/var/lib/vco/downloads/migration-tool.zip ./
```

- c Execute o comando `unzip` para extrair o arquivo da ferramenta de migração.

```
unzip migration-tool.zip
```

- 2 Exporte a configuração do Orchestrator do servidor do Orchestrator de origem.

- a No diretório `/var/lib/vco/migration-cli/bin`, execute o comando `export`.

```
./vro-migrate.sh export
```

Esse comando combina os arquivos de configuração e plug-ins do VMware vRealize Orchestrator em um arquivo de exportação.

Um arquivo com nome de arquivo `orchestrator-config-export-orchestrator_ip_address-date_hour.zip` é criado na pasta `/var/lib/vco`.

3 Migre a configuração exportada para o servidor Orchestrator incorporado no vRealize Automation 7.4.

- a Faça login para o Appliance do vRealize Automation pelo SSH como **raiz**.
- b No diretório `/usr/lib/vco/tools/configuration-cli/bin`, execute o comando `scp` para baixar o arquivo de configuração exportado.

```
scp root@orchestrator_ip_or_DNS_name:/var/lib/vco/orchestrator-config-export-orchestrator_ip_address-date_hour.zip ./
```

- c Altere a propriedade do arquivo de configuração exportado do Orchestrator.

```
chown vco:vco orchestrator-config-export-orchestrator_ip_address-date_hour.zip
```

- d Pare o serviço do servidor Orchestrator e o serviço do Centro de Controle do servidor vRealize Orchestrator integrado.

```
service vco-server stop && service vco-configurator stop
```

- e Importe o arquivo de configuração do Orchestrator para o servidor integrado vRealize Orchestrator, ao executar o script `vro-configure` com o comando `import`.

```
./vro-configure.sh import --skipDatabaseSettings --skipLicense --skipSettings --skipSslCertificate --notForceImportPlugins --notRemoveMissingPlugins --skipTrustStore --path orchestrator-config-export-orchestrator_appliance_ip-date_hour.zip
```

4 Se o servidor Orchestrator externo do qual você deseja migrar usar o banco de dados PostgreSQL integrado, edite os arquivos de configuração do banco de dados.

- a No arquivo `/var/vmware/vpostgres/current/pgdata/postgresql.conf`, remova o comentário da linha `listen_addresses`.
- b Defina os valores de `listen_addresses` para um caractere universal (*).

```
listen_addresses = '*'
```

- c Anexe a linha ao arquivo `/var/vmware/vpostgres/current/pgdata/pg_hba.conf`.

```
host all all vra-va-ip-address/32 md5
```

Observação O arquivo `pg_hba.conf` exige o uso de um prefixo do formato CIDR em vez de um endereço IP e de uma máscara de sub-rede.

- d Reinicia o serviço de servidor do PostgreSQL.

```
service vpostgres restart
```

- 5 Migre o banco de dados para o banco de dados PostgreSQL interno, executando o script vro-configure com o comando db-migrate.

```
./vro-configure.sh db-migrate --sourceJdbcUrl JDBC_connection_URL --sourceDbUsername database_user
--sourceDbPassword database_user_password
```

Observação Coloque entre aspas simples as senhas que contenham caracteres especiais.

O *JDBC_connection_URL* depende do tipo de banco de dados que você usa.

PostgreSQL: `jdbc:postgresql://host:port/database_name`

MSSQL: `jdbc:jtds:sqlserver://host:port/database_name\;` if using SQL authentication and MSSQL:
`jdbc:jtds:sqlserver://host:port/database_name\;domain=domain\;useNTLMv2=TRUE` if using Windows authentication.

Oracle: `jdbc:oracle:thin:@host:port:database_name`

As informações de login do banco de dados padrão são:

| | |
|-------------------------------|--------|
| <i>database_name</i> | vmware |
| <i>database_user</i> | vmware |
| <i>database_user_password</i> | vmware |

- 6 Se você migrou o vRealize Automation em vez de atualizá-lo, exclua os certificados de Single Sign-On do banco de dados da instância integrada do Orchestrator.

```
sudo -u postgres -i -- /opt/vmware/vpostgres/current/bin/psql vcac -c "DELETE FROM vmo_keystore
WHERE id='cakeystore-id';"
```

- 7 Reverte para a configuração padrão dos arquivos postgresql.conf e pg_hba.conf.

- a Reinicia o serviço de servidor do PostgreSQL.

Você migrou com sucesso um Appliance Virtual do vRealize Orchestrator 6.x externo para uma instância do vRealize Orchestrator incorporada no vRealize Automation 7.4.

Próximo passo

Definir o servidor integrado do vRealize Orchestrator. Consulte [Configure o Servidor vRealize Orchestrator integrado](#).

Configure o Servidor vRealize Orchestrator integrado

Depois de exportar a configuração de um servidor Orchestrator externo e importá-la para o vRealize Automation 7.4, você deve configurar o servidor Orchestrator integrado ao vRealize Automation.

Pré-requisitos

Migre a configuração do vRealize Orchestrator externo para o interno.

Procedimentos

- 1 Faça login para o Appliance do vRealize Automation pelo SSH como **raiz**.
- 2 Inicie o serviço do Centro de Controle e o serviço do servidor Orchestrator do servidor vRealize Orchestrator integrado.

```
service vco-configurator start && service vco-server start
```

- 3 Faça login no Centro de Controle do servidor Orchestrator integrado como um **administrador**.

Observação Se você migrar de uma instância externa do vRealize Orchestrator 7.4, pule para a etapa 5.

- 4 Verifique se o Orchestrator está configurado adequadamente na página **Validar Configuração** no Centro de controle.
- 5 Se o Orchestrator externo foi configurado para funcionar em modo cluster, reconfigure o cluster do Orchestrator em vRealize Automation.

- a Vá para a página avançada do **Gerenciamento do Cluster do Orchestrator** em https://vra-va-hostname.domain.name_or_load_balancer_address:8283/vco-controlcenter/#!/control-app/ha?remove-nodes.

Observação Se as caixas de seleção **Remove** ao lado dos nós existentes no cluster não aparecerem, você deve atualizar a página do navegador clicando no botão F5, no teclado.

- b Selecione as caixas de seleção ao lados dos nós do Orchestrator externo e clique em **Remove** para removê-los do cluster.
 - c Para sair da página de gerenciamento avançada do cluster, exclua a cadeia de caracteres `remove-nodes` do URL e atualize a página do navegador clicando no botão F5, no teclado.
 - d Na página **Validar Configuração** no Centro de Controle, verifique se o Orchestrator está configurado adequadamente.
- 6 (Opcional) Na guia **Certificado de Assinatura do Pacote** na página de **Certificados**, gere um novo certificado de assinatura do pacote.
 - 7 (Opcional) Altere os valores para **Tenant padrão** e **Grupo de Admin** na página **Configura Provedor de Autenticação**.
 - 8 Verifique se o serviço `vco-server` aparece como REGISTRADO na guia **Serviços** no console de gerenciamento do Appliance do vRealize Automation.
 - 9 Selecione os serviços do vco do servidor externo do Orchestrator e clique em **Cancelar o registro**.

Próximo passo

- Importe quaisquer certificados que eram confiáveis no servidor externo do Orchestrator para o armazenamento de confiança do Orchestrator integrado.
- Associe os nós de réplica do vRealize Automation ao cluster vRealize Automation para sincronizar a configuração do Orchestrator.

Para mais informações, consulte *Reconfigurar o vRealize Orchestrator integrado para suportar alta disponibilidade* em *Instalando ou Atualizando o vRealize Automation*.

Observação As instâncias vRealize Orchestrator são automaticamente clusterizadas e disponibilizadas para uso.

- Reinicie o serviço vco-configurator em todos os nós do cluster.
- Atualize o endpoint vRealize Orchestrator para apontar para o servidor Orchestrator integrado migrado.
- Adicione o host vRealize Automation e o host IaaS ao inventário do plug-in vRealize Automation ao executar Adicionar um host vRA e Adicionar o host IaaS de fluxos de trabalho de um host vRA.

Atualizando o appliance autônomo do vRealize Orchestrator para uso com o vRealize Automation

Se você mantiver um vRealize Orchestrator Appliance autônomo para uso com o vRealize Automation, será preciso atualizá-lo ao fazer a atualização do vRealize Automation da versão 6.2.5 para a versão 7.4.

As instâncias incorporadas do vRealize Orchestrator são atualizadas como parte da atualização do appliance do vRealize Automation. Nenhuma ação extra é necessária para instâncias integradas.

Se você estiver fazendo a atualização de um cluster de appliance do vRealize Orchestrator, veja [Atualizando o cluster do appliance externo do vRealize Orchestrator para uso com o vRealize Automation](#).

Pré-requisitos

- [Instalar a atualização no appliance do vRealize Automation](#).
- Atualize os componentes do IaaS conforme descrito em [Atualizar os componentes do servidor de IaaS após atualizar o vRealize Automation](#).
- Desmonte todos os sistemas do arquivo de rede. Consulte *Administração da Máquina virtual do vSphere* na documentação do vSphere.
- Aumente a memória do Orchestrator Appliance do vSphere para pelo menos 6 GB. Consulte *Administração da Máquina virtual do vSphere* na documentação do vSphere.
- Tire um snapshot da máquina virtual Orchestrator do vSphere. Consulte *Administração da Máquina virtual do vSphere* na documentação do vSphere.
- Se utilizar um banco de dados externo, faça backup dele.

- Se você usar o banco de dados PostgreSQL pré-configurado no Orchestrator vSphere, faça backup do banco de dados usando o menu **Exportar banco de dados** menu no Centro de controle do vSphere.

Procedimentos

- 1 Use um dos métodos documentados para atualizar o seu vRealize Orchestrator independente.
 - [Atualizar o Orchestrator Appliance usando o Repositório VMware padrão.](#)
 - [Atualizado o Orchestrator Appliance usando uma imagem ISO.](#)
 - [Atualizar o Orchestrator Appliance usando um Repositório Específico.](#)
- 2 No Centro de Controle, atualize o NSX plug-in do vRealize Automation.

Atualizar o Orchestrator Appliance usando o Repositório VMware padrão

Você pode configurar o Orchestrator para baixar o pacote de atualização do repositório VMware padrão.

Pré-requisitos

- Desmonte todos os sistemas do arquivo de rede. Para obter mais informações, consulte a documentação *Administração da Máquina Virtual vSphere*.
- Aumente a memória do Orchestrator Appliance para pelo menos 6 GB. Para obter mais informações, consulte a documentação *Administração da Máquina Virtual vSphere*.
- Aumente o tamanho do disco da máquina virtual do vRealize Orchestrator: Disco 1 = 7 GB, Disco 2 = 10 GB.
- Certifique-se de que a partição raiz do Orchestrator Appliance tenha pelo menos de 3 GB de espaço livre disponível. Para obter mais informações sobre como aumentar o tamanho de uma partição de disco, consulte KB 1004071: <http://kb.vmware.com/kb/1004071>.
- Tire um snapshot da máquina virtual Orchestrator. Para obter mais informações, consulte a documentação *Administração da Máquina Virtual vSphere*.
- Se utilizar um banco de dados externo, faça backup dele.
- Se você usar o pré-configurado no banco de dados Orchestrator PostgreSQL, faça backup do banco de dados usando o menu **Exportar banco de dados** menu no Centro de controle.

Procedimentos

- 1 Vá para a Interface de Gerenciamento do Appliance Virtual (VAMI) em https://orchestrator_server:5480 e faça login como **raiz**.
- 2 Na guia **Atualizar**, clique em **Configurações**.
O botão de seleção próximo da opção **Use o Repositório Especificado** está selecionado.
- 3 Na página **Status**, clique em **Verificar Atualizações**.
- 4 Se houver alguma atualização disponível, clique em **Instalar Atualizações**.
- 5 Aceite o acordo de licença do usuário final VMware e confirme que você deseja instalar a atualização.

- 6 Para concluir a atualização, reinicie o Orchestrator Appliance.
 - a Faça login novamente na Interface de Gerenciamento do Appliance Virtual (VAMI) como **raiz**.
- 7 (Opcional) Na guia **Atualizar**, verifique se a última versão do Orchestrator Appliance está instalada com sucesso.
- 8 Faça login no Control Center como **root**.
- 9 Se você planeja criar um cluster de instâncias do Orchestrator, redefina as configurações dos hosts.
 - a Na página **Configurações do Host** do Centro de Controle, clique em **CHANGE**.
 - b Insira o nome do host do servidor do balanceador de carga em vez de inserir o nome do appliance do vRealize Orchestrator.
- 10 Reconfigure a autenticação.
 - a Se, antes da atualização, o servidor Orchestrator foi configurado para usar **LDAP** ou **SSO (legado)** como o método de autenticação, configure o **vSphere** ou o **vRealize Automation** como um provedor de autenticação.
 - b Se a autenticação já estiver definida como **vSphere** ou **vRealize Automation**, remova as configurações e registre-as novamente.

Observação Se, antes da atualização, o Orchestrator tiver usado o **vSphere** como um provedor de autenticação e tiver sido configurado para se conectar ao nome de domínio totalmente qualificado ou endereço IP do vCenter Server, caso você tenha um Platform Services Controller externo, após a atualização, você deverá configurar o Orchestrator para conectar-se ao nome de domínio totalmente qualificado ou endereço IP da instância do Controlador de Serviços de Plataforma que contém o vCenter Single Sign-On. Você também deve importar para o Orchestrator manualmente os certificados de todos os Platform Services Controllers que compartilham o mesmo domínio do vCenter Single Sign-On.

Você atualizou com êxito o Orchestrator Appliance.

Próximo passo

Verifique se o Orchestrator está configurado adequadamente na página **Validar Configuração** no Centro de controle.

Atualizado o Orchestrator Appliance usando uma imagem ISO

Você pode configurar o Orchestrator para baixar o pacote de atualização de um arquivo de imagem ISO montado na unidade de CD-ROM do appliance.

Pré-requisitos

- Desmonte todos os sistemas do arquivo de rede. Para obter mais informações, consulte a documentação *Administração da Máquina Virtual vSphere*.
- Aumente a memória do Orchestrator Appliance para pelo menos 6 GB. Para obter mais informações, consulte a documentação *Administração da Máquina Virtual vSphere*.

- Aumente o tamanho do disco da máquina virtual do vRealize Orchestrator: Disco 1 = 7 GB, Disco 2 = 10 GB.
- Certifique-se de que a partição raiz do Orchestrator Appliance tenha pelo menos de 3 GB de espaço livre disponível. Para obter mais informações sobre como aumentar o tamanho de uma partição de disco, consulte KB 1004071: <http://kb.vmware.com/kb/1004071>.
- Tire um snapshot da máquina virtual Orchestrator. Para obter mais informações, consulte a documentação *Administração da Máquina Virtual vSphere*.
- Se utilizar um banco de dados externo, faça backup dele.
- Se você usar o pré-configurado no banco de dados Orchestrator PostgreSQL, faça backup do banco de dados usando o menu **Exportar banco de dados** menu no Centro de controle.

Procedimentos

- 1 Baixe o arquivo VMware-vRO-Appliance-version-build_number-updaterepo.iso do site de download oficial da VMware.
- 2 Conecte a unidade de CD-ROM da máquina virtual Orchestrator Appliance. Para obter mais informações, consulte a documentação *Administração da Máquina Virtual vSphere*.
- 3 Monte o arquivo de imagem ISO para a unidade CD-ROM do appliance. Para obter mais informações, consulte a documentação *Administração da Máquina Virtual vSphere*.
- 4 Vá para a Interface de Gerenciamento do Appliance Virtual (VAMI) em https://orchestrator_server:5480 e faça login como **raiz**.
- 5 Na guia **Atualizar**, clique em **Configurações**.
- 6 Selecione o botão de seleção próximo da opção **Use as atualizações do CD-ROM**.
- 7 Retorne para página de **Status**.
A versão da atualização disponível é exibida.
- 8 Clique em **Instalar Atualizações**.
- 9 Aceite o acordo de licença do usuário final VMware e confirme que você deseja instalar a atualização.
- 10 Para concluir a atualização, reinicie o Orchestrator Appliance.
 - a Faça login novamente na Interface de Gerenciamento do Appliance Virtual (VAMI) como **raiz**.
- 11 (Opcional) Na guia **Atualizar**, verifique se a última versão do Orchestrator Appliance está instalada com sucesso.
- 12 Faça login no Control Center como **root**.
- 13 Se você planeja criar um cluster de instâncias do Orchestrator, redefina as configurações dos hosts.
 - a Na página **Configurações do Host** do Centro de Controle, clique em **CHANGE**.
 - b Insira o nome do host do servidor do balanceador de carga em vez de inserir o nome do appliance do vRealize Orchestrator.

14 Reconfigure a autenticação.

- a Se, antes da atualização, o servidor Orchestrator foi configurado para usar **LDAP** ou **SSO (legado)** como o método de autenticação, configure o **vSphere** ou o **vRealize Automation** como um provedor de autenticação.
- b Se a autenticação já estiver definida como **vSphere** ou **vRealize Automation**, remova as configurações e registre-as novamente.

Observação Se, antes da atualização, o Orchestrator tiver usado o **vSphere** como um provedor de autenticação e tiver sido configurado para se conectar ao nome de domínio totalmente qualificado ou endereço IP do vCenter Server, caso você tenha um Platform Services Controller externo, após a atualização, você deverá configurar o Orchestrator para conectar-se ao nome de domínio totalmente qualificado ou endereço IP da instância do Controlador de Serviços de Plataforma que contém o vCenter Single Sign-On. Você também deve importar para o Orchestrator manualmente os certificados de todos os Platform Services Controllers que compartilham o mesmo domínio do vCenter Single Sign-On.

Você atualizou com êxito o Orchestrator Appliance.

Próximo passo

Verifique se o Orchestrator está configurado adequadamente na página **Validar Configuração** no Centro de controle.

Atualizar o Orchestrator Appliance usando um Repositório Específico

Você pode configurar o Orchestrator para usar um repositório local no qual você carrega o arquivo de atualização.

Pré-requisitos

- Desmonte todos os sistemas do arquivo de rede. Para obter mais informações, consulte a documentação *Administração da Máquina Virtual vSphere*.
- Aumente a memória do Orchestrator Appliance para pelo menos 6 GB. Para obter mais informações, consulte a documentação *Administração da Máquina Virtual vSphere*.
- Aumente o tamanho do disco da máquina virtual do vRealize Orchestrator: Disco 1 = 7 GB, Disco 2 = 10 GB.
- Certifique-se de que a partição raiz do Orchestrator Appliance tenha pelo menos de 3 GB de espaço livre disponível. Para obter mais informações sobre como aumentar o tamanho de uma partição de disco, consulte KB 1004071: <http://kb.vmware.com/kb/1004071>.
- Tire um snapshot da máquina virtual Orchestrator. Para obter mais informações, consulte a documentação *Administração da Máquina Virtual vSphere*.
- Se utilizar um banco de dados externo, faça backup dele.
- Se você usar o pré-configurado no banco de dados Orchestrator PostgreSQL, faça backup do banco de dados usando o menu **Exportar banco de dados** menu no Centro de controle.

Procedimentos

- 1 Preparar o repositório local para atualizações.
 - a Instalar e configurar um servidor web local.
 - b Baixe o arquivo `VMware-vR0-Appliance-version-build_number-updaterepo.zip` do site de download oficial da VMware.
 - c Extraia o arquivo .ZIP para o repositório local.
- 2 Vá para a Interface de Gerenciamento do Appliance Virtual (VAMI) em `https://orchestrator_server:5480` e faça login como **raiz**.
- 3 Na guia **Atualizar**, clique em **Configurações**.
- 4 Selecione o botão de seleção próximo da opção **Use o Repositório Especificado**.
- 5 Insira o endereço do URL do repositório local apontando para o diretório `Update_Repo`.
`http://local_web_server:port/build/mts/release/bora-build_number/publish/exports/Update_Repo`
- 6 Caso o repositório local necessite de autenticação, insira o nome de usuário e senha.
- 7 Clique em **Salvar Configurações**.
- 8 Na página **Status**, clique em **Verificar Atualizações**.
- 9 Se houver alguma atualização disponível, clique em **Instalar Atualizações**.
- 10 Aceite o acordo de licença do usuário final VMware e confirme que você deseja instalar a atualização.
- 11 Para concluir a atualização, reinicie o Orchestrator Appliance.
 - a Faça login novamente na Interface de Gerenciamento do Appliance Virtual (VAMI) como **raiz**.
- 12 (Opcional) Na guia **Atualizar**, verifique se a última versão do Orchestrator Appliance está instalada com sucesso.
- 13 Faça login no Control Center como **root**.
- 14 Se você planeja criar um cluster de instâncias do Orchestrator, redefina as configurações dos hosts.
 - a Na página **Configurações do Host** do Centro de Controle, clique em **CHANGE**.
 - b Insira o nome do host do servidor do balanceador de carga em vez de inserir o nome do appliance do vRealize Orchestrator.

15 Reconfigure a autenticação.

- a Se, antes da atualização, o servidor Orchestrator foi configurado para usar **LDAP** ou **SSO (legado)** como o método de autenticação, configure o **vSphere** ou o **vRealize Automation** como um provedor de autenticação.
- b Se a autenticação já estiver definida como **vSphere** ou **vRealize Automation**, remova as configurações e registre-as novamente.

Observação Se, antes da atualização, o Orchestrator tiver usado o **vSphere** como um provedor de autenticação e tiver sido configurado para se conectar ao nome de domínio totalmente qualificado ou endereço IP do vCenter Server, caso você tenha um Platform Services Controller externo, após a atualização, você deverá configurar o Orchestrator para conectar-se ao nome de domínio totalmente qualificado ou endereço IP da instância do Controlador de Serviços de Plataforma que contém o vCenter Single Sign-On. Você também deve importar para o Orchestrator manualmente os certificados de todos os Platform Services Controllers que compartilham o mesmo domínio do vCenter Single Sign-On.

Você atualizou com êxito o Orchestrator Appliance.

Próximo passo

Verifique se o Orchestrator está configurado adequadamente na página **Validar Configuração** no Centro de controle.

Atualizando o cluster do appliance externo do vRealize Orchestrator para uso com o vRealize Automation

Se você usa uma cluster do vRealize Orchestrator Appliance com o vRealize Automation, você deve atualizar o cluster do Orchestrator Appliance para a versão 7.4 atualizando um única instância e juntando novos nós 7.4 instalados para a instância atualizada.

Pré-requisitos

- [Instalar a atualização no appliance do vRealize Automation.](#)
- Atualize os componentes do IaaS. Consulte [Atualizar os componentes do servidor de IaaS após atualizar o vRealize Automation.](#)
- Configure um balanceador de carga para distribuir o tráfego entre as várias instâncias do vRealize Orchestrator. Consulte o [Guia de Configuração do Balanceador de Carga do vRealize Orchestrator.](#)
- Faça um snapshot de todos os nós do servidor vRealize Orchestrator.
- Faça backup do banco de dados compartilhado vRealize Orchestrator.

Procedimentos

- 1 No Centro de Controle, atualize o NSX plug-in do vRealize Automation.
- 2 Pare os serviços do Orchestrator vco-server e vco-configurator em todos os nós do cluster.

- 3 Atualize apenas uma das instâncias do servidor do Orchestrator no seu cluster usando um dos procedimentos documentados.
- 4 Implante um novo Orchestrator Appliance na versão 7.4.
 - a Configure o novo nó com as configurações de rede de uma instância existente não atualizada que seja parte do cluster.
- 5 Acesse o Centro de Controle do segundo nó para iniciar o assistente de configuração.
 - a Navegue para `https://your_orchestrator_server_IP_or_DNS_name:8283/vco-controlcenter`.
 - b Faça login como **raiz** com a senha que você inseriu durante a implantação OVA.
- 6 Selecione o tipo de implantação **Orchestrator Clusterizado**.

Ao escolher este tipo, você seleciona associar o nó a um cluster existente do Orchestrator.
- 7 Na caixa de texto **Hostname** insira o nome do host ou o endereço IP da primeira instância do servidor do Orchestrator.

Observação Deve ser o IP local ou nome do host da instância do Orchestrator para a qual você está associando o segundo nó. Você não deve utilizar o endereço do balanceador de carga.

- 8 Nas caixas de texto **Nome de Usuário** e **Senha**, insira as credenciais raiz da primeira instância do servidor Orchestrator.
- 9 Clique em **Associar**. A instância do Orchestrator clona a configuração do nó ao qual ela se associa. O serviço do servidor Orchestrator de ambos os nós reinicia automaticamente.
- 10 Acesse o Centro de Controle do cluster do Orchestrator atualizado através do endereço do balanceador de carga e faça login como **administrador**.
- 11 Na página **Gerenciamento de Cluster do Orchestrator**, verifique se as cadeias de caracteres **Configuração de Impressão Digital Ativa** e **Configuração de Impressão Digital Pendente** em todos os nós do cluster são correspondentes.

Observação Talvez seja preciso atualizar a página diversas vezes até que as duas cadeias de caracteres correspondam-se.

- 12 Verifique se o cluster do vRealize Orchestrator está configurado adequadamente abrindo a página **Validar Configuração** no Centro de controle.
- 13 (Opcional) Repita os passos de 3 a 8 para cada nó adicional no cluster.
- 14 No Centro de Controle, atualize o NSX plug-in do vRealize Automation.

Você atualizou com êxito o cluster do Orchestrator.

Próximo passo

[Ativar os balanceadores de carga.](#)

Adicionar usuários ou grupos a uma conexão do Active Directory

É possível adicionar usuários ou grupos a uma conexão do Active Directory existente.

O sistema de autenticação de usuários do Gerenciamento de Diretórios importa dados do Active Directory ao adicionar grupos e usuários. A velocidade do transporte de dados está limitada à capacidade do Active Directory. Como resultado, ações podem levar muito tempo dependendo do número de grupos e usuários que são adicionados. Para minimizar problemas, limite os grupos e usuários a apenas os grupos e usuários exigidos para uma ação do vRealize Automation. Se ocorrerem problemas, feche aplicativos desnecessários e verifique se a sua implantação tem a memória alocada adequada para o Active Directory. Se o problema persistir, aumente a alocação de memória do Active Directory. Para implantações com um grande número de usuários e grupos, talvez você precise aumentar a alocação de memória do Active Directory para até 24 GB.

Quando você sincroniza uma implantação vRealize Automation com grande número de usuários e grupos, pode haver um atraso antes de Detalhes de registro estão disponíveis. O carimbo de hora no arquivo de registro pode ser diferente da hora de conclusão exibida no console.

Se membros de um grupo não estão na lista de Usuários, quando você adiciona o grupo a partir do Active Directory, os membros são adicionados à lista. Quando você sincroniza um grupo, todos os usuários que não possuem Usuários de Domínio como grupo primário no Active Directory não são sincronizados.

Observação Não é possível cancelar uma operação de sincronização após iniciá-la.

Pré-requisitos

- Conector instalado e o código de ativação ativado. Selecione os atributos padrão necessários e adicione atributos adicionais na página Atributos de Usuário.

Consulte [PLUGINS_ROOT/com.vmware.vra.prepare.use.doc/GUID-9B25F502-EC8C-40CF-8ACF-4731B5A6903A.html](https://docs.vmware.com/en/VMware-Realize-Automation/7.0/PLUGINS_ROOT/com.vmware.vra.prepare.use.doc/GUID-9B25F502-EC8C-40CF-8ACF-4731B5A6903A.html).
- 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 de base, o DN de associação e a senha do DN de associação.
- Para autenticação integrada do Windows no Active Directory, as informações necessárias incluem a senha e o endereço UPN do usuário de associação do domínio.
- Se o Active Directory for acessado através de SSL, é necessária uma cópia do certificado SSL.
- Se você tem um Active Directory multi-floresta integrado com a autenticação do Windows e o grupo local de domínio contém membros de diferentes florestas, faça o seguinte. Adicione o usuário vinculado ao grupo de Administradores do grupo local de domínio. Se o usuário vinculado não for adicionado, esses membros estarão ausentes do grupo local de domínio.
- Faça logon no vRealize Automation como **administrador de tenants**.

Procedimentos

- 1 Selecione **Administração > Gerenciamento de Diretórios > Diretórios**.
- 2 Clique no nome do diretório desejado.
- 3 Clique em **Configurações de Sincronização** para abrir uma caixa de diálogo com as opções de sincronização.
- 4 Clique no ícone apropriado, dependendo se você deseja alterar a configuração do usuário ou grupo.

Para editar a configuração do grupo:

- Para adicionar grupos, clique no ícone **+** para adicionar uma linha para definições de DN do grupo e insira o DN do grupo apropriado.
- Se você quiser excluir uma definição de DN do grupo, clique no ícone **x** do DN do grupo desejado.

Para editar a configuração do usuário:

- ◆ Para adicionar usuários, clique no ícone **+** para adicionar uma linha para definição de DN do usuário e insira o DN do usuário apropriado.

Se você quiser excluir uma definição de DN do usuário, clique no ícone **x** do DN do usuário desejado.

- 5 Clique em **Salvar** para salvar as alterações sem sincronizar suas atualizações imediatamente. Clique em **Salvar e sincronizar** para salvar as alterações e sincronizar suas atualizações imediatamente.

Ativar os balanceadores de carga

Se a sua implantação usar balanceadores de carga, reative os nós secundários e as verificações de integridade e reverta as configurações de tempo limite do balanceador de carga.

As checagens de integridade para vRealize Automation variam de acordo com a versão. Para obter informações, consulte o *Guia de Configuração de Balanceamento de Carga do vRealize Automation* na [Documentação do VMware vRealize Automation](#).

Altere as configurações de tempo limite do balanceador de carga de 10 minutos de volta para as configurações padrão.

Tarefas de pós-atualização para atualizar o vRealize Automation

Depois de atualizar o vRealize Automation 6.2.5 para a versão 7.4, realize qualquer etapa de pós-atualização necessária.

Configuração de porta para implantações de alta disponibilidade

Depois de terminar um upgrade em uma implantação de alta disponibilidade, você deve configurar o balanceador de carga para passar o tráfego na porta 8444 para o appliance do vRealize Automation, a fim de oferecer suporte a recursos de console remoto.

Para obter mais informações, consulte o *Guia de Configuração de Balanceamento de Carga do vRealize Automation* na [Documentação do vRealize Automation](#).

Reconfigurar o vRealize Orchestrator integrado para dar suporte à alta disponibilidade

Para uma implantação de alta disponibilidade, você deve reassociar manualmente cada appliance vRealize Automation de réplica de destino ao cluster para ativar o suporte à alta disponibilidade para o vRealize Orchestrator incorporado.

Pré-requisitos

Faça login no console de gerenciamento do appliance vRealize Automation de réplica de destino.

- 1 Inicie um navegador e abra o console de gerenciamento do vRealize Automation de réplica de destino usando o nome de domínio totalmente qualificado (FQDN) do appliance virtual de réplica de destino://vra-va-hostname.domain.name:5480.
- 2 Faça login com o nome de usuário **root** e a senha que você inseriu quando implantou o appliance vRealize Automation de réplica de destino.

Procedimentos

- 1 Selecione **Configurações do vRA > Cluster**.
- 2 Na caixa de texto **Nó de Cluster Principal**, insira o FQDN do appliance vRealize Automation mestre de destino.
- 3 Insira a senha root na caixa de texto **Senha**.
- 4 Clique em **Unir cluster**.
Ignore todos os avisos de certificado para continuar. O sistema reinicia serviços para o cluster.
- 5 Verifique se os serviços estão em execução.
 - a Na barra de guias superior, clique em **Serviços**.
 - b Clique em **Atualizar** para monitorar o progresso da inicialização dos serviços.

Ativando a ação Conectar-se ao console remoto para consumidores

A ação do console remoto para consumidores tem suporte para appliances provisionados pelo vSphere no vRealize Automation.

Edite o blueprint depois de atualizar a versão e selecione a ação **Conectar-se ao console remoto** na guia **Ação**.

Para obter mais informações, consulte o [artigo 2109706 da base de dados de conhecimento](#).

Restaurar arquivos de limite de fluxo de trabalho externo.

Você deve reconfigurar os arquivos de tempo limite de fluxo de trabalho externo do vRealize Automation, pois o processo de atualização substituiu os arquivos xmldb.

Procedimentos

- 1 Abra os arquivos de configuração de fluxo de trabalho externo (xmldb) no sistema do diretório a seguir.
`\\VMware\vcac\Server\ExternalWorkflows\xmldb\.`

- 2 Substitua os arquivos xmldb pelos arquivos que você fez backup antes da migração. Caso não tenha os arquivos de backup, redefina as configurações de tempo limite de fluxo de trabalho externo.
- 3 Salve as configurações.

Verificar se o serviço do vRealize Orchestrator está disponível

Após atualizar para a versão mais recente do vRealize Automation, você deve verificar a conexão entre o vRealize Automation e o vRealize Orchestrator. Após a atualização, às vezes é preciso restaurar a conexão.

Pré-requisitos

Faça login na interface de configuração do vRealize Orchestrator.

Procedimentos

- 1 Clique em **Validar Configuração**.
- 2 Se a seção Autenticação tiver uma marca de seleção verde, vá para a etapa 5.
- 3 Se a seção Autenticação não tiver uma marca de seleção verde, realize as seguintes etapas para restaurar a conexão com o vRealize Orchestrator.
 - a Clique em **Início**.
 - b Clique em **Configurar Provedor de Autenticação**.
 - c Na caixa de texto **Grupo de administradores**, selecione **Alterar** e escolha um novo Grupo de administradores que possa ser corretamente resolvido.

O grupo vcoadmins está disponível apenas no tenant padrão vsphere.local. Se estiver usando outro tenant para o vRealize Orchestrator, você deverá selecionar outro grupo.
 - d Clique em **Salvar Alterações** e, se solicitado, reinicie o servidor vRealize Orchestrator.
 - e Clique em **Início**.
- 4 Repita a etapa 1 para confirmar se a seção Autenticação ainda tem uma marca de seleção verde.
- 5 Clique em **Início** e feche o vRealize Orchestrator Control Center.

Reconfigurar o endpoint de infraestrutura do vRealize Orchestrator incorporado no vRealize Automation de destino

Ao migrar de um ambiente do vRealize Automation 6.2.x, você deve atualizar o URL do endpoint de infraestrutura que aponta para o servidor vRealize Orchestrator incorporado de destino.

Pré-requisitos

- Faça a migração bem-sucedida para o vRealize Automation 7.4.
- Faça login no console de destino do vRealize Automation.
 - a Abra o console do vRealize Automation usando o nome de domínio totalmente qualificado do appliance virtual de destino: `https://vra-va-hostname.domain.name/vcac`.

Para um ambiente de alta disponibilidade, abra o console usando o nome de domínio totalmente qualificado do balanceador de carga do appliance virtual de destino: `https://vra-va-lb-hostname.domain.name/vcac`.

- b Faça login como um usuário administrador do IaaS.

Procedimentos

- 1 Selecione **Infraestrutura > Endpoints > Endpoints**.
- 2 Na página Endpoints, selecione o endpoint do vRealize Orchestrator e clique em **Editar**.
- 3 Na caixa de texto Endereço, edite o URL do endpoint do vRealize Orchestrator.
 - Se você tiver migrado para um ambiente mínimo, substitua o URL do endpoint do vRealize Orchestrator por `https://vra-va-hostname.domain.name:443/vco`.
 - Se você tiver migrado para um ambiente de alta disponibilidade, substitua o URL do endpoint do vRealize Orchestrator por `https://vra-va-lb-hostname.domain.name:443/vco`.
- 4 Clique em **OK**.
- 5 Execute manualmente uma coleta de dados no endpoint do vRealize Orchestrator.
 - a Na página Endpoints, selecione o endpoint do vRealize Orchestrator.
 - b Selecione **Ações > Coleta de Dados**.

Verifique se a coleta de dados foi bem-sucedida.

Restaurar alterações de registro no arquivo `app.config`

O processo de atualização substitui as alterações feitas no processo de registro nos arquivos de configuração. Depois de concluir uma atualização, você deve restaurar todas as alterações feitas ao arquivo `app.config` antes da atualização.

Ativar o Failover automático do Manager Service após a atualização

O failover automático do Manager Service está desativado por padrão com a atualização do vRealize Automation.

Conclua essas etapas para ativar o failover automático do Manager Service após a atualização.

Procedimentos

- 1 Abra um prompt de comando como root no appliance vRealize Automation.
- 2 Mude para o diretório `/usr/lib/vcac/tools/vami/commands`.
- 3 Para ativar o failover automático do Manager Service, execute o seguinte comando.

