

Instalando o vRealize Automation

21 de julho de 2021

vRealize Automation 7.6

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

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

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

Copyright © 2014-2021 VMware, Inc. Todos os direitos reservados. [Informações sobre direitos autorais e marca registrada.](#)

Conteúdo

vRealize Automation Instalação	7
Informações atualizadas	8
1 Visão geral da instalação	9
Sobre a instalação	9
Novidade nesta instalação	10
Componentes de instalação	10
O appliance do vRealize Automation	10
Infraestrutura como Serviço	11
Tipo de implantação	14
Implementações mínimas	14
Implementações distribuídas	15
Escolhendo o método de instalação	18
2 Preparando para a instalação	19
Preparo geral	19
Contas e senhas	20
Nomes de host e endereços IP	22
Latência e largura de banda	23
Appliance do vRealize Automation	23
Portas do appliance do vRealize Automation	24
Servidores Windows do IaaS	26
Portas do Servidor Windows de IaaS	27
Servidor Web de IaaS	29
Host do Serviço de Gerenciador do IaaS	30
Host do servidor SQL de IaaS	31
Host do Distributed Execution Manager do IaaS	32
Trabalhadores do DEM com o Amazon Web Services	32
DEM Workers com OpenStack ou PowerVC	32
DEM Workers com Red Hat Enterprise Virtualization	33
DEM Workers com SCVMM	33
Certificados	35
Requisitos de certificado do vRealize Automation	36
Extraindo certificados e chaves privadas	37
3 Implantar appliance do vRealize Automation	39
Sobre a implantação do appliance	39

Implantar o appliance do vRealize Automation	39
Adicionar controladores de interface de rede antes de executar o instalador	42

4 Instalando com o assistente de instalação 45

Usando o assistente de instalação para implantações mínimas	45
Iniciar o assistente de instalação para uma implantação mínima	45
Instalar o Agente de gerenciamento	46
Concluindo o Assistente de Instalação	48
Usando o assistente de instalação para implantações corporativas	48
Inicie o assistente de instalação para uma implantação corporativa	49
Instalar o Agente de Gerenciamento	49
Concluindo o Assistente de Instalação	51

5 As interfaces de instalação padrão 53

Usando as interfaces padrão para implantações mínimas	53
Lista de verificação da implantação mínima	54
Configurar o appliance do vRealize Automation	54
Instalando componentes do IaaS	58
Usando as interfaces padrão para implantações distribuídas	65
Lista de verificação de implantação distribuída	65
Desativando verificações de integridade do balanceador de carga	66
Requisitos de confiança de certificado em um ambiente distribuído	67
Configurar a confiança de certificado do componente Web, do serviço de gerenciador e do host DEM	69
Planilhas de instalação	70
Configurar o balanceador de carga	72
Configurando dispositivos para ovRealize Automation	73
Instalar os componentes do IaaS em uma configuração distribuída	80
Instalando agentes	110
Definir a política de execução do PowerShell como RemoteSigned	111
Escolhendo o cenário de instalação do agente	111
Localização e requisitos de instalação de agente	112
Instalando e configurando o agente de proxy do vSphere	112
Instalando o agente de proxy do Hyper-V ou do XenServer	119
Instalando o agente do VDI do XenDesktop	123
Instalando o agente do EPI para Citrix	128
Instalando o agente do EPI para scripts do Visual Basic	131
Instalando o agente do WMI para solicitações remotas do WMI	135

6 Instalação silenciosa 139

Sobre a instalação silenciosa	139
Realizar uma instalação silenciosa	140

Realizar uma instalação silenciosa do Agente de Gerenciamento	140
Arquivo de resposta de instalação silenciosa	142
A linha de comando de instalação	143
Noções básicas sobre linha de comando de instalação	143
Nomes de comandos de instalação	144
O API de instalação	144
Converter entre propriedades silenciosas e JSON	146
7 Tarefas pós instalação	147
Não alterar o fuso horário	147
Configurar a criptografia em conformidade com FIPS	148
Ativar o failover automático do Serviço de Gerenciador	149
Sobre o failover automático do Serviço de Gerenciador	149
Failover automático do banco de dados PostgreSQL	150
Substituindo certificados autoassinados por certificados fornecidos por uma autoridade	151
Alterando nomes de host e endereços IP	151
Alterar o nome de host do appliance	151
Alterar o endereço IP do Appliance	152
Ajustando o banco de dados SQL para um nome de host alterado	154
Alterar um endereço de servidor IP do IaaS	154
Alterar um nome do host do servidor do IaaS	156
Definir a URL de login como um nome personalizado	158
Remover um nó de appliance do vRealize Automation	158
Instalando o agente do vRealize Log Insight	159
Alterar a porta de proxy do VMware Remote Console	159
Altere um FQDN do appliance de volta para o FQDN original	159
Configurar Grupo de Disponibilidade AlwaysOn do SQL	161
Adicionar controladores de interface de rede após a instalação do vRealize Automation	161
Configurar rotas estáticas	162
Gerenciamento de patches de acesso	163
Configurar o acesso ao tenant padrão	164
8 Solucionando problemas com uma instalação	166
Revertendo uma instalação com falha	166
Reverter uma instalação mínima	166
Reverter uma instalação distribuída	167
Criar um pacote de suporte	168
Solução de problemas gerais com a instalação	169
A instalação ou a atualização falha com um erro de tempo limite do balanceador de carga	169
Os horários do servidor não estão sincronizados	170
Podem aparecer páginas em branco ao usar o Internet Explorer 9 ou 10 no Windows 7	170

