

# Instalando o vRealize Automation

vRealize Automation 7.1

Este documento dá suporte à versão de cada produto listado e a todas as versões subsequentes, até ser substituído por uma nova edição. Para verificar se há edições mais recentes deste documento, consulte <http://www.vmware.com/br/support/pubs>.

PT\_BR-002088-04

**vmware**<sup>®</sup>

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

<http://www.vmware.com/br/support/>

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

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

[docfeedback@vmware.com](mailto:docfeedback@vmware.com)

Copyright © 2017 VMware, Inc. Todos os direitos reservados. [Informações de direitos autorais e marcas registradas.](#)

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

# Conteúdo

vRealize Automation Instalação	7
Informações atualizadas	9
<b>1 Visão geral de instalação do vRealize Automation</b>	<b>11</b>
Escolhendo o caminho de implantação	11
Visão geral da implantação mínima	12
Visão geral da implantação corporativa	13
Componentes de instalação do vRealize Automation	14
O appliance do vRealize Automation	15
Agentes de gerenciamento	15
Infrastructure as a Service do vRealize Automation	15
<b>2 Preparando para a instalação do vRealize Automation</b>	<b>19</b>
Nomes de host e endereços IP	19
Requisitos de hardware e da máquina virtual	20
Considerações sobre o navegador	20
Considerações sobre senhas	21
Requisitos do Windows Server	21
Requisitos do servidor de banco de dados do IaaS	21
Requisitos de Servidor do Model Manager e do Serviço Web IaaS	22
IaaS Manager Service	23
Requisitos do Distributed Execution Manager	23
Requisitos de porta do vRealize Automation	26
Contas de usuário e credenciais necessárias para a instalação	29
Segurança	30
Certificados	30
Extraindo certificados e chaves privadas	31
Senha de segurança	31
Software de terceiros	31
Sincronização de hora	31
<b>3 Instalando o vRealize Automation com o assistente de instalação</b>	<b>33</b>
Implantar o appliance do vRealize Automation	33
Usando o assistente de instalação para implantações mínimas	35
Executar o assistente de instalação para uma implantação mínima	35
Instalando o Agente de gerenciamento	36
Sincronizar horários dos servidores	39
Executar o verificador de pré-requisitos	39
Especificar parâmetros mínimos de implantação	40
Criar snapshots antes de iniciar a instalação	40
Cenário: concluir a instalação	40

Abordagem das falhas de instalação	41
Configurar credenciais para a configuração de conteúdo inicial	42
Usando o assistente de instalação para implantações corporativas	42
Executar o assistente de instalação para uma implantação corporativa	43
Instalando o Agente de gerenciamento	43
Sincronizar horários dos servidores	46
Executar o verificador de pré-requisitos	46
Especificar parâmetros de implantação corporativa	47
Criar snapshots antes de iniciar a instalação	47
Concluir a instalação	47
Abordagem das falhas de instalação	48
Configurar credenciais para a configuração de conteúdo inicial	49
<b>4 As interfaces de instalação padrão do vRealize Automation</b>	<b>51</b>
Usando as interfaces padrão para implantações mínimas	51
Lista de verificação da implantação mínima	52
Implantar e configurar o appliance do vRealize Automation	52
Instalando componentes do IaaS	57
Usando as interfaces padrão para implantações distribuídas	63
Lista de verificação de implantação distribuída	63
Componentes da instalação distribuída	64
Desativando verificações de integridade do balanceador de carga	65
Requisitos de confiança de certificado em um ambiente distribuído	65
Configurar a confiança de certificado do componente Web, do serviço de gerenciador e do host DEM	66
Planilhas de instalação	66
Implantar o appliance do vRealize Automation	68
Configurar o balanceador de carga	70
Configurando dispositivos para o vRealize Automation	70
Instalar os componentes do IaaS em uma configuração distribuída	77
Instalando agentes do vRealize Automation	101
Definir a política de execução do PowerShell como RemoteSigned	102
Escolhendo o cenário de instalação do agente	102
Localização e requisitos de instalação de agente	103
Instalando e configurando o agente de proxy do vSphere	103
Instalando o agente de proxy do Hyper-V ou do XenServer	108
Instalando o agente do VDI do XenDesktop	112
Instalando o agente do EPI para Citrix	115
Instalando o agente do EPI para scripts do Visual Basic	118
Instalando o agente do WMI para solicitações remotas do WMI	121
<b>5 Tarefas pós instalação do vRealize Automation</b>	<b>125</b>
Substituindo certificados autoassinados por certificados fornecidos por uma autoridade	125
Instalando o agente do vRealize Log Insight em servidores IaaS	125
Configurar o acesso ao tenant padrão	125
<b>6 Solucionando problemas com uma instalação do vRealize Automation</b>	<b>127</b>
Localidades do log padrão	127

Revertendo uma instalação com falha	128
Reverter uma instalação mínima	129
Reverter uma instalação distribuída	129
Criar um pacote de suporte do vRealize Automation	130
Solução de problemas gerais com a instalação	131
A instalação ou a atualização falha com um erro de tempo limite do balanceador de carga	131
Os horários do servidor não estão sincronizados	131
Podem aparecer páginas em branco ao usar o Internet Explorer 9 ou 10 no Windows 7	132
Não é possível estabelecer uma relação confiável para o canal seguro de SSL/TLS	132
Conectar-se à rede por meio de um servidor proxy	133
Etapas do console para a configuração de conteúdo inicial	133
Solucionando problemas com o appliance do vRealize Automation	134
Falha no download dos instaladores	134
O arquivo Encryption.key tem permissões incorretas	135
O Identity Manager não inicia após o reinício do espaço de trabalho do Horizon	135
Atribuições de funções de appliance incorretas após o failover	136
Solucionando problemas de componentes do IaaS	137
Validando certificados de servidor do IaaS	137
Erro de credenciais ao executar o instalador do IaaS	137
O aviso "Salvar Configurações" é exibido durante a instalação do IaaS	138
Falha na instalação do servidor de site e dos Distributed Execution Managers	138
A autenticação do IaaS falha durante Instalação do IaaS Web e do Gerenciamento de Modelos	138
Falha ao instalar os dados e os componentes da Web do Model Manager	139
Servidores Windows IaaS não oferecem suporte ao FIPS	140
A adição de um endpoint do XaaS causa um erro interno	140
A desinstalação de um agente de proxy falha	141
Falha nas solicitações de máquina quando as transações remotas estão desativadas	141
Erro na comunicação do Manager Service	142
O comportamento de personalização de e-mails foi alterado	143
Solução de erros de login	143
As tentativas de fazer login como o administrador do IaaS com credenciais incorretas no formato UPN apresentam falhas sem explicação	143
O login falha com alta disponibilidade	144
O proxy impede o login do usuário do VMware Identity Manager	144
<b>7 Instalação silenciosa do vRealize Automation</b>	<b>147</b>
Realizar uma instalação silenciosa do vRealize Automation	147
Realizar uma instalação silenciosa do Agente de Gerenciamento do vRealize Automation	148
Arquivo de resposta de instalação silenciosa do vRealize Automation	149
A linha de comando de instalação do vRealize Automation	150
Noções básicas sobre a linha de comando de instalação do vRealize Automation	150
Nomes de comandos de instalação do vRealize Automation	150
<b>Índice</b>	<b>153</b>



# vRealize Automation Instalação

---

*vRealize Automation Instalação* explica como instalar 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.

## Glossário de publicações técnicas do VMware

O documento Publicações técnicas do VMware fornece um glossário de termos que podem não ser familiares para você. Para conhecer definições de termos usados na documentação técnica do VMware, acesse <http://www.vmware.com/support/pubs>.





# Informações atualizadas

---

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

Revisão	Descrição
PT_BR-002088-04	Adicionado Configurar uma permissão de cluster do repositório de dados para <a href="#">“Requisitos do agente do vSphere”</a> , na página 103.
PT_BR-002088-03	<ul style="list-style-type: none"><li>■ <a href="#">“Configurar a conta de serviços do Windows para usar a autenticação SQL”</a>, na página 100 revisado.</li><li>■ <a href="#">“Requisitos do agente do vSphere”</a>, na página 103 revisado.</li></ul>
PT_BR-002088-02	Pré-requisitos de atualizações para o servidor Windows de IaaS.
PT_BR-002088-01	<ul style="list-style-type: none"><li>■ Adicionado 5480 às portas de saída do IaaS. Consulte <a href="#">“Requisitos de porta do vRealize Automation”</a>, na página 26.</li><li>■ Corrigido o local no qual você cria um pacote de suporte. Consulte <a href="#">“Criar um pacote de suporte do vRealize Automation”</a>, na página 130.</li><li>■ Adicionado o requisito do modo de compatibilidade para bancos de dados separados do SQL Server. Consulte <a href="#">“Requisitos do servidor de banco de dados do IaaS”</a>, na página 21.</li></ul>
PT_BR-002088-00	Versão inicial do documento.



# Visão geral de instalação do vRealize Automation

# 1

É possível implantar o vRealize Automation em uma variedade de configurações. Para garantir o sucesso, familiarize-se com as opções de configuração e implantação e com a sequência de tarefas necessárias.

Se tiver instalado versões anteriores do vRealize Automation, observe as seguintes alterações antes de começar.

- Esta versão do vRealize Automation inclui o Assistente de Instalação, que foi introduzido no vRealize Automation 7.0. O assistente continua a ser o método recomendado para instalações sem script e oferece suporte para implantações mínimas ou distribuídas.
- Esta versão do vRealize Automation introduz uma instalação com script baseada em console, que funciona em conjunto com um arquivo de resposta que você configura com antecedência.
- Esta versão introduz uma interface de linha de comando para tarefas de instalação que você pode querer realizar após a instalação inicial, como adicionar outro vRealize Automation appliance à sua implantação para alta disponibilidade.
- Esta versão move a página de download do instalador do agente de software e do guest.

<https://vrealize-automation-appliance-FQDN/software/index.html>

Após a instalação, você começa a usar o vRealize Automation personalizando o ambiente e configurando um ou mais tenants, o que configura o acesso ao provisionamento de autoatendimento e ao gerenciamento do ciclo de vida de serviços em nuvem. O portal da Web seguro do vRealize Automation permite que administradores, desenvolvedores ou usuários de negócios solicitem serviços de TI e gerenciem recursos específicos de TI e de nuvem com base em suas funções e privilégios. Os usuários solicitam infraestrutura, aplicativos, desktops e serviços de TI por meio de um catálogo de serviços comum.

Este capítulo inclui os seguintes tópicos:

- [“Escolhendo o caminho de implantação”](#), na página 11
- [“Componentes de instalação do vRealize Automation”](#), na página 14

## Escolhendo o caminho de implantação

Dependendo dos requisitos de implantação, você pode instalar e configurar componentes do vRealize Automation usando o cenário de instalação do Rainpole, o Assistente de Instalação ou por meio do console de gerenciamento.

Escolha uma instalação mínima para implantar um ambiente de desenvolvimento ou de prova de conceito (PoC) ou com uma topologia básica. Escolha uma instalação corporativa para implantar um ambiente de produção com a topologia mais adequada às necessidades da organização.

**Tabela 1-1.** Escolhendo o método de instalação

Método de instalação	Detalhes
Assistente de Instalação	<p>O assistente de instalação fornece o caminho de instalação mais rápido para a maioria das implantações. Você pode escolher uma implantação mínima ou corporativa para dar suporte a componentes distribuídos com ou sem balanceadores de carga. Conclua e verifique todos os pré-requisitos antes de iniciar o assistente.</p> <p>Para obter mais informações, consulte <a href="#">Capítulo 2, “Preparando para a instalação do vRealize Automation”</a>, na página 19.</p>
Instalação manual	<p>A instalação através do console de gerenciamento também é suportada para instalações mínimas, distribuídas e de alta disponibilidade. Conclua e verifique todos os pré-requisitos antes de iniciar a instalação.</p> <p>Para obter mais informações, consulte <a href="#">Capítulo 2, “Preparando para a instalação do vRealize Automation”</a>, na página 19.</p> <p><b>OBSERVAÇÃO</b> Se você usar o console de gerenciamento para iniciar ou configurar qualquer parte da instalação, não poderá iniciar nem continuar o uso do Assistente de Instalação.</p>
<i>Instalando e configurando o vRealize Automation para o cenário do Rainpole</i>	<p>Como administrador do vSphere, você deseja instalar uma implantação mínima do vRealize Automation no seu ambiente vSphere existente. Use o assistente de instalação para instalar o vRealize Automation e criar itens de catálogo de conteúdo iniciais que ajudam a configurar rapidamente um ambiente para o uso de uma prova de conceito.</p> <p>Uma implementação de prova de conceito não é adequada para produção. Ao concluir a implantação de prova de conceito, configure-a como um ambiente de desenvolvimento no qual você e a sua equipe de TI criam e testam blueprints. Você pode exportar blueprints e outros elementos de design do seu ambiente de desenvolvimento para o seu ambiente de produção.</p> <p>Para iniciar esse cenário, consulte <i>Instalando e configurando o vRealize Automation para o cenário do Rainpole</i>.</p>

**Tabela 1-2.** Escolhendo o tipo de implantação

Objetivo da implantação	Escolher este tipo de implantação
Implante um ambiente de desenvolvimento ou de prova de conceito (PoC) com uma topologia básica.	<p>Instale uma implantação mínima.</p> <p>Você implanta uma única instância do vRealize Automation appliance e instala todos os componentes do IaaS em uma única máquina com servidor Windows. Você pode instalar os bancos de dados na mesma máquina Windows ou em um SQL Server dedicado.</p>
Implante um ambiente de produção com a topologia mais adequada às necessidades da sua organização.	<p>Instale uma implantação corporativa.</p> <p>Distribua os componentes em vários servidores.</p> <p>Como opção, você pode implantar balanceadores de carga para distribuir o trabalho nos servidores e fornecer capacidade de failover e redundância em um ambiente de alta disponibilidade.</p>

Para obter mais informações sobre escalabilidade e alta disponibilidade, consulte o guia *Arquitetura de Referência do vRealize Automation*.

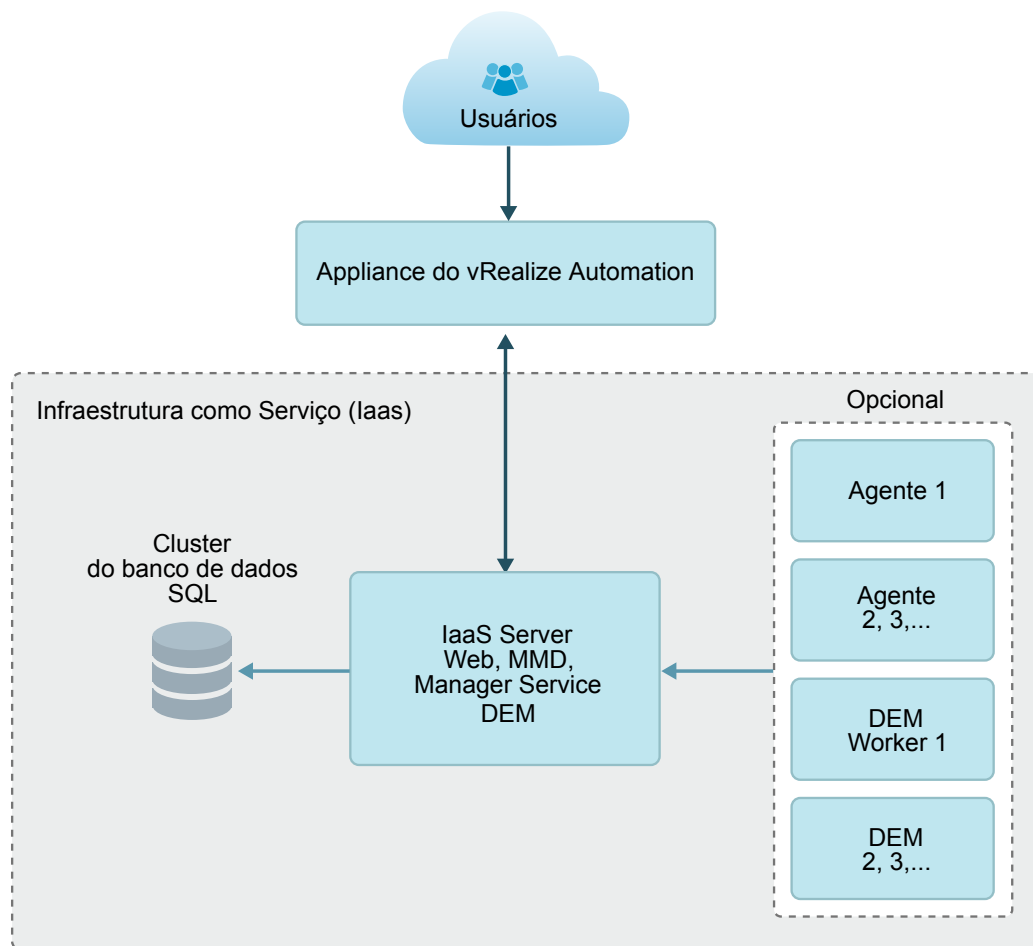
## Visão geral da implantação mínima

Para concluir uma implementação mínima, um administrador de sistema instala os componentes do vRealize Automation appliance e do Infrastructure as a Service (IaaS).

- O vRealize Automation appliance inclui a interface do console da Web e suporte a recursos de single sign-on. Ele é instalado como um appliance virtual.
- O Infrastructure as a Service (IaaS) é instalado em uma máquina Windows Server.

- O IaaS usa um banco de dados SQL que pode ser instalado na mesma máquina que o IaaS ou em seu próprio servidor.

A figura a seguir mostra a relação e a finalidade dos componentes de uma instalação mínima.



## Visão geral da implantação corporativa

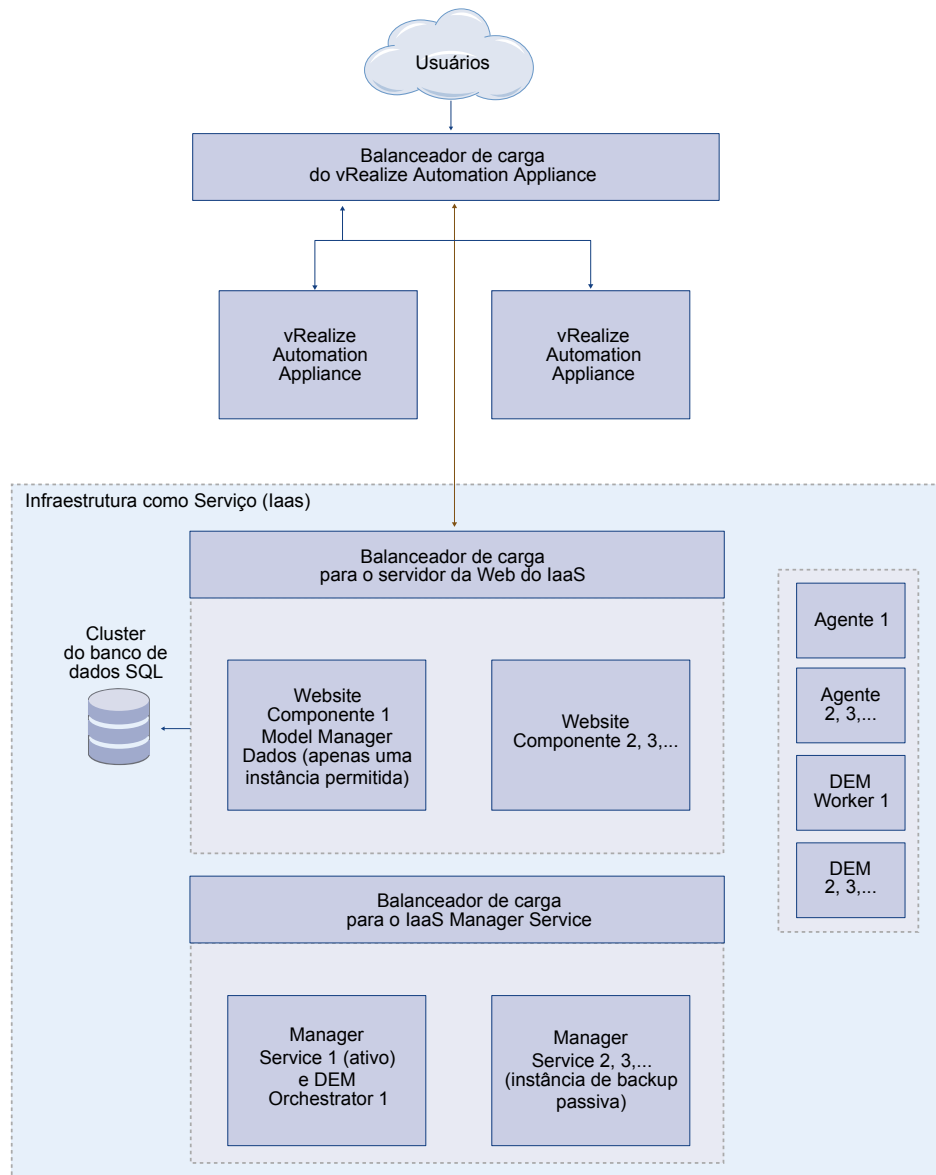
O administrador de sistema pode implantar e instalar várias instâncias do vRealize Automation appliance e componentes individuais do IaaS para dimensionamento, redundância, alta disponibilidade e recuperação de desastres.

Em uma arquitetura típica, os componentes do IaaS são distribuídos em várias máquinas.