```
python ./manager-service-automatic-failover ENABLE
```

Para desativar o failover automático em toda uma implantação do IaaS, execute o seguinte comando.

```
python ./manager-service-automatic-failover DISABLE
```

Sobre o failover automático do Serviço de Gerenciador

Você pode configurar o Serviço de Gerenciador do IaaS para realizar um failover de um backup vRealize Automation automaticamente se o Serviço de Gerenciador primário parar.

A partir do vRealize Automation 7.3, não será mais necessário iniciar ou interromper manualmente o Serviço de Gerenciador em cada servidor Windows para controlar qual servirá como primário ou backup. O failover automático do Manager Service está desativado por padrão quando você atualiza o IaaS com o Script de shell de upgrade ou usa o arquivo executável do instalador do Installer.

Quando o failover automático está ativado, o Serviço de Gerenciador é iniciado automaticamente em todos os hosts do Serviço de Gerenciador, incluindo backups. O recurso de failover automático permite aos hosts monitorar uns aos outros de maneira transparente e realizar o failover quando necessário, mas o serviço Windows deve estar sendo executado em todos os hosts.

Observação Não é obrigatório utilizar o failover automático. É possível desativá-lo e continuar a iniciar e parar manualmente o serviço Windows para controlar qual host servirá como primário ou backup. Se você optar pela abordagem de failover, será necessário iniciar o serviço em um host por vez. Com o failover automático desativado, executar o serviço simultaneamente em vários servidores IaaS torna o vRealize Automation inutilizável.

Não tente ativar ou desativar seletivamente o failover automático. O failover automático deve estar sempre sincronizado como ligado ou desligado, em todos os hosts do Serviço de Gerenciador em uma implantação do IaaS.

Executar a Conexão de Teste e verificar endpoints atualizados

Atualizar do vRealize Automation 7.3 ou anterior para o 7.4 faz alterações nos endpoints no ambiente de destino.

Depois de atualizar para o vRealize Automation 7.4, você deve usar a ação **Testar Conexão** para todos os endpoints aplicáveis. Você pode precisar também de fazer ajustes a alguns endpoints atualizados. Para mais informações, consulte [Considerações ao trabalhar com endpoints atualizados ou migrados](#).

A configuração de segurança padrão para endpoints atualizados ou migrados é não aceitar certificados não confiáveis.

Após a atualização ou migração de uma instalação anterior do vRealize Automation, se você estiver usando certificados não confiáveis, execute as seguintes etapas para todos os endpoints vSphere e NSX para ativar a validação do certificado. Caso contrário, as operações de endpoint falharão com erros de certificado. Para obter mais informações, consulte os artigos da Base de conhecimento da VMware *A comunicação do endpoint está interrompida após a atualização para o vRA 7.3 (2150230)* em <http://kb.vmware.com/kb/2150230> e *Como baixar e instalar os certificados raiz do vCenter Server para evitar avisos de certificado do navegador da Web (2108294)* em <http://kb.vmware.com/kb/2108294>.

- 1 Após a atualização ou migração, faça login na máquina do agente do vRealize Automation vSphere e reinicie seus agentes do vSphere usando a guia **Serviços**.

A migração pode não reiniciar todos os agentes. Portanto, reinicialize-os manualmente, se necessário.

- 2 Aguarde a conclusão de pelo menos um relatório ping. O relatório leva de um a dois minutos para ser concluído.
- 3 Quando os agentes do vSphere terminarem a coleta de dados, faça login no vRealize Automation como administrador de IaaS.
- 4 Clique em **Infraestrutura > Endpoints > Endpoints**.
- 5 Edite um endpoint do vSphere e clique em **Testar Conexão**.
- 6 Se aparecer um prompt de certificado, clique em **OK** para aceitar o certificado.

Se não aparecer um prompt de certificado, o certificado pode estar armazenado corretamente no momento em uma autoridade raiz confiável do serviço de hospedagem de máquina do Windows para o endpoint, por exemplo como uma máquina de agente de proxy ou máquina do DEM.
- 7 Clique em **OK** para aplicar a aceitação do certificado e salvar o endpoint.
- 8 Repita este procedimento para cada endpoint do vSphere.
- 9 Repita este procedimento para cada endpoint do NSX.

Se a ação **Testar Conexão** for bem-sucedida, mas algumas operações de coleta ou provisionamento de dados falharem, você pode instalar o mesmo certificado em todas as máquinas do agente que sirvam o endpoint e em todas as máquinas do DEM. Como alternativa, você pode desinstalar o certificado das máquinas existentes e repetir o procedimento anterior para o endpoint com falha.

Importar plug-in DynamicTypes

Se você estiver usando o plug-in DynamicTypes e exportado a configuração como um pacote antes da atualização, deverá importar o seguinte fluxo de trabalho:

```
/Library/Dynamic Types/Configuration/Import Configuration From Package
```

O comando `/Library` é executado do Cliente Java do vRealize Orchestrator.

Solucionando problemas de atualização do vRealize Automation

Os tópicos de solução de problemas de atualização fornecem soluções para problemas que você pode enfrentar ao atualizar o vRealize Automation 6.2.5 para a versão 7.4.

A instalação ou a atualização falha com um erro de tempo limite do balanceador de carga

Uma instalação ou atualização do vRealize Automation para um ambiente distribuído com um balanceador de carga falha com um erro 503, serviço indisponível.

Problema

A instalação ou atualização falha porque a configuração de tempo limite balanceador de carga não permite tempo suficiente para que a tarefa seja concluída.

Causa

Uma configuração insuficiente de tempo limite do balanceador de carga pode causar falhas. Você pode corrigir o problema aumentando a configuração de tempo limite do balanceador de carga para 100 segundos ou mais e executando novamente a tarefa.

Solução

- 1 Aumente o valor do tempo limite do balanceador de carga para pelo menos 100 segundos.
- 2 Execute novamente a instalação ou atualização.

Falha na atualização para o componente do site do IaaS

A atualização do IaaS falha e você não pode continuá-la.

Problema

A atualização do IaaS falha para o componente do site. As seguintes mensagens de erro aparecem no arquivo de log do instalador.

- System.Data.Services.Client.DataServiceQueryException:
An error occurred while processing this request. --->
System.Data.Services.Client.DataServiceClientException: <!DOCTYPE html>
- Description: An application error
occurred on the server. The current custom error settings for this application
prevent the details of the application error from being viewed remotely (for
security reasons). It could, however, be viewed by browsers running on the
local server machine.
- Warning: Non-zero return code. Command failed.
- Done Building Project "C:\Program Files
(x86)\VMware\VCAC\Server\Model Manager Data\DeployRepository.xml"
(InstallRepoModel target(s)) -- FAILED.

As seguintes mensagens de erro aparecem no arquivo de log do repositório.

- [Error]: [sub-thread-Id="20"
context="" token=""] Failed to start repository service. Reason:
System.InvalidOperationException: Configuration section encryptionKey is not
protected
at
DynamicOps.Common.Utils.EncryptionHelpers.ReadKeyFromConfiguration(Configuration
config)

```
at DynamicOps.Common.Utils.EncryptionHelpers.Decrypt(String value)
at DynamicOps.Repository.Runtime.CoreModel.GlobalPropertyItem.Decrypt(Func`2
decryptFunc)
at
DynamicOps.Common.Entity.ContextHelpers.OnObjectMaterializedCallbackEncryptable(Object
sender, ObjectMaterializedEventArgs e)
at
System.Data.Common.Internal.Materialization.Shaper.RaiseMaterializedEvents()
at
System.Data.Common.Internal.Materialization.Shaper`1.SimpleEnumerator.MoveNext()
at System.Linq.Enumerable.FirstOrDefault[TSource](IEnumerable`1 source)
at System.Linq.Queryable.FirstOrDefault[TSource](IQueryable`1 source)
at
DynamicOps.Repository.Runtime.Common.GlobalPropertyHelper.GetGlobalPropertyValue(Core
ModelEntities
coreModelContext, String propertyName, Boolean throwIfPropertyNotFound)
at
DynamicOps.Repository.Runtime.CafeClientAbstractFactory.LoadSolutionUserCertificate()
at
DynamicOps.Repository.Runtime.CafeClientAbstractFactory.InitializeFromDb(String
coreModelConnectionString)
at DynamicOps.Repository.Runtime.Common.RepositoryRuntime.Initialize().
```

Causa

A atualização do IaaS falha quando a data de criação do arquivo `web.config` é igual ou posterior à data de modificação.

Solução

- 1 No host do IaaS, faça login no Windows.
- 2 Abra o prompt de comando do Windows.
- 3 Mude de diretório para a pasta de instalação do vRealize Automation.
- 4 Inicie seu editor de texto preferencial com a opção **Executar como administrador**.
- 5 Localize e selecione o arquivo `web.config` e salve-o para alterar a data de modificação do arquivo.

- 6 Examine as propriedades do arquivo `web.config` para confirmar se a data de modificação do arquivo é posterior à data de criação.
- 7 Atualizar IaaS.

Falha de execução do Manager Service devido a erros de validação de SSL durante o tempo de execução

Ocorre uma falha na execução do Manager Service devido a erros de validação de SSL.

Problema

Ocorre falha do Manager Service com a seguinte mensagem de erro no log:

```
[Info]: Thread-Id="6" - context="" token="" Failed to connect to the core database, will retry in 00:00:05, error details: A connection was successfully established with the server, but then an error occurred during the login process. (provider: SSL Provider, error: 0 - The certificate chain was issued by an authority that is not trusted.)
```

Causa

Durante o tempo de execução, ocorre uma falha na execução do Manager Service devido a erros de validação de SSL.

Solução

- 1 Abra o arquivo de configuração `ManagerService.config`.
- 2 Atualize **Encrypt=False** na seguinte linha:

```
<add name="vcac-repository" providerName="System.Data.SqlClient"
connectionString="Data Source=iaas-db.sqa.local;Initial Catalog=vcac;Integrated
Security=True;Pooling=True;Max Pool
Size=200;MultipleActiveResultSets=True;Connect Timeout=200, Encrypt=True" />
```

Falha de login após a atualização

Você deve sair do navegador e repetir o login após uma atualização para sessões que usam contas de usuário não sincronizadas.

Problema

Após a atualização do vRealize Automation, o sistema bloqueia o acesso a contas de usuário não sincronizadas no login.

Solução

Saia do navegador e reinicie o vRealize Automation.

Itens de catálogo aparecem no catálogo de serviços após atualização, mas não estão disponíveis para solicitação

Os itens de catálogo que utilizam determinadas definições de propriedade de versões anteriores aparecem no catálogo de serviço; apesar disso, não estão disponíveis para requisição após a atualização para a versão mais recente do vRealize Automation.

Problema

Se você atualizou da versão 6.2.x ou anterior e tinha definições de propriedade com os tipos de controle ou de atributos a seguir, esses atributos estarão ausentes nas definições de propriedade, e nenhum dos itens de catálogo que as utilizar funcionará como antes da atualização.

- Tipos de controle. Caixa de seleção ou link.
- Atributos. Relacionamento, expressões regulares ou layouts de propriedades.

Causa

No vRealize Automation 7.0 e versões posteriores, as definições de propriedades não usam mais os atributos. Você deverá recriar a definição de propriedade ou configurá-la para utilizar uma ação de script do vRealize Orchestrator em vez dos tipos de controle ou atributos incorporados.

Migre o tipo de controle ou os atributos para o vRealize Automation 7.x usando uma ação de script.

Solução

- 1 No vRealize Orchestrator, crie uma ação de script que retorne os valores de propriedade. A ação deve retornar um tipo simples. Por exemplo, cadeias de retorno, números inteiros ou outros tipos compatíveis. A ação pode considerar como um parâmetro de entrada as outras propriedades das quais ela depende.
- 2 No console do vRealize Automation, configure a definição do produto.
 - a Selecione **Administração > Dicionário de propriedades > Definições de propriedades**.
 - b Selecione a definição da propriedade e clique em **Editar**.
 - c No menu suspenso Exibir aviso, selecione **Lista Suspensa**.
 - d No menu suspenso Valores, selecione **Valores Externos**.
 - e Selecione a ação de script.
 - f Clique em **OK**.
 - g Configure os Parâmetros de Entrada incluídos na ação de script. Para preservar a relação existente, vincule o parâmetro à outra propriedade.
 - h Clique em **OK**.

Mesclagem sem sucesso do banco de dados externo PostgreSQL

A mesclagem do banco de dados PostgreSQL externo com o banco de dados PostgreSQL incorporado não é bem-sucedida.

Problema

Se a versão do banco de dados PostgreSQL externo for anterior à do banco de dados PostgreSQL incorporado, a mesclagem não terá êxito.

Solução

- 1 Faça login no host do banco de dados PostgreSQL externo.
- 2 Execute o comando `psql --version`.
Anote a versão do PostgreSQL para o banco de dados externo.
- 3 Faça login no host do banco de dados PostgreSQL incorporado.
- 4 Execute o comando `psql --version`.
Anote a versão do PostgreSQL para o banco de dados incorporado.

Se a versão do PostgreSQL externo for anterior à do PostgreSQL incorporado, entre em contato com o suporte para obter assistência com a migração do seu banco de dados PostgreSQL.

O comando Unir Cluster parece falhar após a atualização de um ambiente de alta disponibilidade

Depois de clicar em **Unir Cluster** no console de gerenciamento em um nó de cluster secundário, o indicador de progresso desaparece.

Problema

Quando você usa o console de gerenciamento do appliance do vRealize Automation após a atualização para unir um nó de cluster secundário ao nó primário, o indicador de progresso desaparece e nenhuma mensagem de erro ou êxito é exibida. Esse comportamento é um problema intermitente.

Causa

O indicador de progresso desaparece porque alguns navegadores param de aguardar uma resposta do servidor. Esse comportamento não interrompe o processo de união ao cluster. Você pode confirmar se o processo de união ao cluster foi bem-sucedido visualizando o arquivo de registro em `/var/log/vmware/vcac/vcac-config.log`.

A atualização é bem-sucedida quando a partição raiz não fornece espaço livre suficiente

Se não houver espaço livre suficiente na partição raiz do host do appliance vRealize Automation, a atualização não poderá continuar.

Solução

Esse procedimento aumenta o espaço livre na partição raiz do Disco 1 do host do appliance do vRealize Automation. Em uma implantação distribuída, realize esse procedimento para aumentar o espaço livre em cada nó de réplica sequencialmente e, em seguida, aumente o espaço livre no nó principal.

Observação Ao realizar esse procedimento, talvez você veja as mensagens de aviso a seguir:

- ```
WARNING: Re-reading the partition table failed with error 16:
Device or resource busy. The kernel still uses the old table. The
new table will be used at the next reboot or after you run
partprobe(8) or kpartx(8) Syncing disks.
```
- ```
Error: Partition(s) 1 on /dev/sda have been written, but we have been unable to inform the kernel
of the change, probably because it/they are in use. As a result, the old partition(s) will remain
in use. You should reboot now before making further changes.
```

Ignore a mensagem `Você deve reinicializar agora antes de realizar mais alterações`. Se você reinicializar o sistema antes da etapa 10, o processo de atualização ficará corrompido.

Procedimentos

- 1 Ligue a máquina virtual do host do appliance do vRealize Automation e faça login com uma conexão de shell seguro como usuário root.
- 2 Execute os seguintes comandos para interromper serviços.
 - a `service vcac-server stop`
 - b `service vco-server stop`
 - c `service vpostgres stop`
- 3 Execute o seguinte comando para desmontar a partição de permuta.

```
swapoff -a
```
- 4 Execute o seguinte comando para excluir as partições existentes do Disco 1 e criar uma partição raiz de 44-GB e uma partição de permuta de 6 GB.

```
(echo d; echo 2; echo d; echo 1; echo n; echo p; echo ; echo ; echo '+44G';
echo n; echo p; echo ; echo ; echo ; echo w; echo p; echo q) | fdisk /dev/sda
```
- 5 Execute o seguinte comando para alterar o tipo de partição de permuta.

```
(echo t; echo 2; echo 82; echo w; echo p; echo q) | fdisk /dev/sda
```
- 6 Execute o seguinte comando para definir o sinalizador de inicializável do Disco 1.

```
(echo a; echo 1; echo w; echo p; echo q) | fdisk /dev/sda
```

- 7 Execute o seguinte comando para registrar as alterações de partição com o kernel do Linux.

```
partprobe
```

Se você vir uma mensagem solicitando a reinicialização antes de realizar mais alterações, ignore essa mensagem. Reinicializar o sistema antes da etapa 10 corrompe o processo de atualização.

- 8 Execute o seguinte comando para formatar a nova partição de permuta.