Não é possível estabelecer uma relação confiável para o canal seguro de SSL/TLS	171
Conectar-se à rede por meio de um servidor proxy	172
Etapas do console para a configuração de conteúdo inicial	172
Não é possível fazer downgrade de licenças do vRealize Automation	173
Solucionando problemas com o appliance do vRealize Automation	174
Falha no download dos instaladores	174
O arquivo Encryption.key tem permissões incorretas	174
O Gerenciamento de Diretórios do Identity Manager não é iniciado após o reinício do espaço de trabalho do Horizon	175
Atribuições de funções de appliance incorretas após o failover	176
Falhas após promoção de nós mestres e réplicas	177
Registros de serviço incorretos do componente	178
NIC adicional provoca erros na interface de gerenciamento	181
Não é possível promover um appliance virtual secundário a um mestre	181
Tempo de retenção do log de sincronização do Active Directory é muito curto	182
O RabbitMQ não pode resolver os nomes de host	182
Solucionando problemas de componentes do IaaS	183
Conexões do Distributed Transaction Coordinator são recusadas	184
Os servidores IaaS parecem estar desconectados	184
Corretor de pré-requisito não pode instalar os recursos .NET	185
Validando certificados de servidor do IaaS	186
Erro de credenciais ao executar o instalador do IaaS	187
O aviso "Salvar Configurações" é exibido durante a instalação do IaaS	187
Falha na instalação do servidor de site e dos Distributed Execution Managers	188
A autenticação do IaaS falha durante Instalação do IaaS Web e do Gerenciamento de Modelos	188
Falha ao instalar os dados e os componentes da Web do Model Manager	188
Servidores Windows IaaS não oferecem suporte ao FIPS	190
A adição de um endpoint do XaaS causa um erro interno	191
A desinstalação de um agente de proxy falha	191
Falha nas solicitações de máquina quando as transações remotas estão desativadas	192
Erro na comunicação do serviço de gerenciador	193
O comportamento de personalização de e-mails foi alterado	193
Solução de erros de login	194
As tentativas de fazer login como o administrador do IaaS com credenciais incorretas no formato UPN apresentam falhas sem explicação	194
O login falha com alta disponibilidade	195
O proxy impede que os usuários do VMware Identity Manager façam login	196

vRealize Automation Instalação

Esse guia de instalação do *vRealize Automation* contém instruções de instalação com assistente, manual e silenciosa para o VMware vRealize™ Automation.

Observação Nem todos os recursos e capacidades do vRealize Automation estão disponíveis em todas as edições. Para ver uma comparação de conjuntos de recursos em cada edição, consulte <https://www.vmware.com/products/vrealize-automation/>.

Público-alvo

Essas informações foram concebidas para administradores de sistema experientes do Windows ou do Linux que estão familiarizados com a tecnologia de máquinas virtuais e com operações de operações de data center.

Informações atualizadas

A seguinte tabela lista as alterações em *Instalando o vRealize Automation* para esta versão do produto.

Revisão	Descrição
XX TBD 202X	<ul style="list-style-type: none">■ Instalar o Agente de Gerenciamento do vRealize Automation atualizado.■ Ativar o failover automático do Serviço de Gerenciador atualizado.■ Registros de serviço incorretos do componente vRealize Automation atualizado.
12 DE AGOSTO DE 2020	Extraindo certificados e chaves privadas atualizado.
14 FEV 2020	<ul style="list-style-type: none">■ Servidores Windows do IaaS atualizado.■ Host do Serviço de Gerenciador do IaaS atualizado.■ Host do servidor SQL de IaaS atualizado.■ Não alterar o fuso horário do vRealize Automation atualizado.■ Gerenciamento de patches de acesso atualizado.■ Conexões do Distributed Transaction Coordinator são recusadas adicionado.■ Falha nas solicitações de máquina quando as transações remotas estão desativadas atualizado.
24 DE OUT DE 2019	Lembrete do conector adicionado ao Adicionar outro appliance do vRealize Automation ao cluster .
9 SET 2019	<ul style="list-style-type: none">■ Appliance do vRealize Automation atualizado.■ Não alterar o fuso horário do vRealize Automation adicionado.
14 JUN 2019	<ul style="list-style-type: none">■ Configurações de política de grupo atualizadas em Contas e senhas.■ Local em inglês atualizado em Servidores Windows do IaaS.■ Os servidores IaaS parecem estar desconectados adicionado.
30 MAIO DE 2019	<ul style="list-style-type: none">■ Configurações de política de grupo adicionadas em Contas e senhas.■ Foi removido o PowerShell 2 e o local em inglês adicionado a Servidores Windows do IaaS.
7 DE MAIO DE 2019	Corrigimos alguns hiperlinks.
11 DE ABRIL DE 2019	Versão inicial do documento.

Visão geral de instalação do vRealize Automation

1

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.

Este capítulo inclui os seguintes tópicos:

- [Sobre a instalação do vRealize Automation](#)
- [Novidade nesta instalação do vRealize Automation](#)
- [Componentes de instalação do vRealize Automation](#)
- [Tipo de implantação](#)
- [Escolhendo o método de instalação](#)

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 Lifecycle Manager. Para obter mais informações, consulte o [Guia de instalação, atualização e gerenciamento do vRealize Suite Lifecycle Manager](#).

O vRealize Suite Lifecycle Manager automatiza a instalação, a configuração, a atualização, o patch, o gerenciamento de configuração, a correção de desvio e a integridade em um painel único. Clique aqui para instalar o [vRealize Suite Lifecycle Manager](#). O Lifecycle Manager fornece aos gerentes de TI recursos de administração em nuvem para se concentrarem em iniciativas críticas para os negócios, ao mesmo tempo em que melhoram o retorno de valor, confiabilidade e consistência.

Novidade nesta instalação do vRealize Automation

Se você instalou versões anteriores do vRealize Automation, esteja ciente das alterações no processo de instalação desta versão.

- Quando você faz login após a instalação, a interface de administração do dispositivo do vRealize Automation é aberta em uma nova página de resumo com informações do sistema, status e estatísticas de uso.
- Agora a guia Cluster da interface de administração do dispositivo do vRealize Automation pode relatar uma variedade de estatísticas de integridade.

Para alterar o relatório de cluster padrão, edite o seguinte arquivo no dispositivo do vRealize Automation.

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

Algumas configurações de arquivo também afetam o status da página Resumo.

- Esta versão corrige problemas relatados conforme detalhado nas notas de versão.

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 AutomationIaaS 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 AutomationIaaS 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 AutomationIaaS 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.

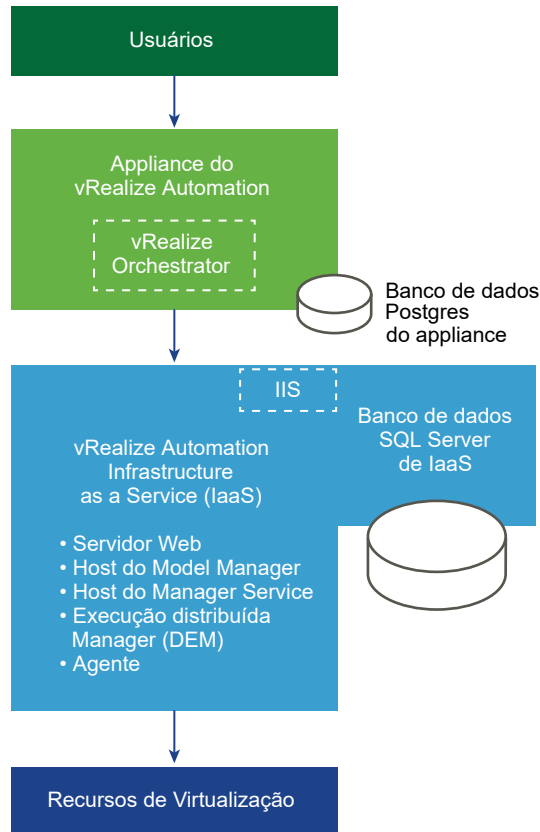
Tipo de implantação

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 1-1. Implementação mínima do vRealize Automation