Para implantações de alta disponibilidade, os balanceadores de carga distribuem a carga de trabalho no ambiente de computação. Os administradores de sistema configuram os balanceadores de carga fora da estrutura do vRealize Automation.

A figura a seguir mostra os componentes de uma implantação corporativa com componentes distribuídos, redundância e balanceadores de carga.

**Figura 1-1.** Configuração de implantação para instalações corporativas



## Componentes de instalação do vRealize Automation

A instalação do vRealize Automation inclui a instalação e a configuração de recursos de single sign-on (SSO), do portal de interface do usuário e de componentes do Infrastructure as a Service (IaaS).

Uma instalação consiste nos componentes a seguir.

- O vRealize Automation appliance, que implanta o console de gerenciamento, gerencia recursos SSO (Single Sign-on) para autorização e autenticação e inclui uma instância do vRealize Orchestrator.
- Os componentes de Infraestrutura como Serviço (IaaS) que são instalados em máquinas Windows virtuais ou físicas e são exibidos em grande parte na guia **Infraestrutura** do console.
- Um banco de dados Microsoft SQL Server, que é implantado durante a instalação do IaaS.

## O appliance do vRealize Automation

O vRealize Automation appliance é um appliance virtual Linux pré-configurado que contém o servidor do vRealize Automation.

O vRealize Automation é fornecido como um arquivo aberto de virtualização .ovf ou .ova. O appliance virtual é implantado na infraestrutura virtualizada existente.

O servidor inclui o console de produto do vRealize Automation appliance, que fornece um único portal para o provisionamento e o gerenciamento de autoatendimento dos serviços em nuvem, da criação, da administração e da governança.

### Banco de Dados do Appliance

Durante a implantação dos appliances virtuais, é criado um banco de dados de appliance do PostgreSQL automaticamente no primeiro vRealize Automation appliance. Um banco de dados de réplica pode ser instalado em um segundo appliance do vRealize Automation para alta disponibilidade.

## Agentes de gerenciamento

Os agentes de gerenciamento são componentes de IaaS autônomos que registram nós de IaaS com appliances do vRealize Automation, automatizam a instalação e o gerenciamento de componentes de IaaS e coletam informações de suporte e de telemetria

É preciso instalar um agente de gerenciamento em cada máquina Windows que hospeda componentes do IaaS.

## Infrastructure as a Service do vRealize Automation

O IaaS (Infraestrutura como Serviço) permite modelar e provisionar rapidamente servidores e desktops em infraestruturas de nuvens privadas, públicas ou híbridas.

O administrador do sistema instala os componentes do IaaS em uma máquina Windows. Os recursos do IaaS também estão disponíveis na guia **Infraestrutura** do console de gerenciamento. O IaaS tem vários componentes que você pode instalar em uma configuração personalizada para atender às necessidades da sua organização.

### Site do IaaS

O componente de site do IaaS fornece os recursos de autorização de serviço e administração de infraestrutura para o console do vRealize Automation. O componente do site se comunica com o Manager Service, que fornece as atualizações do Distributed Execution Manager (DEM), dos agentes de proxy e do banco de dados.

### Model Manager

Os modelos do vRealize Automation facilitam a integração com sistemas externos e bancos de dados. Eles implementam a lógica de negócios que um Distributed Execution Manager (DEM) usa.

O Model Manager fornece serviços e utilitários para persistência, controle de versões, proteção e distribuição de elementos de modelo. Ele se comunica com o banco de dados, os DEMs e o site do console.

## Manager Service

O Manager Service 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.

Sua implantação do IaaS requer apenas uma máquina Windows para executar ativamente o Manager Service. Para backup ou alta disponibilidade, será possível implantar máquinas Windows adicionais onde você inicia manualmente o Manager Service se o serviço ativo parar.

---

**IMPORTANTE** A execução simultânea de um Manager Service ativo em vários servidores Windows do IaaS torna o vRealize Automation inutilizável.

---

O Manager Service comunica-se com o site IaaS por meio do Model Manager e deve ser executado em uma conta de domínio com privilégios de administrador em todas as máquinas Windows IaaS.

## Banco de dados do IaaS

O componente IaaS do vRealize Automation usa um banco de dados do Microsoft SQL Server para manter as informações sobre as máquinas que gerencia e seus próprios elementos e políticas. Normalmente, o banco de dados é criado para você durante a instalação. o entanto, um administrador de sistemas também pode criar o banco de dados separadamente.

## Distributed Execution Managers

Um Distributed Execution Manager (DEM) executa a lógica de negócios dos modelos personalizados, interagindo com o banco de dados e com os bancos de dados e os sistemas externos conforme necessário.

Cada instância do DEM age em uma função Worker ou Orchestrator. A função Worker é responsável pela execução de fluxos de trabalho. A função Orchestrator é responsável pelo monitoramento de instâncias do DEM Worker, pelo pré-processamento de fluxos de trabalho para execução e pelo agendamento de fluxos de trabalho.

O DEM Orchestrator executa essas tarefas específicas.

- Monitora o status dos DEM Workers e garante que, se uma instância Worker parar ou perder a conexão com o Model Manager, os respectivos fluxos de trabalho serão enfileirados novamente para que outro DEM Worker colete.
- Gerencia fluxos de trabalho agendados por meio da criação de novas instâncias de fluxo de trabalho no horário agendado.
- Assegura que somente uma instância de um fluxo de trabalho agendado específico esteja em execução em um determinado momento.
- Pré-processa os fluxos de trabalho antes que sejam executados, incluindo a verificação das pré-condições dos fluxos de trabalho utilizados na implementação do recurso RunOneOnly e a criação do histórico de execução de fluxo de trabalho.

Uma instância do DEM Orchestrator é designada como o Orchestrator ativo que executa essas tarefas. Como o DEM Orchestrator é essencial para executar fluxos de trabalho, instale pelo menos uma instância adicional do Orchestrator em uma máquina separada para obter redundância. O Orchestrator é instalado automaticamente na máquina que também executa um Serviço de Gerenciador. O DEM Orchestrator adicional monitora o status do Orchestrator ativo para que ele possa assumir caso o Orchestrator ativo ficar offline.



## Agentes do vRealize Automation

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

Geralmente, você instala o agente vSphere como parte de uma implantação. É possível instalar outros agentes de acordo com os requisitos do site.

### Agentes de integração

Os agentes PowerShell de VDI (infraestrutura de desktop virtual) permitem que o vRealize Automation faça integração a sistemas externos de desktop virtual. Atualmente, as máquinas virtuais provisionadas pelo vRealize Automation podem ser registradas com o XenDesktop em um Citrix Desktop Delivery Controller (DDC) e seus proprietários podem acessar a XenDesktop Web Interface pelo vRealize Automation.

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 VDI e EPI requerem acesso no nível do administrador aos sistemas externos com os quais eles interagem.

### Agentes de proxy de virtualização

As máquinas virtuais que o vRealize Automation gerencia são criadas em hosts de virtualização. O vRealize Automation usa agentes de proxy de virtualização para enviar comandos e coletar dados dos hosts de virtualização do Server, XenServer e Hyper-V do vSphere ESX e das máquinas virtuais provisionadas nele. Um agente de proxy possui as seguintes características.

- Normalmente requer acesso no nível de administrador à plataforma de virtualização que ele gerencia.
- Comunica-se com o Manager Service
- É instalado separadamente com seu próprio arquivo de configuração

### 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 remotos a partir de uma localização remota. Ele permite a coleta de dados a partir de máquinas do Windows gerenciadas pelo vRealize Automation.



# Preparando para a instalação do vRealize Automation

# 2

Os Administradores do Sistema instala o vRealize Automation nos ambientes de virtualização existentes. Antes de iniciar uma instalação, prepare o ambiente de implantação para atender aos requisitos de sistema.

Este capítulo inclui os seguintes tópicos:

- “Nomes de host e endereços IP”, na página 19
- “Requisitos de hardware e da máquina virtual”, na página 20
- “Considerações sobre o navegador”, na página 20
- “Considerações sobre senhas”, na página 21
- “Requisitos do Windows Server”, na página 21
- “Requisitos de porta do vRealize Automation”, na página 26
- “Contas de usuário e credenciais necessárias para a instalação”, na página 29
- “Segurança”, na página 30
- “Sincronização de hora”, na página 31

## 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 quando for identificar ou selecionar uma máquina. Não insira endereços IP.

- 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.

- Faça o planejamento prévio da nomenclatura do domínio e das máquinas para que as máquinas do vRealize Automation comecem e terminem com letras do alfabeto (a-z) ou dígitos (0-9) e contenham apenas caracteres alfanuméricos ou hífens (-). 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](http://www.ietf.org).

- Espere manter os nomes de hosts e FQDNs que você planejou para sistemas vRealize Automation. Alterar um nome de host após a instalação torna o vRealize Automation inutilizável.

- Uma prática recomendada é reservar e usar endereços IP estáticos para todos os servidores Windows vRealize Automation appliance e 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 vRealize Automation appliance durante a implantação do OVF ou OVA.
- Para os servidores WindowsIaaS, você segue o processo habitual do sistema operacional. Defina o endereço IP antes de instalar o IaaS do vRealize Automation.

## Requisitos de hardware e da máquina virtual

A implantação deve atender aos requisitos mínimos de recursos de sistema para instalar appliances virtuais e aos requisitos mínimos de hardware para instalar componentes IaaS no Windows Server.

Para obter informações sobre requisitos do sistema operacional e ambiente de alto nível, incluindo navegadores e sistemas operacionais suportados, consulte o *Matriz de suporte do vRealize Automation*.

A tabela de requisitos de hardware exibe os requisitos mínimos de configuração para a implantação de dispositivos virtuais e instalação de componentes do IaaS. Dispositivos são máquinas virtuais pré-configuradas que você adiciona ao seu inventário do vCenter Server ou do ESXi. Os componentes do IaaS são instalados em servidores físicos ou virtuais do Windows 2008 R2 SP1 ou do Windows 2012 R2.

Um Active Directory é considerado pequeno quando há até 25.000 usuários no UO para ser sincronizados na configuração do Armazenamento de ID. Um Active Directory é considerado grande quando há mais de 25.000 usuários no UO.

**Tabela 2-1.** Requisitos de hardware

<b>vRealize Automation appliance para instâncias pequenas do Active Directory</b>	<b>vRealize Automation appliance para instâncias grandes do Active Directory</b>	<b>Componentes do IaaS (Windows Server).</b>
<ul style="list-style-type: none"> <li>■ 4 CPUs</li> <li>■ 18 GB de memória</li> <li>■ 60 GB de armazenamento de disco</li> </ul>	<ul style="list-style-type: none"> <li>■ 4 CPUs</li> <li>■ 22 GB de memória</li> <li>■ 60 GB de armazenamento de disco</li> </ul>	<ul style="list-style-type: none"> <li>■ 2 CPUs</li> <li>■ 8 GB de memória</li> <li>■ 30 GB de armazenamento de disco</li> </ul> <p>São necessários recursos adicionais quando você está incluso em um Servidor SQL ou em um host do Windows.</p>

## Considerações sobre o navegador

Existem algumas restrições sobre o uso do navegador com o vRealize Automation.

- 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 a um subconjunto de navegadores aos quais o vRealize Automation também oferece suporte.

Para obter informações sobre requisitos do sistema operacional e ambiente de alto nível, incluindo navegadores e sistemas operacionais suportados, consulte o *Matriz de suporte do vRealize Automation*.

## Considerações sobre senhas

As restrições de caracteres se aplicam a algumas senhas.

A senha de administrador do VMware vRealize™ Automation não pode conter um caractere "=" à direita. Tais senhas são aceitas quando você as atribui, mas resultam em erros quando você executa operações como o salvamento de endpoints.

## Requisitos do Windows Server

A máquina virtual ou física do Windows que hospeda os componentes do IaaS deve atender aos requisitos de configuração do banco de dados IaaS, dos componentes de servidor IaaS, do IaaS Manager Service e dos Distributed Execution Managers.

O Assistente de Instalação executa um verificador de pré-requisitos do vRealize Automation em todos os servidores Windows IaaS para garantir que elas atendam à configuração necessária para a instalação. Além do verificador de pré-requisitos, aborde os seguintes pré-requisitos separadamente.

- Como prática recomendada, coloque todos os servidores Windows IaaS no mesmo domínio.
- Crie ou identifique uma conta de domínio a ser usada para instalação e que tenha privilégios de administrador em todos os servidores Windows IaaS.

## Requisitos do servidor de banco de dados do IaaS

O servidor Windows que hospeda o banco de dados do SQL Server do IaaS do vRealize Automation deve atender a certos pré-requisitos.

Os requisitos serão aplicados se você executar o assistente de instalação ou o instalador `setup_vrealize-automation-appliance-URL.exe` herdado e selecionar a função de banco de dados para a instalação. Os pré-requisitos também serão aplicados se você criar separadamente um banco de dados vazio do SQL Server para ser usado com o IaaS.

- Use uma versão do SQL Server com suporte do *Matriz de suporte do vRealize Automation*.
- Ative o protocolo TCP/IP para o SQL Server.
- Ative o serviço Coordenador de Transações Distribuídas (DTC) em todos os servidores Windows do IaaS e a máquina que hospeda o SQL Server. 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 Manager Service”](#), na página 142.

---

Para obter mais informações sobre a ativação do DTC, consulte o [Artigo da base de conhecimento da VMware 2038943](#).

- Abra portas entre todos os servidores Windows do IaaS e a máquina que hospeda o SQL Server. Consulte [“Requisitos de porta do vRealize Automation”](#), na página 26.

Como alternativa, se as políticas do site permitirem, você poderá desativar os firewalls entre os servidores Windows do IaaS e o SQL Server.

- Esta versão do vRealize Automation não tem suporte para o modo de compatibilidade 130 do SQL Server 2016. 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 de um instalador do vRealize Automation, a compatibilidade já estará configurada.

- O Grupo de Disponibilidade AlwaysOn (AAG) é o único com suporte no SQL Server 2016.

## Requisitos de Servidor do Model Manager e do Serviço Web IaaS

O seu ambiente deve atender aos pré-requisitos de software e configuração que oferecem suporte à instalação dos componentes do servidor do IaaS.

### Requisitos de ambiente e banco de dados para o IaaS

Sua configuração de host e do banco de dados MS SQL deve atender aos seguintes requisitos.

**Tabela 2-2.** Requisitos do IaaS

Área	Requisitos
Configuração do host	<p>Os seguintes componentes devem estar instalados no host antes da instalação do IaaS:</p> <ul style="list-style-type: none"> <li>■ O Microsoft .NET Framework 4.5.2 ou posterior.</li> <li>■ Microsoft PowerShell 2.0 (incluído com o Windows Server 2008 R2 SP1 e versões posteriores) ou Microsoft PowerShell 3.0 no Windows Server 2012 R2.</li> <li>■ Microsoft Internet Information Services 7.5.</li> <li>■ O Java deve estar instalado na máquina que executa o componente Web principal para dar suporte à implantação do banco de dados MS SQL durante a instalação.</li> </ul>
Requisitos do banco de dados Microsoft SQL	<p>O banco de dados SQL pode residir em um dos seus servidores Windows IaaS ou em um host separado.</p> <p>Se o banco de dados SQL estiver em um dos seus servidores Windows IaaS, configure os seguintes requisitos Java.</p> <ul style="list-style-type: none"> <li>■ Instale o Java 1.8 ou posterior de 64 bits. Não use 32 bits.</li> <li>■ Defina a variável de ambiente JAVA_HOME como a pasta de instalação Java.</li> <li>■ Verifique se o arquivo %JAVA_HOME%\bin\java.exe está disponível.</li> </ul>

### Requisitos do Microsoft Internet Information Services

Configure o Internet Information Services (IIS) para atender aos seguintes requisitos.

Além das definições de configuração, evite hospedar sites adicionais no IIS no host do servidor Web IaaS. 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 2-3.** Configuração necessária para o Microsoft Internet Information Services

Componente do IIS	Configuração
Módulos do Internet Information Services (IIS) instalados	<ul style="list-style-type: none"> <li>■ WindowsAuthentication</li> <li>■ StaticContent</li> <li>■ DefaultDocument</li> <li>■ ASPNET 4.5</li> <li>■ ISAPIExtensions</li> <li>■ ISAPIFilter</li> </ul>
Configurações de Autenticação do IIS	<ul style="list-style-type: none"> <li>■ Autenticação do Windows ativada</li> <li>■ AnonymousAuthentication desativada</li> <li>■ Negotiate Provider ativado</li> <li>■ NTLM Provider ativado</li> <li>■ Modo Kernel da Autenticação do Windows ativado</li> <li>■ Proteção Estendida da Autenticação do Windows desativada</li> <li>■ Para certificados que usam SHA512, o TLS1.2 deve ser desativado nos servidores Windows 2012 ou Windows 2012 R2</li> </ul>
Funções Serviço de Ativação de Processos do Windows do IIS	<ul style="list-style-type: none"> <li>■ ConfigurationApi</li> <li>■ NetEnvironment</li> <li>■ ProcessModel</li> <li>■ WcfActivation (somente Windows 2008)</li> <li>■ HttpActivation</li> <li>■ NonHttpActivation</li> </ul>

## IaaS Manager Service

O seu ambiente deve atender a alguns requisitos gerais que oferecem suporte à instalação do IaaS Manager Service.

- O Microsoft .NET Framework 4.5.2 está instalado.
- Microsoft PowerShell 2.0, 3.0 ou 4.0. Algumas atualizações ou migrações do vRealize Automation podem exigir a instalação de uma versão mais antiga ou mais recente do PowerShell, além daquela que está em execução no momento.
- O SecondaryLogOnService está em execução.
- Nenhum firewall pode existir entre o host DEM e o Windows Server. Para obter informações sobre portas, consulte [“Requisitos de porta do vRealize Automation”](#), na página 26.
- O IIS está instalado e configurado.

## Requisitos do Distributed Execution Manager

O seu ambiente deve atender a alguns requisitos gerais que oferecem suporte à instalação de Distributed Execution Managers (DEMs).

- O Microsoft .NET Framework 4.5.2 está instalado.
- Microsoft PowerShell 2.0, 3.0 ou 4.0. Algumas atualizações ou migrações do vRealize Automation podem exigir a instalação de uma versão mais antiga ou mais recente do PowerShell, além daquela que está em execução no momento.
- O SecondaryLogOnService está em execução.

- Nenhum firewall entre o host DEM e o servidor Windows, ou portas abertas, conforme descrito em [“Requisitos de porta do vRealize Automation”](#), na página 26.

Os servidores que hospedam as instâncias do DEM Worker podem apresentar requisitos adicionais, dependendo dos recursos de provisionamento com os quais interagem.

## Requisitos do Amazon Web Services EC2

O servidor Windows IaaS do vRealize Automation se comunica com a conta do Amazon EC2 e coleta dados dessa conta.

Quando você usa o Amazon Web Services (AWS) para provisionamento, os servidores Windows IaaS que hospedam os trabalhadores do DEM devem atender aos seguintes requisitos.

- Os hosts do trabalhador do DEM devem ter acesso à Internet.
- Se os hosts do trabalhador do DEM estiverem atrás de um firewall, o tráfego HTTPS deverá ser permitido de e para `aws.amazon.com`, bem como as 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 os hosts do trabalhador do DEM acessarem a Internet através de um servidor proxy, o serviço DEM deverá ser executado com credenciais que possam ser autenticadas no servidor proxy.



## Requisitos para Openstack e PowerVC

As máquinas nas quais você instala seus DEMs devem atender a certos requisitos para se comunicarem com a instância do Openstack ou PowerVC e coletarem dados dela.

**Tabela 2-4.** Requisitos do host DEM

Sua instalação	Requisitos
Tudo	<p>No Registro do Windows, habilite o suporte ao TLS v1.2 para .NET Framework. Por exemplo:  [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319]  "SchUseStrongCrypto"=dword:00000001</p> <p>[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319]  "SchUseStrongCrypto"=dword:00000001</p>
Host DEM do Windows 2008	<p>No Registro do Windows, habilite o protocolo TLS v1.2. Por exemplo:  [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</p> <p>[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server]  "DisabledByDefault"=dword:00000000  "Enabled"=dword:00000001</p>
Certificados auto-assinados no seu host de endpoint de infraestrutura	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.

## Requisitos do Red Hat Enterprise Virtualization KVM (RHEV)

Quando você usa o Red Hat Enterprise Virtualization para realizar o provisionamento, o servidor Windows do IaaS comunica-se com essa conta e coleta dados dela.

Seu ambiente deve atender aos requisitos do Red Hat Enterprise a seguir.

- Cada ambiente KVM (RHEV) deve ser unido ao domínio que contém o servidor do IaaS.
- As credenciais utilizadas para gerenciar o endpoint que representa um ambiente KVM (RHEV) devem ter privilégios de Administrador no ambiente RHEV. Essas credenciais também devem ter privilégios suficientes para criar objetos nos hosts no ambiente.

## Requisitos do SCVMM

Qualquer trabalhador DEM usado para gerenciar máquinas virtuais por meio do SCVMM deve ser instalado em um host no qual o console do SCVMM já está instalado.

Além disso, os seguintes requisitos devem ser atendidos:

- O DEM deve ter acesso ao módulo SCVMM PowerShell instalado com o console.

- A Política de execução do MS PowerShell deve ser definida como RemoteSigned ou Unrestricted.