```
mkswap /dev/sda2
```

- 9 Execute o seguinte comando para montar a partição de permuta.

```
swapon -a
```

- 10 Reinicie o dispositivo do vRealize Automation.

- 11 Após a reinicialização do appliance, execute o seguinte comando para redimensionar a tabela de partição do Disco 1.

```
resize2fs /dev/sda1
```

- 12 Para verificar se a expansão de disco teve êxito, execute o `df -h` e verifique se o espaço disponível em disco no `/dev/sda1` é maior que 30 GB.

Cópias de backup de arquivos .xml fazem com que o sistema atinja o tempo limite

O vRealize Automation registra qualquer arquivo com uma extensão .xml no diretório `\\VMware\CAC\Server\ExternalWorkflows\xmlldb\`. Se esse diretório contiver arquivos de backup com extensão .xml, o sistema executará fluxos de trabalho duplicados que farão com que ele atinja o tempo limite.

Solução

Solução alternativa: quando você fizer o backup de arquivos nesse diretório, mova os backups para outro diretório ou altere a extensão do nome do arquivo de backup para algo diferente de .xml.

Excluir nós órfãos no vRealize Automation

Um nó órfão é um nó duplicado que está relatado no host, mas que não existe no host.

Problema

Ao verificar que todos os nós IaaS e do appliance virtual estão em estado íntegro, você pode descobrir que um host tem um ou mais nós órfãos. Você deve excluir todos eles.

Solução

- 1 No appliance do vRealize Automation primário, faça login no Gerenciamento do Appliance do vRealize Automation como **root** usando a senha que você inseriu quando implantou o appliance do vRealize Automation.
- 2 Selecione **Configurações do vRA > Cluster**.
- 3 Para cada nó órfão na tabela, clique em **Excluir**.

Não foi possível criar um novo diretório em vRealize Automation

Tentando adicionar um novo diretório com a falha do conector de sincronização.

Problema

Este problema ocorre em função de um arquivo `config-state.json` localizado em `usr/local/horizon/conf/states/VSPHERE.LOCAL/3001/`.

Para obter informações sobre como reparar esse erro, consulte o [Artigo 2145438 da Base de Conhecimento](#).

Algumas máquinas virtuais não possuem uma implantação criada durante a atualização

As máquinas virtuais que se encontram no estado ausente no momento da atualização não possuem uma implantação correspondente criada no ambiente de destino.

Problema

Se uma máquina virtual estiver no estado ausente no ambiente de origem durante a migração, não será criada uma atualização correspondente no ambiente de destino. Se uma máquina virtual sair do estado ausente após a atualização, você poderá importar a máquina para a implantação de destino com a importação em massa.

Erro de certificado não confiável

Ao visualizar a página Visualizador de Registros da infraestrutura no console do Appliance do vRealize Automation, você pode ver um relatório de falha de conexão com o endpoint contendo as seguintes palavras: `Certificate is not trusted`.

Problema

No console Appliance do vRealize Automation, selecione **Infraestrutura > Monitoramento > Registro**. Na página Visualizador de Registros, você pode ver um relatório semelhante a este:

Falha ao se conectar ao endpoint. Para verificar se uma conexão segura pode ser estabelecida com esse endpoint, acesse o endpoint do vSphere na página Endpoints e clique no botão Testar Conexão.

Exceção interna: o certificado não é confiável (RemoteCertificateChainErrors). Assunto: C=US, CN=vc6.mycompany.com Impressão digital: DC5A8816231698F4C9013C42692B0AF93D7E35F1

Causa

Atualizar do vRealize Automation 7.3 ou anterior para o 7.4 faz alterações nos endpoints do seu ambiente original. Para ambientes recentemente atualizados para o vRealize Automation 7.4, o administrador do IaaS deve rever cada endpoint existente que utiliza uma conexão https segura. Se um endpoint tiver um erro `Certificate is not trusted`, ele não funcionará corretamente.

Solução

- 1 Faça login no console do vRealize Automation como administrador de infraestrutura.
- 2 Selecione **Infraestrutura > Pontos de extremidade > Pontos de extremidade**.

- 3 Conclua essas etapas para cada endpoint com uma conexão segura.
 - a Clique em **Editar**.
 - b Clique em **Testar Conexão**.
 - c Reveja os detalhes do certificado e clique em **OK** se confiar nesse certificado.
 - d Reinicie os serviços Windows para todos os Agentes Proxy IaaS usados por esse endpoint.
- 4 Verifique se erros `Certificate is not trusted` deixaram de aparecer na página Visualizador de Registros da infraestrutura.

Falha na instalação ou no upgrade para vRealize Automation

A instalação ou a atualização do vRealize Automation apresenta uma falha e uma mensagem de erro aparece no arquivo de log.

Problema

Quando você instala ou atualiza o vRealize Automation, o procedimento falha. Normalmente, isso ocorre quando uma correção aplicada durante a instalação ou a atualização não é bem-sucedida. Uma mensagem de erro, parecida com a seguinte, aparece no arquivo de registro: `Security error. Applying automatic fix for FIREWALL prerequisite failed. RPM Status 1: Pre install script failed, package test and installation skipped.`

Causa

O ambiente Windows tem uma política de grupo para a execução de script PowerShell definida como ativado.

Solução

- 1 Na máquina host do Windows, execute o `gpedit.msc` para abrir o Editor de Política de Grupo Local.
- 2 No painel esquerdo em **Configuração do Computador**, clique o botão de expansão para abrir os **Modelos Administrativos > Componentes do Windows > PowerShell do Windows**.
- 3 Para **Ligar Execução de Script**, altere o estado de `Enabled` para `Not Configured`.

Falha na atualização do Agente de Gerenciamento

Aparece uma mensagem de erro sobre o agente de gerenciamento quando se clica em **Instalar Atualizações** na página Status de Atualização do console de gerenciamento do Appliance do vRealize Automation.

Problema

O processo de atualização não foi bem-sucedido. Mensagem aparece: `Não é possível atualizar o agente de gerenciamento no nó x.` Às vezes a mensagem lista mais de um nó.

Causa

Muitas circunstâncias podem causar esse problema. A mensagem de erro identifica apenas a ID de nó da máquina afetada. Mais informações podem ser encontradas no arquivo All.log do Agente de Gerenciamento na máquina na qual o comando falhou.

Realize estas tarefas nos nós afetados de acordo com a sua situação:

Solução

- Se o serviço do Agente de Gerenciamento não estiver em execução, inicie o serviço e reinicie a atualização no appliance virtual.
- Se o serviço do Agente de Gerenciamento estiver em execução e o Agente de Gerenciamento for atualizado, reinicie a atualização no appliance virtual.
- Se o serviço do Agente de Gerenciamento estiver em execução, mas o Agente de Gerenciamento não estiver atualizado, realize uma atualização manual.
 - a Abra um navegador e navegue até a página de instalação do IaaS vRealize Automation no appliance do vRealize Automation em `https:// va-hostname.domain.name:5480/install`.
 - b Baixe e execute o instalador do agente de gerenciamento.
 - c Reinicialize a máquina do Agente de Gerenciamento.
 - d Reinicie a atualização no appliance virtual.

A atualização do Agente de Gerenciamento não é bem-sucedida

A atualização do Agente de Gerenciamento não é bem-sucedida durante a atualização do vRealize Automation para a versão 7.2. - 7.3.x.

Problema

Se um incidente de failover tiver trocado os hosts primário e secundário do Agente de Gerenciamento, a atualização não será bem-sucedida, pois o processo de atualização automatizado não conseguirá encontrar o host esperado. Realize esse procedimento em cada nó IaaS em que o Agente de gerenciamento não está atualizado.

Solução

- 1 Abra o arquivo All.log na pasta de registros do Agente de Gerenciamento, localizada em `C:\Program Files (x86)\VMware\vCAC\Management Agent\Log\`.

A localização da pasta de instalação pode ser diferente da localização padrão.

- 2 Pesquise o arquivo de registro em busca de uma mensagem sobre um appliance virtual desatualizado ou desligado.

Por exemplo, EXCEÇÃO INTERNA: System.Net.WebException: Não é possível conectar-se ao servidor remoto ---> System.Net.Sockets.SocketException: Uma tentativa de conexão falhou porque a parte conectada não respondeu corretamente após um período de tempo, ou a conexão estabelecida falhou porque o host conectado não conseguiu responder *Endereço_IP:5480*

- 3 Edite o arquivo de configuração do Agente de Gerenciamento em C:\Program Files (x86)\VMware\VCAC\Management Agent\VMware.IaaS.Management.Agent.exe.config para substituir o valor existente de alternativeEndpointaddress pela URL do endpoint do appliance virtual primário.

A localização da pasta de instalação pode ser diferente da localização padrão.

Exemplo de alternativeEndpointaddress em VMware.IaaS.Management.Agent.exe.config.