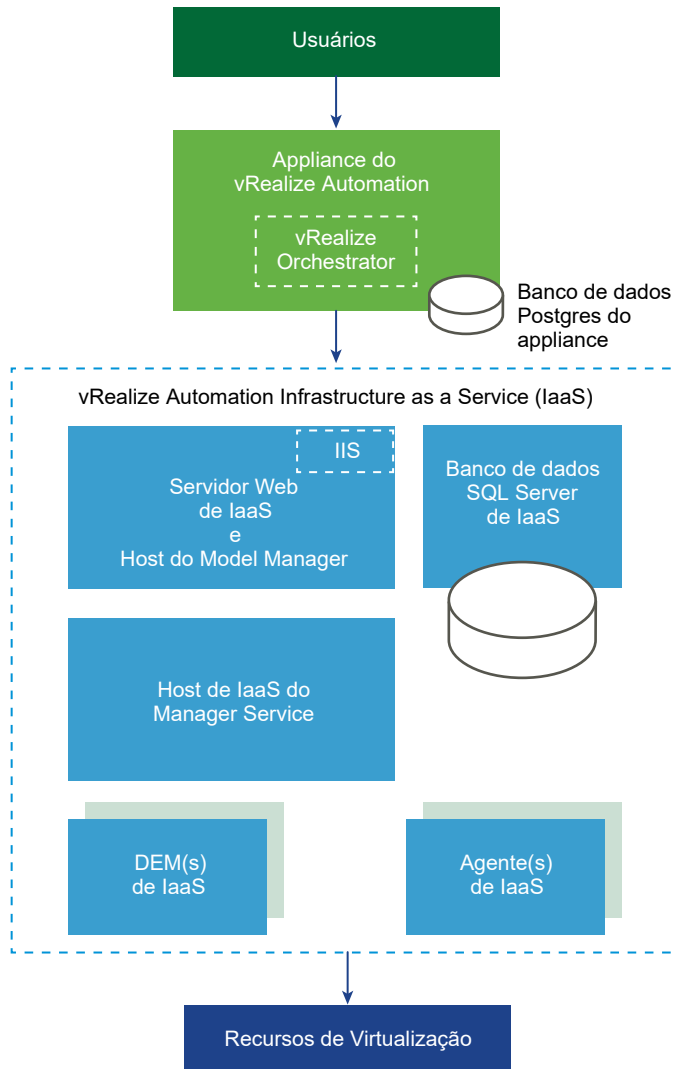


Não é possível converter uma implantação mínima em uma implantação corporativa. Para expandir uma implantação, comece com uma pequena implantação corporativa e adicione componentes a ela. Não é possível iniciar com uma implantação mínima.

Implementações distribuídas do vRealize Automation

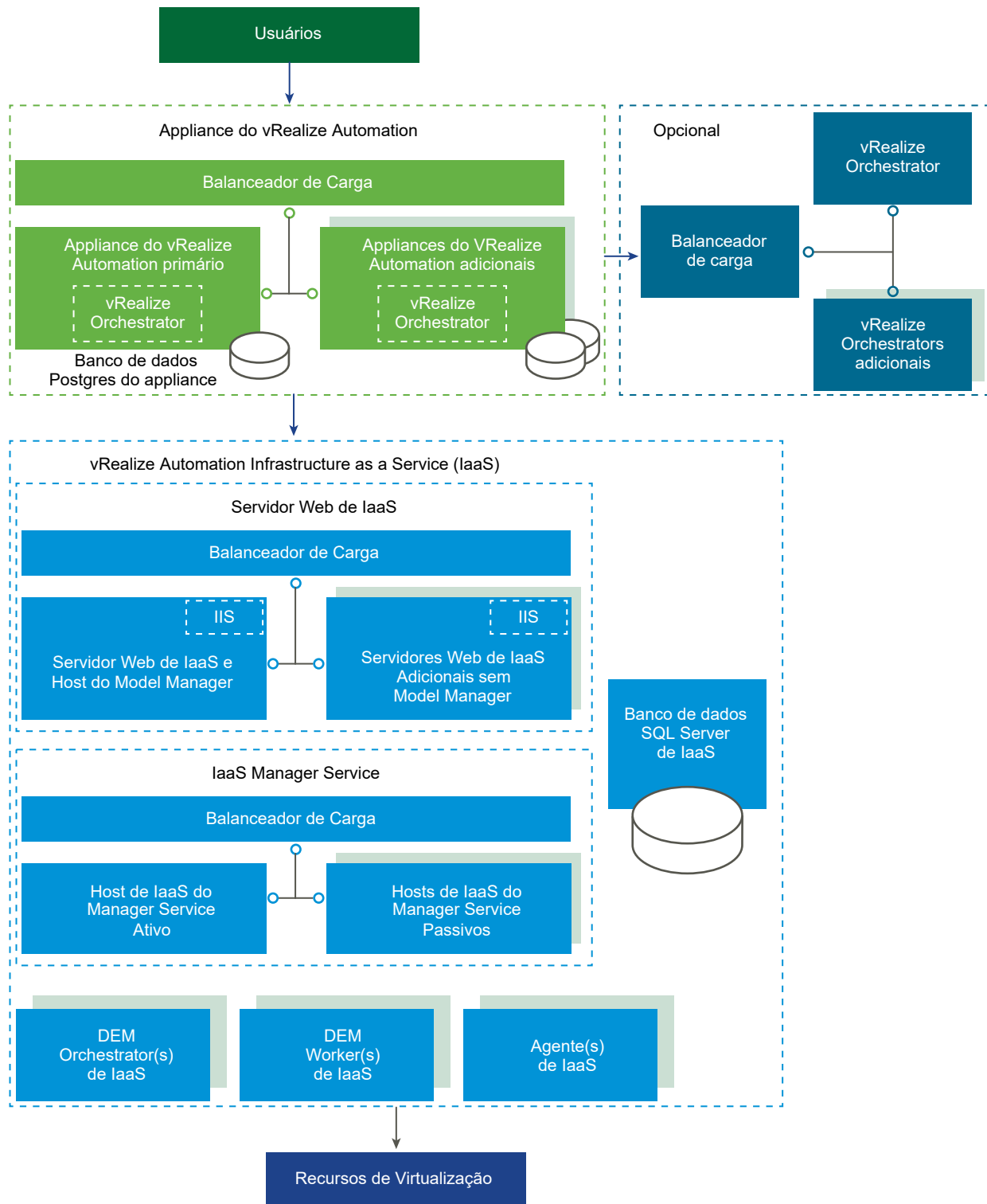
Implementações corporativas distribuídas podem ser de diferentes tamanhos. Uma implementação distribuída básica pode melhorar o vRealize Automation ao hospedar componentes do IaaS em servidores Windows diferentes, como mostrado na figura a seguir.