Para obter informações sobre a Política de execução do PowerShell, emita um dos seguintes comandos no prompt de comando do PowerShell:

```
help about_signing
help Set-ExecutionPolicy
```

- Se todos os Trabalhadores DEM da instância não estiverem em recursos de processamento que atendem a esses requisitos, as Habilidades deverão ser usadas para direcionar todos os fluxos de trabalho relacionados ao SCVMM para aqueles que atendem.

Os requisitos adicionais a seguir se aplicam ao SCVMM.

- Você deve instalar o console do SCVMM antes de instalar os trabalhadores DEM que consomem itens de trabalho do SCVMM.

Se você instalar o trabalhador DEM antes do console do SCVMM, verá erros de log semelhantes ao seguinte:

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 isso, verifique se o console do SCVMM está instalado e reinicie o serviço do trabalhador DEM.

- 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. Essas credenciais também devem ter privilégios de administrador nos servidores Hyper-V da instância.
- 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 máquinas em um recurso de processamento SCVMM, um usuário deve ser adicionado a pelo menos uma função de segurança na instância do SCVMM.

## Requisitos de porta do vRealize Automation

O vRealize Automation usa portas designadas para comunicação e acesso a dados.

Embora o vRealize Automation use somente a porta 443 para comunicação, pode haver outras portas a serem abertas no sistema. Como portas abertas e desprotegidas podem apresentar vulnerabilidades de segurança, certifique-se de que apenas as portas necessárias pelos seus aplicativos de negócios estejam abertas.

## Appliance do vRealize Automation

Os seguintes portas são usadas pelo vRealize Automation appliance.

**Tabela 2-5.** Portas de entrada do vRealize Automation appliance

Porta	Protocolo	Comentários
22	TCP	Opcional. Acesso para sessões SSH.
80	TCP	Opcional. Redireciona para 443.
111	TCP, UDP	RPC.

**Tabela 2-5.** Portas de entrada do vRealize Automation appliance (Continuação)

Porta	Protocolo	Comentários
443	TCP	Acesso ao console do vRealize Automation e às chamadas de API.
443	TCP	Acesso para máquinas para baixar o agente guest e o agente de bootstrap do software.
5480	TCP	Acesso à interface de gerenciamento Web do appliance virtual.
5480	TCP	Usado pelo Agente de Gerenciamento.
5488, 5489	TCP	Usado internamente pelo vRealize Automation appliance para atualizações.
4369, 25672, 5671, 5672	TCP	Mensagens do RabbitMQ.
8230, 8280, 8281	TCP	Instância interna do vRealize Orchestrator.
8444	TCP	Comunicação do proxy do console para conexões do vSphere VMware Remote Console.

**Tabela 2-6.** Portas de saída do Appliance do vRealize Automation

Porta	Protocolo	Comentários
25, 587	TCP, UDP	SMTP para o envio de e-mails de notificação de saída.
53	TCP, UDP	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.
110, 995	TCP, UDP	POP para receber e-mails de notificação de entrada.
143, 993	TCP, UDP	IMAP para receber e-mails de notificação de entrada.
123	TCP, UDP	Opcional. Para conexão direta com o NTP em vez de usar o tempo do host.
443	TCP	Comunicação por HTTPS com o IaaS Manager Service e hosts de endpoint de infraestrutura.
443	TCP	Comunicação com o agente de bootstrap de software via HTTPS.
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.
5432	TCP, UDP	Opcional. Para comunicação com um Banco de Dados do Appliance.
8281	TCP	Opcional. Para comunicação com uma instância externa do vRealize Orchestrator.

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.

## Infraestrutura como Serviço

As portas nas tabelas Portas de entrada dos componentes do Infrastructure as a Service e Portas de saída do Infrastructure as a Service devem estar disponíveis para uso pelo Windows Server do IaaS.

**Tabela 2-7.** Portas de entrada dos componentes do Infrastructure as a Service

Componente	Porta	Protocolo	Comentários
Manager Service	443	TCP	Comunicação com os componentes do IaaS e do vRealize Automation appliance sobre HTTPS.
vRealize Automation appliance	443	TCP	Comunicação com os componentes do IaaS e do vRealize Automation appliance sobre HTTPS.
Hosts de endpoint de infraestrutura	443	TCP	Comunicação com os componentes do IaaS e do vRealize Automation appliance 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.
Instância do SQL Server	1433	TCP	MSSQL.

**Tabela 2-8.** Portas de saída dos componentes do Infrastructure as a Service

Componente	Porta	Protocolo	Comentários
Tudo	53	TCP, UDP	DNS.
Tudo	67, 68, 546, 547	TCP, UDP	DHCP.
Tudo	123	TCP, UDP	Opcional. NTP.
Manager Service	443	TCP	Comunicação com o vRealize Automation appliance sobre HTTPS.
Website	443	TCP	Comunicação com o Manager Service sobre HTTPS. Comunicação com o vCenter Server via HTTPS.
Distributed Execution Managers	443	TCP	Comunicação com o Manager Service sobre HTTPS.
Agentes de proxy	443	TCP	Comunicação por HTTPS com o Manager Service e hosts de endpoint de infraestrutura.
Agente de gerenciamento	443	TCP	Comunicação com o vRealize Automation appliance.
Agente guest Agente de bootstrap de software	443	TCP	Comunicação com o Manager Service sobre HTTPS.
Manager Service Website	1433	TCP	MSSQL.
Tudo	5480	TCP	Comunicação com o vRealize Automation appliance.

## Serviço do Microsoft Distributed Transaction Coordinator

Além de verificar se as portas listadas nas tabelas anteriores estão livres para uso, você deve ativar a comunicação do Serviço do Microsoft Distributed Transaction Coordinator (MS DTC) entre todos os servidores na implantação. O MS DTC exige o uso de porta 135 sobre TCP e de uma porta aleatória entre 1024 e 65535.

O Verificador de Pré-requisitos valida se o MS DTC está em execução e se as portas obrigatórias estão abertas.

## Contas de usuário e credenciais necessárias para a instalação

Você deve verificar se tem as funções e credenciais para instalar os componentes do vRealize Automation.

### Conta do serviço vCenter

Se você planeja usar um endpoint do vSphere, precisa de um domínio e de uma conta local que tenha o nível apropriado de acesso configurado no vCenter.

### Instalação do appliance virtual

Para implantar o vRealize Automation appliance, você deve ter os privilégios apropriados na plataforma de implantação (por exemplo, credenciais do administrador do vSphere).

Durante o processo de implantação, você especifica a senha para a conta de administrador do appliance virtual. Essa conta fornece acesso ao console de gerenciamento do vRealize Automation appliance a partir do qual você configura e administra os appliances virtuais.

### Instalação do IaaS

Antes de instalar os componentes do IaaS, adicione o usuário sob o qual você pretende executar os programas de instalação do IaaS ao grupo Administrador no host de instalação.

### Credenciais de banco de dados do IaaS

Você pode criar o banco de dados durante a instalação do produto ou criá-lo manualmente no servidor SQL.

Quando você cria ou preenche um banco de dados MS SQL por meio do vRealize Automation, usando o assistente de instalação ou o console de gerenciamento, os seguintes requisitos se aplicam:

- Se você escolher a opção **Usar a autenticação do Windows**, a função **sysadmin** no SQL Server deverá ser concedida ao usuário que executa o Agente de gerenciamento no servidor da Web primário do IaaS para criar e alterar o tamanho do banco de dados.
- Se você não escolher a opção **Usar a autenticação do Windows**, a função **sysadmin** no SQL Server também deverá ser concedida ao usuário que executa o Agente de gerenciamento no servidor da Web primário do IaaS. As credenciais são usadas durante o tempo de execução.
- Se você usar o vRealize Automation para preencher um banco de dados previamente criado, as credenciais do usuário fornecidas (o usuário atual do Windows ou o usuário especificado do SQL) precisarão somente dos privilégios **dbo** para o banco de dados do IaaS.

---

**OBSERVAÇÃO** Os usuários do vRealize Automation também exigem o nível correto de acesso à autenticação do Windows para fazer login e usar o vRealize Automation.

---

### Credenciais do usuário do serviço IaaS

O IaaS instala vários serviços do Windows que compartilham um único usuário do serviço.

Os seguintes requisitos se aplicam ao usuário do serviço para os serviços do IaaS:

- O usuário deve ser um usuário do domínio.
- O usuário deve ter privilégios de Administrador locais em todos os hosts nos quais o componente Manager Service ou o site está instalado. Não realize uma instalação de grupo de trabalho.
- O usuário está configurado com os privilégios **Fazer logon como um serviço**. Esse privilégio garante que o Manager Service é iniciado e gera arquivos de log.

- O usuário deve ter os privilégios **dbo** para o banco de dados do IaaS. Se você usar o instalador para criar o banco de dados, verifique se o login do usuário do serviço é adicionado ao SQL Server antes de executar o instalador. O instalador concede os privilégios **dbo** ao usuário do serviço após a criação do banco de dados.
- O instalador é executado na conta que executa o agente de gerenciamento no servidor da Web primário. Se quiser usar o instalador para criar um banco de dados MS SQL durante a instalação, você deve ter a função **sysadmin** ativada em MS SQL. Isso não será um requisito se você optar por usar um banco de dados vazio pré-criado.
- A conta de usuário do domínio que você planeja usar como a identidade do pool de aplicativos do IIS para o Model Manager Web Service está configurada com os privilégios **Fazer logon como trabalho em lote**.

## Especificações do Servidor Model Manager

Especifique o nome do servidor Model Manager usando um nome de domínio totalmente qualificado (FQDN). Não use um endereço IP para especificar o servidor.

## Segurança

O vRealize Automation usa SSL para garantir uma comunicação segura entre os componentes. As senhas são usadas para garantir um armazenamento seguro em banco de dados.

Para obter mais informações, consulte [“Requisitos de confiança de certificado em um ambiente distribuído”](#), na página 65.

## Certificados

O vRealize Automation usa certificados SSL para uma comunicação segura entre componentes e instâncias do IaaS do vRealize Automation appliance. 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 solução de problemas, suporte e requisitos de confiança para certificados, consulte o [artigo da base de dados de conhecimento 2106583 da VMware](#).

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 2-9.** 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.

## Extraindo certificados e chaves privadas

Os certificados que você usa com os appliances virtuais devem estar no formato de arquivo PEM.

Os exemplos na seguinte tabela usam comandos do Gnu openssl para extrair as informações de certificado que você precisa para configurar os appliances virtuais.

**Tabela 2-10.** Valores e comandos de certificado de amostra (openssl)

A autoridade de certificação fornece	Comando	Entradas de appliance virtual
Chave privada RSA	<code>openssl pkcs12 -in <i>path_to_pfx_certificate_file</i> -nocerts -out key.pem</code>	<b>Chave privada RSA</b>
Arquivo PEM	<code>openssl pkcs12 -in <i>path_to_pfx_certificate_file</i> -clcerts -nokeys -out cert.pem</code>	<b>Cadeia de certificados</b>
(Opcional) Código de acesso	n/d	<b>Código de acesso</b>

## Senha de segurança

O vRealize Automation usa senhas de segurança para segurança do banco de dados. Uma senha é uma série de palavras usadas para criar uma frase que gera a chave de criptografia, que protege os dados durante o repouso no banco de dados.

Siga estas diretrizes ao criar uma senha de segurança pela primeira vez.

- Use a mesma senha em toda a instalação para garantir que cada componente tenha a mesma chave de criptografia.
- Use uma frase maior que oito caracteres.
- Inclua caracteres em letras maiúsculas, minúsculas, numéricos e símbolos.
- Memorize a senha ou mantenha-a em um lugar seguro. A senha é necessária para restaurar as informações do banco de dados caso ocorra uma falha no sistema ou para adicionar componentes após a instalação inicial. Sem a senha, não é possível restaurar com sucesso.

## Software de terceiros

Alguns componentes do vRealize Automation dependem de software de terceiros, incluindo o Microsoft Windows e o SQL Server. Para se proteger contra vulnerabilidades de segurança dos produtos de terceiros, verifique se o seu software está atualizado com as últimas correções do fornecedor.

## Sincronização de hora

Um administrador do sistema deve configurar a pontualidade rigorosa, como parte da instalação do vRealize Automation.

A instalação falhará se a sincronização de hora for configurada incorretamente.

A pontualidade deve ser consistente e sincronizada no vRealize Automation appliance e nos servidores do Windows. Usando o mesmo método de pontualidade em cada componente, você pode garantir essa consistência.

Para máquinas virtuais, você pode usar os seguintes métodos:

- Configuração usando o protocolo NTP (diretamente).
- Configuração usando o protocolo NTP por meio do ESXi com o VMware Tools. Você deve ter o NTP configurado no ESXi.

Para servidores do Windows, consulte [Timekeeping best practices for Windows, including NTP](#).



# Instalando o vRealize Automation com o assistente de instalação

## 3

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 vRealize Automation appliance e configura servidores Windows IaaS para atender os pré-requisitos. O Assistente de Instalação aparece na primeira vez que você faz login no vRealize Automation appliance recém-implantado.

- 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 4, “As interfaces de instalação padrão do vRealize Automation”](#), na página 51.

Este capítulo inclui os seguintes tópicos:

- [“Implantar o appliance do vRealize Automation”](#), na página 33
- [“Usando o assistente de instalação para implantações mínimas”](#), na página 35
- [“Usando o assistente de instalação para implantações corporativas”](#), na página 42

## Implantar o appliance do vRealize Automation

Para implantar o vRealize Automation appliance, um administrador de sistema deve fazer login no cliente do vSphere e selecionar as configurações de implantação.

Algumas restrições se aplicam à senha raiz criada para o administrador do vRealize Automation.

### Pré-requisitos

- Faça download do vRealize Automation appliance no site da VMware.
- Faça login no cliente do vSphere como usuário com privilégios de administrador de sistema.

### Procedimentos

- 1 Selecione **Arquivo > Implantar Modelo OVF** no cliente do vSphere.
- 2 Navegue até o arquivo do vRealize Automation appliance que você fez download e clique em **Abrir**.
- 3 Clique em **Avançar**.
- 4 Clique em **Avançar** na página Detalhes do Modelo OVF.
- 5 Aceite o contrato de licença e clique em **Avançar**.

- 6 Insira um nome exclusivo de appliance virtual, de acordo com a convenção de nomenclatura de TI da sua organização, na caixa de texto **Nome**, selecione o centro de dados e o local no qual você deseja implantar o appliance virtual e clique em **Avançar**.
- 7 Siga os prompts até que a página Formato do Disco seja exibida.
- 8 Verifique na página Formato do Disco se existe espaço suficiente para implantar o appliance virtual e clique em **Avançar**.
- 9 Siga os prompts até a página Propriedades.  
As opções que são exibidas dependem da configuração do vSphere.
- 10 Configure os valores na página Propriedades.
  - a Insira a senha raiz a ser usada quando você faz login no console do appliance virtual nas caixas de texto **Inserir senha** e **Confirmar senha**.
  - b Marque ou desmarque a caixa de seleção **Serviço SSH** para escolher se o serviço SSH será ativado para o appliance.  
  
Esse valor é utilizado para definir o status inicial do serviço SSH no appliance. Se você estiver instalando com o Assistente de Instalação, habilite isso antes de iniciar o assistente. É possível alterar essa configuração a partir do console de gerenciamento do appliance após a instalação.
  - c Insira o nome de domínio completo da máquina virtual na caixa de texto **Nome do host**.
  - d Configure as propriedades de rede.
- 11 Clique em **Avançar**.
- 12 Dependendo da sua implantação, do vCenter e da configuração de DNS, selecione uma das seguintes maneiras de finalizar a implantação do OVA e ligar o vRealize Automation 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, clique em **Fechar**.
    - c Aguarde até que a máquina 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, clique em **Fechar**.
    - b Ligue o vRealize Automation appliance.
    - c Aguarde até que a máquina seja iniciada, o que pode demorar até 5 minutos.
    - d Verifique se você pode efetuar o ping do DNS para o vRealize Automation appliance. Se você não puder executar um ping do DNS, reinicie a máquina virtual.
    - e Aguarde até que a máquina seja iniciada, o que pode demorar até 5 minutos.
  - Se você tiver implantado o vRealize Automation appliance 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 vRealize Automation appliance.
    - b Clique com o botão direito do mouse no vRealize Automation appliance 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 vRealize Automation appliance.
  - f Aguarde até que a máquina seja iniciada, o que pode demorar até 5 minutos.
- 13 Abra um prompt de comando e execute ping no FQDN para verificar se o nome de domínio totalmente qualificado pode ser resolvido em relação ao endereço IP do vRealize Automation appliance.

## Usando o assistente de instalação para implantações mínimas

### Executar o assistente de instalação para uma implantação mínima

Instale uma implantação mínima para verificação de conceito. O assistente de instalação mínima assume que você está instalando todos os componentes do IaaS em uma única máquina Windows.

Implantações mínimas normalmente oferecem suporte a um único vRealize Automation appliance e um servidor IaaS e usam um agente do vSphere para oferecer suporte a endpoints.

#### Pré-requisitos

- Verifique se você atendeu aos pré-requisitos descritos em [Capítulo 2, “Preparando para a instalação do vRealize Automation”](#), na página 19
- [“Implantar o appliance do vRealize Automation”](#), na página 68

#### Procedimentos

- 1 Abra um navegador da Web.
- 2 Navegue até o console de gerenciamento do vRealize Automation appliance usando o respectivo nome de domínio totalmente qualificado, <https://vra-va-nomedohost.domínio.nome:5480>.
- 3 Faça login usando o nome de usuário **root** e a senha que você especificou quando o appliance foi implantado.
- 4 Quando o assistente de instalação aparecer, clique em **Avançar**.
- 5 Aceite o Contrato de Licença de Usuário Final e clique em **Avançar**.
- 6 Selecione **Implantação mínima** e **Instalar a infraestrutura como serviço** na tela Tipo de implantação e clique em **Avançar**.
- 7 Verifique se os pré-requisitos listados na página Pré-requisitos de instalação foram atendidos e se o servidor Windows no qual você instalou o Agente de Gerenciamento está listado.
- 8 Se necessário, você pode alterar o método de controle de horário para o appliance do vRealize Automation. Clique em **Alterar Configurações de Horário**, se fizer alterações.
- 9 Clique em **Avançar**.
- 10 Clique em **Executar** na tela Executar o Verificador de Pré-requisitos para verificar se o servidor Windows na implantação mínima está configurado corretamente para o uso do vRealize Automation.

Como essa etapa é executada remotamente, pode levar vários minutos para que ela seja executada.

- a Se um status com falha for retornado para uma máquina, clique em **Corrigir** para iniciar correções automáticas ou clique em **Mostrar detalhes** e siga as instruções.

A opção **Corrigir** aplica correções e reinicia o servidor Windows IaaS.

- b Clique em **Executar** para executar novamente o verificador.
- c Quando todos os status mostrarem "sucesso", clique em **Avançar**.

- 11 Prossiga para as próximas telas, fornecendo as informações solicitadas para configurar os componentes da implantação, incluindo o Servidor Web, o Manager Service, Distributed Execution Manager, o agente de proxy do vSphere e informações do certificado.

Informações adicionais estão disponíveis nos botões Ajuda.

#### Próximo passo

[“Criar snapshots antes de iniciar a instalação”](#), na página 40

## Instalando o Agente de gerenciamento

É preciso instalar um agente de gerenciamento em cada máquina Windows que hospeda componentes do IaaS.

Para instalações corporativas, o agente de gerenciamento não é necessário para o host MS SQL.

Se ocorrer falha no appliance principal do vRealize Automation, será preciso reinstalar os agentes de gerenciamento.

Os agentes de gerenciamento não são automaticamente excluídos quando você desinstala um componente do IaaS. Desinstale o Agente de Gerenciamento da mesma forma que você desinstalaria qualquer programa do Windows com a ferramenta Adicionar ou remover programas.

#### Procedimentos

- 1 [Localizar a Impressão digital de certificado SSL para o Serviço de site de gerenciamento](#) na página 36  
Ao instalar um agente de gerenciamento, você deve validar a impressão digital do certificado SSL do serviço de Site de Gerenciamento.
- 2 [Baixar e instalar um agente de gerenciamento](#) na página 37  
Um administrador baixa e instala um Agente de Gerenciamento na máquina IaaS da sua implantação. O Agente de Gerenciamento deve ser instalado no servidor IaaS, mas não precisará ser instalado no servidor de banco de dados SQL se este for separado.

### Localizar a Impressão digital de certificado SSL para o Serviço de site de gerenciamento

Ao instalar um agente de gerenciamento, você deve validar a impressão digital do certificado SSL do serviço de Site de Gerenciamento.

É possível obter a impressão digital no prompt de comando do vRealize Automation appliance.

#### Procedimentos

- 1 Faça login no console do vRealize Automation appliance como root.
- 2 Insira o seguinte comando:  

```
openssl x509 -in /opt/vmware/etc/lighttpd/server.pem -fingerprint -noout -sha1
```

  
A impressão digital SHA1 é exibida. Por exemplo:  

```
SHA1 Fingerprint=E4:F0:37:9A:32:52:FA:7D:2E:91:BD:12:7A:2F:A3:75:F8:A1:7B:C4
```
- 3 Copie o UID da impressão digital. Para validação, talvez você precise remover os dois pontos.

#### Próximo passo

Mantenha a impressão digital que você copiou para uso com o instalador do Agente de Gerenciamento.