```
<alternativeEndpoint address="https://FQDN:5480/" thumbprint="número da impressão digital" />
```

- 4 Reinicie o serviço do Windows do Agente de Gerenciamento e consulte o arquivo All.log para verificar se ele está funcionando.
- 5 Execute o procedimento de atualização no appliance primário do vRealize Automation.

Falha na atualização do vRealize Automation devido às configurações de tempo limite padrão

Você poderá aumentar a configuração de tempo para atualização se a configuração padrão para a sincronização dos bancos de dados for muito curta para o seu ambiente.

Problema

A configuração de tempo limite para o comando Vcac-Config SynchronizeDatabases não é suficiente para alguns ambientes nos quais a sincronização dos bancos de dados demora mais do que o valor padrão de 3600 segundos.

Os valores de propriedade `cafeTimeoutInSeconds` e `cafeRequestPageSize` no arquivo `Vcac-Config.exe.config` controlam a comunicação entre a API e a ferramenta do utilitário `Vcac-config.exe`. O arquivo está no *local de instalação do IaaS\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe.config*.

Você pode substituir o valor de tempo limite padrão apenas para o comando `SynchronizeDatabases`, fornecendo um valor para esses parâmetros opcionais.

| Parâmetro | Nome abreviado | Descrição |
|------------------------|----------------|--|
| --DatabaseSyncTimeout | -dstm | Define o valor de tempo limite de solicitação http apenas para <code>SynchronizeDatabases</code> em segundos. |
| --DatabaseSyncPageSize | -dsps | Define o tamanho de página de solicitação de sincronização apenas para a sincronização de Reserva ou Política de Reserva. O padrão é 10. |

Se esses parâmetros não estiverem definidos no arquivo `Vcac-Config.exe.config`, o sistema usará o valor de tempo limite padrão.

Falha na atualização do IaaS em um ambiente de alta disponibilidade

Falha na execução do processo de atualização do IaaS no nó do servidor da Web primário com balanceamento de carga ativado. Você poderá ver essas mensagens de erro:

"System.Net.WebException: A operação expirou" ou "401 - Não autorizado: acesso negado devido a credenciais inválidas".

Problema

Atualizar o IaaS com o balanceamento de carga ativado pode causar uma falha intermitente. Quando isso acontece, você deve executar a atualização do vRealize Automation novamente com o balanceamento de carga desativado.

Solução

- 1 Reverta seu ambiente para os snapshots anteriores à atualização.
- 2 Abra uma conexão de área de trabalho remota para o nó primário do servidor de Web do IaaS.
- 3 Navegue até o arquivo dos hosts do Windows em `c:\windows\system32\drivers\etc`.
- 4 Abra o arquivo dos hosts e adicione esta linha para ignorar o balanceador de carga do servidor da Web.

IP_address_of_primary_iaas_website_node vrealizeautomation_iaas_website_lb_fqdn

Exemplo:

10.10.10.5 vra-iaas-web-lb.domain.com

- 5 Salve o arquivo dos hosts e tente atualizar o vRealize Automation novamente.
- 6 Quando a atualização do vRealize Automation for concluída, abra o arquivo dos hosts e remova a linha que você adicionou na etapa 4.

Solucionar problemas de atualização

Você pode modificar o processo de atualização para solucionar problemas de atualização.

Solução

Quando você tiver problemas de atualização do ambiente do vRealize Automation, use esse procedimento para modificar o processo de atualização selecionando um dos sinalizadores disponíveis.

Procedimentos

- 1 Abra uma conexão de shell seguro para o nó do appliance primário do vRealize Automation.

- 2 No prompt de comando, execute este comando para criar o arquivo de toggle:

touch available_flag

Por exemplo: **touch /tmp/disable-iaas-upgrade**

Tabela 1-72. Sinalizadores disponíveis

| Sinalizador | Descrição |
|-----------------------------|--|
| /tmp/disable-iaas-upgrade | <ul style="list-style-type: none"> ■ Impede o processo de atualização do IaaS depois do reinício do appliance virtual. ■ Impede a atualização do Agente de Gerenciamento. ■ Impede as verificações e correções de pré-requisito automáticas. ■ Impede a parada dos serviços do IaaS. |
| /tmp/do-not-upgrade-ma | Impede a atualização do Agente de Gerenciamento. Este sinalizador é adequado quando o Agente de Gerenciamento é atualizado manualmente. |
| /tmp/skip-prereq-checks | Impede as verificações e correções de pré-requisito automáticas. Este sinalizador é adequado quando há um problema com as correções de pré-requisito automáticas e as correções foram aplicadas manualmente. |
| /tmp/do-not-stop-services | Impede a parada dos serviços do IaaS. A atualização não interrompe os serviços do IaaS Windows como o Serviço de Gerenciador, DEMs e agentes. |
| /tmp/do-not-upgrade-servers | <p>Impede a atualização automática de todos os componentes do IaaS do servidor como o banco de dados, site da web, WAPI, repositório, os dados do Modelo Mfrontanager e o Manager Service.</p> <p>Observação Este sinalizador também impede a ativação do modo de failover automático do Manager Service.</p> |
| /tmp/do-not-upgrade-dems | Impede a atualização do DEM. |
| /tmp/do-not-upgrade-agents | Impede a atualização do agente de proxy do IaaS. |

3 Conclua as tarefas para o sinalizador escolhido.

Tabela 1-73. Tarefas adicionais

| Sinalizador | Tarefas |
|-----------------------------|--|
| /tmp/disable-iaas-upgrade | <ul style="list-style-type: none"> ■ Atualize o Agente de Gerenciamento manualmente. ■ Aplique quaisquer pré-requisitos do IaaS manualmente. ■ Pare manualmente os serviços do IaaS. <ol style="list-style-type: none"> a Faça login no seu servidor Windows do IaaS. b Selecione Iniciar > Ferramentas administrativas > Serviços. c Para os serviços na seguinte ordem. <p>Observação Não encerre o servidor Windows do IaaS.</p> <ol style="list-style-type: none"> a Cada Agente de Proxy do VMware vRealize Automation. b Cada trabalhador do VMware DEM. c O orchestrator do VMware DEM. d O serviço do VMware vCloud Automation Center. ■ Inicie a atualização do IaaS manualmente depois que a atualização do appliance virtual estiver concluída. |
| /tmp/do-not-upgrade-ma | Atualize o Agente de Gerenciamento manualmente. |
| /tmp/skip-prereq-checks | Aplique quaisquer pré-requisitos do IaaS manualmente. |
| /tmp/do-not-stop-services | <p>Pare manualmente os serviços do IaaS.</p> <ol style="list-style-type: none"> 1 Faça login no seu servidor Windows do IaaS. 2 Selecione Iniciar > Ferramentas administrativas > Serviços. 3 Para os serviços na seguinte ordem. <p>Observação Não encerre o servidor Windows do IaaS.</p> <ol style="list-style-type: none"> a Cada Agente de Proxy do VMware vRealize Automation. b Cada trabalhador do VMware DEM. c O orchestrator do VMware DEM. d O serviço do VMware vCloud Automation Center. |
| /tmp/do-not-upgrade-servers | |
| /tmp/do-not-upgrade-dems | |
| /tmp/do-not-upgrade-agents | |

- 4 Acesse o console de gerenciamento do appliance primário do vRealize Automation e atualize o appliance primário do vRealize Automation.

Observação Como cada sinalizador permanece ativo até que ele seja removido, execute este comando para remover o sinalizador escolhido após a atualização: `rm /flag_path/flag_name`. Por exemplo, `rm /tmp/disable-iaas-upgrade`.

Migrando para o vRealize Automation 7.4

Você pode realizar uma atualização lado a lado do seu ambiente atual do vRealize Automation para a versão mais recente usando a migração.

Estas informações são específicas para atualizar o vRealize Automation 7.4.x usando a migração. Para obter informações sobre outros caminhos de atualização suportados, consulte [Atualizando o vRealize Automation](#).

Migrando o vRealize Automation

Você pode realizar uma atualização lado a lado do seu ambiente atual do vRealize Automation usando a migração.

A migração move todos os dados, exceto tenants e repositórios de identidades, do seu ambiente vRealize Automation de origem atual para uma implantação de destino da última versão do vRealize Automation. Além disso, a migração move todos os dados do vRealize Orchestrator 7.x incorporado para a implantação de destino.

A migração não altera seu ambiente de origem, exceto para interromper os serviços do vRealize Automation pelo tempo necessário para coletar e copiar os dados com segurança para o seu ambiente de destino. Dependendo do tamanho do banco de dados vRealize Automation de origem, a migração poderá demorar de alguns minutos até horas.

Você pode migrar o ambiente de origem para uma implantação mínima ou uma implantação de alta disponibilidade.

Se você planeja colocar seu ambiente de destino em produção após a migração, não volte a colocar seu ambiente de origem em operação. As alterações no seu ambiente de origem após a migração não são sincronizadas com o seu ambiente de destino.

Se o seu ambiente de origem estiver integrado com o vCloud Air ou com o vCloud Director ou tiver endpoints físicos, será necessário usar a migração para realizar uma atualização. A migração remove esses endpoints e todos os itens associados a eles no ambiente de destino. A migração também remove uma integração 6.x do VMware vRealize Application Services do ambiente de destino.

Observação Você deve concluir as tarefas adicionais para preparar suas máquinas virtuais do vRealize Automation antes de migrar. Antes de migrar, veja o artigo [51531](#) da Base de conhecimento.

Se você migrar do vRealize Automation 6.2.x para a versão mais recente, poderá enfrentar esses problemas.

| Problema | Resolução |
|--|---|
| <p>Após migrar do vRealize Automation 6.2.x para a versão mais recente, os itens de catálogo que utilizam essas definições de propriedades aparecem no catálogo de serviços, mas não estão disponíveis para solicitação.</p> <ul style="list-style-type: none"> Tipos de controle: caixa de seleção ou link. Atributos: Relacionamento, expressões regulares ou layouts de propriedades. <p>No vRealize Automation 7.x, as definições de propriedades não usam mais estes elementos.</p> | <p>Você deverá recriar a definição de propriedade ou configurá-la para utilizar uma ação de script do vRealize Orchestrator em vez dos tipos de controle ou atributos incorporados. Para obter mais informações, consulte Itens de catálogo aparecem no catálogo de serviços após a migração, mas não estão disponíveis para solicitação.</p> |
| <p>As expressões regulares utilizadas para definir as relações primárias e secundárias em um menu suspenso do vRealize Automation 6.2 x não têm suporte na 7.x. Na 6.2.x, você pode usar expressões regulares para definir um ou mais itens do menu secundário que estão disponíveis somente para um certo item do menu primário. Somente os itens de menu secundário aparecem quando você seleciona o item de menu primário.</p> <p>Após a migração para a 7.x, todos os itens de menu disponíveis aparecem no menu suspenso secundário, independentemente do que você escolher no menu suspenso primário. Para mostrar que os valores dinâmicos definidos previamente não funcionam, o primeiro item do menu suspenso secundário exibe "Aviso! Usar fluxos de trabalho do vRO para definir valores dinâmicos".</p> | <p>Após a migração, você deverá recriar a definição da propriedade para restaurar os valores dinâmicos anteriores. Para obter informações sobre como criar um relacionamento primário-secundário entre o menu suspenso primário e o menu suspenso secundário, consulte Como utilizar definições de propriedade dinâmicas no vRA 7.2.</p> |

Interfaces de usuário do ambiente do vRealize Automation

Você usa e gerencia seu ambiente do vRealize Automation com várias interfaces.

Interfaces do Usuário

Estas tabelas descrevem as interfaces que você usa para gerenciar seu ambiente do vRealize Automation.

Tabela 1-74. vRealize Automation Console administrativo

| Finalidade | Acesso | Credenciais necessárias |
|---|--|---|
| <p>Use o console do vRealize Automation para estas tarefas de administrador do sistema.</p> <ul style="list-style-type: none"> Adicionar tenants. Personalizar a interface do usuário do vRealize Automation. Configurar servidores de e-mail. Exibir logs de evento. Configure o vRealize Orchestrator. | <ol style="list-style-type: none"> Inicie um navegador e abra a tela inicial do appliance do vRealize Automation usando o nome de domínio totalmente qualificado do appliance virtual: https://vra-va-hostname.domain.name. Clique em Console do vRealize Automation. Você também pode usar esta URL para abrir o console do vRealize Automation: https://vra-va-hostname.domain.name/vcac Faça login. | <p>Você deve ser um usuário com a função de administrador de sistema.</p> |

Tabela 1-75. Console do tenant do vRealize Automation . Essa interface é a interface de usuário principal que você pode usar para criar e gerenciar seus serviços e recursos.

| Finalidade | Acesso | Credenciais necessárias |
|---|---|---|
| <p>Use o vRealize Automation para estas tarefas.</p> <ul style="list-style-type: none"> ■ Solicite novos blueprints de serviço de TI. ■ Criar e gerenciar recursos de TI e da nuvem. ■ Criar e gerenciar grupos personalizados. ■ Crie e gerencie grupos de negócios. ■ Atribuir funções a usuários. | <p>1 Inicie um navegador e insira a URL da sua locação usando o nome de domínio totalmente qualificado do appliance virtual e o nome da URL do tenant:</p> <p><code>https://vra-va-hostname.domain.name/vcac/org/nome_URL_tenant.</code></p> <p>2 Faça login.</p> | <p>Você deve ser um usuário com uma ou mais destas funções:</p> <ul style="list-style-type: none"> ■ Arquiteto de aplicativos ■ Administrador de aprovação ■ Administrador do catálogo ■ Administrador do contentor ■ Arquiteto do contentor ■ Consumidor de integridade ■ Arquiteto de infraestrutura ■ Consumidor de Exportação Segura ■ Arquiteto de software ■ Administrador de tenant ■ Arquiteto do XaaS |

Tabela 1-76. Gerenciamento do Appliance do vRealize Automation . Às vezes, esta interface é chamada de Interface de Gerenciamento do Appliance Virtual (VAMI).

| Finalidade | Acesso | Credenciais necessárias |
|--|---|---|
| <p>Use o Gerenciamento do Appliance do vRealize Automation para estas tarefas.</p> <ul style="list-style-type: none"> ■ Visualizar o status de serviços registrados. ■ Visualizar informações do sistema e reinicializar ou desligar o appliance. ■ Gerenciar a participação no Programa de Aperfeiçoamento da Experiência do Cliente. ■ Visualizar o status da rede. ■ Visualizar o status da atualização e instalar atualizações. ■ Gerenciar configurações de administração. ■ Gerenciar configurações do host vRealize Automation. ■ Gerenciar configurações de SSO. ■ Gerenciar licenças de produto. ■ Configurar o banco de dados Postgres do vRealize Automation. ■ Configurar mensagens do vRealize Automation. ■ Configurar o registro em log do vRealize Automation. ■ Instalar componentes do IaaS. ■ Migrar de uma instalação existente do vRealize Automation. ■ Gerenciar certificados de componentes do IaaS. ■ Configurar o serviço Xenon. | <ol style="list-style-type: none"> 1 Inicie um navegador e abra a tela inicial do appliance do vRealize Automation usando o nome de domínio totalmente qualificado do appliance virtual: <code>https://vra-va-hostname.domain.name.</code> 2 Clique em Gerenciamento do Appliance do vRealize Automation. Você também pode usar esta URL para abrir o Gerenciamento do Appliance do vRealize Automation: <code>https://vra-va-hostname.domain.name:5480.</code> 3 Faça login. | <ul style="list-style-type: none"> ■ Nome de usuário: root ■ Senha: senha que você inseriu quando implantou o appliance do vRealize Automation. |

Tabela 1-77. Cliente vRealize Orchestrator

| Finalidade | Acesso | Credenciais necessárias |
|--|--|--|
| <p>Use o Cliente vRealize Orchestrator para estas tarefas.</p> <ul style="list-style-type: none"> ■ Desenvolver ações. ■ Desenvolver fluxos de trabalho. ■ Gerenciar políticas. ■ Instalar pacotes. ■ Gerenciar usuários e permissões de grupos de usuários. ■ Anexar marcas a objetos de URI. ■ Visualizar o inventário. | <ol style="list-style-type: none"> 1 Inicie um navegador e abra a tela inicial do appliance vRealize Automation usando o nome de domínio totalmente qualificado do appliance virtual: <code>https://vra-va-hostname.domain.name.</code> 2 Para baixar o arquivo <code>client.jnlp</code> no seu computador local, clique em Cliente vRealize Orchestrator. 3 Clique com o botão direito do mouse no arquivo <code>client.jnlp</code> e selecione Iniciar. 4 Na caixa de diálogo Deseja Continuar?, clique em Continuar. 5 Faça login. | <p>Você deve ser um usuário com a função de administrador de sistema ou parte do grupo <code>vcoadmins</code> definido nas configurações do Provedor de Autenticação do Centro de Controle do vRealize Orchestrator.</p> |

Tabela 1-78. Centro de Controle do vRealize Orchestrator

| Finalidade | Acesso | Credenciais necessárias |
|---|---|--|
| <p>Use o Centro de Controle do vRealize Orchestrator para editar a configuração da instância do vRealize Orchestrator padrão que está incorporada no vRealize Automation.</p> | <ol style="list-style-type: none"> 1 Inicie um navegador e abra a tela inicial do appliance do vRealize Automation usando o nome de domínio totalmente qualificado do appliance virtual: <code>https://vra-va-hostname.domain.name.</code> 2 Clique em Gerenciamento do Appliance do vRealize Automation. Você também pode usar esta URL para abrir o Gerenciamento do Appliance do vRealize Automation: <code>https://vra-va-hostname.domain.name:5480.</code> 3 Faça login. 4 Clique em Configurações do vRA > Orchestrator. 5 Selecione a interface de usuário do Orchestrator. 6 Clique em Iniciar. 7 Clique na URL da interface de usuário do Orchestrator. 8 Faça login. | <p>Nome do usuário</p> <ul style="list-style-type: none"> ■ Insira a raiz se a autenticação com base na função não estiver configurada. ■ Insira seu nome de usuário vRealize Automation se ele estiver configurado para autenticação com base na função. <p>Senha</p> <ul style="list-style-type: none"> ■ Insira a senha que você inseriu quando implantou o appliance do vRealize Automation se a autenticação com base na função não estiver configurada. ■ Insira a senha para o seu nome de usuário, se o seu nome de usuário estiver configurado para autenticação com base na função. |

Tabela 1-79. Prompt de Comando do Linux

| Finalidade | Acesso | Credenciais necessárias |
|--|--|---|
| <p>Você pode usar o prompt de comando do Linux em um host, como o host do appliance do vRealize Automation, para estas tarefas.</p> <ul style="list-style-type: none"> ■ Parar ou iniciar serviços ■ Editar arquivos de configuração ■ Executar comandos ■ Recuperar dados | <p>1 No host do appliance do vRealize Automation, abra um prompt de comando.</p> <p>Uma maneira de abrir o prompt de comando no computador local é iniciar uma sessão no host usando um aplicativo, como o PuTTY.</p> <p>2 Faça login.</p> | <ul style="list-style-type: none"> ■ Nome de usuário: root ■ Senha: senha que você criou quando implantou o appliance do vRealize Automation. |

Tabela 1-80. Prompt de Comando do Windows

| Finalidade | Acesso | Credenciais necessárias |
|--|--|---|
| <p>Você pode usar um prompt de comando do Windows em um host, como o host laaS, para executar scripts.</p> | <p>1 No host do laaS, faça login no Windows.</p> <p>Uma maneira de fazer logon no seu computador local é iniciar uma sessão de área de trabalho remota.</p> <p>2 Abra o prompt de comando do Windows.</p> <p>Uma maneira de abrir o prompt de comando é clicar com o botão direito no ícone Iniciar no host e selecionar Prompt de Comando ou Prompt de Comando (Admin).</p> | <ul style="list-style-type: none"> ■ Nome de usuário: usuário com privilégios administrativos. ■ Senha: Senha do usuário. |

Pré-requisitos de Migração

Os pré-requisitos de migração diferem dependendo do ambiente de destino.

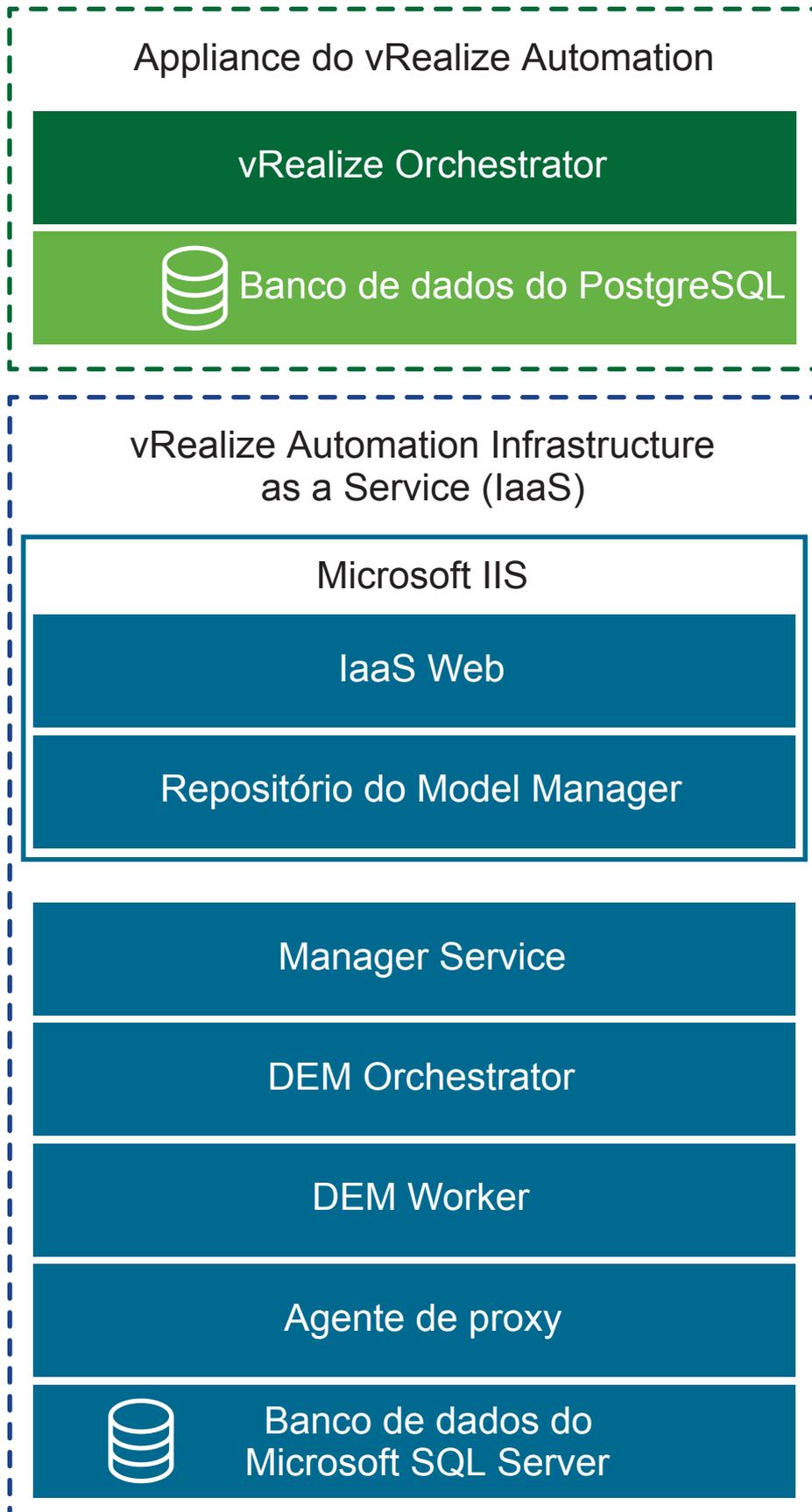
Você pode migrar para um ambiente mínimo ou para um ambiente de alta disponibilidade.

Pré-requisitos para a migração para um ambiente mínimo

Assegure uma migração bem-sucedida para um ambiente mínimo revendo estes pré-requisitos.

As implantações mínimas incluem um appliance do vRealize Automation e um servidor Windows que hospeda os componentes do laaS. Em uma implantação mínima, o banco de dados SQL Server do vRealize Automation pode estar no mesmo servidor Windows do laaS com os componentes do laaS ou em um servidor Windows separado.

Figura 1-17. Implantação mínima do vRealize Automation



Pré-requisitos

- Verifique se você tem um novo ambiente de servidor do vRealize Automation.
- Instale agentes de proxy relevantes no ambiente de destino, de acordo com esses requisitos.
 - O nome do agente de proxy de destino deve corresponder ao nome do agente de proxy de origem para os agentes de proxy do vSphere, do Hyper-V, do Citrix XenServer e de teste.

Observação Conclua essas etapas para obter um nome de agente.

- 1 No host do IaaS, faça login no Windows como usuário local com privilégios de **administrador**.
- 2 Use o Windows Explorer para acessar o diretório de instalação do agente.
- 3 Abra o arquivo `VRMAgent.exe.config`.
- 4 Na marca `serviceConfiguration`, procure o valor do atributo `agentName`.

-
- Veja o artigo [51531](#) da Base de Conhecimento.
 - O nome do endpoint do agente de proxy de destino deve corresponder ao nome do endpoint do agente de proxy de origem para os agentes de proxy do vSphere, do Hyper-V, do Citrix XenServer e de teste.
 - Não crie um endpoint para agentes de proxy do vSphere, do Hyper-V, do Citrix XenServer ou de teste no ambiente de destino.
 - Revise os números de versão dos componentes de vRealize Automation no appliance do vRealize Automation de destino.
 - a Faça login no Gerenciamento do Appliance do vRealize Automation de destino como **root** usando a senha que você inseriu quando implantou o appliance do vRealize Automation de destino.
 - b Selecione **Configurações do vRA > Cluster**.
 - c Expanda os registros de Nome do Host/Nó clicando no triângulo.

Verifique se os números de versão dos componentes IaaS do vRealize Automation correspondem.
 - Verifique se a versão do Microsoft SQL Server de destino para o banco de dados IaaS de destino do vRealize Automation é 2012, 2014 ou 2016.
 - Verifique se a porta 22 está aberta entre os ambientes do vRealize Automation de origem e destino. A porta 22 é necessária para estabelecer conexões Secure Shell (SSH) entre appliances virtuais de origem e de destino.
 - Verifique se o vCenter do endpoint tem recursos suficientes para concluir a migração.
 - Verifique se a hora do sistema do ambiente de destino do vRealize Automation está sincronizada entre o CAFE e os componentes do IaaS.

- Verifique se o nó do servidor IaaS no ambiente de destino tem pelo menos o Java SE Runtime Environment (JRE) 8, 64 bits, atualização 161 instalado. Depois de instalar o JRE, verifique se a variável do ambiente JAVA_HOME aponta para a versão do Java que você instalou em cada nó do IaaS. Revise o caminho se necessário.
- Verifique se cada nó IaaS tem o PowerShell 3.0 ou versão posterior instalado.
- Verifique se os ambientes do vRealize Automation de origem e destino estão em execução.
- Certifique-se de que nenhuma atividade de usuário e provisionamento esteja ocorrendo no ambiente vRealize Automation de origem.
- Verifique se que qualquer software antivírus ou de segurança em execução nos nós do IaaS no ambiente de destino do vRealize Automation que possa interagir com o sistema operacional e seus componentes está configurado corretamente ou desativado.
- Verifique se o serviço da Web do IaaS e do Model Manager não precisam ser reiniciados devido a atualizações de instalação do Windows pendentes. As atualizações pendentes podem impedir que a migração inicie ou termine o serviço do World Wide Web Publishing.

Próximo passo

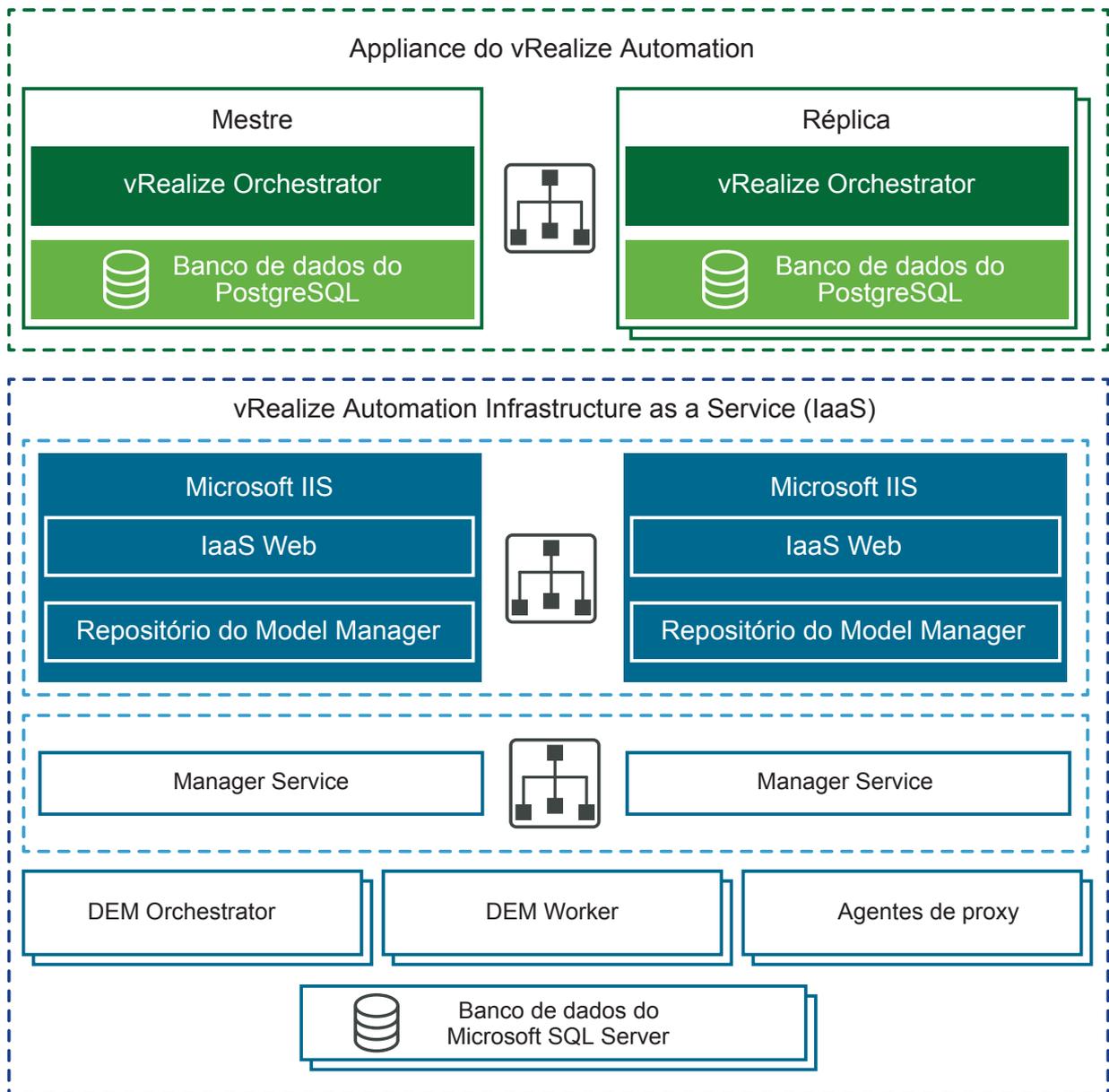
[Tarefas de pré-migração.](#)

Pré-requisitos para a migração para um ambiente de alta disponibilidade

Assegure uma migração bem-sucedida para um ambiente de alta disponibilidade revendo estes pré-requisitos.

Os ambientes de alta disponibilidade podem ter diferentes tamanhos. Uma implantação distribuída básica pode melhorar o vRealize Automation ao hospedar componentes do IaaS em servidores separados do Windows. Muitos ambientes de alta disponibilidade vão além, com appliances redundantes, servidores redundantes e balanceamento de carga para ainda mais capacidade. Implementações distribuídas grandes fornecem melhor dimensionamento, alta disponibilidade e recuperação de desastres.

Figura 1-18. Ambiente de alta disponibilidade d vRealize Automation



Pré-requisitos

- Verifique se você possui uma nova instalação de destino do vRealize Automation com um appliance virtual mestre e de réplica configurados para alta disponibilidade. Consulte [Considerações de Configuração de Alta Disponibilidade do vRealize Automation](#).
- Verifique se todos os appliances virtuais do vRealize Automation usam a mesma senha para o usuário raiz.
- Instale agentes de proxy relevantes no ambiente de destino, de acordo com esses requisitos.
 - O nome do agente de proxy de destino deve corresponder ao nome do agente de proxy de origem para os agentes de proxy do vSphere, do Hyper-V, do Citrix XenServer e de teste.

Observação Conclua essas etapas para obter um nome de agente.

- 1 No host do IaaS, faça login no Windows como usuário local com privilégios de **administrador**.
 - 2 Use o Windows Explorer para acessar o diretório de instalação do agente.
 - 3 Abra o arquivo `VRMAgent.exe.config`.
 - 4 Na marca `serviceConfiguration`, procure o valor do atributo `agentName`.
-
- O nome do endpoint do agente de proxy de destino deve corresponder ao nome do endpoint do agente de proxy de origem para os agentes de proxy do vSphere, do Hyper-V, do Citrix XenServer e de teste.
 - Não crie um endpoint para agentes de proxy do vSphere, do Hyper-V, do Citrix XenServer ou de teste no ambiente de destino.
- Verifique os números de versão dos componentes do vRealize Automation no appliance de destino do vRealize Automation.
 - a No seu ambiente de destino do vRealize Automation, inicie um navegador e acesse o console de gerenciamento do appliance do vRealize Automation em `https:// vra-va-hostname.domain.name:5480`.
 - b Faça login com o nome de usuário `root` e a senha que você digitou quando implantou o appliance.
 - c Selecione **Configurações do vRA > Cluster**.
 - d para expandir os registros de Nome do Host/Nó, para que você possa ver os componentes, clique no botão de expandir.

Verifique se os números de versão dos componentes do vRealize Automation correspondem em todos os nós do appliance virtual.

Verifique se os números de versão dos componentes IaaS do vRealize Automation correspondem em todos os nós IaaS.
 - Veja o artigo [51531](#) da Base de Conhecimento.

- Execute os seguintes passos para direcionar o tráfego apenas para o nó mestre.
 - a Desativar todos os nós redundantes.
 - b Remover os monitores de integridade para estes itens de acordo com a documentação do seu balanceador de carga:
 - Appliance virtual vRealize Automation
 - Site do IaaS
 - IaaS Manager Service
- Verifique se a versão do Microsoft SQL Server de destino para o banco de dados IaaS de destino do vRealize Automation é 2012, 2014 ou 2016.
- Verifique se a porta 22 está aberta entre os ambientes do vRealize Automation de origem e destino. A porta 22 é necessária para estabelecer conexões Secure Shell (SSH) entre appliances virtuais de origem e de destino.
- Verifique se o vCenter do endpoint tem recursos suficientes para concluir a migração.
- Verifique se você alterou as configurações de tempo limite do balanceador de carga do padrão para pelo menos 10 minutos.
- Verifique se a hora do sistema do ambiente de destino do vRealize Automation está sincronizada entre Cafe e os componentes do IaaS.
- Verifique se os nós do IaaS Web Service e do Model Manager no ambiente de destino têm o Java Runtime Environment correto. É preciso ter o Java SE Runtime Environment (JRE) 8, 64 bits, atualização 161 ou posterior instalado. Certifique-se de que as variáveis do sistema JAVA_HOME apontam para a versão Java que você tem instalada em cada nó IaaS. Revise o caminho se necessário.
- Verifique se cada nó IaaS tem pelo menos o PowerShell 3.0 ou versão posterior instalado.
- Verifique se os ambientes do vRealize Automation de origem e destino estão em execução.
- Certifique-se de que nenhuma atividade de usuário e provisionamento esteja ocorrendo no ambiente vRealize Automation de origem.
- Verifique se que qualquer software antivírus ou de segurança em execução nos nós do IaaS no ambiente de destino do vRealize Automation que possa interagir com o sistema operacional e seus componentes está configurado corretamente ou desativado.
- Verifique se o serviço da Web do IaaS e do Model Manager não precisam ser reiniciados devido a atualizações de instalação do Windows pendentes. As atualizações pendentes podem impedir que a migração inicie ou termine o serviço do World Wide Web Publishing.

Próximo passo

[Tarefas de pré-migração.](#)

Tarefas de pré-migração

Antes de migrar, você deve executar várias tarefas de pré-migração.

As tarefas de pré-migração realizadas antes da migração dos seus dados do ambiente do vRealize Automation de origem para o ambiente do vRealize Automation de destino variam dependendo do seu ambiente de origem.

Revisar as alterações introduzidas pela migração do vRealize Automation 6.2.x para o 7.x

O vRealize Automation 7 e versões posteriores introduzem várias mudanças funcionais durante e após o processo de atualização. Revise estas alterações antes de atualizar sua implantação do vRealize Automation 6.2.x para a versão mais recente.

Para obter informações sobre as diferenças entre o vRealize Automation 6.2.x e o 7.x, consulte [Considerações sobre a atualização para esta versão do vRealize Automation](#) em *Atualizando o vRealize Automation 6.2.5 para o 7.4*.

Observação A vRealize Production Test Upgrade Assist Tool analisa seu ambiente do vRealize Automation 6.2.x em busca de qualquer configuração de recurso que possa causar problemas de atualização e verifica se o seu ambiente está pronto para atualização. Para baixar essa ferramenta e a documentação relacionada, acesse a página de download do produto [VMware vRealize Production Test Tool](#).

Após migrar do vRealize Automation 6.2.x para a versão mais recente, os itens de catálogo que utilizam essas definições de propriedades aparecem no catálogo de serviços, mas não estão disponíveis para solicitação.

- Tipos de controle: caixa de seleção ou link.
- Atributos: Relacionamento, expressões regulares ou layouts de propriedades.

No vRealize Automation 7.x, as definições de propriedades não usam mais estes elementos. Você deverá recriar a definição de propriedade ou configurá-la para utilizar uma ação de script do vRealize Orchestrator em vez dos tipos de controle ou atributos incorporados. Para obter mais informações, consulte [Itens de catálogo aparecem no catálogo de serviços após a migração, mas não estão disponíveis para solicitação](#).

Aplicar o patch do agente de software

Antes de migrar do vRealize Automation 7.1 ou 7.3 para 7.4, você deve aplicar um hotfix ao appliance de origem para que possa atualizar os Agentes de Software para o TLS 1.2.

O protocolo Transport Layer Security (TLS) fornece a integridade de dados entre o navegador e o vRealize Automation. Esse hotfix possibilita aos Agentes de Software em seu ambiente de origem atualizar para o TLS 1.2. Essa atualização garante o mais alto nível de segurança e é necessária para o vRealize Automation 7.1 ou 7.3. Cada versão tem seu próprio hotfix.

Pré-requisitos

Um ambiente de origem do vRealize Automation 7.1 ou 7.3 em execução.

Procedimentos

- ◆ Aplique esse hotfix ao seu appliance do vRealize Automation 7.1 ou 7.3 de origem antes de migrar para o 7.4. Consulte o [artigo 52897 da Base de Conhecimento](#).

Próximo passo

[Alterar a configuração de DoDeletes no agente do vSphere para falso.](#)

Alterar a configuração de DoDeletes no agente do vSphere para falso

Se você migrar de um ambiente do 6.2.x vRealize Automation, deverá alterar o valor de DoDeletes de **verdadeiro** para **Falso** em seu agente de destino do vSphere antes da migração.

Pré-requisitos

Termine os pré-requisitos para a migração.

Procedimentos

- 1 Altere o valor de DoDeletes para **falso**.

Isso impede a exclusão de suas máquinas virtuais do ambiente de origem. Os ambientes de origem e de destino são executados em paralelo. As discrepâncias de lease podem surgir após a migração de produção ser validada.

- 2 Defina o valor de DoDeletes como **verdadeiro**, após a migração de produção ser validada, e seu ambiente de origem for encerrado.
- 3 Siga as etapas no procedimento do [Configure o vSphere Agent](#) para definir DoDeletes como **false**.

Próximo passo

[Preparar as máquinas virtuais do vRealize Automation para migração.](#)

Selecionar modelos no seu ambiente de origem do vRealize Automation 6.x

Antes de migrar de um vRealize Automation 6.x para 7.4, você deve selecionar os modelos da sua máquina virtual para se certificar de que cada modelo tenha uma configuração de memória mínima de pelo menos 4 MB.

Se você tiver um modelo de máquina virtual no seu ambiente de origem do vRealize Automation 6.x com menos de 4 MB de memória, a migração falhará. Conclua este procedimento para determinar se qualquer blueprint no ambiente de origem do 6.x possui menos de 4 MB de memória.

Pré-requisitos

Você está migrando do vRealize Automation 6.x para 7.4.

Procedimentos

- 1 Faça login no appliance do vRealize Automation primário pelo SSH como **raiz**.
Se seu vRealize Orchestrator for externo, faça login na máquina de host do Orchestrator.
- 2 Mude os diretórios para a pasta de dados PostgreSQL no host primário em `/var/vmware/vpostgres/current/pgdata/`.

- 3 Execute esse script para verificar se existem blueprints com memória especificada em menos de 4 MB.

```
select * from [vCAC].[dbo].[VirtualMachineTemplate] where IsHidden = 0 and
MemoryMB < 4;
```

onde vCAC é o nome do banco de dados.

- 4 Se o script encontrar algum blueprint com memória especificada em menos de 4 MB, execute esse script para atualizar a memória para pelo menos 4 MB.

```
update [vCAC].[dbo].[VirtualMachineTemplate] set MemoryMB = 4 where IsHidden = 0
and MemoryMB < 4;
```

onde vCAC é o nome do banco de dados.

Próximo passo

[Preparar as máquinas virtuais do vRealize Automation para migração.](#)

Preparar as máquinas virtuais do vRealize Automation para migração

Problemas conhecidos com a migração de máquinas virtuais do vRealize Automation 6.2.x podem causar problemas após a migração.

Veja o [artigo 000051531 da Base de conhecimento](#) e realize as correções relevantes nos seus ambientes antes da migração.

Próximo passo

[Reunir informações necessárias para a migração.](#)

Reunir informações necessárias para a migração

Use essas tabelas para registrar as informações necessárias para a migração dos seus ambientes de origem e destino.

Pré-requisitos

Termine de verificar os pré-requisitos para a sua situação.

- [Pré-requisitos para a migração para um ambiente mínimo.](#)
- [Pré-requisitos para a migração para um ambiente de alta disponibilidade.](#)

Tabela 1-81. Appliance de origem do vRealize Automation

| Opção | Descrição | Valor |
|----------------------|---|-------|
| Nome do host | Faça login no Gerenciamento do Appliance do vRealize Automation de origem. Localize o nome do host na guia Sistema . O nome de host deve ser um nome de domínio totalmente qualificado (FQDN). | |
| Nome de usuário raiz | raiz | |

Tabela 1-81. Appliance de origem do vRealize Automation (Continuação)

| Opção | Descrição | Valor |
|-----------------------------|--|-------|
| Senha raiz | A senha da raiz que você inseriu ao implementar o Appliance do vRealize Automation de origem. | |
| Local do pacote de migração | Caminho para um diretório existente no appliance de origem do vRealize Automation 6.2.x ou 7.x no qual o pacote de migração é criado. O diretório deve ter um espaço disponível de duas vezes o tamanho do banco de dados do vRealize Automation. A localização padrão é /storage. | |

Tabela 1-82. Appliance de destino do vRealize Automation

| Opção | Descrição | Valor |
|----------------------------------|--|-------|
| Nome de usuário raiz | raiz | |
| Senha raiz | A senha da raiz que você inseriu ao implementar o appliance do vRealize Automation de destino. | |
| Tenant padrão | vsphere.local | |
| Nome de usuário do administrador | administrador | |
| Senha do administrador | Senha do usuário administrator@vsphere.local que você digitou quando implantou o ambiente de destino do vRealize Automation. | |

Tabela 1-83. Banco de dados de destino do IaaS

| Opção | Descrição | Valor |
|--------------------------------|---|-------|
| Servidor de banco de dados | Local da instância do Microsoft SQL Server onde reside o banco de dados clonado. Se forem usadas uma instância denominada e uma porta não padrão, especifique no formato SERVER,PORT\INSTANCE-NAME. | |
| Nome do banco de dados clonado | Nome do banco de dados Microsoft SQL de IaaS do vRealize Automation 6.2.x/7.x de origem clonado para a migração. | |
| Modo de autenticação | Selecione Windows ou SQL Server. Se selecionar SQL Server, você precisará inserir nome e senha de login. | |
| Nome de login | Nome de login para o usuário do SQL Server que tenha a função db_owner para o banco de dados IaaS Microsoft SQL. | |
| Senha | Senha para o usuário do SQL Server. | |

Tabela 1-83. Banco de dados de destino do IaaS (Continuação)

| Opção | Descrição | Valor |
|--------------------------------|--|-------|
| Chave de criptografia original | Chave de criptografia original que você recupera do ambiente de origem. Consulte Obter a chave de criptografia do ambiente vRealize Automation de origem . | |
| Novo código de acesso | Uma série de palavras usadas para gerar uma nova chave de criptografia. Você usa essa senha toda vez que instala um novo componente de IaaS no ambiente de destino do vRealize Automation. | |

Próximo passo

[Obter a chave de criptografia do ambiente vRealize Automation de origem](#).

Obter a chave de criptografia do ambiente vRealize Automation de origem

Você deve inserir a chave de criptografia do ambiente vRealize Automation de origem como parte do procedimento de migração.

Pré-requisitos

Verifique se você tem privilégios de administrador na máquina virtual host do Manager Service no seu ambiente de origem.

Procedimentos

- 1 Abra um prompt de comando como administrador na máquina virtual que hospeda o Manager Service ativo no seu ambiente de origem e execute esse comando.