Figura 1-2. 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 1-3. 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

2

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.

Este capítulo inclui os seguintes tópicos:

- [Preparo geral](#)
- [Contas e senhas](#)
- [Nomes de host e endereços IP](#)
- [Latência e largura de banda](#)
- [Appliance do vRealize Automation](#)
- [Servidores Windows do IaaS](#)
- [Servidor Web de IaaS](#)
- [Host do Serviço de Gerenciador do IaaS](#)
- [Host do servidor SQL de IaaS](#)
- [Host do Distributed Execution Manager do IaaS](#)
- [Certificados](#)

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.

- Se o seu site usar configurações de segurança de política de grupo, verifique as seguintes configurações para a conta. Execute o editor de política de grupo gpedit.msc e procure em **Configuração do Computador > Configurações do Windows > Configurações de Segurança > Políticas Locais > Atribuição de Direitos de Usuário**.
 - Negar logon localmente — Não adicione a conta.
 - Permitir logon localmente — Adicione a conta.
 - Negar acesso a este computador pela rede — Não adicione a conta.
 - Acessar este computador pela rede — Adicione a conta.

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 dbo 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 hífens (-) 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.

O dispositivo executa o SUSE Linux Enterprise 11 de 64 bits. A VMware não oferece suporte a modificações ou personalizações de appliances. Nunca adicione, remova ou atualize pacotes ou scripts personalizados, incluindo software antivírus.

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 2-1. 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 ■ 140 GB de armazenamento de disco 	<ul style="list-style-type: none"> ■ 4 CPUs ■ 22 GB de memória ■ 140 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 2-2. 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.
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.

Tabela 2-2. Portas de entrada (continuação)

Porta	Protocolo	Comentários
8494	TCP	Sincronização de cluster do serviço de contêiner
9300–9400	TCP	Acesso às auditorias do Identity Manager.
54328	UDP	
40002, 40003	TCP	sincronização de cluster do vIDM
8090, 8092	TCP	Usado pelo Serviço de Integridade para se conectar entre nós do vRA

Tabela 2-3. 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.

Tabela 2-3. Portas de saída (continuação)

Porta	Protocolo	Comentários
8281	TCP	Opcional. Para comunicação com uma instância externa do vRealize Orchestrator.
8494	TCP	Sincronização de cluster do serviço de contêiner
9300-9400	TCP	Acesso às auditorias do Identity Manager.
54328	UDP	
40002, 40003	TCP	sincronização de cluster do vIDM

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.

Importante A instalação desativa Firewall do Windows. Se as políticas do site exigirem o Firewall do Windows, ative-o novamente após a instalação e abra individualmente as portas do servidor Windows IaaS. Consulte o [Portas do Servidor Windows de IaaS](#).

- 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.

- Os servidores Windows IaaS e o host do banco de dados SQL Server devem ser capazes de resolver um ao outro pelo nome NETBIOS. Se necessário, adicione os nomes NETBIOS ao arquivo `/etc/hosts` em cada servidor Windows IaaS e ao host do banco de dados SQL Server e reinicie as máquinas.
- 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 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.
- Para qualquer implantação maior que um mínimo, defina servidores Windows do IaaS para a localidade inglês.
- 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 2-4. 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 2-5. 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 201 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 2-6. IaaS Internet Information Services

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.

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 requisito é o mesmo independentemente de o host do Serviço de Gerenciador ser primário ou de backup.

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 mesmo comportamento também se aplica ao SQL Server 2017.

- O Grupo de Disponibilidade AlwaysOn (AAG) só tem suporte no SQL Server 2016 Enterprise ou SQL Server 2017 Enterprise. Ao usar o AAG, você especifica o FQDN do ouvinte AAG como host do SQL Server. Ao criar o AAG, defina DTC_Support = Per_DB. Não é possível defini-lo após a criação do AAG.
- Quando hospedado junto com componentes de IaaS, configure o Java.
 - Instale o Java 1.8, 64 bits, atualização 201 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 e valores máximos de capacidade* no guia do *Arquitetura de referência* vRealize Automation.

- 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 2-7. 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 mais informações sobre preparar o ambiente de SCVMM, consulte *Configurando o vRealize Automation*.

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 2-8. 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 para dispositivos virtuais devem estar no formato PEM.

Se a autoridade de certificação tiver fornecido um certificado no formato PFX, use o OpenSSL para converter o PFX em PEM.

```
openssl pkcs12 -in caminho-para-pfx -out caminho-desejado-para-pem -nodes
```

Por exemplo:

```
openssl pkcs12 -in C:\vra-cert.pfx -out C:\vra-cert.pem -nodes
```

Talvez seja necessário inserir um código de acesso se o certificado PFX incluir um.

Implantar appliance do vRealize Automation

3

O appliance do vRealize Automation é entregue como um arquivo de virtualização aberto que você implementa em uma infraestrutura virtualizada existente.

Este capítulo inclui os seguintes tópicos:

- [Sobre a implantação do appliance do vRealize Automation](#)
- [Implantar o appliance do vRealize Automation](#)
- [Adicionar controladores de interface de rede antes de executar o instalador](#)

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 hospederá 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 3-1. 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 it later 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 a static IP. 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 later (by 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-addressnetmaskgateway-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

4

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 [Capítulo 5 As interfaces de instalação padrão do vRealize Automation](#).

Este capítulo inclui os seguintes tópicos:

- [Usando o assistente de instalação para implantações mínimas](#)
- [Usando o assistente de instalação para implantações corporativas](#)

Usando o assistente de instalação para implantações mínimas

Implementações mínimas demonstram como o vRealize Automation funciona, mas não têm capacidade 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

- Satisfça os pré-requisitos no [Capítulo 2 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 4-1. 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.

Resultados

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 [Capítulo 6 Instalação silenciosa do vRealize Automation](#).
- Se você tiver criado o conteúdo inicial, poderá efetuar login no locatário padrão como o usuário configurationadmin e solicitar os itens de catálogo.
- 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

- Satisfça os pré-requisitos no [Capítulo 2 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 ao dispositivo vRealize Automation primário.