## Baixar e instalar um agente de gerenciamento

Um administrador baixa e instala um Agente de Gerenciamento na máquina IaaS da sua implantação. O Agente de Gerenciamento deve ser instalado no servidor IaaS, mas não precisará ser instalado no servidor de banco de dados SQL se este for separado.

O Agente de Gerenciamento registra o nó IaaS no vRealize Automation appliance, automatiza a instalação e o gerenciamento de componentes IaaS e coleta informações de telemetria e suporte. O agente de gerenciamento é executado como serviço do Windows em sua máquina IaaS, e você deve ter direitos de administrador local para instalar o agente.

### Pré-requisitos

- Faça uma cópia temporária da impressão digital do certificado do vRealize Automation appliance, conforme descrito em [“Localizar a Impressão digital de certificado SSL para o Serviço de site de gerenciamento”](#), na página 36.
- Verifique se o usuário da conta de serviço é uma conta de domínio com privilégios de administrador no servidor Windows IaaS.

### Procedimentos

- 1 Abra o vRealize Automation appliance especificando um endereço da seguinte forma em um navegador da Web, em que *vra-va-hostname.domain.name* é o nome de domínio totalmente qualificado do vRealize Automation appliance. Não use um endereço de balanceador de carga.  
  
`https://vrealize-automation-appliance-FQDN:5480/installer`
- 2 Clique no **instalador do agente de gerenciamento** para baixar o instalador.
- 3 Execute o instalador do Agente de gerenciamento, vCAC-IaaSManagementAgent-Setup.msi.  
O local de instalação padrão é %Program Files(x86)%\VMware\vCAC\Management Agent\
- 4 Clique em **Avançar** na página Bem-vindo.
- 5 Aceite o EULA e clique em **Avançar**.
- 6 Forneça um caminho de instalação alternativo ou aceite o valor padrão.
- 7 Clique em **Avançar**.
- 8 Digite os detalhes do Serviço de site de gerenciamento nos seguintes campos. e clique em **Avançar**.

Caixa de texto	Entrada
Endereço de appliance do vRA	<code>https://vrealize-automation-appliance-FQDN:5480</code> Você deve especificar o número da porta.
Nome de usuário raiz	O usuário raiz do vRealize Automation appliance.
Senha	A senha de usuário raiz do vRealize Automation appliance.

Caixa de texto	Entrada
<b>Certificado de servidor do Site de gerenciamento</b>	A impressão digital SHA1 do certificado de serviço do Site de gerenciamento. O Serviço do site de gerenciamento é hospedado no vRealize Automation appliance. Exemplo de impressão digital SHA1: DFF5FA0886DA2920D227ADF8BC9CDE4EF13EEF78.
<b>Carregar</b>	Clique em <b>Carregar</b> para carregar uma impressão digital padrão.

**VMware vRealize Automation Management Agent Setup**

**Management Site Service**

Specify the VA host for the Management Site Service to use for the agent.

vRA appliance address:  
  
 Specify the scheme and the port (hosted by default on 5480). Example: https://va-address:5...

Root username:  Password:

Provide vRealize Automation appliance root user credentials

Management Site Service certificate SHA1 fingerprint:

☒ I confirm the fingerprint matches the Management Site Service SSL certificate

- 9 Marque a caixa de seleção **Confirmação de correspondência de impressão digital** após confirmar que a impressão digital exibida corresponde à impressão digital do certificado SSL do Site de gerenciamento.  
Se as impressões digitais não corresponderem, confirme se o endereço na caixa de texto **Endereço de appliance do vRA** está correto.
- 10 Clique em **Avançar**.
- 11 Insira o nome do usuário e a senha da conta de serviço.
- 12 Clique em **Avançar**.
- 13 Clique em **Instalar**.
- 14 Clique em **Concluir**.
- 15 Repita essas etapas para cada host de IaaS do Windows.

Depois de instalar o agente de gerenciamento, o servidor do Windows estará listado na página Pré-requisitos de instalação do assistente de instalação.

## Sincronizar horários dos servidores

Os relógios nos servidores do vRealize Automation e nos servidores Windows devem estar sincronizados para garantir uma instalação bem-sucedida.

As opções na página Pré-requisitos do assistente de instalação permitem que você selecione um método de sincronização de horário para os appliances virtuais. A tabela de host do IaaS informa a você as variações de horário.

### Procedimentos

- 1 Selecione uma opção no menu **Modo de Sincronização de Horário**.

Opção	Ação
<b>Usar Servidor de Horário</b>	Selecione <b>Usar Servidor de Horário</b> no menu <b>Modo de Sincronização de Horário</b> para usar o protocolo NTP. Para cada servidor de horário que você estiver usando, insira o endereço IP ou o nome de host na caixa de texto <b>Servidor de horário</b> .
<b>Usar Horário do Host</b>	Selecione <b>Usar Horário do Host</b> no menu <b>Modo de Sincronização de Horário</b> para usar a sincronização de horário do VMware Tools. Você deve configurar as conexões com os servidores do protocolo NTP antes de usar a sincronização de tempo do VMware Tools.

- 2 Clique em **Alterar configurações de horário**.
- 3 Clique em **Avançar**.

### Próximo passo

Certifique-se de que os servidores do IaaS estejam configurados corretamente.

## Executar o verificador de pré-requisitos

Execute o verificador de pré-requisitos para verificar se o servidor Windows para componentes do IaaS está corretamente configurado.

### Procedimentos

- 1 Clique em **Executar** na tela Verificador de pré-requisito.  
À medida que as verificações são feitas, o servidor Windows para componentes do IaaS é listado com um status.
- 2 Se aparecer um aviso, você poderá obter mais informações sobre o erro ou optar por corrigir automaticamente o erro.
  - ◆ Clique em **Mostrar detalhes** para obter mais informações sobre o erro e a ação a ser seguida para solucioná-lo.
  - ◆ Clique em **Corrigir** para corrigir automaticamente o erro.  
A opção **Corrigir** aplica correções e reinicia o servidor Windows IaaS.
- 3 Clique em **Executar** para verificar as correções.
- 4 Clique em **Avançar** quando todos os erros forem resolvidos.

Seu servidor Windows está corretamente configurado para instalação de componentes do IaaS.

### Próximo passo

Prossiga para a tela Host do vRealize Automation.

## Especificar parâmetros mínimos de implantação

Use o Assistente de Instalação do vRealize Automation para inserir definições de configuração para os componentes mínimos de implantação.

### Pré-requisitos

#### Procedimentos

- ◆ Siga as páginas do Assistente de Instalação para inserir FQDNs de servidores Windows vRealize Automation appliance e IaaS, credenciais de conta, a senha do tenant padrão e outras configurações.

O assistente verifica sistemas em busca de pré-requisitos antes de você começar a inserir configurações e valida essas configurações antes de iniciar a instalação do produto.

### Próximo passo

No vSphere, crie um snapshot de cada servidor Windows vRealize Automation appliance e IaaS antes de iniciar a instalação do produto.

## Criar snapshots antes de iniciar a instalação

Tire snapshots de todos os seus appliances e Windows Servers. Se ocorrer falha na instalação, você poderá reverter para esses snapshots e tentar instalar de novo.

Os snapshots preservam seu trabalho de configuração. Certifique-se de incluir um snapshot do vRealize Automation appliance no em que você estiver executando o assistente.

São fornecidas instruções para os usuários do vSphere.

---

**OBSERVAÇÃO** Não saia do assistente de instalação nem cancele a instalação.

---

#### Procedimentos

- 1 Abra outro navegador e faça login no vSphere Client.
- 2 Localize seu servidor ou appliance no inventário do vSphere Client.
- 3 Clique com o botão direito do mouse no inventário do servidor e marque **Tirar snapshot**.
- 4 Insira um nome de snapshot.
- 5 Marque a caixa de seleção **Tirar snapshot da máquina virtual** para capturar memória do servidor e clique em **OK**.

O snapshot é criado.

Repita essas etapas para tirar snapshots de cada um dos servidores ou appliances.

### Próximo passo

[“Concluir a instalação”](#), na página 62

## Cenário: concluir a instalação

Como administrador do vSphere, você está na última parte do processo de instalação. Inicie a instalação do vRealize Automation e espere a instalação ser concluída com êxito.

#### Procedimentos

- 1 Volte ao assistente de instalação.
- 2 Veja o resumo da instalação e clique em **Avançar**.



- 3 Digite a chave de licença do produto e clique em **Avançar**.
- 4 Aceite ou altere as configurações padrão de telemetria e clique em **Avançar**.
- 5 Clique em **Avançar**.
- 6 Clique em **Concluir**.

A instalação é iniciada. A instalação pode levar de quinze minutos a uma hora, dependendo da configuração de rede.

É exibida uma mensagem de confirmação no momento que a instalação é concluída.

### Próximo passo

Agora você já pode configurar a implantação.

## Abordagem das falhas de instalação

Quando você instala a partir da página Detalhes da instalação, será informado de quaisquer problemas que estão impedindo o término da instalação.

Quando forem encontrados problemas, o componente é sinalizado e aparecem informações detalhadas sobre a falha, juntamente com as etapas para averiguar as soluções. Depois de ter abordado o problema, repita a etapa de instalação. Dependendo do tipo de falha, siga etapas de correção diferentes.

### Procedimentos

- 1 Se o botão **Falha ao tentar novamente** estiver habilitado, execute as seguintes etapas.
  - a Verifique a falha.
  - b Avalie o que precisa ser mudado e faça as mudanças necessárias.
  - c Volte para a tela Instalação e clique em **Falha ao tentar novamente**.  
O instalador tenta instalar todos os componentes que apresentaram falha.
- 2 Se o botão **Tentar novamente todo o IaaS** estiver habilitado, execute as seguintes etapas.
  - a Verifique a falha.
  - b Avalie o que precisa ser alterado.
  - c Reverta todos os servidores do IaaS para os snapshots criados anteriormente
  - d Exclua o banco de dados MS SQL se você estiver usando um banco de dados externo.
  - e Faça as alterações necessárias.
  - f Clique em **Tentar novamente todo o IaaS**.
- 3 Se a falha estiver nos componentes de virtual appliance, use as seguintes etapas.
  - a Verifique a falha.
  - b Avalie o que precisa ser alterado.
  - c Reverter todos os servidores para snapshots, incluindo aquele do qual você está executando o assistente.
  - d Faça as alterações necessárias.
  - e Atualize a página do assistente.
  - f Faça login e execute novamente o assistente.  
O assistente abre na etapa de pré-instalação.

## Configurar credenciais para a configuração de conteúdo inicial

Opcionalmente, você pode iniciar um fluxo de trabalho de conteúdo inicial para um endpoint do vSphere. O processo usa um usuário local chamado configurationadmin que tem direitos de administrador.

### Procedimentos

- 1 Crie e insira uma senha para a conta configurationadmin na caixa de texto **Senha**.
- 2 Insira novamente a senha na caixa de texto **Confirmar Senha**. Anote a senha para lembrar futuramente.
- 3 Clique em **Criar conteúdo inicial**.
- 4 Clique em **Avançar**.

Um usuário admin de configuração é criado e um item de catálogo de configuração é criado no tenant padrão. O admin de configuração tem os direitos a seguir:

- Administrador de aprovação
- Administrador do catálogo
- Administrador do IaaS
- Arquiteto de infraestrutura
- Administrador de tenant
- Arquiteto do XaaS

### Próximo passo

- Quando você concluir o assistente, poderá fazer login no tenant padrão como o usuário configurationadmin e solicitar os itens de catálogo de conteúdo inicial. Para obter um exemplo de como solicitar o item e concluir a ação manual do usuário, consulte *Instalando e configurando o vRealize Automation para o cenário do Rainpole*.
- Configurar o acesso ao tenant padrão para outros usuários. Consulte [“Configurar o acesso ao tenant padrão”](#), na página 125.

## 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 vRealize Automation appliance fazem com que haja falha na instalação. Apenas uma instância do servidor Web e um único vRealize Automation appliance devem estar ativos durante a instalação.

## Executar o assistente de instalação para uma implantação corporativa

As implantações corporativas são utilizadas para o ambiente 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 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.

### Pré-requisitos

- Verifique se você atendeu aos pré-requisitos descritos em [Capítulo 2, “Preparando para a instalação do vRealize Automation”](#), na página 19
- [“Implantar o appliance do vRealize Automation”](#), na página 68.

### Procedimentos

- 1 Abra o vRealize Automation appliance em um navegador da Web. Use o nome de domínio totalmente qualificado (FQDN).  
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Faça login como root e use a senha que você criou durante a implantação do OVA.  
No seu primeiro login, o Assistente de Instalação é exibido.
- 3 Aceite o Contrato de Licença de Usuário Final.
- 4 Na página Tipo de Implantação, selecione **Implantação corporativa** e **Instalar Infrastructure as a Service**.
- 5 Na página Instalação de Pré-requisitos, você pausa para fazer login em seus servidores Windows IaaS e instalar o Agente de Gerenciamento. O Agente de Gerenciamento permite que o assistente descubra servidores IaaS e se conecte a eles.

### Próximo passo

Consulte [“Instalando o Agente de gerenciamento”](#), na página 43.

## Instalando o Agente de gerenciamento

É preciso instalar um agente de gerenciamento em cada máquina Windows que hospeda componentes do IaaS.

Se ocorrer falha no appliance principal do vRealize Automation, será preciso reinstalar os agentes de gerenciamento.

Os agentes de gerenciamento não são automaticamente excluídos quando você desinstala um componente do IaaS. Desinstale o Agente de Gerenciamento da mesma forma que você desinstalaria qualquer programa do Windows com a ferramenta Adicionar ou remover programas.

### Localizar a Impressão digital de certificado SSL para o Serviço de site de gerenciamento

Ao instalar um agente de gerenciamento, você deve validar a impressão digital do certificado SSL do serviço de Site de Gerenciamento.

É possível obter a impressão digital no prompt de comando do vRealize Automation appliance.

## Procedimentos

- 1 Faça login no console do vRealize Automation appliance como root.
- 2 Insira o seguinte comando:  
  

```
openssl x509 -in /opt/vmware/etc/httpsd/server.pem -fingerprint -noout -sha1
```

É exibida a impressão digital SHA1. Por exemplo:

```
SHA1 Fingerprint=E4:F0:37:9A:32:52:FA:7D:2E:91:BD:12:7A:2F:A3:75:F8:A1:7B:C4
```
- 3 Copie o UID da impressão digital. Para validação, talvez você precise remover os dois pontos.

## Próximo passo

Mantenha a impressão digital que você copiou para uso com o instalador do Agente de Gerenciamento.

## Baixar e instalar um agente de gerenciamento

Um administrador baixa e instala um agente de gerenciamento em máquinas IaaS na sua implantação. O agente de gerenciamento deve ser instalado em todos os servidores IaaS, exceto naqueles usados exclusivamente para seu banco de dados MS SQL.

O agente de gerenciamento registra nós IaaS no vRealize Automation appliance, automatiza a instalação e o gerenciamento de componentes IaaS e coleta informações de telemetria e suporte. O agente de gerenciamento é executado como serviço do Windows em sua máquina IaaS, e você deve ter direitos de administrador local para instalar o agente.

## Pré-requisitos

- Faça uma cópia temporária da impressão digital do certificado do vRealize Automation appliance, conforme descrito em [“Localizar a Impressão digital de certificado SSL para o Serviço de site de gerenciamento”](#), na página 36.
- Verifique se o usuário da conta de serviço é uma conta de domínio com privilégios de administrador no servidor Windows IaaS.

## Procedimentos

- 1 Abra o vRealize Automation appliance especificando um endereço da seguinte forma em um navegador da Web, em que *vra-va-hostname.domain.name* é o nome de domínio totalmente qualificado do vRealize Automation appliance. Não use um endereço de balanceador de carga.  
  

```
https://vrealize-automation-appliance-FQDN:5480/installer
```
- 2 Clique no **instalador do agente de gerenciamento** para baixar o instalador.
- 3 Execute o instalador do Agente de gerenciamento, vCAC-IaaSManagementAgent-Setup.msi.  
O local de instalação padrão é *%Program Files(x86)%\VMware\ vCAC\Management Agent\*
- 4 Clique em **Avançar** na página Bem-vindo.
- 5 Aceite o EULA e clique em **Avançar**.
- 6 Forneça um caminho de instalação alternativo ou aceite o valor padrão.
- 7 Clique em **Avançar**.
- 8 Digite os detalhes do Serviço de site de gerenciamento nos seguintes campos. e clique em **Avançar**.

Caixa de texto	Entrada
Endereço de appliance do vRA	<b>https://vrealize-automation-appliance-FQDN:5480</b> Você deve especificar o número da porta.
Nome de usuário raiz	O usuário raiz do vRealize Automation appliance.

Caixa de texto	Entrada
<b>Senha</b>	A senha de usuário raiz do vRealize Automation appliance.
<b>Certificado de servidor do Site de gerenciamento</b>	A impressão digital SHA1 do certificado de serviço do Site de gerenciamento. O Serviço do site de gerenciamento é hospedado no vRealize Automation appliance. Exemplo de impressão digital SHA1: DFF5FA0886DA2920D227ADF8BC9CDE4EF13EEF78.
<b>Carregar</b>	Clique em <b>Carregar</b> para carregar uma impressão digital padrão.

**VMware vRealize Automation Management Agent Setup**

**Management Site Service**

Specify the VA host for the Management Site Service to use for the agent.

vRA appliance address:  
  
 Specify the scheme and the port (hosted by default on 5480). Example: https://va-address:5...

Root username:  Password:

Provide vRealize Automation appliance root user credentials

Management Site Service certificate SHA1 fingerprint:

☒ I confirm the fingerprint matches the Management Site Service SSL certificate

- 9 Marque a caixa de seleção **Confirmação de correspondência de impressão digital** após confirmar que a impressão digital exibida corresponde à impressão digital do certificado SSL do Site de gerenciamento.  
Se as impressões digitais não corresponderem, confirme se o endereço na caixa de texto **Endereço de appliance do vRA** está correto.
- 10 Clique em **Avançar**.
- 11 Insira o nome do usuário e a senha da conta de serviço.
- 12 Clique em **Avançar**.
- 13 Clique em **Instalar**.
- 14 Clique em **Concluir**.
- 15 Repita essas etapas para cada host de IaaS do Windows.

Depois de instalar o agente de gerenciamento, o servidor do Windows estará listado na página Pré-requisitos de instalação do assistente de instalação.

## Sincronizar horários dos servidores

Os relógios nos servidores do vRealize Automation e nos servidores Windows devem estar sincronizados para garantir uma instalação bem-sucedida.

As opções na página Pré-requisitos do assistente de instalação permitem que você selecione um método de sincronização de horário para os appliances virtuais. A tabela de host do IaaS informa a você as variações de horário.

### Procedimentos

- 1 Selecione uma opção no menu **Modo de Sincronização de Horário**.

Opção	Ação
<b>Usar Servidor de Horário</b>	Selecione <b>Usar Servidor de Horário</b> no menu <b>Modo de Sincronização de Horário</b> para usar o protocolo NTP. Para cada servidor de horário que você estiver usando, insira o endereço IP ou o nome de host na caixa de texto <b>Servidor de horário</b> .
<b>Usar Horário do Host</b>	Selecione <b>Usar Horário do Host</b> no menu <b>Modo de Sincronização de Horário</b> para usar a sincronização de horário do VMware Tools. Você deve configurar as conexões com os servidores do protocolo NTP antes de usar a sincronização de tempo do VMware Tools.

- 2 Clique em **Alterar configurações de horário**.
- 3 Clique em **Avançar**.

### Próximo passo

Certifique-se de que os servidores do IaaS estejam configurados corretamente.

## Executar o verificador de pré-requisitos

Execute o verificador de pré-requisitos para saber se os Windows Servers para componentes do IaaS estão configurados corretamente.

### Procedimentos

- 1 Clique em **Executar** na tela Verificador de pré-requisito.  
Assim que as verificações forem feitas, cada Windows Server para componentes do IaaS será listado com um status.
- 2 Se aparecer um aviso, você poderá obter mais informações sobre o erro ou optar por corrigir automaticamente o erro.
  - ◆ Clique em **Mostrar detalhes** para obter mais informações sobre o erro e a ação a ser seguida para solucioná-lo.
  - ◆ Clique em **Corrigir** para corrigir automaticamente o erro.  
A opção **Corrigir** aplica correções e reinicia todas as máquinas IaaS, incluindo aquelas que podem não ter sofrido correções.
- 3 Clique em **Executar** para verificar as correções.
- 4 Clique em **Avançar** quando todos os erros forem resolvidos.

Seus servidores Windows estão corretamente configurados para instalação dos componentes do IaaS.

### Próximo passo

Prossiga para a tela Host do vRealize Automation.

## Especificar parâmetros de implantação corporativa

Use o Assistente de Instalação do vRealize Automation para inserir definições de configuração para os componentes da implantação corporativa.

### Pré-requisitos

#### Procedimentos

- ◆ Siga as páginas do Assistente de Instalação para inserir FQDNs de servidores Windows vRealize Automation appliance e IaaS, credenciais de conta, a senha do tenant padrão e outras configurações.

O assistente verifica sistemas em busca de pré-requisitos antes de você começar a inserir configurações e valida essas configurações antes de iniciar a instalação do produto.

### Próximo passo

No vSphere, crie um snapshot de cada servidor Windows vRealize Automation appliance e IaaS antes de iniciar a instalação do produto.