```
"C:\Program Files
(x86)\VMware\VCAC\Server\ConfigTool\EncryptionKeyTool\DynamicOps.Tools.Encryption
KeyTool.exe" key-read -c "C:\Program Files
(x86)\VMware\VCAC\Server\ManagerService.exe.config" -v
```

Se o seu diretório de instalação não estiver na localização padrão, C:\Program Files (x86)\VMware\VCAC, edite o caminho para exibir o seu diretório real de instalação.

- 2 Salve a chave que aparece após a execução do comando.

A chave é uma cadeia de caracteres longa parecida com este exemplo:

```
NRH+f/BlnCB6yvasLS3sxespgdkcFWAEuyV0g4lfryg=.
```

Próximo passo

- Se estiver migrando de um ambiente do vRealize Automation 6.2.x: [Adicionar cada tenant do ambiente de origem do vRealize Automation ao ambiente de destino](#).
- Se estiver migrando de um ambiente do vRealize Automation 7.x: [Listar administradores de tenants e IaaS do ambiente do vRealize Automation 6.2.x de origem](#).

Listar administradores de tenants e IaaS do ambiente do vRealize Automation 6.2.x de origem

Antes de migrar um ambiente vRealize Automation 6.2.x, você deve fazer uma lista dos administradores de tenants e do IaaS para cada tenant.

Realize o seguinte procedimento para cada tenant no console do vRealize Automation de origem.

Observação Se você migrar de um ambiente do vRealize Automation 7.x, não será necessário realizar esse procedimento.

Pré-requisitos

Faça login no console do vRealize Automation de origem como **Administrador** com a senha que você inseriu quando implantou o appliance do vRealize Automation de origem.

Observação Para um ambiente de alta disponibilidade, abra o console usando o nome de domínio totalmente qualificado do balanceador de carga do appliance virtual de origem: `https://vra-va-lb-hostname.domain.name/vcac`.

Procedimentos

- 1 Selecione **Administração > Tenants**.
- 2 Clique em um nome de tenant.
- 3 Clique em **Administradores**.
- 4 Faça uma lista de cada nome de usuário de administrador de tenants e do IaaS.
- 5 Clique em **Cancelar**.

Próximo passo

[Adicionar cada tenant do ambiente de origem do vRealize Automation ao ambiente de destino.](#)

Adicionar cada tenant do ambiente de origem do vRealize Automation ao ambiente de destino

Você deve adicionar tenants no ambiente de destino usando o nome de cada tenant no ambiente de origem.

Para uma migração bem-sucedida, é obrigatório que cada tenant no ambiente de origem seja criado no ambiente de destino. Você também deve usar um URL de acesso específica do tenant para cada tenant que for adicionado com o uso do nome do URL do tenant do ambiente de origem. Se houver tenants não utilizados no ambiente de origem que você não deseja migrar, exclua-os do ambiente de origem antes da migração.

Observação A validação de migração garante que o sistema de destino tenha pelo menos os mesmos tenants configurados na origem exigidos pelos pré-requisitos. Ela executa comparação de tenants com base nos nomes de URL de tenant que diferenciam maiúsculas de minúsculas, não nos nomes de tenant.

Realize esse procedimento para cada tenant no seu ambiente de origem.

- Ao migrar de um ambiente do vRealize Automation 6.2.x, você migra os tenants SSO2 e os repositório de identidades existentes para o VMware Identity Manager no ambiente de destino.
- Ao migrar de um ambiente do vRealize Automation 7.x, você migra os tenants e os repositório de identidades existentes do VMware Identity Manager no ambiente de origem para o VMware Identity Manager no ambiente de destino.

Pré-requisitos

- [Reunir informações necessárias para a migração.](#)
- Faça login no console do vRealize Automation de destino como **Administrador** com a senha que você inseriu quando implantou o appliance do vRealize Automation de destino.

Observação Para um ambiente de alta disponibilidade, abra o console usando o nome de domínio totalmente qualificado do balanceador de carga do appliance virtual de destino: `https://vra-va-lb-hostname.domain.name/vcac`.

Procedimentos

- 1 Selecione **Administração > Tenants**.
- 2 Clique no ícone **Novo** (+).
- 3 Na caixa de texto **Nome**, digite um nome de tenant que corresponda a um nome de tenant no ambiente de origem.
Por exemplo, se o nome do tenant no ambiente de origem for DEVTenant, insira **DEVTenant**.
- 4 (Opcional) Insira uma descrição na caixa de texto **Descrição**.
- 5 Na caixa de texto **Nome do URL**, insira um nome de URL de tenant que corresponda ao nome do URL do tenant no ambiente de origem.
O nome da URL é usado para anexar um identificador específico de tenant à URL do console do vRealize Automation.
Por exemplo, se o nome do URL para DEVTenant no ambiente de origem for dev, insira **dev** para criar o URL `https://vra-va-hostname.domain.name/vcac/org/dev`.
- 6 (Opcional) Insira um endereço de e-mail na caixa de texto **E-mail de contato**.
- 7 Clique em **Enviar e Avançar**.

Próximo passo

[Criar um administrador para cada tenant adicionado.](#)

Criar um administrador para cada tenant adicionado

Você deve criar um administrador para cada tenant adicionado ao ambiente de destino. Para criar um administrador, crie uma conta de usuário local e atribua privilégios de administrador de tenants à conta de usuário local.

Execute esse procedimento para cada tenant no seu ambiente de destino.

Pré-requisitos

- [Adicionar cada tenant do ambiente de origem do vRealize Automation ao ambiente de destino.](#)
- Faça login no console do vRealize Automation de destino como **Administrador** com a senha que você inseriu quando implantou o appliance do vRealize Automation de destino.

Observação Para um ambiente de alta disponibilidade, abra o console usando o nome de domínio totalmente qualificado do balanceador de carga do appliance virtual de destino: `https://vra-va-lb-hostname.domain.name/vcac`.

Procedimentos

- 1 Selecione **Administração > Tenants**.
- 2 Clique em um tenant que você adicionou.
Por exemplo, para DEVTenant, clique em **DEVTenant**.
- 3 Clique em **Usuários locais**.
- 4 Clique no ícone **Novo (+)**.
- 5 Em **Detalhes do usuário**, digite as informações solicitadas para criar uma conta de usuário local para atribuir a função de administrador de tenant.
O nome do usuário local deve ser exclusivo para o diretório local padrão, vsphere.local.
- 6 Clique em **OK**.
- 7 Clique em **Administradores**.
- 8 Insira o nome de usuário local na caixa de pesquisa **Administradores de tenant** e pressione Enter.
- 9 Clique no nome apropriado na pesquisa retorna para adicionar o usuário à lista de administradores de tenant.
- 10 Clique em **Concluir**.
- 11 Faça logoff do console.

Próximo passo

- Para uma implantação mínima: [Sincronizar usuários e grupos para um link do Active Directory Link antes da migração para um ambiente mínimo](#)
- Para uma implantação de alta disponibilidade: [Sincronizar usuários e grupos para um link do Active Directory antes da migração para um ambiente de alta disponibilidade](#)

Sincronizar usuários e grupos para um link do Active Directory Link antes da migração para um ambiente mínimo

Antes de importar seus usuários e grupos para uma implantação mínima do vRealize Automation, você deve conectar o vRealize Automation de destino ao seu link do Active Directory.

Realize esse procedimento para cada tenant. Se um tenant tiver mais de um Active Directory, realize este procedimento para cada Active Directory usado por esse tenant.

Pré-requisitos

- [Criar um administrador para cada tenant adicionado.](#)
- Verifique se você tem privilégios de acesso ao Active Directory.
- Faça logon no vRealize Automation como **administrador de tenants**.

Procedimentos

- 1 Selecione **Administração > Gerenciamento de Diretórios > Diretórios**.
- 2 Clique no ícone **Acrescentar Diretório** (+) e selecione **Acrescentar Active Directory sobre LDAP/IWA**.
- 3 Insira suas configurações de conta do Active Directory.
 - ◆ Para Active Directories não nativos

| Opção | Entrada de amostra |
|---|---|
| Nome do diretório | Insira um nome de diretório exclusivo. Selecione Active Directory sobre LDAP ao usar o Active Directory não nativo. |
| Esse diretório dá suporte à localização do serviço DNS | Desmarque esta opção. |
| DN base | Insira o nome diferenciado (DN) do ponto de início para as pesquisas do servidor de diretórios. Por exemplo, cn=users,dc=rainpole,dc=local . |
| Vincular DN | Insira todo o nome diferenciado (DN), incluindo o nome comum (CN), de uma conta de usuário do Active Directory que tenha privilégios para pesquisar os usuários. Por exemplo, cn=config_admin infra,cn=users,dc=rainpole,dc=local . |
| Vincular senha do DN | Digite a senha do Active Directory da conta que pode pesquisar usuários e clique em Testar Conexão para testar a conexão com o diretório configurado. |

- ◆ Para Active Directories nativos

| Opção | Entrada de amostra |
|---|--|
| Nome do diretório | Insira um nome de diretório exclusivo. Selecione Active Directory (Autenticação integrada do Windows) ao usar Active Directory nativo. |
| Nome do domínio | Insira o nome do domínio ao qual deseja ingressar. |
| Nome de usuário Admin do domínio | Insira o nome do usuário para o administrador do domínio. |
| Senha Admin do domínio | Insira a senha para o admin do domínio. |

| Opção | Entrada de amostra |
|-------------------------|---|
| Vincular UPN de usuário | Use o formato de endereço de e-mail para inserir o nome do usuário que pode autenticar com o domínio. |
| Vincular senha do DN | Insira a senha da conta vinculada ao Active Directory para a conta que pode pesquisar usuários. |

4 Clique em **Salvar e Avançar**.

A opção **Selecionar os Domínios** exibe uma lista de domínios.

5 Aceite a configuração de domínio padrão e clique em **Avançar**.

6 Verifique se os nomes de atributo estão mapeados para os atributos corretos do Active Directory e clique em **Avançar**.

7 Selecione os grupos e usuários para sincronizar.

a Clique no ícone **Novo** (+).

b Insira o nome do domínio e clique em **Localizar Grupos**.

Por exemplo, insira **dc=vcac,dc=local**.

c Para selecionar os grupos para sincronizar, clique em **Selecionar** e depois em **Avançar**.

d Em **Selecionar Usuários**, selecione os usuários que você deseja sincronizar e clique em **Avançar**.

Adicione somente usuários e grupos que são obrigados a usar o vRealize Automation. Não selecione **Sincronizar grupos aninhados**, a menos que todos os grupos em um ninhos precisem usar o vRealize Automation.

8 Confirme os usuários e grupos que estão sendo sincronizados com o diretório e clique em **Sincronizar Diretório**.

A sincronização de diretórios demora um pouco e é executada em segundo plano.

Próximo passo

[Executar a coleta de dados de Inventário de Segurança e Rede do NSX no ambiente do vRealize Automation de origem](#)

Sincronizar usuários e grupos para um link do Active Directory antes da migração para um ambiente de alta disponibilidade

Antes de importar usuários e grupos para um ambiente vRealize Automation de alta disponibilidade, você deve se conectar ao seu link do Active Directory.

- Realize as etapas de 1 a 8 para cada tenant. Se um tenant tiver mais de um Active Directory, realize este procedimento para cada Active Directory usado por esse tenant.
- Repita as etapas de 9 a 10 para cada provedor de identidade associado a um tenant.

Pré-requisitos

- [Criar um administrador para cada tenant adicionado](#).

- Verifique se você tem privilégios de acesso ao Active Directory.
- Faça login no vRealize Automation como **administrador de tenants**.

Procedimentos

- 1 Selecione **Administração > Gerenciamento de Diretórios > Diretórios**.
- 2 Clique no ícone **Acrescentar Diretório (+)** e selecione **Acrescentar Active Directory sobre LDAP/IWA**.
- 3 Insira suas configurações de conta do Active Directory.

◆ Para Active Directories não nativos

| Opção | Entrada de amostra |
|---|---|
| Nome do diretório | Insira um nome de diretório exclusivo. Selecione Active Directory sobre LDAP ao usar o Active Directory não nativo. |
| Esse diretório dá suporte à localização do serviço DNS | Desmarque esta opção. |
| DN base | Insira o nome diferenciado (DN) do ponto de início para as pesquisas do servidor de diretórios. Por exemplo, cn=users,dc=rainpole,dc=local . |
| Vincular DN | Insira todo o nome diferenciado (DN), incluindo o nome comum (CN), de uma conta de usuário do Active Directory que tenha privilégios para pesquisar os usuários. Por exemplo, cn=config_admin infra,cn=users,dc=rainpole,dc=local . |
| Vincular senha do DN | Digite a senha do Active Directory da conta que pode pesquisar usuários e clique em Testar Conexão para testar a conexão com o diretório configurado. |

◆ Para Active Directories nativos

| Opção | Entrada de amostra |
|---|--|
| Nome do diretório | Insira um nome de diretório exclusivo. Selecione Active Directory (Autenticação integrada do Windows) ao usar Active Directory nativo. |
| Nome do domínio | Insira o nome do domínio ao qual deseja ingressar. |
| Nome de usuário Admin do domínio | Insira o nome do usuário para o administrador do domínio. |
| Senha Admin do domínio | Insira a senha para a conta Admin do domínio. |
| Vincular UPN de usuário | Use o formato de endereço de e-mail para inserir o nome do usuário que pode autenticar com o domínio. |
| Vincular senha do DN | Insira a senha da conta vinculada ao Active Directory para a conta que pode pesquisar usuários. |

- 4 Clique em **Salvar e Avançar**.
A página **Selecionar os Domínios** exibe a lista de domínios.
- 5 Aceite a configuração de domínio padrão e clique em **Avançar**.

- 6 Verifique se os nomes de atributo estão mapeados para os atributos corretos do Active Directory e clique em **Avançar**.
- 7 Selecione os grupos e usuários para sincronizar.
 - a Clique no ícone **Novo** .
 - b Insira o nome do domínio e clique em **Localizar Grupos**.
Por exemplo, insira **dc=vcac,dc=local**.
 - c Para selecionar os grupos para sincronizar, clique em **Selecionar** e depois em **Avançar**.
 - d Na página **Selecionar Usuários**, selecione os usuários para sincronizar e clique em **Avançar**.
Adicione somente usuários e grupos que são obrigados a usar o vRealize Automation. Não selecione **Sincronizar grupos aninhados**, a menos que todos os grupos em um ninhos precisem usar o vRealize Automation.
- 8 Confirme os usuários e grupos que estão sendo sincronizados com o diretório e clique em **Sincronizar Diretório**.
A sincronização de diretórios demora um pouco e é executada em segundo plano.
- 9 Selecione **Administração > Gerenciamento de Diretórios > Provedores de Identidade** e clique no seu novo provedor de identidade.
Por exemplo, **WorkspaceIDP__1**.
- 10 Na página do provedor de identidade que você selecionou, adicione um conector para cada nó.
 - a Siga as instruções para **Adicionar um Conector**.
 - b Atualize o valor da propriedade do **Nome do host IdP** para apontar para o nome de domínio totalmente qualificado (FQDN) do balanceador de carga do vRealize Automation.
 - c Clique em **Salvar**.

Próximo passo

[Executar a coleta de dados de Inventário de Segurança e Rede do NSX no ambiente do vRealize Automation de origem.](#)

Executar a coleta de dados de Inventário de Segurança e Rede do NSX no ambiente do vRealize Automation de origem

Antes de migrar, você deve executar a coleta de dados de Inventário de Segurança e Rede do NSX no ambiente de origem de vRealize Automation.

Essa coleta de dados é necessária para que a ação de reconfiguração do balanceador de carga funcione no vRealize Automation 7.4 quando você migrar de implantações das versões 7.1, 7.2 ou 7.3.

Observação Você não precisa executar a coleta de dados no seu ambiente de origem quando migra do vRealize Automation 6.2.x. O vRealize Automation 6.2.x não é compatível com a ação Reconfigurar o Balanceador de Carga.

Procedimentos

- ◆ Execute a coleta de dados de Inventário de Segurança e Rede do NSX no seu ambiente do vRealize Automation de origem antes de migrar para o vRealize Automation 7.4. Consulte [Iniciar a coleta de dados do endpoint manualmente](#), no *Gerenciando o vRealize Automation*.

Próximo passo

[Clonar manualmente o banco de dados Microsoft SQL vRealize Automation do IaaS de origem.](#)

Clonar manualmente o banco de dados Microsoft SQL vRealize Automation do IaaS de origem

Antes da migração, você deve fazer backup do seu banco de dados Microsoft SQL do IaaS no ambiente de origem do vRealize Automation e restaurá-lo para um novo banco de dados em branco criado no ambiente de destino do vRealize Automation.

Pré-requisitos

- [Executar a coleta de dados de Inventário de Segurança e Rede do NSX no ambiente do vRealize Automation de origem.](#)
- Obtenha informações sobre como fazer o backup e a restauração de um banco de dados do SQL Server. Encontre artigos na [Microsoft Developer Network](#) sobre como criar um backup completo do banco de dados SQL Server e restaurar um banco de dados SQL Server para uma nova localização.

Procedimentos

- ◆ Crie um backup completo do banco de dados Microsoft SQL IaaS do vRealize Automation 6.2.x ou 7.0x de origem. Você pode usar o backup para restaurar o banco de dados SQL em um novo banco de dados em branco criado no ambiente de destino.

Próximo passo

[Tirar um snapshot do ambiente vRealize Automation de destino.](#)

Tirar um snapshot do ambiente vRealize Automation de destino

Tire um snapshot de todas as máquinas virtuais do vRealize Automation. Se a migração não for concluída com sucesso, você poderá tentar novamente usando os snapshots da máquina virtual.

Para obter mais informações, consulte a documentação do vSphere.

Pré-requisitos

[Clonar manualmente o banco de dados Microsoft SQL vRealize Automation do IaaS de origem.](#)

Próximo passo

Execute um dos procedimentos a seguir:

- [Migrar dados de origem do vRealize Automation para um ambiente mínimo do vRealize Automation 7.4.](#)
- [Migrar os dados de origem do vRealize Automation para um ambiente de alta disponibilidade do vRealize Automation 7.4.](#)

Procedimentos de migração

O procedimento que você executa para migrar os seus dados do ambiente vRealize Automation de origem depende de a migração estar sendo feita para um ambiente mínimo ou para um ambiente de alta disponibilidade.

Migrar dados de origem do vRealize Automation para um ambiente mínimo do vRealize Automation 7.4

É possível migrar dados do seu ambiente do vRealize Automation atual para uma nova instalação do vRealize Automation 7.4.

Todos os tenants no sistema de origem devem ser recriados no destino e passar pelo procedimento de migração dos repositórios de identidades. Para obter mais informações, consulte [Migrar repositórios de identidades para VMware Identity Manager](#).

Pré-requisitos

- [Reunir informações necessárias para a migração.](#)
- [Obter a chave de criptografia do ambiente vRealize Automation de origem.](#)
- [Adicionar cada tenant do ambiente de origem do vRealize Automation ao ambiente de destino.](#)
- [Criar um administrador para cada tenant adicionado.](#)
- [Sincronizar usuários e grupos para um link do Active Directory Link antes da migração para um ambiente mínimo.](#)
- [Clonar manualmente o banco de dados Microsoft SQL vRealize Automation do IaaS de origem.](#)
- [Tirar um snapshot do ambiente vRealize Automation de destino.](#)
- Faça login no Gerenciamento do Appliance do vRealize Automation de destino como **root** usando a senha que você inseriu quando implantou o appliance do vRealize Automation de destino.

Procedimentos

- 1 Selecione **Configurações do vRA > Migração**.
- 2 Insira as informações do appliance do vRealize Automation de origem.

| Opção | Descrição |
|-----------------------------|---|
| Nome do host | Nome do host do appliance do vRealize Automation de origem. |
| Nome de usuário raiz | raiz |
| Senha raiz | A senha raiz que você inseriu ao implementar o appliance do vRealize Automation. |
| Local do pacote de migração | Caminho para um diretório existente no appliance de origem do vRealize Automation 6.2.x ou 7.x no qual o pacote de migração é criado. |

3 Insira as informações do appliance do vRealize Automation de destino.

| Opção | Descrição |
|----------------------------------|--|
| Nome de usuário raiz | raiz |
| Senha raiz | A senha da raiz que você inseriu ao implementar o appliance do vRealize Automation de destino. |
| Tenant padrão | vsphere.local Não é possível modificar esse campo. |
| Nome de usuário do administrador | administrador Não é possível modificar esse campo. |
| Senha do administrador | Senha do usuário administrator@vsphere.local que você digitou quando implantou o ambiente de destino do vRealize Automation. |

4 Insira as informações para o servidor de banco de dados IaaS de destino.

| Opção | Descrição |
|--------------------------------|--|
| Servidor de banco de dados | O local do Microsoft SQL Server na qual o banco de dados Microsoft SQL IaaS do vRealize Automation restaurado reside. Se uma instância nomeada e uma porta não padrão forem usadas, insira-as no formato <i>SERVER,PORT\INSTANCE-NAME</i> . Se você configurar o Microsoft SQL Server de destino para usar o recurso de Grupo de Disponibilidade AlwaysOn (AAG), o SQL Server de destino deverá ser inserido como o nome do ouvinte AAG, sem uma porta ou nome de instância. |
| Nome do banco de dados clonado | Nome do banco de dados de origem Microsoft SQL de IaaS do vRealize Automation 6.2.x ou 7.x que você fez backup na origem e restaurou no destino. |
| Modo de autenticação | <ul style="list-style-type: none"> ■ Windows Se você usar o modo de autenticação do Windows, o usuário do serviço IaaS deverá ter a função db_owner do SQL Server. As mesmas permissões se aplicam ao utilizar o modo de autenticação do Servidor SQL. ■ SQL Server O SQL Server abre as caixas de texto Nome de login e Senha. |
| Nome de login | Nome de login do usuário do SQL Server com a função db_owner para o banco de dados Microsoft SQL de IaaS clonado. |
| Senha | Senha de usuário do SQL Server com a função db_owner para o banco de dados Microsoft SQL de IaaS clonado. |
| Chave de criptografia original | Chave de criptografia original que você recupera do ambiente de origem. Consulte Obter a chave de criptografia do ambiente vRealize Automation de origem . |
| Novo código de acesso | Uma série de palavras usadas para gerar uma nova chave de criptografia. Você usa essa senha toda vez que instala um novo componente de IaaS no ambiente de destino do vRealize Automation. |

5 Clique em **Validar**.

A página exibe o progresso da validação.

- Se todos os itens forem validados com êxito, vá para a etapa 8.

- Se a validação de um item falhar, inspecione a mensagem de erro e o arquivo de log de validação nos nós IaaS. Para conhecer as localizações do arquivo de log, consulte [Localizações dos logs de migração](#). Clique em **Editar Configurações** e edite o item com problema. Vá para a etapa 7.

6 Clique em **Migrar**.

A página exibe o progresso da migração.

- Se a migração for bem-sucedida, a página exibirá todas as tarefas de migração como concluídas.
- Se a migração não tiver êxito, inspecione os arquivos de log da migração no appliance virtual e nos nós IaaS. Para conhecer as localizações do arquivo de log, consulte [Localizações dos logs de migração](#).

Conclua essas etapas antes de reiniciar a migração.

- a Reverta seu ambiente vRealize Automation de destino para o estado que você capturou quando tirou um snapshot antes da migração.
- b Restaure o banco de dados Microsoft SQL de IaaS de destino usando o backup do banco de dados de IaaS da origem.

Próximo passo

[Tarefas de pós-migração](#).

Migrar os dados de origem do vRealize Automation para um ambiente de alta disponibilidade do vRealize Automation 7.4

É possível migrar seus dados do ambiente do vRealize Automation atual para uma nova instalação do vRealize Automation 7.4 configurada como ambiente de alta disponibilidade.

Todos os tenants no sistema de origem devem ser recriados no destino e passar pelo procedimento de migração dos repositórios de identidades. Para obter mais informações, consulte [Migrar repositórios de identidades para VMware Identity Manager](#).

Pré-requisitos

- [Reunir informações necessárias para a migração](#).
- [Obter a chave de criptografia do ambiente vRealize Automation de origem](#).
- [Adicionar cada tenant do ambiente de origem do vRealize Automation ao ambiente de destino](#).
- [Criar um administrador para cada tenant adicionado](#).
- [Sincronizar usuários e grupos para um link do Active Directory antes da migração para um ambiente de alta disponibilidade](#).
- [Clonar manualmente o banco de dados Microsoft SQL vRealize Automation do IaaS de origem](#).
- [Tirar um snapshot do ambiente vRealize Automation de destino](#).
- Faça login no Gerenciamento do Appliance do vRealize Automation de destino como **root** usando a senha que você inseriu quando implantou o appliance do vRealize Automation de destino.

Procedimentos

1 Selecione **Configurações do vRA > Migração**.

2 Insira as informações do Appliance do vRealize Automation de origem.

| Opção | Descrição |
|----------------------|--|
| Nome do host | Nome do host do appliance do vRealize Automation de origem. |
| Nome de usuário raiz | raiz |
| Senha raiz | A senha raiz que você inseriu ao implementar o appliance do vRealize Automation de origem. |

3 Insira as informações para a localização do pacote de migração no appliance do vRealize Automation de origem.

| Opção | Descrição |
|-----------------------------|---|
| Local do pacote de migração | Caminho para um diretório existente no appliance de origem do vRealize Automation 6.2.x ou 7.x no qual o pacote de migração é criado. |

4 Insira as informações do appliance do vRealize Automation de destino.

| Opção | Descrição |
|----------------------------------|--|
| Nome de usuário raiz | raiz |
| Senha raiz | A senha da raiz que você inseriu ao implementar o appliance do vRealize Automation de destino. |
| Tenant padrão | vsphere.local |
| Nome de usuário do administrador | administrador |
| Senha do administrador | Senha do usuário administrator@vsphere.local que você digitou quando implantou o ambiente de destino do vRealize Automation. |

5 Insira as informações para o servidor de banco de dados laaS de destino.

| Opção | Descrição |
|--------------------------------|---|
| Servidor de banco de dados | O local da instância do Microsoft SQL Server na qual o banco de dados Microsoft SQL laaS do vRealize Automation restaurado reside. Se uma instância nomeada e uma porta não padrão forem usadas, insira-as no formato <i>SERVER,PORT\INSTANCE-NAME</i> . Se você configurar o Microsoft SQL Server de destino para usar o recurso de Grupo de Disponibilidade AlwaysOn (AAG), o SQL Server de destino deverá ser inserido como o nome do ouvinte AAG, sem uma porta ou nome de instância. |
| Nome do banco de dados clonado | Nome do banco de dados de origem Microsoft SQL de laaS do vRealize Automation 6.2.x ou 7.x que você fez backup na origem e restaurou no destino. |

| Opção | Descrição |
|---------------------------------------|--|
| Modo de autenticação | <ul style="list-style-type: none"> ■ Windows Se você usar o modo de autenticação do Windows, o usuário do serviço IaaS deverá ter a função db_owner do SQL Server. As mesmas permissões se aplicam ao utilizar o modo de autenticação do Servidor SQL. ■ SQL Server O SQL Server abre as caixas de texto Nome de login e Senha. |
| Nome de login | Nome de login do usuário do SQL Server com a função db_owner para o banco de dados Microsoft SQL de IaaS clonado. |
| Senha | Senha de usuário do SQL Server com a função db_owner para o banco de dados Microsoft SQL de IaaS clonado. |
| Chave de criptografia original | Chave de criptografia original que você recupera do ambiente de origem. Consulte Obter a chave de criptografia do ambiente vRealize Automation de origem . |
| Novo código de acesso | Uma série de palavras usadas para gerar uma nova chave de criptografia. Você usa essa senha toda vez que instala um novo componente de IaaS no ambiente de destino do vRealize Automation. |

6 Clique em **Validar**.

A página exibe o progresso da validação.

- Se todos os itens forem validados com êxito, vá para a etapa 8.
- Se a validação de um item falhar, inspecione a mensagem de erro e o arquivo de log de validação nos nós IaaS. Para conhecer as localizações do arquivo de log, consulte [Localizações dos logs de migração](#). Clique em **Editar Configurações** e edite o item com problema. Vá para a etapa 7.

7 Clique em **Migrar**.

A página exibe o progresso da migração.

- Se a migração for bem-sucedida, a página exibirá todas as tarefas de migração como concluídas.
- Se a migração não tiver êxito, inspecione os arquivos de log da migração no appliance virtual e nos nós IaaS. Para conhecer as localizações do arquivo de log, consulte [Localizações dos logs de migração](#).

Conclua essas etapas antes de reiniciar a migração.

- a Reverta seu ambiente vRealize Automation de destino para o estado que você capturou quando tirou um snapshot antes da migração.
- b Restaure seu banco de dados Microsoft SQL IaaS de destino usando o backup do banco de dados IaaS de origem.

Próximo passo

[Tarefas de pós-migração](#).

Tarefas de pós-migração

Depois de migrar o vRealize Automation, realize as tarefas pós-migração que se aplicam à sua situação.

Observação Após migrar os armazenamentos de identidade, usuários do vRealize Code Stream devem reatribuir manualmente as funções do vRealize Code Stream.

Adicionar administradores de tenant e IaaS do ambiente do vRealize Automation 6.2.x de origem

Você deve excluir e restaurar os administradores tenant do vRealize Automation 6.2.x em cada tenant após a migração.

Realize o seguinte procedimento para cada tenant no console do vRealize Automation de destino.

Observação Se você migrar de um ambiente do vRealize Automation 7.x, não será necessário realizar esse procedimento.

Pré-requisitos

- Migração bem-sucedida para a versão mais recente do vRealize Automation.
- Faça login no console do vRealize Automation de destino como **Administrador** com a senha que você inseriu quando implantou o appliance do vRealize Automation de destino.

Procedimentos

- 1 Selecione **Administração > Tenants**.
- 2 Clique em um nome de tenant.
- 3 Clique em **Administradores**.
- 4 Faça uma lista de cada nome de administrador tenant e nome de usuário.
- 5 Aponte para cada administrador e clique no ícone excluir (Excluir) até excluir todos os administradores.
- 6 Clique em **Concluir**.
- 7 Na página Tenants, clique novamente no nome do tenant.
- 8 Clique em **Administradores**.
- 9 Insira o nome de cada usuário que você excluiu na caixa de pesquisa apropriada e pressione Enter.
- 10 Clique no nome do usuário apropriado dos resultados da pesquisa para voltar a adicionar esse usuário como administrador.

Quando terminar, a lista de administradores de tenants será igual à lista de administradores excluídos.

- 11 Clique em **Concluir**.

Executar a Conexão de Teste e verificar endpoints migrados

A migração para o vRealize Automation 7.4 faz alterações nos endpoints do ambiente de destino.

Depois de migrar para o vRealize Automation 7.4, você deve usar a ação **Testar Conexão** para todos os endpoints aplicáveis. Você pode precisar também de fazer ajustes a alguns endpoints migrados. Para mais informações, consulte [Considerações ao trabalhar com endpoints atualizados ou migrados](#).

A configuração de segurança padrão para endpoints atualizados ou migrados é não aceitar certificados não confiáveis.

Após a atualização ou migração de uma instalação anterior do vRealize Automation, se você estiver usando certificados não confiáveis, execute as seguintes etapas para todos os endpoints vSphere e NSX para ativar a validação do certificado. Caso contrário, as operações de endpoint falharão com erros de certificado. Para obter mais informações, consulte os artigos da Base de conhecimento da VMware *A comunicação do endpoint está interrompida após a atualização para o vRA 7.3 (2150230)* em <http://kb.vmware.com/kb/2150230> e *Como baixar e instalar os certificados raiz do vCenter Server para evitar avisos de certificado do navegador da Web (2108294)* em <http://kb.vmware.com/kb/2108294>.

- 1 Após a atualização ou migração, faça login na máquina do agente do vRealize Automation vSphere e reinicie seus agentes do vSphere usando a guia **Serviços**.

A migração pode não reiniciar todos os agentes. Portanto, reinicialize-os manualmente, se necessário.

- 2 Aguarde a conclusão de pelo menos um relatório ping. O relatório leva de um a dois minutos para ser concluído.

- 3 Quando os agentes do vSphere terminarem a coleta de dados, faça login no vRealize Automation como administrador de IaaS.

- 4 Clique em **Infraestrutura > Endpoints > Endpoints**.

- 5 Edite um endpoint do vSphere e clique em **Testar Conexão**.

- 6 Se aparecer um prompt de certificado, clique em **OK** para aceitar o certificado.

Se não aparecer um prompt de certificado, o certificado pode estar armazenado corretamente no momento em uma autoridade raiz confiável do serviço de hospedagem de máquina do Windows para o endpoint, por exemplo como uma máquina de agente de proxy ou máquina do DEM.

- 7 Clique em **OK** para aplicar a aceitação do certificado e salvar o endpoint.

- 8 Repita este procedimento para cada endpoint do vSphere.

- 9 Repita este procedimento para cada endpoint do NSX.

Se a ação **Testar Conexão** for bem-sucedida, mas algumas operações de coleta ou provisionamento de dados falharem, você pode instalar o mesmo certificado em todas as máquinas do agente que sirvam o endpoint e em todas as máquinas do DEM. Como alternativa, você pode desinstalar o certificado das máquinas existentes e repetir o procedimento anterior para o endpoint com falha.

Executar a coleta de dados de Inventário de Segurança e Rede do NSX no seu ambiente do vRealize Automation 7.4 de destino

Depois de migrar, você deve executar a coleta de dados de Inventário de Segurança e Rede do NSX no ambiente do vRealize Automation 7.4 de destino.

Essa coleta de dados é necessária para que a ação de reconfiguração do balanceador de carga funcione no vRealize Automation 7.4 para implantações das versões 7.1, 7.2 e 7.3.

Observação Você não precisará realizar essa coleta de dados se tiver migrado do vRealize Automation 6.2.x para a versão 7.4.

Pré-requisitos

- [Executar a coleta de dados de Inventário de Segurança e Rede do NSX no ambiente do vRealize Automation de origem](#) .
- Faça a migração bem-sucedida para o vRealize Automation 7.4.

Procedimentos

- ◆ Execute a coleta de dados de Inventário de Segurança e Rede do NSX no seu ambiente do vRealize Automation de destino antes de migrar para o vRealize Automation 7.4. Consulte [Iniciar a coleta de dados do endpoint manualmente](#), no *Gerenciando o vRealize Automation*.

Reconfigure balanceadores de carga após a migração para um ambiente de alta disponibilidade

Ao migrar para um ambiente de alta disponibilidade, você deve realizar essas tarefas para cada balanceador de carga depois de concluir a migração.

Pré-requisitos

[Migrar os dados de origem do vRealize Automation para um ambiente de alta disponibilidade do vRealize Automation 7.4](#).

Procedimentos

- 1 Restaure as configurações de verificação de integridade originais de forma que os nós de réplica possam aceitar o tráfego de entrada configurando os balanceadores de carga para esses itens.
 - Appliance do vRealize Automation.
 - Servidor Web IaaS que hospeda o Model Manager.
 - Manager Service.
- 2 Altere as configurações de tempo limite do balanceador de carga de volta para o padrão.

Migrando um servidor Orchestrator externo para o vRealize Automation 7.4.

Você pode migrar o servidor Orchestrator externo existente para uma instância do vRealize Orchestrator incorporada no vRealize Automation.

Você pode implantar o vRealize Orchestrator como uma instância do servidor externo e configurar o vRealize Automation para funcionar com essa instância externa, ou você pode configurar e usar o servidor vRealize Orchestrator que está incluído no Appliance do vRealize Automation.

A VMware recomenda que você migre o vRealize Orchestrator externo para o servidor Orchestrator que está incorporado no vRealize Automation. A migração de um Orchestrator externo para um incorporado fornece os seguintes benefícios:

- Reduz o custo total de propriedade.
- Simplifica o modelo de implantação.
- Melhora a eficiência operacional.

Observação Considere utilizar o vRealize Orchestrator externo nos seguintes casos:

- Múltiplos locatários no ambiente do vRealize Automation.
- Ambiente geograficamente disperso.
- Manipulação da carga de trabalho.
- Utilização de plug-ins específicos, como as versões do plug-in Site Recovery Manager anteriores à versão 6.5.

Migration Scenarios

The procedure of migrating an external vRealize Orchestrator instance to a vRealize Orchestrator instance embedded in vRealize Automation varies depending on the setup that you have. Several migration scenarios exist based on whether the external Orchestrator server is Windows-based or a virtual appliance, using the embedded database or an external one, and other conditions. You can combine the migration process with an upgrade of vRealize Orchestrator, vRealize Automation, or both. In this case, the migration procedure depends on the source versions of the products.

Migration Scenario Matrix

You can choose a migration scenario based on the source deployment.

| vRealize Orchestrator Deployment | vRealize Automation Deployment | Migration Scenario |
|---|---------------------------------|---|
| vRealize Orchestrator 6.0.3 Virtual Appliance | vRealize Automation 6.2.3 | Migrar um Appliance Virtual externo do vRealize Orchestrator 6.x para o vRealize Automation 7.4 |
| vRealize Orchestrator 6.0.4 on Windows | vRealize Automation 6.2.4 | Migrar um vRealize Orchestrator 6.x externo no Windows para o vRealize Automation 7.4 |
| vRealize Orchestrator 6.0.4 Virtual Appliance | vRealize Automation 6.2.4 | Migrar um Appliance Virtual externo do vRealize Orchestrator 6.x para o vRealize Automation 7.4 |
| vRealize Orchestrator 6.0.5 Virtual Appliance | vRealize Automation 6.2.5 | Migrar um Appliance Virtual externo do vRealize Orchestrator 6.x para o vRealize Automation 7.4 |
| vRealize Orchestrator 7.0 Virtual Appliance with an external Oracle Database 12 c | vRealize Automation 7.0 or IaaS | Migrate an External vRealize Orchestrator 7.x to vRealize Automation 7.2 |

| vRealize Orchestrator Deployment | vRealize Automation Deployment | Migration Scenario |
|--|-----------------------------------|--|
| vRealize Orchestrator 7.0.1 Virtual Appliance with an external PostgreSQL 9.3.9 database | vRealize Automation 7.0.1 or IaaS | Migrate an External vRealize Orchestrator 7.x to vRealize Automation 7.2 |
| vRealize Orchestrator 7.1 Virtual Appliance | vRealize Automation 7.1 | Migrate an External vRealize Orchestrator 7.x to vRealize Automation 7.2 |
| vRealize Orchestrator 7.2 Virtual Appliance | vRealize Automation 7.2 | Migrate an External vRealize Orchestrator 7.x to vRealize Automation 7.2 |
| vRealize Orchestrator 7.3 Virtual Appliance | vRealize Automation 7.3 | Migrar um vRealize Orchestrator 7.x externo para o vRealize Automation 7.4 |
| vRealize Orchestrator 6.0.3 on Windows | vRealize Automation 6.2.3 | Migrar a configuração do Orchestrator do Windows para o appliance virtual |

Migrar a configuração do Orchestrator do Windows para o appliance virtual

Migre sua configuração do Orchestrator Windows 5.5.x e 6.x autônomo para o Orchestrator Appliance.

Pré-requisitos

- Implante e configure um nó do Orchestrator na versão de destino. Veja [Configurando um servidor Orchestrator autônomo](#).
- Se o Orchestrator de origem usar um certificado de assinatura de pacote SHA1, certifique-se de regenerar o certificado usando um algoritmo de assinatura mais forte. O algoritmo de assinatura recomendado é SHA2.
- Pare o serviço do servidor do Orchestrator nas instâncias de origem e destino do Orchestrator.
- Faça backup do banco de dados do servidor Orchestrator de origem, incluindo o esquema do banco de dados.

Observação Se você pretende usar o ambiente de origem do Orchestrator até que o novo seja completamente configurado, crie uma cópia do banco de dados de origem. Caso contrário, você pode configurar o Orchestrator de destino para usar o mesmo banco de dados. Porém, nesse caso, o ambiente do Orchestrator de origem não funcionará mais porque o esquema do banco de dados é atualizado para a versão do Orchestrator de destino.

Procedimentos

- 1 Baixe a ferramenta de migração do servidor de destino do Orchestrator.
 - a Faça login no Control Center como **root**.
 - b Abra a página **Exportar/Importar Configuração** e clique na guia **Importar Configuração**.
 - c Baixe a ferramenta de migração conforme especificado na descrição na página ou baixe-a diretamente de https://orchestrator_server_IP_or_DNS_name:8283/vco-controlcenter/api/server/migration-tool.

2 Exporte a configuração do Orchestrator do servidor do Orchestrator de origem.

- a Extraia o arquivo baixado na pasta de instalação do Orchestrator.

O caminho padrão para a pasta de instalação do Orchestrator em uma instalação padrão do Windows é C:\Program Files\VMware\Orchestrator.

- b Defina a variável do ambiente PATH apontando-a para pasta lixeira do Java JRE instalado com o Orchestrator.

- c Use o prompt de comando do Windows para navegar até a pasta bin na pasta de instalação do Orchestrator.

Por padrão, o caminho para a pasta de lixeira é C:\Program Files\VMware\Orchestrator\migration-cli\bin.

- d Execute o comando export da linha de comando.