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 no dispositivo vRealize Automation primário, automatiza a instalação e gerenciamento dos componentes IaaS e coleta informações de suporte e telemetria. 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 ou mais dispositivos 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 dispositivo vRealize Automation primário 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 a URL do instalador do dispositivo vRealize Automation primário.

```
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 dispositivo vRealize Automation primário:

- Insira o endereço HTTPS do dispositivo primário, incluindo FQDN e o número da porta :5480.
- Insira as credenciais da conta raiz do dispositivo primário.
- 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 4-2. 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.

Resultados

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 [Capítulo 6 Instalação silenciosa do vRealize Automation](#).
- Se você tiver criado o conteúdo inicial, poderá efetuar login no locatário padrão como o usuário configurationadmin e solicitar os itens de catálogo.
- Para configurar o acesso ao locatário padrão para outros usuários, consulte [Configurar o acesso ao tenant padrão](#).

As interfaces de instalação padrão do vRealize Automation

5

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 [Capítulo 4 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.

Este capítulo inclui os seguintes tópicos:

- [Usando as interfaces padrão para implantações mínimas](#)
- [Usando as interfaces padrão para implantações distribuídas](#)
- [Instalando agentes do vRealize Automation](#)

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 5-1. Lista de verificação da implantação mínima

Tarefa	Detalhes
<input type="checkbox"/> Planeje o ambiente e satisfaça os pré-requisitos de instalação.	Capítulo 2 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
<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 **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	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 . 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 .

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 a ação adequada 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	<p>a Selecione Gerar Solicitação de Assinatura.</p> <p>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.</p> <p>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.</p> <p>d Quando receber o certificado preparado, clique em Importar e siga as instruções para importar um certificado no vRealize Automation.</p>
Importar	<p>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.</p> <p>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> <hr/> <p>Observação No caso dos certificados encadeados, atributos adicionais podem estar disponíveis.</p> <hr/> <p>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.</p>

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 **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 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.

Resultados

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 deseja 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 a interface de gerenciamento do appliance do vRealize Automation é acessada 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**.

Resultados

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**.

Resultados

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 5-2. 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.	Capítulo 2 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

Tabela 5-2. Lista de verificação de implantação distribuída (continuação)

Tarefa	Detalhes
<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 *Usando o plug-in do 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.

Para obter mais informações sobre como configurar o Gerenciamento de Diretórios para alta disponibilidade, consulte o guia *Configurando o vRealize Automation*.

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 inelegíveis 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 em cluster, uma organização de certificados segue em grande parte a arquitetura de três camadas do vRealize Automation.

- Dispositivos do vRealize Automation
- Componentes Web IaaS
- Componentes IaaS do Service Manager

Em uma implantação distribuída, cada máquina em um determinado nível compartilha um certificado. Por exemplo, cada dispositivo do vRealize Automation compartilha um certificado comum e cada host do Manager Service compartilha um certificado comum.

Quando os componentes Web e do Manager Service estão hospedados na mesma máquina, um certificado é suficiente para ambas as camadas.

Certificados gerados pelo sistema

Começando na versão 7.0, se você não fornecer seus próprios certificados, o Assistente de instalação do vRealize Automation poderá gerar automaticamente certificados autoassinados e colocá-los nos repositórios de confiança apropriados dos componentes distribuídos que precisam deles.

Se precisar atualizar os certificados autoassinados gerados pelo sistema com certificados fornecidos pelo usuário ou pela CA, consulte *Gerenciando o vRealize Automation*.

Fornecendo seus próprios certificados

Ao executar o instalador manual padrão, você fornece seus próprios certificados autoassinados gerados ou certificados da autoridade de certificação (CA).

Ao fornecer ou gerar seus próprios certificados usando o OpenSSL ou outro método, você pode usar certificados-curinga ou SAN (Nome alternativo do emissor).

Os certificados IaaS devem ser de uso múltiplo. Ao fornecer certificados, você deve obter um certificado de uso múltiplo que inclua os componentes IaaS no cluster e copiá-lo para o repositório confiável de cada componente.

Balanceadores de Carga

Para alta disponibilidade e failover, você pode adicionar balanceadores de carga na frente de componentes do vRealize Automation distribuídos. A VMware recomenda uma configuração de passagem para balanceadores de carga do vRealize Automation. Em uma configuração de passagem, os balanceadores de carga passam solicitações para componentes sem descriptografia. Os dispositivos do vRealize Automation e hosts IaaS realizam a descriptografia necessária.

Se você usar balanceadores de carga, deverá incluir o FQDN do balanceador de carga no endereço confiável dos certificados de uso múltiplo do cluster.

Para obter mais informações sobre como usar e configurar balanceadores de carga, consulte *Balanceamento de carga do vRealize Automation*.

Requisitos de confiança de certificados

A tabela a seguir resume os requisitos de registro de confiança para vários certificados importados.

Importar	Registrar
Cluster do appliance do vRealize Automation	Cluster de componentes IaaS Web
Cluster de componentes Web IaaS	<ul style="list-style-type: none"> Cluster do appliance do vRealize Automation Cluster de componente do Manager Service Componentes do DEM Orchestrator e do DEM Worker
Cluster de componentes IaaS do Manager Service	<ul style="list-style-type: none"> Componentes do DEM Orchestrator e do DEM Worker Agentes e agentes proxy

Confiança de certificado e o instalador padrão

Sempre que você executa pela primeira vez ou novamente o instalador manual padrão para criar componentes IaaS, deve configurar a confiança de certificado nesses componentes IaaS. Por exemplo, você pode usar o instalador padrão para dimensionar horizontalmente uma implantação existente.

- Hosts IaaS Web e do Manager Service

Importe os arquivos `web.pfx` e `ms.pfx` para os seguintes locais.

```
Host Computer/Certificates/Personal certificate store
Host Computer/Certificates/Trusted People certificate store
```

- Hosts IaaS do DEM Orchestrator, do DEM Worker e do agente de proxy

Importe os arquivos `web.pfx` e `ms.pfx` para o seguinte local.