## Criar snapshots antes de iniciar a instalação

Tire snapshots de todos os seus appliances e Windows Servers. Se ocorrer falha na instalação, você poderá reverter para esses snapshots e tentar instalar de novo.

Os snapshots preservam seu trabalho de configuração. Certifique-se de incluir um snapshot do vRealize Automation appliance no em que você estiver executando o assistente.

São fornecidas instruções para os usuários do vSphere.

---

**OBSERVAÇÃO** Não saia do assistente de instalação nem cancele a instalação.

---

#### Procedimentos

- 1 Abra outro navegador e faça login no vSphere Client.
- 2 Localize seu servidor ou appliance no inventário do vSphere Client.
- 3 Clique com o botão direito do mouse no inventário do servidor e marque **Tirar snapshot**.
- 4 Insira um nome de snapshot.
- 5 Marque a caixa de seleção **Tirar snapshot da máquina virtual** para capturar memória do servidor e clique em **OK**.

O snapshot é criado.

Repita essas etapas para tirar snapshots de cada um dos servidores ou appliances.

### Próximo passo

[“Concluir a instalação”](#), na página 62

## Concluir a instalação

Após a criação dos snapshots, inicie a instalação do vRealize Automation e espere a instalação ser concluída com êxito.

#### Procedimentos

- 1 Volte ao assistente de instalação.
- 2 Veja o resumo da instalação e clique em **Avançar**.

- 3 Clique em **Avançar**.
- 4 Clique em **Concluir**.

A instalação é iniciada. A instalação pode levar de quinze minutos a uma hora, dependendo da configuração de rede.

É exibida uma mensagem de confirmação no momento que a instalação é concluída.

### Próximo passo

Agora você já pode configurar a implantação.

## Abordagem das falhas de instalação

Quando você instala a partir da página Detalhes da instalação, será informado de quaisquer problemas que estão impedindo o término da instalação.

Quando forem encontrados problemas, o componente é sinalizado e aparecem informações detalhadas sobre a falha, juntamente com as etapas para averiguar as soluções. Depois de ter abordado o problema, repita a etapa de instalação. Dependendo do tipo de falha, siga etapas de correção diferentes.

### Procedimentos

- 1 Se o botão **Falha ao tentar novamente** estiver habilitado, execute as seguintes etapas.
  - a Verifique a falha.
  - b Avalie o que precisa ser mudado e faça as mudanças necessárias.
  - c Volte para a tela Instalação e clique em **Falha ao tentar novamente**.

O instalador tenta instalar todos os componentes que apresentaram falha.
- 2 Se o botão **Tentar novamente todo o IaaS** estiver habilitado, execute as seguintes etapas.
  - a Verifique a falha.
  - b Avalie o que precisa ser alterado.
  - c Reverta todos os servidores do IaaS para os snapshots criados anteriormente
  - d Exclua o banco de dados MS SQL se você estiver usando um banco de dados externo.
  - e Faça as alterações necessárias.
  - f Clique em **Tentar novamente todo o IaaS**.
- 3 Se a falha estiver nos componentes de virtual appliance, use as seguintes etapas.
  - a Verifique a falha.
  - b Avalie o que precisa ser alterado.
  - c Reverter todos os servidores para snapshots, incluindo aquele do qual você está executando o assistente.
  - d Faça as alterações necessárias.
  - e Atualize a página do assistente.
  - f Faça login e execute novamente o assistente.

O assistente abre na etapa de pré-instalação.



## Configurar credenciais para a configuração de conteúdo inicial

Opcionalmente, você pode iniciar um fluxo de trabalho de conteúdo inicial para um endpoint do vSphere.

O processo usa um usuário local chamado configurationadmin que tem direitos de administrador.

### Procedimentos

- 1 Crie e insira uma senha para a conta configurationadmin na caixa de texto **Senha**.
- 2 Insira novamente a senha na caixa de texto **Confirmar Senha**. Anote a senha para lembrar futuramente.
- 3 Clique em **Criar conteúdo inicial**.
- 4 Clique em **Avançar**.

Um usuário admin de configuração é criado e um item de catálogo de configuração é criado no tenant padrão. O admin de configuração tem os direitos a seguir:

- Administrador de aprovação
- Administrador do catálogo
- Administrador do IaaS
- Arquiteto de infraestrutura
- Administrador de tenant
- Arquiteto do XaaS

### Próximo passo

- Quando você concluir o assistente, poderá fazer login no tenant padrão como o usuário configurationadmin e solicitar os itens de catálogo de conteúdo inicial. Para obter um exemplo de como solicitar o item e concluir a ação manual do usuário, consulte *Instalando e configurando o vRealize Automation para o cenário do Rainpole*.
- Configurar o acesso ao tenant padrão para outros usuários. Consulte [“Configurar o acesso ao tenant padrão”](#), na página 125.



# As interfaces de instalação padrão do vRealize Automation

---

# 4

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 3, “Instalando o vRealize Automation com o assistente de instalação”](#), na página 33 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 por algum motivo.
- Você deseja adicionar outro vRealize Automation appliance 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”](#), na página 51
- [“Usando as interfaces padrão para implantações distribuídas”](#), na página 63
- [“Instalando agentes do vRealize Automation”](#), na página 101

## 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

Um administrador pode implantar um vRealize Automation completo em uma configuração mínima. Implantações mínimas são normalmente usadas em um ambiente de desenvolvimento ou como evidência de conceito e precisam de poucas etapas para ser instaladas.

A Lista de verificação da implantação mínima fornece uma visão geral de alto nível da sequência de tarefas que deve realizar para completar a instalação mínima.

Imprima uma cópia da lista de verificação e use-a para rastrear seu trabalho conforme conclui a instalação. Conclua as tarefas na ordem em que são dadas.

**Tabela 4-1.** Lista de verificação da implantação mínima

Tarefa	Detalhes
<input type="checkbox"/> Planeje e prepare o ambiente de instalação e verifique se todos os pré-requisitos de instalação foram atendidos.	<a href="#">Capítulo 2, “Preparando para a instalação do vRealize Automation”, na página 19</a>
<input type="checkbox"/> Configure o vRealize Automation appliance	<a href="#">“Implantar e configurar o appliance do vRealize Automation”, na página 52</a>
<input type="checkbox"/> Instale os componentes do IaaS em um único servidor do Windows.	<a href="#">“Instalando componentes do IaaS”, na página 57</a>
<input type="checkbox"/> Instale agentes adicionais, se necessário.	<a href="#">“Instalando agentes do vRealize Automation”, na página 101</a>
<input type="checkbox"/> Realize as tarefas pós-instalação como a configuração do tenant padrão.	

## Implantar e configurar o appliance do vRealize Automation

O vRealize Automation appliance é um appliance virtual pré-configurado que implanta o servidor e o console da Web (o portal do usuário) do vRealize Automation appliance. Ele é fornecido como um modelo de formato de virtualização aberto (OVF). O administrador de sistema baixa o appliance e implanta-o no inventário do vCenter Server ou do ESX/ESXi.

- 1 [Implantar o appliance do vRealize Automation](#) na página 52  
Para implantar o vRealize Automation appliance, um administrador de sistema deve fazer login no cliente do vSphere e selecionar as configurações de implantação.
- 2 [Ativar a sincronização data/hora no appliance do vRealize Automation](#) na página 54  
Os relógios no servidor do vRealize Automation e no servidor Windows devem estar sincronizados para garantir uma instalação bem-sucedida.
- 3 [Configurar o appliance do vRealize Automation](#) na página 55  
Para preparar o vRealize Automation appliance para uso, o administrador do sistema define as configurações de host, gera um certificado SSL e fornece informações de conexão SSO.

### Implantar o appliance do vRealize Automation

Para implantar o vRealize Automation appliance, um administrador de sistema deve fazer login no cliente do vSphere e selecionar as configurações de implantação.

Algumas restrições se aplicam à senha raiz criada para o administrador do vRealize Automation.

#### Pré-requisitos

- Faça download do vRealize Automation appliance no site da VMware.
- Faça login no cliente do vSphere como usuário com privilégios de administrador de sistema.

## Procedimentos

- 1 Selecione **Arquivo > Implantar Modelo OVF** no cliente do vSphere.
- 2 Navegue até o arquivo do vRealize Automation appliance que você fez download e clique em **Abrir**.
- 3 Clique em **Avançar**.
- 4 Clique em **Avançar** na página Detalhes do Modelo OVF.
- 5 Aceite o contrato de licença e clique em **Avançar**.
- 6 Insira um nome exclusivo de appliance virtual, de acordo com a convenção de nomenclatura de TI da sua organização, na caixa de texto **Nome**, selecione o centro de dados e o local no qual você deseja implantar o appliance virtual e clique em **Avançar**.
- 7 Siga os prompts até que a página Formato do Disco seja exibida.
- 8 Verifique na página Formato do Disco se existe espaço suficiente para implantar o appliance virtual e clique em **Avançar**.
- 9 Siga os prompts até a página Propriedades.  
As opções que são exibidas dependem da configuração do vSphere.
- 10 Configure os valores na página Propriedades.
  - a Insira a senha raiz a ser usada quando você faz login no console do appliance virtual nas caixas de texto **Inserir senha** e **Confirmar senha**.
  - b Marque ou desmarque a caixa de seleção **Serviço SSH** para escolher se o serviço SSH será ativado para o appliance.  
  
Esse valor é utilizado para definir o status inicial do serviço SSH no appliance. Se você estiver instalando com o Assistente de Instalação, habilite isso antes de iniciar o assistente. É possível alterar essa configuração a partir do console de gerenciamento do appliance após a instalação.
  - c Insira o nome de domínio completo da máquina virtual na caixa de texto **Nome do host**.
  - d Configure as propriedades de rede.
- 11 Clique em **Avançar**.
- 12 Dependendo da sua implantação, do vCenter e da configuração de DNS, selecione uma das seguintes maneiras de finalizar a implantação do OVA e ligar o vRealize Automation 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, clique em **Fechar**.
    - c Aguarde até que a máquina 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, clique em **Fechar**.
    - b Ligue o vRealize Automation appliance.
    - c Aguarde até que a máquina seja iniciada, o que pode demorar até 5 minutos.
    - d Verifique se você pode efetuar o ping do DNS para o vRealize Automation appliance. Se você não puder executar um ping do DNS, reinicie a máquina virtual.

- e Aguarde até que a máquina seja iniciada, o que pode demorar até 5 minutos.
- Se você tiver implantado o vRealize Automation appliance 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 vRealize Automation appliance.
  - b Clique com o botão direito do mouse no vRealize Automation appliance 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 vRealize Automation appliance.
  - f Aguarde até que a máquina seja iniciada, o que pode demorar até 5 minutos.
- 13 Abra um prompt de comando e execute ping no FQDN para verificar se o nome de domínio totalmente qualificado pode ser resolvido em relação ao endereço IP do vRealize Automation appliance.

## Ativar a sincronização data/hora no appliance do vRealize Automation

Os relógios no servidor do vRealize Automation e no servidor Windows devem estar sincronizados para garantir uma instalação bem-sucedida.

Se você vir avisos de certificado durante esse processo, ignore-os para concluir a instalação.

### Pré-requisitos

“Implantar o appliance do vRealize Automation”, na página 33.

### Procedimentos

- 1 Navegue até o console de gerenciamento do vRealize Automation appliance usando o respectivo nome de domínio totalmente qualificado, <https://vra-va-nomedohost.dominio.nome:5480>.
- 2 Faça login usando o nome de usuário **root** e a senha que você especificou quando o appliance foi implantado.
- 3 Selecione **Administração > Configurações de Horário**.
- 4 Selecione uma opção no menu **Modo de Sincronização de Horário**.

Opção	Ação
<b>Usar Servidor de Horário</b>	Selecione <b>Usar Servidor de Horário</b> no menu <b>Modo de Sincronização de Horário</b> para usar o protocolo NTP. Para cada servidor de horário que você estiver usando, insira o endereço IP ou o nome de host na caixa de texto <b>Servidor de horário</b> .
<b>Usar Horário do Host</b>	Selecione <b>Usar Horário do Host</b> no menu <b>Modo de Sincronização de Horário</b> para usar a sincronização de horário do VMware Tools. Você deve configurar as conexões com os servidores do protocolo NTP antes de usar a sincronização de tempo do VMware Tools.

- 5 Clique em **Salvar Configurações**.
- 6 Clique em **Atualizar**.
- 7 Verifique se o valor em **Horário Atual** está correto.

Você pode alterar o fuso horário conforme necessário na página Configurações de Fuso Horário na guia **Sistema**.

- 8 (Opcional) Clique em **Fuso Horário** na guia **Sistema** e selecione um fuso horário do sistema nas opções do menu.  
O padrão é Etc/UTC.
- 9 Clique em **Salvar Configurações**.

## Configurar o appliance do vRealize Automation

Para preparar o vRealize Automation appliance para uso, o administrador do sistema define as configurações de host, gera um certificado SSL e fornece informações de conexão SSO.

### Pré-requisitos

“[Ativar a sincronização data/hora no appliance do vRealize Automation](#)”, na página 54.

### Procedimentos

- 1 Navegue até o console de gerenciamento do vRealize Automation appliance usando o respectivo nome de domínio totalmente qualificado, `https://vra-va-nomedohost.dominio.nome:5480`.
- 2 Ignore o aviso de certificado para continuar.
- 3 Faça login com a raiz do nome de usuário e a senha que você especificou ao implantar o vRealize Automation appliance.
- 4 Selecione **Configurações do vRA > Configurações do Host**.

Opção	Ação
<b>Solucionar automaticamente</b>	Selecione <b>Solucionar Automaticamente</b> para especificar o nome do host atual do vRealize Automation appliance.
<b>Atualizar host</b>	<p>Para novos hosts, selecione <b>Atualizar Host</b>. Insira o nome de domínio totalmente qualificado do vRealize Automation appliance, <code>vra-hostname.domain.name</code> na caixa de texto <b>Nome do Host</b>.</p> <p>Para implantações distribuídas que usam balanceadores de carga, selecione <b>Atualizar Host</b>. Insira o nome de domínio totalmente qualificado do servidor do balanceador de carga, <code>vra-loadbalancername.domain.name</code> na caixa de texto <b>Nome do Host</b>.</p>

**OBSERVAÇÃO** Defina configurações de SSO conforme descrito mais adiante neste procedimento sempre que você usar **Atualizar Host** para definir o nome do host.

5 Selecione o tipo de certificado no menu **Ação de Certificado**.

Se você estiver usando um certificado codificado por PEM, por exemplo, para um ambiente distribuído, selecione **Importar**.

Os certificados que você importa devem ser confiáveis e também aplicáveis a todas as instâncias do vRealize Automation appliance e todos os balanceadores de carga por meio do uso de certificados de Nome Alternativo da Entidade (SAN).

**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
<b>Manter Existentes</b>	Mantenha a configuração SSL atual. Selecione essa opção para cancelar as alterações.
<b>Gerar Certificado</b>	<ul style="list-style-type: none"> <li>a O valor exibido na caixa de texto <b>Nome comum</b> é o Nome de host, conforme ele é exibido na parte superior da página. Se todas as instâncias adicionais do vRealize Automation appliance estiverem disponíveis, os respectivos FQDN serão incluídos no atributo SAN do certificado.</li> <li>b Insira o nome da organização, como o nome da sua empresa, na caixa de texto <b>Organização</b>.</li> <li>c Insira a unidade organizacional, como o nome ou o local do departamento, na caixa de texto <b>Unidade organizacional</b>.</li> <li>d Insira um código de país ISO 3166 de duas letras, como <b>PT_BR</b>, na caixa de texto <b>País</b>.</li> </ul>
<b>Importar</b>	<ul style="list-style-type: none"> <li>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 <b>Chave Privada RSA</b>.</li> <li>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 <b>Cadeia de Certificados</b>. Para vários valores de certificado, inclua um cabeçalho BEGIN CERTIFICATE e um rodapé END CERTIFICATE em cada certificado. <b>OBSERVAÇÃO</b> No caso dos certificados encadeados, atributos adicionais podem estar disponíveis.</li> <li>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 <b>Código de Acesso</b>.</li> </ul>

6 Clique em **Salvar Configurações** para salvar as informações do host e a configuração do SSL.

7 Defina as configurações do SSO.

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



- 9 Clique na guia **Telemetria** para escolher se deseja participar do Programa de Aperfeiçoamento da Experiência do Cliente (CEIP) da VMware.

Os detalhes sobre os dados recolhidos pelo CEIP e os fins para os quais eles são utilizados pelo VMware são estabelecidos pelo Centro de Confiança e Garantia, em

<http://www.vmware.com/trustvmware/ceip.html>.

- Selecione **Participe do Programa de Aperfeiçoamento da Experiência do Cliente da VMware** para participar do programa.
- Desmarque **Participe do Programa de Aperfeiçoamento da Experiência do Cliente da VMware** para não participar do programa.

- 10 Clique em **Serviços** e verifique se os serviços estão registrados.

Dependendo da configuração do seu site, isso pode demorar cerca de 10 minutos.

---

**OBSERVAÇÃO** Você pode fazer login no appliance e executar o `tail -f /var/log/vcac/catalina.out` para monitorar a inicialização dos serviços.

---

- 11 Insira as informações da sua licença.

- a Clique em **Configurações do vRA > Licenciamento**.
- b Clique em **Licenciamento**.
- c Insira uma chave de licença válida do vRealize Automation que você baixou com os arquivos de instalação e clique em **Enviar Chave**.

---

**OBSERVAÇÃO** Se houver um erro de conexão, você poderá ter um problema com o balanceador de carga. Verifique a conectividade de rede do balanceador de carga.

---

- 12 Confirme se você pode fazer login no console do vRealize Automation.

- a Abra um navegador e vá até `https://vcac-hostname.domain.name/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.

O console é aberto na página Tenants na guia **Administração**. Um único tenant nomeado `vsphere.local` aparece na lista.

Você terminou a implantação e configuração do seu vRealize Automation appliance. Se o appliance não funcionar corretamente após a configuração, replante-o e reconfigure-o. Não faça alterações no appliance existente.

### Próximo passo

[“Instalar os componentes de infraestrutura”](#), na página 58

## Instalando componentes do IaaS

O administrador instala um conjunto completo de componentes de infraestrutura (IaaS) em uma máquina Windows (física ou virtual). Os direitos de administrador são obrigatórios para a execução dessas tarefas.

A instalação mínima instala todos os componentes no mesmo servidor Windows, exceto o banco de dados SQL, que você pode instalar em um servidor separado.

## Ativar a sincronização de horário no servidor Windows

Os relógios no servidor do vRealize Automation e no servidor Windows devem estar sincronizados para garantir que a instalação seja bem-sucedida.

As etapas a seguir descrevem como ativar a sincronização de horário com o host ESX/ESXi usando o VMware Tools. Se você estiver instalando os componentes do IaaS em um host físico ou não desejar usar o VMware Tools para a sincronização de horário, verifique se o horário do servidor é preciso usando seu método preferido.

### Procedimentos

- 1 Abra um prompt de comando na máquina de instalação do Windows.

- 2 Digite o comando a seguir para navegar até o diretório do VMware Tools.

```
cd C:\Program Files\VMware\VMware Tools
```

- 3 Digite o comando para exibir o status da sincronização de horário.

```
VMwareToolboxCmd.exe timesync status
```

- 4 Se a sincronização de horário estiver desativada, digite o comando a seguir para ativá-la.

```
VMwareToolboxCmd.exe timesync enable
```

## Certificados do IaaS

Os componentes IaaS do vRealize Automation usam certificados e SSL para proteger as comunicações entre os componentes. Em uma instalação mínima para fins de prova de conceito, você pode usar certificados autoassinados.

Em um ambiente distribuído, obtenha um certificado de domínio de uma autoridade de certificação confiável. Para obter informações sobre como instalar certificados de domínio de componentes IaaS, consulte [“Instalar certificados do IaaS”](#), na página 79 no capítulo sobre implantação distribuída.

## Instalar os componentes de infraestrutura

O administrador de sistema faz login na máquina Windows e segue o assistente de instalação para instalar os componentes de infraestrutura (IaaS) na máquina Windows virtual ou física.

### Pré-requisitos

- Verifique se a sua máquina de instalação atende aos requisitos descritos em [“Requisitos de Servidor do Model Manager e do Serviço Web IaaS”](#), na página 22.
- [“Ativar a sincronização de horário no servidor Windows”](#), na página 58.
- Verifique se você implantou e configurou totalmente o vRealize Automation appliance e se os serviços necessários estão em execução (plugin-service, catalogue-service, iaas-proxy-provider).

### Procedimentos

- 1 [Baixar o Instalador IaaS do vRealize Automation](#) na página 59

Para instalar o IaaS no seu servidor Windows virtual ou físico mínimo, é necessário baixar uma cópia do instalador do IaaS a partir do vRealize Automation appliance.

- 2 [Selecionar o tipo de instalação](#) na página 59

O administrador do sistema executa o assistente de instalação na máquina de instalação do Windows 2008 ou 2012.

- 3 [Verificar pré-requisitos](#) na página 60

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](#) na página 60  
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](#) na página 61  
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](#) na página 62  
O administrador de sistema instala o certificado IaaS e registra os componentes IaaS com o SSO.
- 7 [Concluir a instalação](#) na página 62  
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 vRealize Automation appliance.

Se você vir avisos de certificado durante esse processo, ignore-os para concluir a instalação.