```
C:\Program Files\VMware\Orchestrator\migration-cli\bin\vro-migrate.bat export
```

Esse comando combina os arquivos de configuração e plug-ins do VMware vRealize Orchestrator em um arquivo de exportação.

Um arquivo com o nome de arquivo orchestrator-config-export-orchestrator_ip_address-date_hour.zip é criado em uma pasta igual à pasta migration-cli.

3 Importar a configuração para a instância de destino do Orchestrator.

- a Faça login no Control Center como **root**.

- b Abra **Importar/Exportar Configuração** no Control Center e clique na guia **Importar Configuração**.

- c Procure e selecione o arquivo .ZIP exportado da instância do Orchestrator de origem.

- d Insira a senha que você usou ao exportar a configuração.

Deixe em branco se você não exportou a configuração usando uma senha.

- e Selecione o tipo de importação.

- f Se você estiver importando a configuração para um servidor externo do Orchestrator, escolha se deseja ou não importar as configurações do banco de dados.

Observação Caso os servidores Orchestrator de origem e de destino não estiverem configurados para utilizar o mesmo banco de dados externo, deixe a caixa de seleção **Migrar configurações do banco de dados** desmarcada para evitar atualizar o esquema do banco de dados para uma versão mais recente. Caso contrário, o ambiente Orchestrator de origem para de funcionar.

Você deve configurar o banco de dados que o Orchestrator de destino vai utilizar antes da migração.

- g Clique em **IMPORTAR** para concluir a migração.

Uma mensagem afirma que a configuração foi importada com sucesso. O serviço do servidor Orchestrator da instância de destino do Orchestrator reinicia automaticamente.

- 4 Se o vRealize Orchestrator de destino usa um servidor de provedor de autenticação que seja diferente do que é usado pelo Orchestrator de origem, importe para o armazenamento confiável do Orchestrator de destino o certificado SSL do provedor de autenticação que está configurado para uso.
 - a Na página **Certificados** no Centro de Controle, clique em **Importar da URL**.
 - b Forneça o URL da instância do vRealize Automation ou do vSphere.

Uma mensagem indica que a migração foi concluída com êxito. O serviço do servidor Orchestrator é reiniciado automaticamente.

Próximo passo

Verifique se o Orchestrator está configurado adequadamente na página **Validar Configuração** no Centro de controle.

Migrar um vRealize Orchestrator 6.x externo no Windows para o vRealize Automation 7.4

Depois de atualizar o vRealize Automation da versão 6.x para a versão 7.4, você pode migrar seu Orchestrator 6.x externo existente instalado no Windows para o servidor Orchestrator integrado ao vRealize Automation 7.4.

Observação Se você tem um ambiente vRealize Automation distribuído com múltiplos nós Appliance do vRealize Automation, execute o procedimento de migração apenas no nó primário vRealize Automation.

Pré-requisitos

- Faça o upgrade ou migre o seu vRealize Automation para a versão 7.4. Para obter mais informações, consulte *Upgrade do vRealize Automation em Instalação ou Upgrade do vRealize Automation*.

- Se o Orchestrator de origem usar um certificado de assinatura de pacote SHA1, certifique-se de regenerar o certificado usando um algoritmo de assinatura mais forte. O algoritmo de assinatura recomendado é SHA2.
- Pare o serviço do servidor Orchestrator do Orchestrator externo.
- Faça backup do banco de dados, incluindo o esquema do banco de dados do servidor Orchestrator externo.

Procedimentos

- 1 Baixe a ferramenta de migração do servidor de destino do Orchestrator.
 - a Faça login para o Appliance do vRealize Automation pelo SSH como **raiz**.
 - b Baixe o arquivo `migration-tool.zip` que está localizado no diretório `/var/lib/vco/downloads`.
- 2 Exporte a configuração do Orchestrator do servidor do Orchestrator de origem.
 - a Defina a variável do ambiente PATH apontando-a para pasta lixeira do Java JRE instalado com o Orchestrator.
 - b Carregue a ferramenta de migração para o servidor Windows no qual o Orchestrator externo está instalado.
 - c Extraia o arquivo baixado na pasta de instalação do Orchestrator.

O caminho padrão para a pasta de instalação do Orchestrator em uma instalação padrão do Windows é `C:\Program Files\VMware\Orchestrator`.
 - d Execute o comando prompt do Windows como administrador e navegue para a pasta da lixeira na pasta de instalação do Orchestrator.

Por padrão, o caminho para a pasta de lixeira é `C:\Program Files\VMware\Orchestrator\migration-cli\bin`.
 - e Execute o comando `export` da linha de comando.

```
C:\Program Files\VMware\Orchestrator\migration-cli\bin\vro-migrate.bat export
```

Esse comando combina os arquivos de configuração e plug-ins do VMware vRealize Orchestrator em um arquivo de exportação.

O arquivo é criado na mesma pasta que a pasta `migration-cli`.

3 Migre a configuração exportada para o servidor Orchestrator incorporado no vRealize Automation 7.4.

- a No Appliance do vRealize Automation, pare o serviço do servidor Orchestrator e o serviço do Centro de Controle do servidor vRealize Orchestrator integrado.

```
service vco-server stop && service vco-configurator stop
```

- b Carregue o arquivo exportado de configuração para o diretório `/usr/lib/vco/tools/configuration-cli/bin` no Appliance do vRealize Automation.

- c Altere a propriedade do arquivo de configuração exportado do Orchestrator.

```
chown vco:vco orchestrator-config-export-orchestrator_ip_address-data_hora.zip
```

- d Importe o arquivo de configuração do Orchestrator para o servidor integrado vRealize Orchestrator, ao executar o script `vro-configure` com o comando `import`.

```
./vro-configure.sh import --type embedded --path orchestrator-config-export-orchestrator_appliance_ip-date_hour.zip
```

- e Remova todos os certificados do armazenamento de chaves do banco de dados.

```
./vro-configuration.sh untrust --reset-db
```

4 Migre o banco de dados para o banco de dados PostgreSQL interno, executando o script `vro-configure` com o comando `db-migrate`.

```
./vro-configure.sh db-migrate --sourceJdbcUrl JDBC_connection_URL --sourceDbUsername database_user --sourceDbPassword database_user_password
```

Observação Coloque entre aspas simples as senhas que contenham caracteres especiais.

O `JDBC_connection_URL` depende do tipo de banco de dados que você usa.

```
PostgreSQL: jdbc:postgresql://host:port/database_name
```

```
MSSQL: jdbc:jtds:sqlserver://host:port/database_name\; if using SQL authentication and MSSQL:
jdbc:jtds:sqlserver://host:port/database_name\;domain=domain\;useNTLMv2=TRUE if using Windows
authentication.
```

```
Oracle: jdbc:oracle:thin:@host:port:database_name
```

As informações de login do banco de dados padrão são:

| | |
|-------------------------------------|--------|
| <code>database_name</code> | vmware |
| <code>database_user</code> | vmware |
| <code>database_user_password</code> | vmware |

Você migrou com sucesso um vRealize Orchestrator 6.x externo instalado no Windows para uma instância do vRealize Orchestrator incorporada no vRealize Automation 7.4.

Próximo passo

Definir o servidor integrado do vRealize Orchestrator. Consulte [Configure o Servidor vRealize Orchestrator integrado](#).

Migrar um Appliance Virtual externo do vRealize Orchestrator 6.x para o vRealize Automation 7.4

Depois de atualizar o vRealize Automation da versão 6.x para a versão 7.4, você pode migrar seu Appliance Virtual do Orchestrator 6.x externo existente para o servidor Orchestrator integrado ao vRealize Automation 7.4.

Observação Se você tem um ambiente vRealize Automation distribuído com múltiplos nós Appliance do vRealize Automation, execute o procedimento de migração apenas no nó primário vRealize Automation.

Pré-requisitos

- Faça o upgrade ou migre o seu vRealize Automation para a versão 7.4. Para obter mais informações, consulte *Upgrade do vRealize Automation em Instalação ou Upgrade do vRealize Automation*.
- Se o Orchestrator de origem usar um certificado de assinatura de pacote SHA1, certifique-se de regenerar o certificado usando um algoritmo de assinatura mais forte. O algoritmo de assinatura recomendado é SHA2.
- Pare o serviço do servidor Orchestrator do Orchestrator externo.
- Faça backup do banco de dados, incluindo o esquema do banco de dados do servidor Orchestrator externo.

Procedimentos

- 1 Baixe a ferramenta de migração do servidor de destino do Orchestrator para o Orchestrator de origem.

- a Faça login para o Appliance Virtual 6.x vRealize Orchestrator pelo SSH como **raiz**.
- b No diretório `/var/lib/vco`, execute o comando `scp` para baixar o arquivo `migration-tool.zip`.

```
scp root@vra-va-hostname.domain.name:/var/lib/vco/downloads/migration-tool.zip ./
```

- c Execute o comando `unzip` para extrair o arquivo da ferramenta de migração.

```
unzip migration-tool.zip
```

- 2 Exporte a configuração do Orchestrator do servidor do Orchestrator de origem.

- a No diretório `/var/lib/vco/migration-cli/bin`, execute o comando `export`.

```
./vro-migrate.sh export
```

Esse comando combina os arquivos de configuração e plug-ins do VMware vRealize Orchestrator em um arquivo de exportação.

Um arquivo com nome de arquivo `orchestrator-config-export-orchestrator_ip_address-date_hour.zip` é criado na pasta `/var/lib/vco`.

- 3 Migre a configuração exportada para o servidor Orchestrator incorporado no vRealize Automation 7.4.

- a Faça login para o Appliance do vRealize Automation pelo SSH como **raiz**.
- b Pare o serviço do servidor Orchestrator e o serviço do Centro de Controle do servidor vRealize Orchestrator integrado.

```
service vco-server stop && service vco-configurator stop
```

- c No diretório `/usr/lib/vco/tools/configuration-cli/bin`, execute o comando `scp` para baixar o arquivo de configuração exportado.

```
scp root@orchestrator_ip_or_DNS_name:/var/lib/vco/orchestrator-config-export-orchestrator_ip_address-date_hour.zip ./
```

- d Altere a propriedade do arquivo de configuração exportado do Orchestrator.

```
chown vco:vco orchestrator-config-export-orchestrator_ip_address-date_hour.zip
```

- e Importe o arquivo de configuração do Orchestrator para o servidor integrado vRealize Orchestrator, ao executar o script vro-configure com o comando import.