```
Host Computer/Certificates/Trusted People certificate store
```

No repositório de certificados de Pessoas Confiáveis, você não precisa importar a chave privada junto com o certificado. O processo de instalação automática instala apenas o certificado no repositório de certificados de Pessoas Confiáveis.

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 5-3. 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

Tabela 5-3. Appliance do vRealize Automation (continuação)

Variável	Meu valor	Exemplo
Nome de usuário do tenant padrão	administrator@vsphere.local (padrão)	administrator@vsphere.local
Senha do tenant padrão		login123

Tabela 5-4. 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
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

Tabela 5-4. Servidores Windows do IaaS (continuação)

Variável	Meu valor	Exemplo
Para serviços do IaaS, conta do domínio com direitos de administrador nos hosts		SUPPORT\provisioner
Senha da conta		login123

Tabela 5-5. 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 5-6. Distributed Execution Managers do IaaS

Variável	Meu valor	Exemplo
FQDN do host de DEM		dem.mycompany.com
Endereço IP do host de DEM Somente para referência; não insira endereços IP		123.234.1.111
FQDN do host de DEM		dem2.mycompany.com
Endereço IP do host de DEM Somente para referência; não insira endereços IP		123.234.1.112
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 ovRealize 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 o artigo técnico *Guia de configuração de 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 ovRealize 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 **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 a ação adequada 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. <hr/> <p>Observação No caso dos certificados encadeados, atributos adicionais podem estar disponíveis.</p> <hr/> <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 na interface de gerenciamento do appliance do vRealize Automation como raiz.

`https://vrealize-automation-appliance-FQDN:5480`

- 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 **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 Clique em **Mensagens**. As definições de configuração e o status de mensagens do seu appliance são exibidos. Não altere essas configurações.

12 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.

13 Clique em **Salvar Configurações**.

14 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.

Active Directory — Cada dispositivo do vRealize Automation inclui um conector que suporta a autenticação do usuário, mas apenas um conector normalmente é configurado para executar a sincronização de diretório. Depois de adicionar outro dispositivo, lembre-se de configurar um segundo conector que corresponda ao dispositivo adicionado. O segundo conector se conecta ao seu Provedor de Identidade e aponta para o mesmo Active Directory. Dessa forma, se o primeiro dispositivo falhar, o segundo assumirá o gerenciamento da autenticação do usuário.

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 **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.

Resultados

Se uma operação Unir cluster demorar muito e acabar atingindo o tempo limite, consulte o [artigo 58708 da base de conhecimento da VMware](#).

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 5-7. 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 5-8. 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.

Tabela 5-8. Valores do banco de dados (continuação)

Variável	Valor
<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.

Resultados

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 5-9. 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.

- 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.

- Abra o SQL Server Management Studio.

- Clique em **Nova Consulta**.

Uma janela de Consulta SQL é aberta.

- No menu **Consulta**, verifique se a opção **Modo SQLCMD** está selecionada.

- Cole o conteúdo modificado inteiro do arquivo `CreateDatabase.sql` no painel de consulta.

- Abaixo do conteúdo `CreateDatabase.sql`, cole o conteúdo modificado inteiro de `SetDatabaseSettings.sql`.

- 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 a interface de gerenciamento do appliance do vRealize Automation é acessada 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 credencias 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 credencias usadas para acessar o banco de dados no tempo de execução podem ser configuradas para usar as credencias 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 **Orientar-me pela configuração inicial** e clique em **Avançar**.

20 Clique em **Concluir**.

Resultados

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.

Resultados

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 a interface de gerenciamento do appliance do vRealize Automation é acessada 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 **Orientar-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* na guia *Gerenciando o 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 a interface de gerenciamento do appliance do vRealize Automation é acessada 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 a interface de gerenciamento do appliance do vRealize Automation é acessada 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 instalar 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* na guia *Gerenciando o 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 a interface de gerenciamento do appliance do vRealize Automation é acessada 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 **Orientar-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.](#)

Antes de instalar um novo DEMWorker, exporte o certificado do seu dispositivo virtual de instalação do vRA e importe-o para o local de armazenamento de certificado raiz confiável para a sua máquina local.

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 a interface de gerenciamento do appliance do vRealize Automation é acessada 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 **Orientar-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\Logs.
- 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.

Resultados

Para obter mais informações, consulte [DEM Workers com SCVMM](#).

Informações adicionais sobre preparar o ambiente do SCVMM e criar um endpoint do SCVMM estão disponíveis em *Configurando o vRealize Automation*.

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 VMPSOpsUser.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 VMPSOpsUser.sql na janela de consulta.
- 9 Clique em **Executar**.

Resultados

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:

- Agendamentos 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 5-10. 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

Tabela 5-10. Escolhendo um cenário de agente (continuação)

Cenário de integração	Requisitos e procedimentos do agente
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.

O privilégio VApp.Import permite implantar uma máquina do vSphere usando as configurações importadas de um OVF. Detalhes sobre esse privilégio do vSphere estão disponíveis na [Documentação do SDK do vSphere](#). Se você planeja usar um endpoint do vSphere para implantar VMs com base em modelos OVF, verifique se as suas credenciais incluem o privilégio VApp.Import do vSphere no vCenter Server que está associado ao endpoint.

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 5-11. 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
vApp		Importar
		Configuração de aplicativos vApp
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
		Mover
		Remover
	Interação	Configurar mídia de CD
		Interação do console
		Interação do dispositivo
		Desligar (forçado)

Tabela 5-11. Permissões necessárias para o agente do vSphere gerenciar a instância do vCenter Server (continuação)

Valor do atributo	Permissão
	Ligar
	Redefinir
	Suspender
	Instalação de ferramentas
Configuração	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
	Memória
	Modificar configurações do dispositivo
	Renomear
	Definir anotação (versão 5.0 e posterior)
	Configurações
	Posicionamento de Swapfile
Provisionamento	Personalizar
	Clonar modelo
	Clonar máquina virtual
	Implantar modelo
	Ler especificações de personalização
Estado	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 a interface de gerenciamento do appliance do vRealize Automation é acessada 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 false`

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 AutomationHyper-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 AutomationHyper-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 a interface de gerenciamento do appliance do vRealize Automation é acessada 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.

```
Insira DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config get
```

Veja a seguir um exemplo do comando de saída:

```
Username: XSadmin
```

- 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 a interface de gerenciamento do appliance do vRealize Automation é acessada 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 a interface de gerenciamento do appliance do vRealize Automation é acessada 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 5-12. 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	<p>A Política de execução do MS PowerShell deve ser definida como RemoteSigned ou Unrestricted.</p> <p>Para obter informações sobre a Política de execução do PowerShell, emita um dos seguintes comandos no prompt de comando do PowerShell:</p> <pre>help about_signing help Set-ExecutionPolicy</pre>

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 a interface de gerenciamento do appliance do vRealize Automation é acessada 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 a interface de gerenciamento do appliance do vRealize Automation é acessada 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

6

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.

Este capítulo inclui os seguintes tópicos:

- [Sobre a instalação silenciosa do vRealize Automation](#)
- [Realizar uma instalação silenciosa do vRealize Automation](#)
- [Realizar uma instalação silenciosa do Agente de Gerenciamento do vRealize Automation](#)
- [Arquivo de resposta de instalação silenciosa do vRealize Automation](#)
- [A linha de comando de instalação do vRealize Automation](#)
- [O API de instalação do vRealize Automation](#)
- [Converter entre Propriedades Silenciosas do vRealize Automation e JSON](#)

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-nónome-do-comando --nome-do-parâmetrovalor-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-verso. 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 ou 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
```