#### Pré-requisitos

- O Microsoft .NET Framework 4.5.2 ou posterior. Você pode baixar o instalador do .NET na mesma página da Web do instalador do IaaS.
- Se você estiver usando o Internet Explorer para fazer o download, verifique se a Configuração de Segurança Reforçada está ativada. Aponte o Internet Explorer para `res://iesetup.dll/SoftAdmin.htm` no servidor Windows.

#### Procedimentos

- 1 Usando uma conta com privilégios de administrador, faça login no servidor Windows.
- 2 Aponte um navegador da Web para a seguinte URL no vRealize Automation appliance.  
`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 com o vRealize Automation appliance.

### 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”](#), na página 79.

#### Procedimentos

- 1 Clique com o botão direito do mouse no arquivo de instalação `setup__vra-va-nomedohost.domínio.nome@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 vRealize Automation appliance 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 vRealize Automation appliance.
  - b Selecione **Aceitar Certificado**.
  - c Clique em **Exibir Certificado**.  
Compare a impressão digital do certificado com a impressão digital definida para o vRealize Automation appliance. Você pode exibir o certificado do vRealize Automation appliance no navegador do cliente quando o console de gerenciamento é acessado na porta 5480.
- 5 Selecione **Aceitar Certificado**.
- 6 Clique em **Avançar**.
- 7 Selecione **Instalação completa** na página Tipo de instalação se você estiver criando uma implantação mínima e clique em **Avançar**.

### Verificar pré-requisitos

O Verificador de Pré-requisitos verifica se a sua máquina atende aos requisitos de instalação do IaaS.

### Pré-requisitos

[“Selecionar o tipo de instalação”](#), na página 59.

### Procedimentos

- 1 Conclua o Verificador de Pré-requisitos.

Opção	Descrição
Nenhum erro	Clique em <b>Avançar</b> .
Erros não críticos	Clique em <b>Ignorar</b> .
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 <b>Verificar Novamente</b> para realizar a verificação.

- 2 Clique em **Avançar**.

A máquina atende aos requisitos de instalação.

### Especificar as configurações do servidor e da conta

O administrador do sistema do vRealize Automation especifica as configurações de servidor e de conta para o servidor de instalação do Windows e seleciona uma instância e o método de autenticação do servidor de banco de dados SQL.

### Pré-requisitos

[“Verificar pré-requisitos”](#), na página 60.

### 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 o [artigo 316898 da Base de Dados de Conhecimento da Microsoft](#).

- 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”](#), na página 60.

### 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”](#), na página 59.

#### Procedimentos

- 1 Aceite o valor padrão do **Servidor**, que é preenchido com o nome do domínio totalmente qualificado do servidor vRealize Automation appliance 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 vRealize Automation appliance.  
  
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”](#), na página 62.
- Verifique se a máquina em que você está fazendo a instalação está conectada à rede e é capaz de se conectar ao vRealize Automation appliance a partir do qual você faz download do instalador do IaaS.

#### Procedimentos

- 1 Revise as informações na página Pronto para instalação e clique em **Instalar**.  
  
A instalação é iniciada. A instalação pode levar de cinco minutos a uma hora, dependendo da configuração de rede.
- 2 Quando a mensagem de sucesso aparecer, deixe a caixa de seleção **Orientar-me pela configuração inicial** marcada e clique em **Avançar** e, depois, em **Concluir**.
- 3 Feche a caixa de mensagem **Configurar o sistema**.

Agora a instalação está concluída.

**Próximo passo**

“Verificar os serviços do IaaS”, na página 101.

## Usando as interfaces padrão para implantações distribuídas

Em uma implantação empresarial distribuída, o administrador do sistema instala componentes em várias máquinas no ambiente de implantação.

### 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 4-2.** 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”, na página 19
<input type="checkbox"/> Planejar e obter os seus certificados SSL.	“Requisitos de confiança de certificado em um ambiente distribuído”, na página 65
<input type="checkbox"/> Implantar o servidor do vRealize Automation appliance principal e todos os appliances adicionais que você exigir para obter redundância e alta disponibilidade.	“Implantar o appliance do vRealize Automation”, na página 68
<input type="checkbox"/> Configure o balanceador de carga para lidar com o tráfego do appliance do vRealize Automation.	“Configurar o balanceador de carga”, na página 70
<input type="checkbox"/> Configurar o servidor do vRealize Automation appliance principal e todos os appliances adicionais que você implantou para obter redundância e alta disponibilidade.	“Configurando dispositivos para ovRealize Automation”, na página 70
<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”, na página 77
<input type="checkbox"/> Se necessário, instalar os agentes para integração com sistemas externos.	“Instalando agentes do vRealize Automation”, na página 101
<input type="checkbox"/> Configurar o tenant padrão e fornecer a licença do IaaS.	“Configurar o acesso ao tenant padrão”, na página 125

### vRealize Orchestrator

O vRealize Automation appliance 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*.

## Componentes da instalação distribuída

Em uma instalação distribuída, o administrador de sistema implanta appliances virtuais e componentes relacionados para oferecer suporte ao ambiente de implementação.

**Tabela 4-3.** Appliances virtuais e banco de dados do appliance

Componente	Descrição
vRealize Automation appliance	Um appliance virtual pré-configurado que implanta o servidor do vRealize Automation. O servidor inclui o console do vRealize Automation, que fornece um portal único para o provisionamento de autoatendimento e o gerenciamento de serviços em nuvem, bem como a criação e a administração.
Banco de Dados do Appliance	Armazena as informações exigidas pelos appliances virtuais. A base de dados é incorporada em uma ou duas instâncias do vRealize Automation appliance.

Você pode selecionar os componentes individuais do IaaS que deseja instalar e especificar o local de instalação.

**Tabela 4-4.** Componentes do IaaS

Componente	Descrição
Website	Fornecer os recursos de administração de infraestrutura e de criação de serviços para o console do vRealize Automation. O componente Website comunica-se com o Model Manager, que fornece para ele atualizações do Distributed Execution Manager (DEM), dos agentes de proxy e do banco de dados.
Manager Service	O Manager Service coordena a comunicação entre os agentes, o banco de dados, o Active Directory e o SMTP. O Manager Service comunica-se com o site do console através do Model Manager. Esse serviço exige privilégios administrativos para ser executado.
Model Manager	O Model Manager comunica-se com o banco de dados, os DEMs e o site do portal. O Model Manager é dividido em dois componentes instaláveis separadamente: o serviço da Web do Model Manager e o componente de dados do Model Manager.
Distributed Execution Managers (Orchestrator e Worker)	Um Distributed Execution Manager (DEM) executa a lógica de negócios dos modelos personalizados, interagindo com o banco de dados do IaaS e com os bancos de dados externos. Os DEMs também gerenciar máquinas na nuvem e físicas.
Agentes	Os agentes de virtualização, integração e do WMI que comunicam-se com os recursos de infraestrutura.



## 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 vRealize Automation appliances 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 vRealize Automation appliance ou IaaS 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 vRealize Automation appliance e IaaS, você poderá reativar as verificações de integridade.

## Requisitos de confiança de certificado em um ambiente distribuído

Para uma comunicação segura, o vRealize Automation depende de certificados para criar relações de confiança entre os componentes.

A implementação específica dos certificados necessários para obter essa confiança depende do seu ambiente.

Para oferecer suporte a failover e alta disponibilidade, você pode implantar clusters de componentes com balanceamento de carga. Nesse caso, você obtém um certificado de vários usuários que inclui o componente da Web do IaaS no cluster e, depois, copia esse certificado de vários usuários para cada componente no cluster. É possível usar certificados de Nome Alternativo Para o Requerente (SAN), certificados curinga ou qualquer outro método de certificação multiuso apropriado para o ambiente, desde que as exigências de confiança sejam atendidas. Se você usar balanceadores de carga na sua implantação, deverá incluir o FQDN do balanceador de carga no endereço confiável do certificado multiuso do cluster.

Por exemplo, se você tiver uma configuração de balanceador de carga que requer um certificado no balanceador de carga e em seus componentes, você pode obter um certificado SAN para certificar web-load-balancer.eng.mycompany.com, web-component-1.eng.mycompany.com e web-component-2.eng.mycompany.com. Você teria que copiar esse único certificado de vários usuários para o balanceador de carga e cada um dos aplicativos e, depois, registrar o certificado nas máquinas de componente da Web.

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

**Tabela 4-5.** Requisitos de confiança de certificados

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

## 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

Você pode usar essas planilhas para registrar informações importantes para referência durante o processo de instalação.

São fornecidas aqui uma cópia de cada planilha. Crie cópias adicionais conforme você precisar delas. As configurações diferenciam maiúsculas de minúsculas.

**Tabela 4-6.** Informações do vRealize Automation appliance do cluster principal

Variável	Valor	Exemplo
Nome do host (FQDN)		vcac-va.mycompany.com
IP		192.168.1.105

**Tabela 4-6.** Informações do vRealize Automation appliance do cluster principal (Continuação)

Variável	Valor	Exemplo
Nome de usuário	administrator@vsphere.local (padrão)	administrator@vsphere.local
Senha		vmware

**Tabela 4-7.** Informações adicionais do vRealize Automation appliance

Variável	Valor	Exemplo
Nome do host (FQDN)		vcac-va2.mycompany.com
IP		192.168.1.110
Nome de usuário	administrator@vsphere.local (padrão)	administrator@vsphere.local
Senha		vmware

**Tabela 4-8.** Código de acesso do banco de dados do IaaS

Variável	Valor	Exemplo
Código de acesso (reutilizado no instalador, na atualização e na migração do IaaS)		myPassphrase

**Tabela 4-9.** Site do IaaS

Variável	Valor	Exemplo
Nome do host (FQDN)		iaas-web.mycompany.com
Porta de saída do serviço SSO sobre HTTPS (padrão)		
IP		192.168.1.106
Nome de usuário		
Senha		

**Tabela 4-10.** IaaS Model Manager Data

Variável	Valor	Exemplo
Nome do host (FQDN)		iaas-model-man.mycompany.com
Porta de saída do serviço SSO sobre HTTPS (padrão)		
IP		192.168.1.107
Nome de usuário		
Senha		

**Tabela 4-11.** IaaS Model Service

Variável	Valor	Exemplo
Nome do host (FQDN)		iaas-model-service.mycompany.com
Porta de saída do serviço SSO sobre HTTPS (padrão)		
IP		192.168.1.108
Nome de usuário		
Senha		

**Tabela 4-12.** Distributed Execution Managers

Nome exclusivo	Orchestrator/trabalhador
ex. myuniqueorchestratorname	Orchestrator: Trabalhador:
	Orchestrator: Trabalhador:
	Orchestrator: Trabalhador:
	Orchestrator: Trabalhador:

## Implantar o appliance do vRealize Automation

Para implantar o vRealize Automation appliance, um administrador de sistema deve fazer login no cliente do vSphere e selecionar as configurações de implantação.

Algumas restrições se aplicam à senha raiz criada para o administrador do vRealize Automation.

### Pré-requisitos

- Faça download do vRealize Automation appliance no site da VMware.
- Faça login no cliente do vSphere como usuário com privilégios de administrador de sistema.

### Procedimentos

- 1 Selecione **Arquivo > Implantar Modelo OVF** no cliente do vSphere.
- 2 Navegue até o arquivo do vRealize Automation appliance que você fez download e clique em **Abrir**.
- 3 Clique em **Avançar**.
- 4 Clique em **Avançar** na página Detalhes do Modelo OVF.
- 5 Aceite o contrato de licença e clique em **Avançar**.
- 6 Insira um nome exclusivo de appliance virtual, de acordo com a convenção de nomenclatura de TI da sua organização, na caixa de texto **Nome**, selecione o centro de dados e o local no qual você deseja implantar o appliance virtual e clique em **Avançar**.
- 7 Siga os prompts até que a página Formato do Disco seja exibida.
- 8 Verifique na página Formato do Disco se existe espaço suficiente para implantar o appliance virtual e clique em **Avançar**.
- 9 Siga os prompts até a página Propriedades.

As opções que são exibidas dependem da configuração do vSphere.

- 10 Configure os valores na página Propriedades.
  - a Insira a senha raiz a ser usada quando você faz login no console do appliance virtual nas caixas de texto **Inserir senha** e **Confirmar senha**.
  - b Marque ou desmarque a caixa de seleção **Serviço SSH** para escolher se o serviço SSH será ativado para o appliance.

Esse valor é utilizado para definir o status inicial do serviço SSH no appliance. Se você estiver instalando com o Assistente de Instalação, habilite isso antes de iniciar o assistente. É possível alterar essa configuração a partir do console de gerenciamento do appliance após a instalação.

- c Insira o nome de domínio completo da máquina virtual na caixa de texto **Nome do host**.
  - d Configure as propriedades de rede.
- 11 Clique em **Avançar**.
- 12 Dependendo da sua implantação, do vCenter e da configuração de DNS, selecione uma das seguintes maneiras de finalizar a implantação do OVA e ligar o vRealize Automation 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, clique em **Fechar**.
    - c Aguarde até que a máquina 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, clique em **Fechar**.
    - b Ligue o vRealize Automation appliance.
    - c Aguarde até que a máquina seja iniciada, o que pode demorar até 5 minutos.
    - d Verifique se você pode efetuar o ping do DNS para o vRealize Automation appliance. Se você não puder executar um ping do DNS, reinicie a máquina virtual.
    - e Aguarde até que a máquina seja iniciada, o que pode demorar até 5 minutos.
  - Se você tiver implantado o vRealize Automation appliance 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 vRealize Automation appliance.
    - b Clique com o botão direito do mouse no vRealize Automation appliance 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 vRealize Automation appliance.
    - f Aguarde até que a máquina seja iniciada, o que pode demorar até 5 minutos.

Para verificar se você implantou com êxito o appliance, abra um prompt de comando e execute ping no FQDN do vRealize Automation appliance.

### Próximo passo

Repita esse procedimento para implantar instâncias adicionais do vRealize Automation appliance para redundância em um ambiente de alta disponibilidade.

## 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 vRealize Automation appliance.

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”](#), na página 65. Para obter informações sobre a extração de certificados, consulte [“Extraindo certificados e chaves privadas”](#), na página 31.
- 5 Configure o balanceador de carga para tráfego do vRealize Automation appliance.
- 6 Configure os dispositivos para o vRealize Automation. Consulte [“Configurando dispositivos para o vRealize Automation”](#), na página 70.

---

**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 escalabilidade e alta disponibilidade, consulte o guia *Arquitetura de Referência do vRealize Automation*.

## Configurando dispositivos para o vRealize Automation

Após implantar seus dispositivos e configurar o balanceamento de carga, configure os dispositivos para o vRealize Automation.

### Configurar o appliance primário do vRealize Automation

O vRealize Automation appliance é um appliance virtual pré-configurado que implanta o servidor e o console da Web (o portal do usuário) do vRealize Automation. Ele é fornecido como um modelo de formato de virtualização aberto (OVF). O administrador de sistema faz download do appliance e implanta-o no inventário do vCenter Server ou do ESX/ESXi.

Se a sua rede ou balanceador de carga o exigir, o certificado que você configurar para a instância primária do appliance será copiado para o balanceador de carga e para as instâncias adicionais do appliance nos processos subsequentes.

#### Pré-requisitos

- [“Implantar o appliance do vRealize Automation”](#), na página 68.
- Obter um certificado de domínio para o vRealize Automation appliance.

#### Procedimentos

- 1 [Ativar a sincronização de horário no vRealize Automation appliance](#) na página 71

Os relógios no servidor do vRealize Automation appliance e no servidor Windows devem estar sincronizados para garantir uma instalação bem-sucedida.

## 2 Configurar o appliance do vRealize Automation na página 71

Para preparar o vRealize Automation appliance para uso, o administrador do sistema define as configurações de host, gera um certificado SSL e fornece informações de conexão SSO.

### Ativar a sincronização de horário no vRealize Automation appliance

Os relógios no servidor do vRealize Automation appliance e no servidor Windows devem estar sincronizados para garantir uma instalação bem-sucedida.

Se você vir avisos de certificado durante esse processo, ignore-os para concluir a instalação.

#### Procedimentos

- 1 Navegue até o console de gerenciamento do vRealize Automation appliance usando o respectivo nome de domínio totalmente qualificado, <https://vra-va-nomedohost.domínio.nome:5480>.
- 2 Faça login usando o nome de usuário **root** e a senha que você especificou quando o appliance foi implantado.
- 3 Selecione **Administração > Configurações de Horário**.
- 4 Selecione uma opção no menu **Modo de Sincronização de Horário**.

Opção	Ação
<b>Usar Servidor de Horário</b>	Selecione <b>Usar Servidor de Horário</b> no menu <b>Modo de Sincronização de Horário</b> para usar o protocolo NTP. Para cada servidor de horário que você estiver usando, insira o endereço IP ou o nome de host na caixa de texto <b>Servidor de horário</b> .
<b>Usar Horário do Host</b>	Selecione <b>Usar Horário do Host</b> no menu <b>Modo de Sincronização de Horário</b> para usar a sincronização de horário do VMware Tools. Você deve configurar as conexões com os servidores do protocolo NTP antes de usar a sincronização de tempo do VMware Tools.

- 5 Clique em **Salvar Configurações**.
- 6 Verifique se o valor em **Horário Atual** está correto.  
  
Você pode alterar o fuso horário conforme necessário na página Configurações de Fuso Horário na guia **Sistema**.

### Configurar o appliance do vRealize Automation

Para preparar o vRealize Automation appliance para uso, o administrador do sistema define as configurações de host, gera um certificado SSL e fornece informações de conexão SSO.

#### Procedimentos

- 1 Navegue até o console de gerenciamento do vRealize Automation appliance usando o respectivo nome de domínio totalmente qualificado, <https://vra-va-nomedohost.domínio.nome:5480>.
- 2 Ignore o aviso de certificado para continuar.
- 3 Faça login com a raiz do nome de usuário e a senha que você especificou ao implantar o vRealize Automation appliance.

4 Selecione **Configurações do vRA > Configurações do Host**.

Opção	Ação
<b>Solucionar automaticamente</b>	Selecione <b>Solucionar Automaticamente</b> para especificar o nome do host atual do vRealize Automation appliance.
<b>Atualizar host</b>	<p>Para novos hosts, selecione <b>Atualizar Host</b>. Insira o nome de domínio totalmente qualificado do vRealize Automation appliance, <i>vra-hostname.domain.name</i> na caixa de texto <b>Nome do Host</b>.</p> <p>Para implantações distribuídas que usam balanceadores de carga, selecione <b>Atualizar Host</b>. Insira o nome de domínio totalmente qualificado do servidor do balanceador de carga, <i>vra-loadbalancername.domain.name</i> na caixa de texto <b>Nome do Host</b>.</p>

**OBSERVAÇÃO** Defina configurações de SSO conforme descrito mais adiante neste procedimento sempre que você usar **Atualizar Host** para definir o nome do host.



5 Selecione o tipo de certificado no menu **Ação de Certificado**.

Se você estiver usando um certificado codificado por PEM, por exemplo, para um ambiente distribuído, selecione **Importar**.

Os certificados que você importa devem ser confiáveis e também aplicáveis a todas as instâncias do vRealize Automation appliance e todos os balanceadores de carga por meio do uso de certificados de Nome Alternativo da Entidade (SAN).

**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
<b>Manter Existentes</b>	Mantenha a configuração SSL atual. Selecione essa opção para cancelar as alterações.
<b>Gerar Certificado</b>	<ol style="list-style-type: none"> <li>a O valor exibido na caixa de texto <b>Nome comum</b> é o Nome de host, conforme ele é exibido na parte superior da página. Se todas as instâncias adicionais do vRealize Automation appliance estiverem disponíveis, os respectivos FQDN serão incluídos no atributo SAN do certificado.</li> <li>b Insira o nome da organização, como o nome da sua empresa, na caixa de texto <b>Organização</b>.</li> <li>c Insira a unidade organizacional, como o nome ou o local do departamento, na caixa de texto <b>Unidade organizacional</b>.</li> <li>d Insira um código de país ISO 3166 de duas letras, como <b>PT_BR</b>, na caixa de texto <b>País</b>.</li> </ol>
<b>Importar</b>	<ol style="list-style-type: none"> <li>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 <b>Chave Privada RSA</b>.</li> <li>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 <b>Cadeia de Certificados</b>. Para vários valores de certificado, inclua um cabeçalho BEGIN CERTIFICATE e um rodapé END CERTIFICATE em cada certificado. <b>OBSERVAÇÃO</b> No caso dos certificados encadeados, atributos adicionais podem estar disponíveis.</li> <li>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 <b>Código de Acesso</b>.</li> </ol>

6 Clique em **Salvar Configurações** para salvar as informações do host e a configuração do SSL.

## 7 Se exigido pela sua rede ou balanceador de carga, copie o certificado importado ou recém-criado no balanceador de carga do appliance virtual.

Talvez seja necessário permitir o acesso SSH raiz, a fim de exportar o certificado.

- a Se ainda não estiver conectado, faça login no console de gerenciamento do appliance do vRealize Automation como raiz.
- b Clique na guia **Administração**.
- c Clique no submenu **Administração**.
- d Marque a caixa de seleção **Serviço SSH ativado**.  
Desmarque a caixa de seleção para desativar o SSH quando terminar.