```
./vro-configure.sh import --type embedded --path orchestrator-config-export-orchestrator_appliance_ip-date_hour.zip
```

- 4 Se o servidor Orchestrator externo do qual você deseja migrar usar o banco de dados PostgreSQL integrado, edite os arquivos de configuração do banco de dados.

- a No arquivo `/var/vmware/vpostgres/current/pgdata/postgresql.conf`, remova o comentário da linha `listen_addresses`.

- b Defina os valores de `listen_addresses` para um caractere universal (*).

```
listen_addresses = '*'
```

- c Anexe a linha ao arquivo `/var/vmware/vpostgres/current/pgdata/pg_hba.conf`.

```
host all all vra-va-ip-address/32 md5
```

Observação O arquivo `pg_hba.conf` exige o uso de um prefixo do formato CIDR em vez de um endereço IP e de uma máscara de sub-rede.

- d Reinicia o serviço de servidor do PostgreSQL.

```
service vpostgres restart
```

- 5 Migre o banco de dados para o banco de dados PostgreSQL interno, executando o script vro-configure com o comando db-migrate.

```
./vro-configure.sh db-migrate --sourceJdbcUrl JDBC_connection_URL --sourceDbUsername database_user
--sourceDbPassword database_user_password
```

Observação Coloque entre aspas simples as senhas que contenham caracteres especiais.

O *JDBC_connection_URL* depende do tipo de banco de dados que você usa.

PostgreSQL: `jdbc:postgresql://host:port/database_name`

MSSQL: `jdbc:jtds:sqlserver://host:port/database_name\;` if using SQL authentication and MSSQL:
`jdbc:jtds:sqlserver://host:port/database_name\;domain=domain\;useNTLMv2=TRUE` if using Windows authentication.

Oracle: `jdbc:oracle:thin:@host:port:database_name`

As informações de login do banco de dados padrão são:

| | |
|-------------------------------|--------|
| <i>database_name</i> | vmware |
| <i>database_user</i> | vmware |
| <i>database_user_password</i> | vmware |

- 6 Remova todos os certificados do armazenamento de chaves do banco de dados.

```
./vro-configure.sh untrust --reset-db
```

- 7 Reinstalar os plug-ins do Orchestrator.
 - a Faça login no Control Center como **root**.
 - b Clique em **Solução de Problemas**.
 - c Clique em **Forçar reinstalação de plug-ins**.
- 8 Inicie o serviço do servidor Orchestrator.
- 9 Reverte para a configuração padrão dos arquivos `postgresql.conf` e `pg_hba.conf`.
 - a Reinicia o serviço de servidor do PostgreSQL.

Você migrou com sucesso um Appliance Virtual do vRealize Orchestrator 6.x externo para uma instância do vRealize Orchestrator incorporada no vRealize Automation 7.4.

Próximo passo

Definir o servidor integrado do vRealize Orchestrator. Consulte [Configure o Servidor vRealize Orchestrator integrado](#).

Migrar um vRealize Orchestrator 7.x externo para o vRealize Automation 7.4

Você pode exportar a configuração da instância externa do Orchestrator existente e importá-la para o servidor do Orchestrator que está integrado em vRealize Automation.

Observação Se você tem diversos nós do Appliance do vRealize Automation, execute o procedimento de migração apenas no nó primário vRealize Automation.

Pré-requisitos

- Faça o upgrade ou migre o seu vRealize Automation para a versão 7.4. Para obter mais informações, consulte *Upgrade do vRealize Automation em Instalação ou Upgrade do vRealize Automation*.
- Pare o serviço do servidor Orchestrator do Orchestrator externo.
- Faça backup do banco de dados, incluindo o esquema do banco de dados do servidor Orchestrator externo.

Procedimentos

- 1 Exporte a configuração do servidor Orchestrator externo.
 - a Faça login no Centro de Controle do servidor Orchestrator externo como **raiz** ou como um **administrador**, dependendo da visão de origem.
 - b Pare o serviço do servidor do Orchestrator na página de **Opções de Inicialização** para prevenir alterações não desejadas ao banco de dados.
 - c Vá para a página **Configuração de Exportação/Importação**.
 - d Na página de **Configuração de Exportação**, selecione **Configuração do servidor de exportação**, **Plug-ins de pacote** e **Configurações do plug-in de exportação**.
- 2 Migre a configuração exportada para a instância integrada do Orchestrator.
 - a Carregue o arquivo de configuração exportado para o diretório `/usr/lib/vco/tools/configuration-cli/bin` do Appliance do vRealize Automation.
 - b Faça login para o Appliance do vRealize Automation pelo SSH como **raiz**.
 - c Pare o serviço do servidor Orchestrator e o serviço do Centro de Controle do servidor vRealize Orchestrator integrado.

```
service vco-server stop && service vco-configurator stop
```

- d Importe o arquivo de configuração do Orchestrator para o servidor integrado vRealize Orchestrator, ao executar o script `vro-configure` com o comando `import`.

```
./vro-configure.sh import --type embedded --path orchestrator-config-export-orchestrator_appliance_ip-date_hour.zip
```

3 Se o servidor Orchestrator externo do qual você deseja migrar usar o banco de dados PostgreSQL integrado, edite os arquivos de configuração do banco de dados.

- a No arquivo `/var/vmware/vpostgres/current/pgdata/postgresql.conf`, remova o comentário da linha `listen_addresses`.
- b Defina os valores de `listen_addresses` para um caractere universal (*).

```
listen_addresses = '*'
```

c Anexe a linha ao arquivo `/var/vmware/vpostgres/current/pgdata/pg_hba.conf`.

```
host all all vra-va-ip-address/32 md5
```

Observação O arquivo `pg_hba.conf` exige o uso de um prefixo do formato CIDR em vez de um endereço IP e de uma máscara de sub-rede.

d Reinicia o serviço de servidor do PostgreSQL.

```
service vpostgres restart
```

4 Migre o banco de dados para o banco de dados PostgreSQL interno, executando o script `vro-configure` com o comando `db-migrate`.

```
./vro-configure.sh db-migrate --sourceJdbcUrl JDBC_connection_URL --sourceDbUsername database_user --sourceDbPassword database_user_password
```

Observação Coloque entre aspas simples as senhas que contenham caracteres especiais.

O `JDBC_connection_URL` depende do tipo de banco de dados que você usa.

```
PostgreSQL: jdbc:postgresql://host:port/database_name
```

```
MSSQL: jdbc:jtds:sqlserver://host:port/database_name\; if using SQL authentication and MSSQL:
jdbc:jtds:sqlserver://host:port/database_name\;domain=domain\;useNTLMv2=TRUE if using Windows
authentication.
```

```
Oracle: jdbc:oracle:thin:@host:port:database_name
```

As informações de login do banco de dados padrão são:

| | |
|-------------------------------------|--------|
| <code>database_name</code> | vmware |
| <code>database_user</code> | vmware |
| <code>database_user_password</code> | vmware |

- 5 Remova todos os certificados do armazenamento de chaves do banco de dados.

```
./vro-configuration.sh untrust --reset-db
```

- 6 Reinstalar os plug-ins do Orchestrator.
 - a Faça login no Control Center como **root**.
 - b Clique em **Solução de Problemas**.
 - c Clique em **Forçar reinstalação de plug-ins**.
- 7 Inicie o serviço do servidor Orchestrator.
- 8 Reverte para a configuração padrão dos arquivos `postgresql.conf` e `pg_hba.conf`.
 - a Reinicia o serviço de servidor do PostgreSQL.

Você migrou com êxito uma instância do servidor Orchestrator externo para uma instância vRealize Orchestrator integrada ao vRealize Automation.

Próximo passo

Definir o servidor integrado do vRealize Orchestrator. Consulte [Configure o Servidor vRealize Orchestrator integrado](#).

Configure o Servidor vRealize Orchestrator integrado

Após exportar uma configuração externa do vRealize Orchestrator e importá-la para o vRealize Automation, configure o servidor do vRealize Orchestrator que está integrado ao vRealize Automation.

Pré-requisitos

Migre a configuração do vRealize Orchestrator externo para o interno.

Procedimentos

- 1 Faça login como raiz em uma sessão de prompt de comando no appliance do vRealize Automation.
- 2 Inicie os serviços para o Centro de Controle e o servidor do vRealize Orchestrator:

```
service vco-configuration start && service vco-server start
```

- 3 Faça login como raiz no Centro de Controle do vRealize Orchestrator integrado.

`https://vrealize-automation-appliance-FQDN:8283/vco-controlcenter/config`

Observação Você poderá ignorar a próxima etapa quando as versões internas e externas do vRealize Orchestrator forem as mesmas.

- 4 No Centro de Controle, clique em **Validar Configuração** e verifique se o vRealize Orchestrator está configurado corretamente.

- 5 No Centro de Controle, clique em **Certificados**, clique em **Certificado de Assinatura do Pacote** e gere um novo certificado de assinatura do pacote.
- 6 No Centro de Controle, clique em **Configurar Provedor de Autenticação**.
Tenant padrão e **Grupo de administradores** são definidos como os valores padrão `vsphere.local` e `vsphere.local\vcoadmins`. Altere os padrões para os valores do seu ambiente.
- 7 Na interface de gerenciamento do appliance do vRealize Automation, em **Serviços**, verifique se o `vco-server` está REGISTRADO.
- 8 Selecione os serviços do vco do servidor externo do vRealize Orchestrator e clique em **Cancelar registro**.

Próximo passo

- Importe quaisquer certificados que eram confiáveis no servidor externo do vRealize Orchestrator para o armazenamento de confiança do vRealize Orchestrator integrado. Para obter mais informações, consulte [Gerenciar certificados do Orchestrator](#).
- Associe os nós de réplica do vRealize Automation ao cluster do vRealize Automation para sincronizar a configuração do vRealize Orchestrator.

Para mais informações, consulte *Reconfigurar o vRealize Orchestrator integrado para suportar alta disponibilidade em Instalando ou Atualizando o vRealize Automation*.

Observação As instâncias vRealize Orchestrator são automaticamente clusterizadas e disponibilizadas para uso.

- Reinicie o serviço `vco-configurator` em todos os nós do cluster.
- Atualize o endpoint do vRealize Orchestrator para apontar para o servidor do vRealize Orchestrator integrado migrado.
- Adicione o host vRealize Automation e o host IaaS ao inventário do plug-in vRealize Automation ao executar Adicionar um host vRA e Adicionar o host IaaS de fluxos de trabalho de um host vRA.

Atualizar vRealize Orchestrator integrado para confiar em certificados do vRealize Automation

Se você atualizar ou alterar certificados do Appliance do vRealize Automation ou IaaS, precisará atualizar o vRealize Orchestrator para confiar em certificados novos ou atualizados.

Este procedimento se aplica a todas as implantações do vRealize Automation que usam uma instância integrada do vRealize Orchestrator. Se você usar uma instância externa do vRealize Orchestrator, consulte [Atualizar o vRealize Orchestrator para confiar em certificados do vRealize Automation](#).

Observação Esse procedimento redefine a autenticação do tenant e do grupo de volta para as configurações padrão. Se você tiver personalizado a configuração da autenticação, observe as alterações para que possa configurar a autenticação novamente após concluir o procedimento.

Consulte a documentação do vRealize Orchestrator para obter mais informações sobre como atualizar e substituir certificados do vRealize Orchestrator.

Se você substituir ou atualizar os certificados do vRealize Automation sem concluir esse procedimento, o Centro de Controle do vRealize Orchestrator poderá estar inacessível e poderão aparecer erros nos arquivos de log do vco-server e do vco-configurator.

Problemas com certificados de atualização também poderão ocorrer se o vRealize Orchestrator estiver configurado para ser autenticado em relação a um tenant e um grupo do vRealize Automation diferentes. Consulte <https://kb.vmware.com/kb/2147612>.

Procedimentos

- 1 Interrompa os serviços do servidor e do Centro de Controle do vRealize Orchestrator.

```
service vco-server stop
service vco-configurator stop
```

- 2 Redefina o provedor de autenticação do vRealize Orchestrator.

- a Execute o comando `/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh reset-authentication`.
- b Exclua o `/etc/vco/app-server/vco-registration-id`.
- c Execute o `vcac-vami vco-service-reconfigure`

- 3 Inicie os serviços do servidor e do centro de controle do vRealize Orchestrator.

```
service vco-server start
service vco-configurator start
```

As diferenças do Centro de Controle entre o Orchestrator externo e integrado

Alguns dos itens de menu que estão disponíveis no Centro de Controle de um vRealize Orchestrator externo não estão incluídos na exibição padrão do Centro de Controle de uma instância integrada do Orchestrator.

No centro de controle do servidor do Orchestrator integrado, algumas opções estão ocultas por padrão.

| Item de Menu | Detalhes |
|--|--|
| Licenciamento | O Orchestrator integrado está pré-configurado para usar o vRealize Automation como um provedor de licença. |
| Configuração de Exportação/Importação | A configuração do Orchestrator integrada está incluída nos componentes exportados do vRealize Automation. |
| Configurar banco de dados | O Orchestrator integrado usa o banco de dados que é usado pelo vRealize Automation. |
| Programa de Aperfeiçoamento da Experiência do Cliente | Você pode se associar ao Programa de Aperfeiçoamento da Experiência do Cliente (PAEC) na interface de gerenciamento do appliance vRealize Automation. Consulte o <i>Programa de Aperfeiçoamento da Experiência do Cliente em Gerenciando o vRealize Automation</i> . |

Outras opções que estão ocultas na exibição padrão do Centro de Controle são a caixa de texto do **endereço do host** e o botão **CANCELAR REGISTRO** na página **Configurar Provedor de Autenticação**.

Observação Para consultar todo o conjunto de opções do Centro de Controle no vRealize Orchestrator que está integrado em vRealize Automation, você deve acessar a página avançada de Gerenciamento do Orchestrator em https://vra-va-hostname.domain.name_or_load_balancer_address:8283/vco-controlcenter/#/?advanced e clicar no botão F5, no teclado para atualizar a página.

Reconfigurar o endpoint do vRealize Automation no vRealize Orchestrator de destino

Use o procedimento a seguir para reconfigurar o endpoint do vRealize Automation no vRealize Orchestrator de destino incorporado.

Pré-requisitos

- Migração bem-sucedida para a versão mais recente do vRealize Automation.
- Conecte-se ao vRealize Orchestrator de destino usando o cliente vRealize Orchestrator. Para obter informações, consulte *Usando o cliente do VMware vRealize Orchestrator* na [documentação do vRealize Orchestrator](#).

Procedimentos

- 1 Selecione **Design** no menu suspenso superior.
- 2 Clique em **Inventário**.
- 3 Expanda **vRealize Automation**.

- Se você tiver migrado de um ambiente mínimo, identifique os endpoints que contenham o nome de domínio totalmente qualificado (FQDN) do host do appliance de vRealize Automation de origem. Se você tiver migrado de um ambiente de alta disponibilidade, identifique os endpoints que contenham o FQDN do balanceador de carga de appliance de origem.

| Se você encontrar os endpoints que contenham o FQDN, conclua estas etapas. | Se você não encontrar os endpoints que contenham o FQDN, conclua estas etapas. |
|---|---|
| <ol style="list-style-type: none"> Clique em Fluxos de Trabalho. Clique no botão Expandir para selecionar Biblioteca > vRealize Automation > Configuração. Siga uma destas etapas. <ul style="list-style-type: none"> Se você tiver migrado de um ambiente mínimo, execute o fluxo de trabalho Remover um host vRA para cada endpoint que contenha o FQDN do host de appliance do vRealize Automation de origem. Se você tiver migrado de um ambiente de alta disponibilidade, execute o fluxo de trabalho Remover um host vRA para cada endpoint que contenha o FQDN do balanceador de carga do appliance de origem. | <ol style="list-style-type: none"> Clique em Recursos. Clique no ícone de atualização na barra de ferramentas superior. Clique no botão Expandir para selecionar Biblioteca > vCACCAFE > Configuração. Siga uma destas etapas. <ul style="list-style-type: none"> Se você tiver migrado de um ambiente mínimo, exclua cada recurso que tenha uma propriedade URL que contenha o FQDN do host de appliance do vRealize Automation de origem. Se você tiver migrado de um ambiente de alta disponibilidade, exclua cada recurso que tenha uma propriedade URL que contenha o FQDN do balanceador de carga do appliance do vRealize Automation de origem. |

- Clique em **Fluxos de Trabalho**.
- Clique no botão Expandir para selecionar **Biblioteca > vRealize Automation > Configuração**.
- Para adicionar o appliance vRealize Automation de destino ou, se você tiver migrado para uma implantação de alta disponibilidade, o host com balanceamento de carga, execute o fluxo de trabalho **Adicionar um host vRA usando o registro de componentes**.

Reconfigurar o endpoint de infraestrutura do vRealize Automation no vRealize Orchestrator de destino

Use o procedimento a seguir para reconfigurar o endpoint de Infraestrutura do vRealize Automation no vRealize Orchestrator de destino incorporado.

Pré-requisitos

- Migração bem-sucedida para a versão mais recente do vRealize Automation.
- Conecte-se ao vRealize Orchestrator de destino usando o cliente vRealize Orchestrator. Para obter informações, consulte *Usando o cliente do VMware vRealize Orchestrator* na [documentação do vRealize Orchestrator](#).

Procedimentos

- Selecione **Design** no menu suspenso superior.
- Clique em **Inventário**.
- Expanda **Infraestrutura do vRealize Automation**.

- 4 Caso tenha migrado de um ambiente pequeno, identifique os endpoints que contêm o nome completo do domínio qualificado (FQDN) do host da infraestrutura do vRealize Automation de origem. Se você tiver migrado de um ambiente de alta disponibilidade, identifique os endpoints que contenham o FQDN do balanceador de carga de appliance de origem.

| Se você encontrar os endpoints que contenham o FQDN, conclua estas etapas. | Se você não encontrar os endpoints que contenham o FQDN, conclua estas etapas. |
|---|--|
| <ol style="list-style-type: none"> 1 Clique em Fluxos de Trabalho. 2 Clique no botão Expandir para selecionar Biblioteca > vRealize Automation > Administração de Infraestrutura > Configuração. 3 Siga uma destas etapas. <ul style="list-style-type: none"> ■ Se você tiver migrado de um ambiente mínimo, execute o fluxo de trabalho Remover um host IaaS para cada endpoint que contenha o FQDN do host de infraestrutura do vRealize Automation de origem. ■ Se você tiver migrado de um ambiente de alta disponibilidade, execute o fluxo de trabalho Remover um host IaaS para cada endpoint que contenha o FQDN do balanceador de carga de host de infraestrutura do vRealize Automation de origem. | <ol style="list-style-type: none"> 1 Clique em Recursos. 2 Clique no ícone de atualização na barra de ferramentas superior. 3 Clique no botão Expandir para selecionar Biblioteca > vCAC > Configuração. 4 Siga uma destas etapas. <ul style="list-style-type: none"> ■ Se você tiver migrado de um ambiente mínimo, exclua cada recurso que tenha uma propriedade host que contenha o FQDN do host de infraestrutura do vRealize Automation de origem ■ Se você tiver migrado de um ambiente de alta disponibilidade, exclua cada recurso que tenha uma propriedade host que contenha o FQDN do balanceador de carga do host de infraestrutura do vRealize Automation de origem. |

- 5 Clique em **Fluxos de Trabalho**.
- 6 Clique no botão Expandir para selecionar **Biblioteca > vRealize Automation > Configuração**.
- 7 Para adicionar o host de infraestrutura do vRealize Automation de destino ou, se você tiver migrado para uma implantação de host de alta disponibilidade, execute o fluxo de trabalho **Adicionar o host IaaS de um host vRA**.

Instalar a personalização do vRealize Orchestrator

É possível executar um fluxo de trabalho para instalar os stubs personalizados de fluxo de trabalho de alteração de estado e os fluxos de trabalho de operação de menu do vRealize Orchestrator.

Para obter informações, consulte [Instalar a personalização do vRealize Orchestrator](#).

Pré-requisitos

Migração bem-sucedida para a versão mais recente do vRealize Automation.

Reconfigurar o endpoint de infraestrutura do vRealize Orchestrator incorporado no vRealize Automation de destino

Ao migrar de um ambiente do vRealize Automation 6.2.x, você deve atualizar o URL do endpoint de infraestrutura que aponta para o servidor vRealize Orchestrator incorporado de destino.

Pré-requisitos

- Faça a migração bem-sucedida para o vRealize Automation 7.4.

- Faça login no console de destino do vRealize Automation.
 - a Abra o console do vRealize Automation usando o nome de domínio totalmente qualificado do appliance virtual de destino: `https://vra-va-hostname.domain.name/vcac`.

Para um ambiente de alta disponibilidade, abra o console usando o nome de domínio totalmente qualificado do balanceador de carga do appliance virtual de destino: `https://vra-va-lb-hostname.domain.name/vcac`.
 - b Faça login como um usuário administrador do IaaS.

Procedimentos

- 1 Selecione **Infraestrutura > Endpoints > Endpoints**.
- 2 Na página Endpoints, selecione o endpoint do vRealize Orchestrator e clique em **Editar**.
- 3 Na caixa de texto Endereço, edite o URL do endpoint do vRealize Orchestrator.
 - Se você tiver migrado para um ambiente mínimo, substitua o URL do endpoint do vRealize Orchestrator por `https://vra-va-hostname.domain.name:443/vco`.
 - Se você tiver migrado para um ambiente de alta disponibilidade, substitua o URL do endpoint do vRealize Orchestrator por `https://vra-va-lb-hostname.domain.name:443/vco`.
- 4 Clique em **OK**.
- 5 Execute manualmente uma coleta de dados no endpoint do vRealize Orchestrator.
 - a Na página Endpoints, selecione o endpoint do vRealize Orchestrator.
 - b Selecione **Ações > Coleta de Dados**.

Verifique se a coleta de dados foi bem-sucedida.

Reconfigurar o endpoint do Azure no ambiente vRealize Automation de destino

Após a migração, você deve reconfigurar seu endpoint do Microsoft Azure.

Realize esse procedimento para cada endpoint do Azure.

Pré-requisitos

- Faça a migração bem-sucedida para a versão mais recente do vRealize Automation 7.4.
- Faça login no console de destino do vRealize Automation.
 - a Abra o console do vRealize Automation usando o nome de domínio totalmente qualificado do appliance virtual de destino: `https://vra-va-hostname.domain.name/vcac`.

Para um ambiente de alta disponibilidade, abra o console usando o nome de domínio totalmente qualificado do balanceador de carga do appliance virtual de destino: `https://vra-va-lb-hostname.domain.name/vcac`.
 - b Faça login como um usuário administrador do IaaS.

Procedimentos

- 1 Selecione **Administração > Configuração do vRO > Endpoints**.
- 2 Selecione um endpoint do Azure.
- 3 Clique em **Editar**.
- 4 Clique em **Detalhes**.
- 5 Na caixa de texto **Segredo do cliente**, insira o segredo do cliente original.
- 6 Clique em **Concluir**.
- 7 Repita para cada endpoint do Azure.

Migrar o Automation Application Services do vRealize Automation 6.2.x para a versão 7.4

Você pode usar a VMware vRealize Application Services Migration Tool para migrar seus blueprints de serviços de aplicativos existentes e perfis de implantação do VMware vRealize Application Services 6.2.x para o vRealize Automation 7.4.

Pré-requisitos

Migração bem-sucedida para a versão mais recente do vRealize Automation.

Procedimentos

- ◆ Para baixar a VMware vRealize Application Services Migration Tool, conclua estas etapas.
 - a Clique em [Baixar VMware vRealize Automation](#).
 - b Selecione **Drivers e Ferramentas > VMware vRealize Application Services Migration Tool**.

Excluir o banco de dados Microsoft SQL IaaS do vRealize Automation de destino original

Você pode excluir o banco de dados IaaS original após a conclusão da migração.

Pré-requisitos

Migração bem-sucedida para a versão mais recente do vRealize Automation.

Seu ambiente migrado não usa o banco de dados Microsoft SQL IaaS do vRealize Automation original que foi criado com a instalação do ambiente do vRealize Automation de destino. É possível excluir com segurança esse banco de dados IaaS original do Microsoft SQL Server após a conclusão da migração.

Atualizar o conteúdo do menu Localização do centro de dados após a migração

Após a migração, você deve adicionar qualquer localização de centro de dados personalizada ausente ao menu suspenso **Localização**.

Após a migração para a versão mais recente do vRealize Automation, as localizações de centro de dados no menu suspenso **Localização** na página Recursos de Processamento são revertidas para a lista padrão. Embora as localizações do centro de dados personalizadas estejam ausentes, todas as configurações de recurso de processamento são migradas com êxito, e a propriedade `Vrm.DataCenter.Location` não é afetada. Você ainda pode adicionar localizações de centro de dados personalizadas ao menu **Localização**.

Pré-requisitos

Migre para a versão mais recente do vRealize Automation.

Procedimentos

- ◆ Adicione qualquer localização de centro de dados personalizada ausente ao menu suspenso **Localização**. Consulte o Cenário : [adicionar localizações de centro de dados para implantações entre regiões no](#) .

Atualizando os agentes de software para o TLS 1.2

Depois de migrar o vRealize Automation 7.1, 7.2, 7.3 ou 7.3.1 para a versão 7.4, você deve executar várias tarefas para atualizar os Agentes de Software do seu ambiente de origem para o Transport Layer Security (TLS) 1.2

Começando com o vRealize Automation 7.4, o TLS 1.2 é o único protocolo TLS suportado para comunicação de dados entre o vRealize Automation e seu navegador. Após a migração, você deve atualizar os modelos da máquina virtual existentes do seu ambiente de origem do vRealize Automation 7.1 ou 7.3, bem como quaisquer máquinas virtuais existentes.

Atualizar modelos da máquina virtual do ambiente de origem

Você deve atualizar os modelos existentes do vRealize Automation 7.1, 7.2, 7.3 ou 7.3.1 após concluir a migração para 7.4 para que os Agentes de Software usem o protocolo TLS 1.2.

O agente guest e o código de bootstrap do agente devem ser atualizados nos modelos de ambiente do origem. Se você estiver usando uma opção de clone vinculado, talvez seja necessário remapear os modelos com as máquinas virtuais recém-criadas e seus snapshots.

Para atualizar seus modelos, você deve concluir estas tarefas.

- 1 Faça login no vSphere.
- 2 Converta cada modelo do vRealize Automation 7.1, 7.2, 7.3 ou 7.3.1 em uma máquina virtual e ligue a máquina.
- 3 Importe o instalador de software adequado e execute o instalador de software em cada máquina virtual.
- 4 Converta cada máquina virtual em um modelo novamente.

Use esse procedimento para localizar os instaladores de software para Linux ou Windows.

Pré-requisitos

- [Aplicar o patch do agente de software](#) se você tiver migrado do vRealize Automation 7.1 ou 7.3 para 7.4.
- Migração bem-sucedida do vRealize Automation 7.1, 7.2, 7.3 ou 7.3.1 para 7.4.

Procedimentos

- 1 Inicie um navegador e abra a tela inicial do appliance do vRealize Automation 7.4 usando o nome de domínio completo do appliance virtual: `https://vra-va-hostname.domain.name`.

- 2 Clique na **página de agentes guest e de software**.
- 3 Siga as instruções para os instaladores de software Linux ou Windows.

Próximo passo

[Identificar máquinas virtuais que precisam de atualização do Agente de Software.](#)

Identificar máquinas virtuais que precisam de atualização do Agente de Software

Você pode usar o Serviço de Integridade no Console do vRealize Automation para identificar máquinas virtuais que precisam da atualização do agente para o TLS 1.2.

Às vezes, o patch aplicado ao seu ambiente de origem vRealize Automation não atualiza todas as máquinas virtuais. Você pode usar o Serviço de Integridade para identificar as máquinas virtuais que ainda precisam de uma atualização do agente de software para o TLS 1.2. Todos os agentes de software no ambiente de destino devem ser atualizados para procedimentos de pós-provisionamento.

Pré-requisitos

- [Aplicar o patch do agente de software](#) se você tiver migrado do vRealize Automation 7.1 ou 7.3 para 7.4.
- Você migrou de vRealize Automation 7.1, 7.2, 7.3 ou 7.3.1 para 7.4 com êxito.
- Você está conectado ao vRealize Automation 7.4 no appliance virtual primário.

Procedimentos

- 1 Clique em **Administração > Integridade**.
- 2 Clique em **Nova Configuração**.
- 3 Na página Detalhes da Configuração, forneça as informações solicitadas.

| Opção | Comentário |
|-------------|---|
| Nome | Insira a verificação do Agente de SW |
| Descrição | Adicione uma descrição opcional, por exemplo, Localizar os agentes de software para atualizar para o TLS 1.2 |
| Produto | Selecione vRealize Automation 7.4.0. |
| Programação | Selecione Nenhum(a). |

- 4 Clique em **Avançar**.
- 5 Na página Selecionar pacotes de teste, selecione **Testes do sistema para o vRealize Automation e Testes de Tenant para o vRealize Automation**.
- 6 Clique em **Avançar**.

- 7 Na página Parâmetros da Configuração, forneça as informações solicitadas.

Tabela 1-84. Appliance virtual vRealize Automation

| Opção | Descrição |
|--|---|
| Endereço do Servidor Web Público | <ul style="list-style-type: none"> ■ Para uma implantação mínima, a URL base para o host do appliance do vRealize Automation. Por exemplo, <code>https://va-host.domain/</code>. ■ Para uma implantação de alta disponibilidade, a URL base para o balanceador de carga do vRealize Automation. Por exemplo, <code>https://load-balancer-host.domain/</code>. |
| Endereço do Console SSH | Nome do domínio totalmente qualificado do appliance vRealize Automation. Por exemplo, <code>va-host.domain</code> . |
| Usuário do Console SSH | raiz |
| Senha do Console SSH | Senha para a raiz. |
| Tempo máximo de resposta do serviço (ms) | Aceitar o padrão: 2000 |

Tabela 1-85. Tenant do Sistema vRealize Automation

| Opção | Descrição |
|-------------------------------------|-----------------------------|
| Administrador de Tenants do Sistema | administrador |
| Senha do Tenant do Sistema | Senha para o administrador. |

Tabela 1-86. Monitoramento do Espaço em Disco do vRealize Automation

| Opção | Descrição |
|--------------------------------|---------------------|
| Porcentagem de Limite de Aviso | Aceite o padrão: 75 |
| Porcentagem de Limite Crítico | Aceite o padrão: 90 |

Tabela 1-87. Tenant do vRealize Automation

| Opção | Descrição |
|---|---|
| Tenant em Teste | Tenant selecionado para teste. |
| Nome de usuário do administrador da estrutura | Nome de usuário do administrador da estrutura. Por exemplo, <code>admin@va-host.local</code> . Observação O administrador da estrutura também deve ter um administrador de locatário e uma função de administrador de IaaS para que todos os testes sejam executados. |
| Senha do Administrador da Estrutura | Senha para o administrador da estrutura. |

- 8 Clique em **Avançar**.
- 9 Na página Resumo, revise as informações e clique em **Concluir**.
A configuração de verificação do agente de software está concluída.
- 10 No cartão de verificação do Agente de SW, clique em **Executar**.

- 11 Quando o teste estiver concluído, clique no centro do cartão de verificação do Agente de SW.
- 12 Na página de resultados da verificação do Agente de SW, acesse os resultados do teste e encontre o teste Verificar a versão do Agente de Software na coluna Nome. Se ocorrer um erro no resultado do teste, clique no link **Causa** na coluna Causa para ver as máquinas virtuais com um agente de software desatualizado.

Próximo passo

Se você tiver máquinas virtuais com um agente de software desatualizado, consulte [Atualizar os Agentes de Software no vSphere](#).

Atualizar os Agentes de Software no vSphere

Você pode atualizar qualquer Agente de Software desatualizado no vSphere para o TLS 1.2 após a migração usando o Gerenciamento do Appliance do vRealize Automation.

Esse procedimento atualiza os Agentes de Software desatualizados nas máquinas virtuais do seu ambiente de origem para o TLS 1.2 e é necessário para a migração para vRealize Automation 7.4.

Pré-requisitos

- [Aplicar o patch do agente de software](#) se você tiver migrado do vRealize Automation 7.1 ou 7.3 para 7.4.
- Migração bem-sucedida do vRealize Automation 7.1, 7.2, 7.3 ou 7.3.1 para 7.4.
- Você usou o Serviço de Integridade para identificar os appliances virtuais com os Agentes de Software desatualizados.

Procedimentos

- 1 No appliance do vRealize Automation primário, faça login no Gerenciamento do Appliance do vRealize Automation como **root** usando a senha que você inseriu quando implantou o appliance do vRealize Automation.

Para um ambiente de alta disponibilidade, abra o Gerenciamento do Appliance no appliance mestre.

- 2 Clique em **Configurações do vRA > Agentes de SW**.
- 3 Clique em **Alternar TLS 1.0, 1.1**.

O status do TLS v1.0, v1.1 está HABILITADO.

- 4 Quanto às credenciais de locatário, insira as informações solicitadas para o appliance de origem do vRealize Automation.

| Opção | Descrição |
|-----------------|--|
| Nome do tenant | Nome do locatário no appliance de origem do vRealize Automation. Observação O usuário do locatário deve ter a função de Arquiteto de Software atribuída. |
| Nome de usuário | Nome de usuário de administrador do locatário no appliance de origem do vRealize Automation. |
| Senha | Senha do administrador do locatário. |

- 5 Clique em **Testar conexão**.

Se uma conexão é estabelecida, uma mensagem de êxito é exibida.

- 6 Para o appliance de origem, insira o endereço IP ou o nome de domínio totalmente qualificado do appliance de origem do vRealize Automation.

O appliance de origem e de destino devem usar as mesmas credenciais do locatário.

- 7 Clique em **Listar lotes**.

A tabela Lista de opções de lote é exibida.

- 8 Clique em **Mostrar**.

Uma tabela é exibida com uma lista de máquinas virtuais com os Agentes de Software desatualizados.

- 9 Atualize o Agente de Software para as máquinas virtuais que estão no estado ATUALIZÁVEL.

- Para atualizar o Agente de Software em uma máquina virtual individual, clique em **Mostrar** em um grupo de máquinas virtuais, identifique a máquina virtual que você deseja atualizar e clique em **Executar** para iniciar o processo de atualização.
- Para atualizar o Agente de Software em um lote de máquinas virtuais, identifique o grupo que você deseja atualizar e clique em **Executar** para iniciar o processo de atualização.

Se você tiver mais de 200 máquinas virtuais para atualizar, será possível controlar a velocidade do processo de atualização em lote, inserindo valores para esses parâmetros.

| Opção | Descrição |
|----------------------|---|
| Tamanho do lote | O número de máquinas virtuais selecionadas para a atualização em lote. Você pode variar esse número para ajustar a velocidade de atualização. |
| Profundidade da Fila | O número de execuções de atualização paralelas que ocorrem ao mesmo tempo. Por exemplo, 20 Você pode variar esse número para ajustar a velocidade de atualização. |

| Opção | Descrição |
|------------------|---|
| Erros em Lote | A contagem de erros REST está fazendo com que a atualização em lote seja reduzida. Por exemplo, se você quiser parar a atualização em lote atual após 5 falhas para melhorar a estabilidade da atualização, insira 5 no campo de texto. |
| Falhas em Lote | O número de atualizações do Agente de Software com falha está fazendo com que o processamento em lote seja reduzido. Por exemplo, se você quiser parar a atualização em lote atual após 5 falhas para melhorar a estabilidade da atualização, insira 5 no campo de texto. |
| Sondagem em Lote | Com que frequência o processo de atualização é monitorado para verificar o processo de atualização. Você pode variar esse número para ajustar a velocidade de atualização. |

Se o processo de atualização é muito lento ou produz muitas atualizações bem-sucedidas, você pode ajustar esses parâmetros para melhorar o desempenho da atualização.

Observação A lista de lotes é limpa ao clicar em **Atualizar**. Isso não afeta o processo de atualização. Ele também atualiza as informações no que se refere à definição ou não do TLS 1.2. Além disso, ao clicar em **Atualizar**, uma verificação de integridade dos serviços do vRealize Automation também é realizada. Se os serviços não estão em execução, o sistema exibe uma mensagem de erro e desativa todos os outros botões de ação.

10 Clique em **Alternar TLS 1.0, 1.1**.

O Status do TLS v1.0, v1.1 está DESABILITADO.

Atualizar os Agentes de Software no Amazon Web Services ou Azure

Você pode atualizar os Agentes de Software desatualizados no Amazon Web Service (AWS) ou Azure manualmente.

- Você deve atualizar as propriedades de túnel especificadas na reserva do servidor vRealize Automation migrado.

Pré-requisitos

- [Aplicar o patch do agente de software](#) se você tiver migrado do vRealize Automation 7.1 ou 7.3 para 7.4.
- Migração bem-sucedida do vRealize Automation 7.1, 7.2, 7.3 ou 7.3.1 para 7.4.
- Um túnel de software está presente e o endereço IP da máquina virtual de túnel é conhecido.

Procedimentos

- 1 Crie um arquivo de nó para cada nó que você precisa atualizar.