Resultados

Você também pode exibir a ajuda para o script.

```
/usr/lib/vcac/tools/install/convert-properties --help
```

Tarefas pós instalação do vRealize Automation

7

Após a instalação do vRealize Automation, existem tarefas que podem exigir a sua atenção. Este capítulo inclui os seguintes tópicos:

- Não alterar o fuso horário do vRealize Automation
- Configurar a criptografia em conformidade com o Padrão Federal de Processamento de Informações (FIPS)
- Ativar o failover automático do Serviço de Gerenciador
- Failover automático do banco de dados PostgreSQL do vRealize Automation
- Substituindo certificados autoassinados por certificados fornecidos por uma autoridade
- Alterando nomes de host e endereços IP
- Remover um nó de appliance do vRealize Automation
- Instalando o agente do vRealize Log Insight em servidores IaaS
- Alterar a porta de proxy do VMware Remote Console
- Alterar um FQDN do appliance do vRealize Automation de volta ao FQDN original
- Configurar Grupo de Disponibilidade AlwaysOn do SQL
- Adicionar controladores de interface de rede após a instalação do vRealize Automation
- Configurar rotas estáticas
- Gerenciamento de patches de acesso
- Configurar o acesso ao tenant padrão

Não alterar o fuso horário do vRealize Automation

Mesmo que a interface de gerenciamento do dispositivo do vRealize Automation ofereça uma opção para alterá-la, sempre deixe o limite de tempo vRealize Automation definido como ETC/UTC.

Sabe-se que o uso de um fuso horário diferente de Etc/UTC causa erros incomuns, como migrações com falha e pacotes de log que não contêm entradas de todos os nós do vRealize Automation.

A opção de interface de gerenciamento de dispositivo do vRealize Automation que você deve evitar está abaixo de **Sistema > Fuso Horário**.

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 **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.

Resultados

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.

Em uma configuração de vários nós, você só precisa realizar as etapas uma vez, em qualquer nó de dispositivo vRealize Automation.

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
```

Resultados

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 *Atualização do vRealize Automation 7.1 ou 7.2 para o 7.3* para obter dicas de resolução de problemas.

Para obter informações sobre como balancear a carga de hosts do Manager Service, consulte [Balanceamento de carga do vRealize Automation](#).

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 é definida como Modo Síncrono na guia Cluster da 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 sobre executar um failover manual, consulte *Gerenciando o 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 *Gerenciando o 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 *Gerenciando o vRealize Automation*.
- 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. Restaurar 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.

Resultados

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 OVFe** e ativar a opção **Imagem ISO**.

Virtual Hardware	VM Options	SDRS Rules	vApp Options
<div>IP allocation</div> <div> <div>IP allocation scheme</div> <div> A vApp can obtain its network configuration through the OVF environment or a DHCP server. Specify the network configuration schemes supported by this vApp: <div> <input type="checkbox"/> DHCP <input checked="" type="checkbox"/> OVF environment </div> The IP allocation schemes determine what IP allocation policy options are enabled. </div> </div> <div> <div>IP protocol</div> <div>Specify the IP protocols supported by this vApp:</div> <div>Both</div> </div>			
<div>OVF settings</div> <div> <div>OVF environment</div> <div>View...</div> <div>The OVF environment is only available when the VM is powered on.</div> </div> <div> <div>OVF environment transport</div> <div> <input checked="" type="checkbox"/> ISO image <input checked="" type="checkbox"/> VMware Tools </div> <div> An ISO image, containing the OVF environment document, is mounted on the first available CD-ROM drive. The VMware tools guestInfo.ovfEnv variable is initialized with the OVF environment document. </div> </div> <div> <div>Installation boot</div> <div> <input type="checkbox"/> Enable <div>0</div> </div> <div> The installation boot automatically gets reset upon first power-on of the virtual machine. Specify the delay in seconds to wait for the VM to power off. A value of zero means wait until the VM is powered off </div> </div>			

- 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 com o banco de dados em **Cluster**
- Status do RabbitMQ em **vRA > Mensagens**
- Status do Xenon em **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 informações sobre certificados de atualização, consulte *Gerenciando o 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 7-1. 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\Server\Website</i>	Web.config
	<i>install-folder\Server\Website\Cafe</i>	Vcac-Config.exe.config
	<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 7-2. 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 7-3. 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 **vRA > Configurações do Host**, altere o **Nome do Host** para o CNAME que você escolheu.

Remover um nó de appliance do vRealize Automation

Ao manter um ambiente de HA, talvez você precise remover do cluster um nó de appliance com falha do vRealize Automation.

Para remover um nó, siga as diretrizes no [Artigo 2149866 da Base de Conhecimento da VMware](#).

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 o *Guia de Administração do Agente 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.

Resultados

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 *Configurando o vRealize Automation*.

- 2 Se esse for um ambiente de alta disponibilidade, também siga as etapas sobre como configurar o Gerenciamento de Diretórios para alta disponibilidade em *Configurando o vRealize Automation*.

- 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 **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 **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 7-4. 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.

Como problemas podem ocorrer quase em tempo real, patches, pré-requisitos e instruções de instalação estão contidos no [Base de Conhecimento da VMware](#). Por exemplo, [artigo 70911 da Base de dados de conhecimento da VMware](#) é monitorado e atualizado com as últimas informações sobre o patch 7.6 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

Procedimentos

- 1 Faça login na interface de gerenciamento de appliance do vRealize Automation como raiz.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Clique em **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
```

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 o *Configurando o vRealize Automation*.
- Os administradores do IaaS preparam recursos externos para o provisionamento. Consulte o *Configurando o vRealize Automation*.
- Se você configurou a criação de conteúdo inicial durante a instalação, o administrador de configuração pode solicitar o item de catálogo de Conteúdo Inicial para preencher rapidamente uma prova de conceito.

Solucionando problemas com uma instalação do vRealize Automation

8

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.

Este capítulo inclui os seguintes tópicos:

- [Revertendo uma instalação com falha](#)
- [Criar um pacote de suporte do vRealize Automation](#)
- [Solução de problemas gerais com a instalação](#)
- [Solucionando problemas com o appliance do vRealize Automation](#)
- [Solucionando problemas de componentes do IaaS](#)
- [Solução de erros de login](#)

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

- 1 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.

Resultados

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.