- e Marque a caixa de seleção **Login SSH do administrador**.  
Desmarque a caixa de seleção para desativar o SSH quando terminar.
  - f Clique em **Salvar Configurações**.
- 8 Defina as configurações do SSO.
- 9 Clique em **Serviços**.
- Todos os serviços devem estar em execução antes de você poder instalar uma licença ou fazer login no console. Eles geralmente começam em cerca de 10 minutos.

---

**OBSERVAÇÃO** Você também pode fazer login no appliance e executar o `tail -f /var/log/vcac/catalina.out` para monitorar a inicialização do serviço.

---

- 10 Insira as informações da sua licença.
- a Clique em **Configurações do vRA > Licenciamento**.
  - b Clique em **Licenciamento**.
  - c Insira uma chave de licença válida do vRealize Automation que você baixou com os arquivos de instalação e clique em **Enviar Chave**.

---

**OBSERVAÇÃO** Se houver um erro de conexão, você poderá ter um problema com o balanceador de carga. Verifique a conectividade de rede do balanceador de carga.

---

- 11 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 console do vRealize Automation.
- a Abra um navegador e vá até `https://vcac-hostname.domain.name/vcac/`.  
Se você estiver usando um balanceador de carga, o nome do host deve ser o nome de domínio totalmente qualificado do balanceador de carga.
  - b Se solicitado, continue após os avisos de certificado.
  - c Faça login com **administrador@vsphere.local** e a senha que você especificou na configuração do SSO.  
  
O console é aberto 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 vRealize Automation appliance para garantir a redundância em um ambiente de alta disponibilidade.

Para cada vRealize Automation appliance, você deve habilitar a sincronização de data/hora e adicionar o dispositivo a um cluster. As informações de configuração baseadas nas configurações do vRealize Automation appliance inicial (principal) são automaticamente adicionadas quando você adiciona o dispositivo 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.

### Ativar a sincronização de horário no vRealize Automation Appliance

Os relógios no servidor do vRealize Automation appliance e no servidor Windows devem estar sincronizados para garantir uma instalação bem-sucedida.

Se você vir avisos de certificado durante esse processo, ignore-os para concluir a instalação.

#### Pré-requisitos

“Configurar o appliance primário do vRealize Automation”, na página 70.

#### Procedimentos

- 1 Navegue até o console de gerenciamento do vRealize Automation appliance usando o respectivo nome de domínio totalmente qualificado, <https://vra-va-nomedohost.domínio.nome:5480>.
- 2 Faça login usando o nome de usuário **root** e a senha que você especificou quando o appliance foi implantado.
- 3 Selecione **Administração > Configurações de Horário**.
- 4 Selecione uma opção no menu **Modo de Sincronização de Horário**.

Opção	Ação
<b>Usar Servidor de Horário</b>	Selecione <b>Usar Servidor de Horário</b> no menu <b>Modo de Sincronização de Horário</b> para usar o protocolo NTP. Para cada servidor de horário que você estiver usando, insira o endereço IP ou o nome de host na caixa de texto <b>Servidor de horário</b> .
<b>Usar Horário do Host</b>	Selecione <b>Usar Horário do Host</b> no menu <b>Modo de Sincronização de Horário</b> para usar a sincronização de horário do VMware Tools. Você deve configurar as conexões com os servidores do protocolo NTP antes de usar a sincronização de tempo do VMware Tools.

- 5 Clique em **Salvar Configurações**.
- 6 Verifique se o valor em **Horário Atual** está correto.

Você pode alterar o fuso horário conforme necessário na página Configurações de Fuso Horário na guia **Sistema**.

## 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 do vRealize Automation appliance.

Você usa o console de gerenciamento no novo vRealize Automation appliance para uni-lo a um cluster existente de um ou mais appliances. A operação de união copia informações de configuração para o novo appliance que você está adicionando, incluindo informações de certificado, SSO, licenciamento, banco de dados e mensagens.

Você deve adicionar um appliance de cada vez a um cluster, e não em paralelo.

### Pré-requisitos

- Você já deve ter um ou mais nós do vRealize Automation appliance no cluster, e um desses nós deve ser o nó primário. Consulte [“Configurar o appliance primário do vRealize Automation”](#), na página 70.  
Você poderá definir um novo nó para ser o nó principal somente depois de unir esse novo nó ao cluster.
- Verifique se o balanceador de carga está configurado para uso com o novo vRealize Automation 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.
- Ative a sincronização de horário no novo nó. Consulte [“Ativar a sincronização de horário no vRealize Automation Appliance”](#), na página 75.
- Verifique se todos os serviços do vRealize Automation foram iniciados nos nós de appliances de cluster existente e no novo nó que você está adicionando.

### Procedimentos

- 1 Navegue até o console de gerenciamento do vRealize Automation appliance usando o respectivo nome de domínio totalmente qualificado, <https://vra-va-nomedohost.domínio.nome:5480>.
- 2 Ignore todos os avisos de certificado para continuar.
- 3 Faça login com a raiz do nome de usuário e a senha que você especificou ao implantar o vRealize Automation appliance.
- 4 Selecione **Configurações do vRA > Cluster**.
- 5 Digite o FQDN de uma previamente configurado vRealize Automation appliance na caixa de texto **Nó de Cluster Principal**.  
Você pode usar o FQDN do vRealize Automation appliance primário ou qualquer vRealize Automation appliance que já tenha sido unido ao cluster.
- 6 Insira a senha raiz na caixa de texto **Senha**.
- 7 Clique em **Unir cluster**.
- 8 Ignore todos os avisos de certificado para continuar.  
Os serviços do cluster são reiniciados.
- 9 Verifique se os serviços estão em execução.
  - a Clique na guia **Serviços**.
  - b Clique na guia **Atualizar** para monitorar o andamento da inicialização do serviço.

### Desabilitar serviços não utilizados

Para conservar recursos internos em casos nos quais uma instância externa do vRealize Orchestrator é usada, você pode desativar o serviço vRealize Orchestrator incorporado.

### Pré-requisitos

[“Adicionar outro appliance do vRealize Automation ao cluster”](#), na página 76

### Procedimentos

- 1 Faça login no console do vRealize Automation appliance.
- 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 vRealize Automation appliance, você deveria validar 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 console do vRealize Automation navegando para `https://nome.domínio.do.nome.host-vcac/vcac`, onde `nome.domínio.do.nome.host-vcac` é o endereço do balanceador de carga.
- 3 Depois de verificar que o vRealize Automation appliance pode ser acessado usando o balanceador de carga, habilite novamente 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 appliance primário do vRealize Automation”](#), na página 70.
- Se seu site inclui várias instâncias do vRealize Automation appliance, [“Adicionar outro appliance do vRealize Automation ao cluster”](#), na página 76.
- Verifique se o seu servidor de instalação atende aos requisitos descritos em [“Requisitos de Servidor do Model Manager e do Serviço Web IaaS”](#), na página 22.
- 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](#) na página 79  
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](#) na página 79  
Para instalar o IaaS nos seus servidores Windows virtuais ou físicos distribuídos, é necessário baixar uma cópia do instalador do IaaS a partir do vRealize Automation appliance.
- 3 [Escolhendo um cenário de banco de dados do IaaS](#) na página 80  
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](#) na página 85  
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 Website do IaaS adicionais](#) na página 89  
O componente Website fornece acesso aos recursos de infraestrutura no console da Web do vRealize Automation. O administrador de sistema pode instalar uma ou várias instâncias do componente Website.
- 6 [Instalar o Active Manager Service](#) na página 91  
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](#) na página 94  
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](#) na página 96  
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](#) na página 99  
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](#) na página 101  
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”](#), na página 96.

## 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 TLS1.2, consulte o [artigo 245030 da Base de Dados de Conhecimento Microsoft](#).

### 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”](#), na página 79.

## Baixar o Instalador IaaS do vRealize Automation

Para instalar o IaaS nos seus servidores Windows virtuais ou físicos distribuídos, é necessário baixar uma cópia do instalador do IaaS a partir do vRealize Automation appliance.

Se você vir avisos de certificado durante esse processo, ignore-os para concluir a instalação.

### Pré-requisitos

- [“Configurar o appliance primário do vRealize Automation”](#), na página 70 e, opcionalmente, [“Adicionar outro appliance do vRealize Automation ao cluster”](#), na página 76.
- Verifique se o seu servidor de instalação atende aos requisitos descritos em [“Requisitos de Servidor do Model Manager e do Serviço Web IaaS”](#), na página 22.
- 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 Usando uma conta com privilégios de administrador, faça login no servidor Windows.
- 3 Aponte um navegador da Web para a seguinte URL no vRealize Automation appliance.  
<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 com o vRealize Automation appliance.
- 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”](#), na página 80.

## 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 o [artigo 316898 da Base de Dados de Conhecimento da Microsoft](#).

---



**Tabela 4-13.** 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.	<a href="#">“Criar o banco de dados IaaS manualmente”</a> , na página 81.
Prepare um banco de dados vazio e use o instalador para preencher o esquema do banco de dados. Essa opção permite que o instalador aproveite um usuário do banco de dados com os privilégios <b>dbo</b> para preencher o banco de dados, em vez de exigir privilégios <b>sysadmin</b> .	<a href="#">“Preparar um banco de dados vazio”</a> , na página 82.
Use o instalador para criar o banco de dados. Essa é a opção mais simples, mas requer o uso de privilégios <b>sysadmin</b> no instalador.	<a href="#">“Criar o banco de dados do IaaS usando o assistente de instalação”</a> , na página 83.

### 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

- O Microsoft .NET Framework 4.5.2 ou versão posterior deve estar instalado 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 [“Requisitos do servidor de banco de dados do IaaS”](#), na página 21.
- Baixe os scripts do instalador do banco de dados IaaS no vRealize Automation appliance, na seguinte URL.

<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 4-14.** Valores do banco de dados

Variável	Valor
<i>db_server</i>	Especifica a instância do SQL Server no formato <code>dbhostname[,port number]\SQL instance</code> . 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 <code>localhost</code> .
<i>db_name</i>	Nome do banco de dados. O valor padrão é <code>vra</code> . Nomes de banco de dados não devem consistir em mais de 128 caracteres ASCII.
<i>db_dir</i>	Caminho para o diretório de dados do banco de dados, excluindo a barra final.
<i>log_dir</i>	Caminho para o diretório de log do banco de dados, excluindo a barra final.
<i>service_user</i>	Nome de usuário com o qual o Manager é executado.
<i>Web_user</i>	Nome de usuário com o qual o Web Services é executado.
<i>version_string</i>	A versão do vRealize Automation, encontrado depois de fazer login no vRealize Automation appliance e clicar na guia Atualizar.  Por exemplo, a cadeia de caracteres de versão do vRealize Automation 6.1 é <code>6.1.0.1200</code> .

O banco de dados é criado.

### Próximo passo

“Instalar os componentes do IaaS em uma configuração distribuída”, na página 77.

### 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 “Requisitos do servidor de banco de dados do IaaS”, na página 21.
- Faça download dos scripts do instalador do banco de dados do IaaS do vRealize Automation appliance navegando até `https://vra-va-hostname.domain.name: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 o arquivo `CreateDatabase.sql` e substitua todas as instâncias das variáveis na tabela pelos valores corretos para o seu ambiente.

**Tabela 4-15.** Valores do banco de dados

Variável	Valor
<code>\$(DBName)</code>	Nome do banco de dados, como vra. Nomes de banco de dados não devem consistir em mais de 128 caracteres ASCII.
<code>\$(DBDir)</code>	Caminho para o diretório de dados do banco de dados, excluindo a barra final.
<code>\$(LogDir)</code>	Caminho para o diretório de log do banco de dados, excluindo a barra final.

- 5 Revise as configurações na seção **Configurações de BD** do arquivo `CreateDatabase.sql` e edite-as, se necessário.  
  
As configurações no script são as configurações recomendadas para o banco de dados do IaaS. Somente `ALLOW_SNAPSHOT_ISOLATION ON` e `READ_COMMITTED_SNAPSHOT ON` são obrigatórias.
- 6 Abra o SQL Server Management Studio.
- 7 Clique em **Nova Consulta**.  
  
Uma janela de Consulta SQL é aberta.
- 8 No menu **Consulta**, verifique se a opção **Modo SQLCMD** está selecionada.
- 9 Cole o conteúdo modificado inteiro do arquivo `CreateDatabase.sql` no painel de consulta.
- 10 Clique em **Executar**.  
  
O script é executado e cria o banco de dados.

**Próximo passo**

[“Instalar os componentes do IaaS em uma configuração distribuída”](#), na página 77.

**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”](#), na página 81.

**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”](#), na página 79.

**Procedimentos**

- 1 Clique com o botão direito do mouse no arquivo de instalação `setup__vra-va-nomedohost.domínio.nome@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 vRealize Automation appliance 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 vRealize Automation appliance.
  - b Selecione **Aceitar Certificado**.
  - c Clique em **Exibir Certificado**.  
Compare a impressão digital do certificado com a impressão digital definida para o vRealize Automation appliance. Você pode exibir o certificado do vRealize Automation appliance no navegador do cliente quando o console de gerenciamento é acessado na porta 5480.
- 5 Clique em **Avançar**.
- 6 Selecione **Instalação Personalizada** na página Tipo de Instalação.
- 7 Selecione **Servidor do IaaS** em Seleção de Componentes na página Tipo de Instalação.
- 8 Aceite o local de instalação raiz ou clique em **Alterar** e selecione um caminho de instalação.
- 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 o [artigo 316898 da Base de Dados de Conhecimento da Microsoft](#).
- 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 <b>Avançar</b> .
Erros não críticos	Clique em <b>Ignorar</b> .
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 <b>Verificar Novamente</b> 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**.

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”](#), na página 80.
- Se você tiver instalado anteriormente outros componentes neste ambiente, verifique se você sabe a senha que foi criada. Consulte [“Senha de segurança”](#), na página 31.
- Se você estiver usando balanceadores de carga no ambiente, verifique se eles atendem aos requisitos de configuração.

### Procedimentos

- 1 [Instalar o primeiro componente de site do IaaS](#) na página 85  
O administrador do sistema instala um componente de site para fornecer acesso aos recursos de infraestrutura no console da Web do vRealize Automation.
- 2 [Configurar o Model Manager Data](#) na página 87  
Instale o componente Model Manager na mesma máquina que hospeda o primeiro componente Website. O Model Manager Data pode ser instalado apenas uma vez.

Você pode instalar componentes adicionais do Website ou pode instalar o Manager Service. Consulte [“Instalar componentes Website do IaaS adicionais”](#), na página 89 ou [“Instalar o Active Manager Service”](#), na página 91.

### Instalar o primeiro componente de site do IaaS

O administrador do sistema instala um componente de site para fornecer acesso aos recursos de infraestrutura no console da Web do vRealize Automation.

É possível instalar vários componentes de site, mas apenas um pode conter dados do Model Manager. Os dados do Model Manager devem ser instalados no primeiro componente de site que criar.

### Pré-requisitos

- [“Criar o banco de dados do IaaS usando o assistente de instalação”](#), na página 83.

- Verifique se o seu ambiente atende aos requisitos descritos em “[Requisitos de Servidor do Model Manager e do Serviço Web IaaS](#)”, na página 22.
- Se você tiver instalado anteriormente outros componentes neste ambiente, verifique se você sabe a senha que foi criada. Consulte “[Senha de segurança](#)”, na página 31.
- 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 instalação `setup_vra-va-nomedohost.domínio.nome@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 vRealize Automation appliance 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 vRealize Automation appliance.
  - b Selecione **Aceitar Certificado**.
  - c Clique em **Exibir Certificado**.  
  
Compare a impressão digital do certificado com a impressão digital definida para o vRealize Automation appliance. Você pode exibir o certificado do vRealize Automation appliance no navegador do cliente quando o console de gerenciamento é acessado na porta 5480.
- 6 Clique em **Avançar**.
- 7 Selecione **Instalação Personalizada** na página Tipo de Instalação.
- 8 Selecione **Servidor do IaaS** em Seleção de Componentes na página Tipo de Instalação.
- 9 Aceite o local de instalação raiz ou clique em **Alterar** e selecione um caminho de instalação.
- 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 Website. O Model Manager Data pode ser instalado apenas uma vez.

### Pré-requisitos

[“Instalar o primeiro componente de site do IaaS”](#), na página 85.

### Procedimentos

- 1 Clique na guia **Model Manager Data**.
- 2 Digite o nome de domínio totalmente qualificado do vRealize Automation appliance na caixa de texto **Servidor**.  
Endereços IP não são reconhecidos.  
Por exemplo, **vra.mycompany.com**.
- 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 Digite o nome de domínio totalmente qualificado do servidor Website do IaaS na caixa de texto **Servidor do IaaS**.

Opção	Descrição
<b>Se você estiver usando um balanceador de carga</b>	Digite o nome de domínio totalmente qualificado do balanceador de carga para o servidor Website do IaaS. Por exemplo, <b>IaaS-load-balancer.eng.mycompany.com</b> . Endereços IP não são reconhecidos.
<b>Sem balanceador de carga</b>	Digite o nome de domínio totalmente qualificado do servidor Website do IaaS. Por exemplo, <b>IaaS.eng.mycompany.com</b> . Endereços IP não são reconhecidos.

- 10 Clique em **Testar** para verificar a conexão do servidor.
- 11 Clique em **Avançar**.
- 12 Conclua o Verificador de Pré-requisitos.

Opção	Descrição
<b>Nenhum erro</b>	Clique em <b>Avançar</b> .
<b>Erros não críticos</b>	Clique em <b>Ignorar</b> .
<b>Erros críticos</b>	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 <b>Verificar Novamente</b> 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
<b>Se você já tiver instalado componentes neste ambiente</b>	Digite o código de acesso que você criou anteriormente nas caixas de texto <b>Código de Acesso</b> e <b>Confirmar</b> .
<b>Se esta for a primeira instalação</b>	Digite um código de acesso nas caixas de texto <b>Código de Acesso</b> e <b>Confirmar</b> . 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 Website ou pode instalar o Manager Service. Consulte [“Instalar componentes Website do IaaS adicionais”](#), na página 89 ou [“Instalar o Active Manager Service”](#), na página 91.

## Instalar componentes Website do IaaS adicionais

O componente Website fornece acesso aos recursos de infraestrutura no console da Web do vRealize Automation. O administrador de sistema pode instalar uma ou várias instâncias do componente Website.

Não instale os dados do Model Manager com o componente de site. Só o primeiro componente de site que você instalar pode ter dados do Model Manager.

## Pré-requisitos

- [“Instalar um componente de site do IaaS e dados do Model Manager”](#), na página 85.
- Verifique se o seu ambiente atende aos requisitos descritos em [“Requisitos de Servidor do Model Manager e do Serviço Web IaaS”](#), na página 22.
- Se você tiver instalado anteriormente outros componentes neste ambiente, verifique se você sabe a senha que foi criada. Consulte [“Senha de segurança”](#), na página 31.
- 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 instalação `setup_vra-va-nomedohost.dominio.nome@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 vRealize Automation appliance 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 vRealize Automation appliance.
  - b Selecione **Aceitar Certificado**.
  - c Clique em **Exibir Certificado**.  
  
Compare a impressão digital do certificado com a impressão digital definida para o vRealize Automation appliance. Você pode exibir o certificado do vRealize Automation appliance no navegador do cliente quando o console de gerenciamento é acessado na porta 5480.
- 6 Clique em **Avançar**.
- 7 Selecione **Instalação Personalizada** na página Tipo de Instalação.
- 8 Selecione **Servidor do IaaS** em Seleção de Componentes na página Tipo de Instalação.
- 9 Aceite o local de instalação raiz ou clique em **Alterar** e selecione um caminho de instalação.
- 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 Digite as informações do servidor do IaaS na caixa de texto **Servidor do IaaS**.

Opção	Descrição
<b>Se você estiver usando um balanceador de carga</b>	Digite o nome de domínio totalmente qualificado do balanceador de carga para o servidor Website do IaaS. Por exemplo, <b>IaaS-load-balancer.eng.mycompany.com</b> .
<b>Sem balanceador de carga</b>	Digite o nome de domínio totalmente qualificado do servidor Website do IaaS. Por exemplo, <b>IaaS.eng.mycompany.com</b> .

- 19 Clique em **Testar** para verificar a conexão do servidor.
- 20 Clique em **Avançar**.
- 21 Conclua o Verificador de Pré-requisitos.

Opção	Descrição
<b>Nenhum erro</b>	Clique em <b>Avançar</b> .
<b>Erros não críticos</b>	Clique em <b>Ignorar</b> .
<b>Erros críticos</b>	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 <b>Verificar Novamente</b> 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
<b>Se você já tiver instalado componentes neste ambiente</b>	Digite o código de acesso que você criou anteriormente nas caixas de texto <b>Código de Acesso</b> e <b>Confirmar</b> .
<b>Se esta for a primeira instalação</b>	Digite um código de acesso nas caixas de texto <b>Código de Acesso</b> e <b>Confirmar</b> . 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”](#), na página 91.

## 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.

Sua implantação do IaaS requer apenas uma máquina Windows para executar ativamente o Manager Service. Para backup ou alta disponibilidade, será possível implantar máquinas Windows adicionais onde você inicia manualmente o Manager Service se o serviço ativo parar.

---

**IMPORTANTE** A execução simultânea de um Manager Service ativo em vários servidores Windows do IaaS torna o vRealize Automation inutilizável.

---

#### Pré-requisitos

- Se você tiver instalado anteriormente outros componentes neste ambiente, verifique se você sabe a senha que foi criada. Consulte [“Senha de segurança”](#), na página 31.
- (Opcional) Se você deseja instalar o Manager Service em um site diferente do site padrão, crie primeiro um site no Internet Information Services.
- O Microsoft .NET Framework 4.5.2 está instalado.
- 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”](#), na página 85.