```
/usr/lib/vcac/server/webapps/ROOT/software/initializeUpdateSoftwareAgents.py -a <
$DestinationVRAServer> -t <$Tenant> -tu <$TenantUser> -S <$SourceVRAServer>
```

2 Crie um arquivo de plano para atualizar o Agente de Software em uma máquina virtual do Linux ou Windows.

- Modifique o arquivo de parâmetros de migração em `/var/log/vcac/agentupdate/{tenant}/{subtenant-UUID}` para conter o valor do endereço IP privado correspondente ao endpoint do AWS ou Azure.

```
"key": "ipAddress",
  "value": {
    "type": "string",
    "value": "<$PrivateIp:$PrivatePort>"
  }
}
```

- Utilize este comando para atualizar uma máquina Linux.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer>
-t <$Tenant> -S <$SourceVRAServer> -tu <$TenantUser> -CL Software.LinuxAgentUpdate74 --
source_cloud_provider azure
```

- Utilize este comando para atualizar uma máquina Windows.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer>
-t <$Tenant> -S <$SourceVRAServer> -tu <$TenantUser> -CW Software.WindowsAgentUpdate74 --
source_cloud_provider azure
```

- Este comando executa o arquivo de plano.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer>
-t <$Tenant> -tu <$TenantUser> --plan_file /usr/lib/vcac/server/webapps/ROOT/software/plan
```

- 3 Use este comando para atualizar o Agente de Software usando o arquivo de nó da etapa 1 e o arquivo de plano da etapa 2.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer> -t <$tenant> -tu <$TenantUser> --component_windows Software.WindowsAgentUpdate74 --component_linux Software.LinuxAgentUpdate74 --plan_file /usr/lib/vcac/server/webapps/ROOT/software/plan --plan_index 0 --node_file /usr/lib/vcac/server/webapps/ROOT/software/node --source_cloud_provider azure --action plan_batch -S <$SourceVRAServer>
```

Como alternativa, você pode usar este comando para executar um nó de cada vez do arquivo de nó, fornecendo um índice de nó.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer> -t <$tenant> -tu <$TenantUser> --component_windows Software.WindowsAgentUpdate74 --component_linux Software.LinuxAgentUpdate74 --plan_file /usr/lib/vcac/server/webapps/ROOT/software/plan --plan_index 0 --node_file /usr/lib/vcac/server/webapps/ROOT/software/node --source_cloud_provider azure --action execute_node -S <$SourceVRAServer> --node_index <0 through n-1>
```

Ao realizar esse procedimento, é possível seguir os logs do appliance virtual do vRealize Automation e a máquina do host para ver o processo de atualização do Agente do Servidor.

Após a atualização, o processo de atualização importa um script de atualização de software para Windows ou Linux para o appliance virtual do vRealize Automation 7.4. Você pode fazer login no host do appliance virtual do vRealize Automation para garantir que o componente de software seja importado com êxito. Após a importação do componente, uma atualização de software é enviada para o antigo Serviço de Agente de Eventos (Event Broker Service, EBS) a fim de transmitir os scripts de atualização de software para as máquinas virtuais identificadas. Quando a atualização é concluída e os novos Agentes de Software tornam-se operativos, eles se associam ao novo appliance virtual do vRealize Automation, enviando uma solicitação de ping.

Observação Arquivos de log úteis

- Saída Catalina para a origem vRealize Automation: `/var/log/vcac/catalina.out`. Neste arquivo, você vê as solicitações de atualização que estão sendo feitas quando as migrações do agente são efetuadas. Essa atividade é igual à execução de uma solicitação de provisionamento de software.
- Saída Catalina para o destino vRealize Automation: `/var/log/vcac/catalina.out`. Neste arquivo, você vê as máquinas virtuais migradas, relatando suas solicitações ping aqui para incluir os números da versão 7.4.0-SNAPSHOT. Você pode reunir esses conjuntos comparando os nomes dos tópicos EBS, por exemplo, `sw-agent-UUID`.
- Pasta de atualização do agente no arquivo de log de atualização mestre da máquina vRealize Automation de destino: `/var/log/vmware/vcac/agentupdate/updateSoftwareAgents.log`. É possível seguir este arquivo para ver qual operação de atualização está em andamento.
- Registros individuais disponíveis nas pastas de localitório: `/var/log/vcac/agentupdate/{tenant}/{subtenant-UUID}`. Os nós individuais estão listados aqui como arquivos com falhas e extensões em andamento.

- Máquinas Virtuais (VMs) migradas: /opt/vmware-appdirector/agent/logs/darwin*.log. Você pode verificar essa localização que deve listar as solicitações de atualização de software recebidas, bem como a reinicialização eventual do agent_bootstrap + agente de software.

Alterar a configuração do dicionário de propriedades após a migração

Após a migração do vRealize Automation 6.2.x, defina as propriedades de tipo de controle do Label do dicionário de propriedades como não substituíveis nos seus blueprints.

O controle de rótulo no dicionário de propriedades do vRealize Automation 6.2.x não existe no vRealize Automation 7.x. Durante a migração, o controle de Label é convertido em um controle de tipo de TextBox no dicionário de propriedades migrado.

Após a migração, defina as propriedades afetadas como não substituíveis, manualmente no dicionário de propriedades do vRealize Automation ou usando recursos de exportação e de importação.

Validar o ambiente do vRealize Automation 7.4 de destino

Você pode verificar se todos os dados foram migrados com sucesso para o ambiente do vRealize Automation de destino.

Pré-requisitos

- Migre para a versão mais recente do vRealize Automation.
- Faça login no console de destino do vRealize Automation.
 - a Abra o console do vRealize Automation usando o nome de domínio totalmente qualificado do appliance virtual de destino: `https://vra-va-hostname.domain.name/vcac`.

Para um ambiente de alta disponibilidade, abra o console usando o nome de domínio totalmente qualificado do balanceador de carga do appliance virtual de destino: `https://vra-va-lb-hostname.domain.name/vcac`.
 - b Faça login com o nome de usuário e a senha do administrador de tenants.

Procedimentos

- 1 Selecione **Infraestrutura > Máquinas Gerenciadas** e verifique se todas as máquinas virtuais gerenciadas estão presentes.
- 2 Clique em **Recursos de Processamento**, selecione cada endpoint e clique em **Coleta de Dados, Solicitar agora e Atualizar** para verificar se os endpoints estão funcionando.
- 3 Clique em **Design** e, na página **Blueprints**, verifique os elementos de cada blueprint.
- 4 Clique em **XaaS** e verifique o conteúdo de **Recursos Personalizados, Mapeamentos de Recursos, Blueprints do XaaS e Ações de Recursos**.
- 5 Selecione **Administração > Gerenciamento de Catálogos** e verifique o conteúdo de **Serviços, Itens de Catálogo, Ações e Direitos**.
- 6 Selecione **Itens > Implantações** e verifique os detalhes das máquinas virtuais provisionadas.
- 7 Na página Implantações, selecione uma máquina virtual provisionada e desligada e selecione **Ações > Ligar**, clique em **Enviar** e depois em **OK**. Verifique se a máquina virtual liga corretamente.

- 8 Clique em **Catálogo** e solicite um novo item de catálogo.
- 9 Na guia **Geral**, insira as informações solicitadas.
- 10 Clique no ícone de Máquina, aceite todas as configurações padrão, clique em **Enviar** e depois em **OK**.
- 11 Verifique se a solicitação foi concluída com êxito.

Solucionando problemas de migração

Tópicos de solução de problemas de migração fornecem soluções para problemas que podem ocorrer quando você migra o vRealize Automation.

A versão do PostgreSQL causa um erro

Um ambiente do vRealize Automation 6.2.x de origem contendo um banco de dados PostgreSQL atualizado bloqueia o acesso do administrador.

Problema

Se um banco de dados PostgreSQL atualizado for usado pelo vRealize Automation 6.2.x, um administrador deverá adicionar uma entrada ao arquivo `pg_hba.conf` que forneça acesso a esse banco de dados a partir do vRealize Automation.

Solução

- 1 Abra o arquivo `pg_hba.conf`.
- 2 Para conceder acesso a esse banco de dados, adicione a seguinte entrada.

```
host all vcac-database-user vra-va-ip trust-method
```

Algumas máquinas virtuais não têm uma implantação criada durante a migração

As máquinas virtuais que se encontram no estado ausente no momento da migração não possuem uma implantação correspondente criada no ambiente de destino.

Problema

Se uma máquina virtual estiver no estado ausente no ambiente de origem durante a migração, não será criada uma implantação correspondente no ambiente de destino.

Solução

- ◆ Se uma máquina virtual sair do estado ausente após a migração, você poderá importá-la para a implantação de destino usando a importação em massa.

Localizações dos logs de migração

Você pode resolver problemas de validação ou migração visualizando os logs que registram o processo de migração.

Tabela 1-88. Appliance de origem do vRealize Automation

| Registro | Localização |
|--------------------------|--|
| Log de criação do pacote | /var/log/vmware/vcac/migration-package.log |

Tabela 1-89. Appliance de destino do vRealize Automation

| Registro | Localização |
|---------------------------------------|--|
| Log de migração | /var/log/vmware/vcac/migrate.log |
| Log de execução da migração | /var/log/vmware/vcac/mseq.migration.log |
| Log de saída de execução da migração | /var/log/vmware/vcac/mseq.migration.out.log |
| Log de execução da validação | /var/log/vmware/vcac/mseq.validation.log |
| Log de saída de execução da validação | /var/log/vmware/vcac/mseq.validation.out.log |

Tabela 1-90. Nós de infraestrutura do vRealize Automation de destino

| Registro | Localização |
|------------------|--|
| Log de migração | C:\Program Files (x86)\VMware\VCAC\InstallLogs-YYYYMMDDHHMMXX\Migrate.log |
| Log de validação | C:\Program Files (x86)\VMware\VCAC\InstallLogs-YYYYMMDDHHMMXX\Validate.log |

Itens de catálogo aparecem no catálogo de serviços após a migração, mas não estão disponíveis para solicitação

Os itens de catálogo que utilizam determinadas definições de propriedades de versões anteriores aparecem no catálogo de serviços; apesar disso, não estão disponíveis para requisição após a migração para a versão mais recente do vRealize Automation.

Problema

Se você migrou da versão 6.2.x ou anterior e tinha definições de propriedades com os tipos de controle ou de atributos, esses atributos estarão ausentes nas definições de propriedades e nenhum dos itens de catálogo que utilizar as definições funcionará como antes da migração.

- Tipos de controle. Caixa de seleção ou link.
- Atributos. Relacionamento, expressões regulares ou layouts de propriedades.

Causa

No vRealize Automation 7.0 e versões posteriores, as definições de propriedades não usam mais estes elementos. Você deverá recriar a definição de propriedade ou configurá-la para utilizar uma ação de script do vRealize Orchestrator em vez dos tipos de controle ou atributos incorporados.

Migre o tipo de controle ou os atributos para o vRealize Automation 7.x usando uma ação de script.

Solução

- 1 No vRealize Orchestrator, crie uma ação de script que retorne os valores de propriedade. A ação deve retornar um tipo simples. Por exemplo, cadeias de retorno, números inteiros ou outros tipos compatíveis. A ação pode considerar como um parâmetro de entrada as outras propriedades das quais ela depende.
- 2 No console do vRealize Automation, configure a definição do produto.
 - a Selecione **Administração > Dicionário de propriedades > Definições de propriedades**.
 - b Selecione a definição da propriedade e clique em **Editar**.
 - c No menu suspenso Exibir aviso, selecione **Lista Suspensa**.
 - d No menu suspenso Valores, selecione **Valores Externos**.
 - e Selecione a ação de script.
 - f Clique em **OK**.
 - g Configure os Parâmetros de Entrada incluídos na ação de script. Para preservar a relação existente, vincule o parâmetro à outra propriedade.
 - h Clique em **OK**.

Botões de opção Coleta de Dados desativados em vRealize Automation

Após a migração do vRealize Automation 6.2.x para o 7.x, a página Recursos de Processamento no vRealize Automation de destino contém os botões de opção desativados em Coleta de Dados.

Causa

Se você instalar um agente no ambiente de origem que aponta para um endpoint e instalar um agente no ambiente de destino que aponta para o mesmo endpoint, mas o agente tiver um nome diferente, poderá executar uma conexão de teste para o endpoint como administrador no ambiente de destino. No entanto, se você fizer login no vRealize Automation no ambiente de destino como administrador de estrutura, os botões de opção na página Recursos de Processamento em Coleta de Dados serão desativados.

Solução

Evite essa situação fornecendo o nome do agente instalado no ambiente de destino igual ao nome do agente instalado no ambiente de origem.

Solucionando problemas de atualização do agente de software

Ao usar o Gerenciamento de appliance do vRealize Automation para atualizar os agentes de software, você pode revisar os arquivos de log para identificar a causa de quaisquer problemas ocorridos.

Problema

Você pode ter problemas ao atualizar os agentes de software. Observando os arquivos de log durante o processo de atualização do agente de software, você pode identificar onde há um problema.

Observação

 Logs do servidor

- Veja o arquivo `updateSoftwareAgents.log` no servidor para observar o processo: `/storage/log/vmware/vcac/agentupdate/updateSoftwareAgents.log`.
- Veja o arquivo `catlaina.out` no appliance de destino para ver quais agentes de software estão sendo bem-sucedidos: `/var/log/vcac/catalina.out`.

Procure a cadeia de caracteres `s` como "ping" relatada de volta para 7.4.0-SNAPSHOT.

Você pode encontrar informações adicionais nesses locais.

- `/var/cache/vcac/agentupdate/{Tenant}/{UUID}/UUID.plan`
- `/var/cache/vcac/agentupdate/{Tenant}/{UUID}/UUID.log`
- `/var/cache/vcac/agentupdate/sqa/UUID/UUID.log` (por SO)

Antes de iniciar uma grande atualização em lote, você deve sempre executar uma atualização do agente de software do appliance virtual de teste. Para obter uma visão geral do processo:

- Observe a primeira solicitação feita para o appliance virtual de destino para identificar as versões do agente.
- Observe a solicitação feita para o appliance virtual de origem para atualização.
- Observe os agentes relatando sua nova versão 7.4 no appliance virtual de destino.
- Entre esses eventos, observe o arquivo `updateSoftwareAgents.log` em `/storage/log/vmware/vcac/agentupdate/updateSoftwareAgents.log`

Observação

 Logs do cliente

Os logs do agente Linux estão na pasta de logs de agente `appdirector`: `/opt/vmware-appdirector/agent/logs/*.log`

Você pode ver erros de log como esses, que são temporários porque as filas de EBS entram e saem durante o processo de atualização.

```
15 de fevereiro de 2018 16:54:10.105 ERRO [EventPoller-sw-agent-0ad2418d-5b42-4231-a839-a05dd618e43e] [] com.vmware.vcac.platform.event.broker.client.rest.RestEventSubscribeHandler - Erro ao pesquisar eventos para inscrição '{}'.  
org.springframework.web.client.HttpClientErrorException: 404 não encontrado  
em  
org.springframework.web.client.DefaultResponseErrorHandler.handleError(DefaultResponseErrorHandler.java:91) ~[nobel-agent.jar:na]
```

em org.springframework.web.client.RestTemplate.handleResponse(RestTemplate.java:641) ~[nobel-agent.jar:na]

em org.springframework.web.client.RestTemplate.doExecute(RestTemplate.java:597) ~[nobel-agent.jar:na]

em org.springframework.web.client.RestTemplate.execute(RestTemplate.java:557) ~[nobel-agent.jar:na]

em org.springframework.web.client.RestTemplate.exchange(RestTemplate.java:503) ~[nobel-agent.jar:na]

em

com.vmware.vcac.platform.event.broker.client.rest.RestEventSubscribeHandler.pollEvents(RestEventSubscribeHandler.java:297) ~[nobel-agent.jar:na]

em com.vmware.vcac.platform.event.broker.client.rest.RestEventSubscribeHandler\$EventPoller.run(RestEventSubscribeHandler.java:329) ~[nobel-agent.jar:na]