Resultados

Tabela 8-1. 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 Faça login na interface de gerenciamento de appliance do vRealize Automation como raiz.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Clique em **vRA > Registros**.
- 3 Clique em **Criar Pacote de Suporte**.
- 4 Clique em **Download** e salve o arquivo de pacote de suporte no seu sistema.

Resultados

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.

Linha de comando: para gerar um pacote de suporte a partir da linha de comando do dispositivo vRealize Automation como raiz, você pode executar `vcac-support` ou `vcac-config log-bundle`.

Como alternativa, é possível executar o comando `log-bundle` completo, como mostra o exemplo a seguir. Consulte [Noções básicas sobre linha de comando de instalação do vRealize Automation](#) para obter informações gerais sobre como executar `vra-command`.

```
# vra-command execute --node cafe.node.497772175.21500 log-bundle --requestor va-1.mycompany.com

Parent command with id='981e3028-c99b-5c92-1bae-7d2bf5b6aaaa' was created.
Waiting for all child commands to complete...
...
Command execution result:
Command id: 3d64d122-0af1-28dd-b5a5-d932b78b3678
  Type: log-bundle
  Node id: cafe.node.497772175.21500
  Node host: va-1.mycompany.com
  Result: The command was successfully executed.
  Result description: {"path": "/opt/vmware/var/support-bundle/log/
va-1.mycompany.com_cafe.node.497772175.21500-VA.zip"}

Status: COMPLETED
```

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.

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**).

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

- 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.

Solução

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.

Pré-requisitos

Obtenha nomes de servidor proxy, números de porta e credenciais do administrador para o seu site.

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

- 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.

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.

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 irrecoverável.

Solução

- 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/workflowexecutor.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/workflowexecutor.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.

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.

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

- 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 a interface 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 Cluster em sua interface de gerenciamento ainda lista o nó como o nó mestre, mesmo ele não sendo. Há falhas nas tentativas de usar qualquer interface 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 recolocar um nó mestre antigo no cluster, deixe a máquina antiga ficar online. Em seguida, abra a interface de gerenciamento do novo mestre. Olhe para o nó antigo listado como `invalid` na guia Cluster 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 sua interface 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.
- O serviço SQL pode não estar em execução.

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.

Conexões do Distributed Transaction Coordinator são recusadas

As configurações de Chamada de Procedimento Remoto (RPC) da Microsoft podem afetar o Distributed Transaction Coordinator (DTC) no vRealize Automation.

Problema

Ocorrem erros informando que as conexões do DTC entre servidores Windows IaaS ou o servidor de banco de dados SQL vRealize Automation estão sendo recusadas.

Causa

Uma configuração de conexão RPC restringe o acesso e precisa ser desativada.

Solução

Em todos os servidores Windows IaaS e no servidor de banco de dados SQL vRealize Automation, remova a seguinte chave do Registro ou defina-a como zero.

HKLM\SOFTWARE\Policies\Microsoft\Windows NT\RPC\RestrictRemoteClients

Os servidores IaaS parecem estar desconectados

Os problemas do contador de desempenho do Windows podem fazer com que os servidores do IaaS sejam relatados como desconectados.

Problema

Depois de instalar ou fazer upgrade do Agente de Gerenciamento, o servidor do IaaS envia pings para o dispositivo do vRealize Automation. O problema ocorre quando os pings falham, o que causa um status Não Conectado para o servidor do IaaS na guia Cluster da interface de gerenciamento do dispositivo do vRealize Automation.

No servidor do IaaS, um erro semelhante ao seguinte é exibido no arquivo All.log do Agente de Gerenciamento.

```
[UTC:2019-05-25 16:09:37 Local:2019-05-25 18:09:37] [Error]: [sub-thread-Id="4" context="" token=""]
System.InvalidOperationException: Category does not exist.
at System.Diagnostics.PerformanceCounterLib.CounterExists(String machine, String category, String
counter)
at System.Diagnostics.PerformanceCounter.InitializeImpl()
at System.Diagnostics.PerformanceCounter.NextSample()
at System.Diagnostics.PerformanceCounter.NextValue()
at VMware.IaaS.Component.Metrics.MetricsUtility.CalculateMachineProcessorMeasure(Int32
samplePeriodMilliseconds)
at VMware.IaaS.Management.Agent.ManagementEndpointService.CollectEnvironmentInfo()
at VMware.IaaS.Management.Agent.ManagementEndpointService.<PingAsync>d__0.MoveNext()
--- End of stack trace from previous location where exception was thrown ---
at System.Runtime.CompilerServices.TaskAwaiter.ThrowForNonSuccess(Task task)
at System.Runtime.CompilerServices.TaskAwaiter.HandleNonSuccessAndDebuggerNotification(Task task)
at System.Runtime.CompilerServices.ConfiguredTaskAwaitable`1.ConfiguredTaskAwaiter.GetResult()
at VMware.IaaS.Management.Agent.ManagementAgent.<<PingManagementEndpointAsync>b__1f>d__23.MoveNext()
```



```
--- End of stack trace from previous location where exception was thrown ---
at System.Runtime.CompilerServices.TaskAwaiter.ThrowForNonSuccess(Task task)
at System.Runtime.CompilerServices.TaskAwaiter.HandleNonSuccessAndDebuggerNotification(Task task)
at VMware.IaaS.Management.Agent.ManagementAgent.<ExecutePeriodicAction>d__8.MoveNext()
```

Causa

Existe um problema conhecido em que os contadores de desempenho do Windows ficam corrompidos ao longo do tempo, o que leva a erro.

Solução

Recompile todos os contadores de desempenho, incluindo contadores extensíveis e de terceiros.

- 1 No servidor do IaaS, abra um prompt de comando como Administrador.
- 2 Recompile os contadores:


```
cd C:\Windows\system32

lodctr /R

cd C:\Windows\sysWOW64

lodctr /R
```
- 3 Ressincronize os contadores com a Instrumentação de Gerenciamento do Windows (WMI):


```
WINMGMT.EXE /RESYNCPERF
```
- 4 Pare e reinicie o serviço de Logs e Alertas de Desempenho.
- 5 Pare e reinicie o serviço de Instrumentação de Gerenciamento do Windows.

Próximo passo

Se as etapas anteriores não resolverem o problema, consulte o [Artigo de suporte da Microsoft 300956](#) ou o [Artigo de suporte da Microsoft 2554336](#). Os artigos descrevem como redefinir manualmente os registros associados de Registro. Recomenda-se fazer backup primeiro do Registro.

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 Ao ssistente 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 msixexec 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.

- 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.

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.

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

- ◆ 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.

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](#).

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

- 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`