## 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 instalação `setup__vra-va-nomedohost.domínio.nome@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 vRealize Automation appliance 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 vRealize Automation appliance.
  - b Selecione **Aceitar Certificado**.
  - c Clique em **Exibir Certificado**.  
  
Compare a impressão digital do certificado com a impressão digital definida para o vRealize Automation appliance. Você pode exibir o certificado do vRealize Automation appliance no navegador do cliente quando o console de gerenciamento é acessado na porta 5480.
- 5 Clique em **Avançar**.
- 6 Selecione **Instalação Personalizada** na página Tipo de Instalação.
- 7 Selecione **Servidor do IaaS** em Seleção de Componentes na página Tipo de Instalação.
- 8 Aceite o local de instalação raiz ou clique em **Alterar** e selecione um caminho de instalação.
- 9 Clique em **Avançar**.
- 10 Selecione **Manager Service** na página Instalação Personalizada do Servidor do IaaS.
- 11 Digite as informações do servidor do IaaS na caixa de texto **Servidor do IaaS**.

Opção	Descrição
<b>Se você estiver usando um balanceador de carga</b>	Digite o nome de domínio totalmente qualificado do balanceador de carga para o servidor Website do IaaS. Por exemplo, <b>IaaS-load-balancer.eng.mycompany.com</b> .
<b>Sem balanceador de carga</b>	Digite o nome de domínio totalmente qualificado do servidor Website do IaaS. Por exemplo, <b>IaaS.eng.mycompany.com</b> .

- 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
<b>Se você já tiver instalado componentes neste ambiente</b>	Digite o código de acesso que você criou anteriormente nas caixas de texto <b>Código de Acesso</b> e <b>Confirmar</b> .
<b>Se esta for a primeira instalação</b>	Digite um código de acesso nas caixas de texto <b>Código de Acesso</b> e <b>Confirmar</b> . 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 pode 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”](#), na página 94.

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”](#), na página 99.

## 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.

Sua implantação do IaaS requer apenas uma máquina Windows para executar ativamente o Manager Service. Máquinas que fornecem o Manager Service de backup devem ter o serviço parado e configurado para serem iniciadas manualmente.

---

**IMPORTANTE** A execução simultânea de um Manager Service ativo em vários servidores Windows do IaaS torna o vRealize Automation inutilizável.

---

### Pré-requisitos

- Se você tiver instalado anteriormente outros componentes neste ambiente, verifique se você sabe a senha que foi criada. Consulte [“Senha de segurança”](#), na página 31.
- (Opcional) Se você deseja instalar o Manager Service em um site diferente do site padrão, crie primeiro um site no Internet Information Services.
- O Microsoft .NET Framework 4.5.2 está instalado.
- 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”](#), na página 85.

### 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 instalação `setup__vra-va-nomedohost.domínio.nome@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 vRealize Automation appliance 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 vRealize Automation appliance.
  - b Selecione **Aceitar Certificado**.
  - c Clique em **Exibir Certificado**.  
  
Compare a impressão digital do certificado com a impressão digital definida para o vRealize Automation appliance. Você pode exibir o certificado do vRealize Automation appliance no navegador do cliente quando o console de gerenciamento é acessado na porta 5480.
- 6 Clique em **Avançar**.

- 7 Selecione **Instalação Personalizada** na página Tipo de Instalação.
- 8 Selecione **Servidor do IaaS** em Seleção de Componentes na página Tipo de Instalação.
- 9 Aceite o local de instalação raiz ou clique em **Alterar** e selecione um caminho de instalação.
- 10 Clique em **Avançar**.
- 11 Selecione **Manager Service** na página Instalação Personalizada do Servidor do IaaS.
- 12 Digite as informações do servidor do IaaS na caixa de texto **Servidor do IaaS**.

Opção	Descrição
<b>Se você estiver usando um balanceador de carga</b>	Digite o nome de domínio totalmente qualificado do balanceador de carga para o servidor Website do IaaS. Por exemplo, <b>IaaS-load-balancer.eng.mycompany.com</b> .
<b>Sem balanceador de carga</b>	Digite o nome de domínio totalmente qualificado do servidor Website do IaaS. Por exemplo, <b>IaaS.eng.mycompany.com</b> .

- 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
<b>Se você já tiver instalado componentes neste ambiente</b>	Digite o código de acesso que você criou anteriormente nas caixas de texto <b>Código de Acesso</b> e <b>Confirmar</b> .
<b>Se esta for a primeira instalação</b>	Digite um código de acesso nas caixas de texto <b>Código de Acesso</b> e <b>Confirmar</b> . 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”](#), na página 99.

## 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 [“Requisitos do Distributed Execution Manager”](#), na página 23.



## Instalar os Distributed Execution Managers

Um administrador de sistema instala 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”](#), na página 79.

### Procedimentos

- 1 Clique com o botão direito do mouse no arquivo de instalação `setup__vra-va-nomedohost.domínio.nome@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 vRealize Automation appliance 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 vRealize Automation appliance.
  - b Selecione **Aceitar Certificado**.
  - c Clique em **Exibir Certificado**.  
Compare a impressão digital do certificado com a impressão digital definida para o vRealize Automation appliance. Você pode exibir o certificado do vRealize Automation appliance no navegador do cliente quando o console de gerenciamento é acessado na porta 5480.
- 5 Clique em **Avançar**.
- 6 Selecione **Instalação Personalizada** na página Tipo de Instalação.
- 7 Selecione **Distributed Execution Managers** em Seleção de Componentes na página Tipo de Instalação.
- 8 Aceite o local de instalação raiz ou clique em **Alterar** e selecione um caminho de instalação.
- 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
<b>Worker</b>	O Worker executa fluxos de trabalho.
<b>Orchestrator</b>	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**.

Se você planeja usar a ferramenta de migração, esse nome deverá corresponder exatamente ao nome usado na instalação do vCloud Automation Center 5.2.3. 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
<b>Se você estiver usando um balanceador de carga</b>	Digite os nomes de domínio totalmente qualificados dos balanceadores de carga do Manager Service e do Serviço da Web do Model Manager. Por exemplo, <b>balanceador-carga-manager.eng.minhaempresa.com:443</b> e <b>balanceador-carga-web.eng.minhaempresa.com:443</b> .
<b>Sem balanceador de carga</b>	Digite os nomes de domínio totalmente qualificados do Manager Service e do Serviço da Web do Model Manager. Por exemplo, <b>manager-service.eng.minhaempresa.com:443</b> e <b>model-manager.eng.minhaempresa.com:443</b> .

- 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 que não seja padrão

Por padrão, o arquivo de configuração do DEM Worker (DynamicOps.DEM.exe.config) indica o caminho de instalação padrão do console do Microsoft System Center Virtual Machine Manager (SCVMM): {ProgramFiles}\Microsoft System Center 2012\Virtual Machine Manager\bin. O administrador do sistema deverá alterar o caminho se ele estiver instalado em outra localização.

Esse procedimento é necessário apenas quando você tem endpoints e agentes do SCVMM.

**Pré-requisitos**

- Se o console do SCVMM tiver sido instalado em outra localização, o arquivo de configuração do DEM Worker (localizado em Program Files (x86)\VMware\VCAC\Distributed Execution Manager\<InstanceName>\DynamicOps.DEM.exe.config deverá ser atualizado para alterar o caminho padrão na seção assemblyLoadConfiguration para indicar a nova pasta.

```
<assemblyLoadConfiguration>
    <assemblies>
        <!-- List of required assemblies for Scvmm -->
        <add name="Errors" path="{ProgramFiles}\Microsoft System Center 2012\Virtual
            Machine Manager\bin" />
        [...]
    </assemblies>
</assemblyLoadConfiguration>
```

**Procedimentos**

- 1 Pare o DEM Worker.
- 2 Determine o caminho de instalação.
- 3 Atualize o arquivo DynamicOps.DEM.exe.config.
- 4 Reinicie o DEM Worker.

Assim, o caminho padrão do DEM Worker é atualizado com a nova pasta.

**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”](#), na página 80.
- 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**.

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”](#), na página 80

### Procedimentos

- 1 Usando uma conta com privilégios de administrador, faça login no servidor Windows de IaaS que hospeda o Manager Service.
- 2 Em **Ferramentas Administrativas > Serviços**, pare o serviço do **VMware vCloud Automation Center**.
- 3 Abra os seguintes arquivos no editor de texto.  
  
C:\Program Files (x86)\VMware\VCAC\Server\ManagerService.exe.config  
C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Web\Web.config
- 4 Em cada arquivo, localize a seção <connectionStrings>.
- 5 Substitua  
  
Integrated Security=True;  
  
com  
  
User Id=database-username;Password=database-password;
- 6 Salve e feche os arquivos.  
  
ManagerService.exe.config  
Web.config
- 7 Inicie o serviço do **VMware vCloud Automation Center**.
- 8 Use o comando iisreset para reiniciar o IIS.

## Verificar os serviços do IaaS

Após a instalação, o administrador do sistema verifica se os serviços de IaaS estão em execução. Se os serviços estiverem em execução, a instalação será um sucesso.

### Procedimentos

- 1 Na área de trabalho do Windows na máquina do IaaS, selecione **Ferramentas Administrativas > Serviços**.
- 2 Localize os serviços a seguir e verifique se o status deles é Iniciado e se o Tipo de inicialização está definido como Automático.
  - VMware DEM – Orchestrator – *Nome* em que *Nome* é a cadeia de caracteres fornecida na caixa **Nome do DEM** durante a instalação.
  - VMware DEM – Trabalhador – *Nome* em que *Nome* é a cadeia de caracteres fornecida na caixa **Nome do DEM** durante a instalação.
  - Agente do VMware vCloud Automation Center *Nome do agente*
  - VMware vCloud Automation Center Service
- 3 Feche a janela **Serviços**.

## Instalando agentes do vRealize Automation

O vRealize Automation usa agentes para fazer integração a sistemas externos. Um administrador de sistema pode selecionar os agentes a serem instalados para comunicação com outras plataformas de virtualização.

O vRealize Automation usa os seguintes tipos de agentes para gerenciar sistemas externos:

- Agentes de proxy do Hypervisor (servidores vSphere, Citrix Xen Servers e Microsoft Hyper-V)
- Agentes de integração do External Provisioning Infrastructure (EPI)
- Agentes do Virtual Desktop Infrastructure (VDI)
- Agentes da Instrumentação de Gerenciamento do Windows (WMI)

Para obter alta disponibilidade, você pode instalar vários agentes para um único endpoint. Instale cada agente redundante em um servidor separado, mas nomeie-os e configure-os de forma idêntica. Os agentes redundantes fornecem alguma tolerância a falhas, mas não fornecem failover. Por exemplo, se você instalar dois agentes do vSphere, um no servidor A e um no servidor B, e o servidor A estiver disponível, o agente instalado no servidor B continuará a processar itens de trabalho. No entanto, o agente do servidor B não poderá terminar o processamento de um item de trabalho que o agente do servidor A já tiver iniciado.

Você tem a opção de instalar um agente do vSphere como parte da instalação mínima, mas, após a instalação, você também poderá adicionar outros agentes, incluindo um agente do vSphere adicional. Em uma implantação distribuída, instale todos os seus agentes depois de concluir a instalação distribuída base. Os agentes que você instala dependem dos recursos na sua infraestrutura.

Para obter informações sobre o uso de agentes do vSphere, consulte [“Requisitos do agente do vSphere”](#), na página 103.

## 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 hh847748 do Microsoft Technet](#). Se a sua Política de Execução do PowerShell for gerenciada no nível da política de grupo, entre em contato com o suporte de TI acerca de suas restrições a alterações de políticas e consulte o [artigo jj149004 do Microsoft Technet](#).

### Pré-requisitos

- Faça login como um administrador do Windows.
- 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 Selecione **Iniciar > Todos os Programas > Versão do Windows PowerShell > Windows PowerShell**.
- 2 Para Remote Signed, execute `Set-ExecutionPolicy RemoteSigned`.
- 3 Para Unrestricted, execute `Set-ExecutionPolicy Unrestricted`.
- 4 Verifique se o comando gerou algum erro.
- 5 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 4-16.** 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.	<a href="#">“Instalando e configurando o agente de proxy do vSphere”</a> , na página 103
Provisione máquinas virtuais fazendo a integração a um ambiente Microsoft Hyper-V Server.	<a href="#">“Instalando o agente de proxy do Hyper-V ou do XenServer”</a> , na página 108
Provisione máquinas virtuais fazendo a integração a um ambiente XenServer.	<ul style="list-style-type: none"> <li>■ <a href="#">“Instalando o agente de proxy do Hyper-V ou do XenServer”</a>, na página 108</li> <li>■ <a href="#">“Instalando o agente do EPI para Citrix”</a>, na página 115</li> </ul>
Provisione máquinas virtuais fazendo a integração a um ambiente XenDesktop.	<ul style="list-style-type: none"> <li>■ <a href="#">“Instalando o agente do VDI do XenDesktop”</a>, na página 112</li> <li>■ <a href="#">“Instalando o agente do EPI para Citrix”</a>, na página 115</li> </ul>
Execute scripts do Visual Basic como etapas adicionais no processo de provisionamento antes ou depois de provisionar uma máquina ou ao cancelar o provisionamento.	<a href="#">“Instalando o agente do EPI para scripts do Visual Basic”</a> , na página 118

**Tabela 4-16.** Escolhendo um cenário de agente (Continuação)

Cenário de integração	Requisitos e procedimentos do agente
Colete dados das máquinas Windows provisionadas, por exemplo, o status do Active Directory do proprietário de uma máquina.	<a href="#">“Instalando o agente do WMI para solicitações remotas do WMI”</a> , na página 121
Provisione máquinas virtuais fazendo a integração a outra plataforma virtual suportada.	Você não precisa instalar um agente.

## Localização e requisitos de instalação de agente

O administrador do sistema costuma instalar os agentes no servidor do vRealize Automation que hospeda o componente do Manager Service.

Se um agente estiver instalado em outro host, a configuração de rede deverá permitir a comunicação entre o agente e a máquina de instalação do Manager Services.

Cada agente é instalado com um nome exclusivo em seu próprio diretório, *Agents\agentname*, no diretório de instalação do vRealize Automation (normalmente *Program Files(x86)\VMware\vCAC*), com sua configuração armazenada no arquivo *VRMAgent.exe.config* nesse diretório.

## Instalando e configurando o agente de proxy do vSphere

Um administrador de sistema instala os agentes de proxy para comunicação com as instâncias de servidor do vSphere. Os agentes descobrem trabalhos disponíveis, recuperam informações do host e relatam itens de trabalho concluídos, além de outras alterações de status do host.

### Requisitos do agente do vSphere

As credenciais do endpoint do vSphere, ou as credenciais sob as quais o serviço do agente é executado, devem ter acesso administrativo ao host de instalação. Vários agentes do vSphere devem atender aos requisitos de configuração do vRealize Automation.

#### Credenciais

Ao criar um endpoint que representa a instância do vCenter Server a ser gerenciada por um agente do vSphere, o agente pode usar as credenciais sob as quais o serviço está sendo executado para interagir com o vCenter Server ou especificar credenciais de endpoint separadas.

A tabela a seguir lista as permissões que as credenciais de endpoint do vSphere devem ter para gerenciar uma instância do vCenter Server. As permissões devem ser habilitadas para todos os clusters do vCenter Server, e não apenas para clusters que hospedarão endpoints.

**Tabela 4-17.** 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

**Tabela 4-17.** Permissões necessárias para o agente do vSphere gerenciar a instância do vCenter Server (Continuação)

Valor do atributo		Permissão
Permissões		Modificar permissão
Recurso		Atribuir VM ao pool de res
		Migrar máquina virtual desligada
		Migrar máquina virtual ligada
Máquina virtual	Inventário	Criar com base no existente
		Criar novo
		Mover
		Remover
	Interação	Configurar mídia de CD
		Interação do console
		Interação do dispositivo
		Desligar (forçado)
		Ligar
		Redefinir
		Suspender
		Instalação de ferramentas
	Configuração	Adicionar disco existente
		Adicionar novo disco
		Adicionar ou remover
		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



**Tabela 4-17.** Permissões necessárias para o agente do vSphere gerenciar a instância do vCenter Server (Continuação)

Valor do atributo	Permissão
	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

- Os componentes do IaaS, incluindo Service Manager e Website, estão instalados.
- Verifique se você concluiu todos os [“Requisitos do agente do vSphere”](#), na página 103.
- 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”](#), na página 79.

### Procedimentos

- 1 Clique com o botão direito do mouse no arquivo de instalação `setup__vra-va-nomedohost.domínio.nome@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 vRealize Automation appliance 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 vRealize Automation appliance.
  - b Selecione **Aceitar Certificado**.
  - c Clique em **Exibir Certificado**.  
Compare a impressão digital do certificado com a impressão digital definida para o vRealize Automation appliance. Você pode exibir o certificado do vRealize Automation appliance no navegador do cliente quando o console de gerenciamento é acessado na porta 5480.
- 5 Selecione **Instalação Personalizada** na página Tipo de Instalação.
- 6 Selecione **Seleção de Componentes** na página Tipo de Instalação.
- 7 Aceite o local de instalação raiz ou clique em **Alterar** e selecione um caminho de instalação.
- 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
<b>Instalação de agente redundante</b>	Instale agentes redundantes em servidores diferentes. Nomeie e configure agentes redundantes de forma idêntica.
<b>Instalação de agente único</b>	Selecione um nome exclusivo para o agente.

- 13 Configure uma conexão com o componente Service Manager.

Opção	Descrição
<b>Se você estiver usando um balanceador de carga</b>	Insira o nome de domínio totalmente qualificado e o número de porta do balanceador de carga do componente Manager Service. Por exemplo, <b>balanceador-carga-manager.eng.minhaempresa.com:443</b> . Endereços IP não são reconhecidos.
<b>Sem balanceador de carga</b>	Insira o nome de domínio totalmente qualificado e o número de porta da máquina na qual você instalou o componente Manager Service. Por exemplo, <b>manager_service.minhaempresa.com:443</b> . Endereços IP não são reconhecidos.

A porta padrão é 443.

- 14 Configure uma conexão com o componente Manager Website.

Opção	Descrição
<b>Se você estiver usando um balanceador de carga</b>	Insira o nome de domínio totalmente qualificado e o número de porta do balanceador de carga do componente Manager Website. Por exemplo, <b>balanceador-carga-website.eng.minhaempresa.com:443</b> . Endereços IP não são reconhecidos.
<b>Sem balanceador de carga</b>	Insira o nome de domínio totalmente qualificado e o número de porta da máquina na qual você instalou o componente Manager Website. Por exemplo, <b>componente_website.minhaempresa.com:443</b> . Endereços IP não são reconhecidos.

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”, na página 107.

## Configurar o agente do vSphere

Você pode usar o utilitário de agente proxy para modificar as configurações iniciais que são criptografadas no arquivo de configuração do agente `VRMAgent.exe.config` ou para alterar a política de exclusão de máquinas para plataformas de virtualização.

Configure o agente do vSphere em preparação para criar e usar endpoints do vSphere a serem utilizados em blueprints do vRealize Automation.

---

**OBSERVAÇÃO** Algumas partes do arquivo são criptografadas, mas outras não. Por exemplo, a seção `serviceConfiguration` de `VRMAgent.exe.config` não é criptografada.

---

### Pré-requisitos

Faça login como **administrador do sistema** na máquina em que você instalou o agente do vSphere.

### Procedimentos

- 1 Abra um console de comando do Windows como um administrador.
- 2 Vá para o diretório de instalação de agentes.  
Por exemplo, `cd Program Files (x86)\VMware\VCAC\CD Agents\agent_name.`
- 3 (Opcional) Insira o `DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config get` para exibir as definições de configuração atuais.  
Veja a seguir um exemplo do comando de saída:  
`managementEndpointName: VCEndpoint doDeletes: Verdadeiro`
- 4 (Opcional) Insira o comando `set managementEndpointName` para alterar o nome do endpoint configurado na instalação.  
Por exemplo, `DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set managementEndpointName MeuEndpoint.`  
Você altera essa propriedade para renomear o endpoint no vRealize Automation em vez de alterar os endpoints.
- 5 (Opcional) Insira o comando `set doDeletes` para configurar a política de exclusão da máquina virtual.  
Por exemplo, `DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set doDeletesfalso.`

Opção	Descrição
<b>verdadeiro</b>	(Padrão) Exclua máquinas virtuais destruídas no vRealize Automation do vCenter Server.
<b>falso</b>	Mova as máquinas virtuais destruídas no vRealize Automation para o diretório <code>VRMDeleted</code> no vCenter Server.

- 6 (Opcional) Exija um certificado confiável para o agente do vSphere, definindo o parâmetro `trustAllCertificates` como `False` usando a seguinte instrução na seção `serviceConfiguration` do arquivo `VRMAgent.exe.config`:

```
trustAllCertificates = "false"
```

Como essa configuração não é criptografada, você não pode usar o comando `DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set trustAllCertificates false`.

Opção	Descrição
<b>verdadeiro</b>	(Padrão) O agente do vSphere não requer um certificado confiável do vCenter Server.
<b>falso</b>	O agente do vSphere requer um certificado confiável do vCenter Server.

- 7 Navegue até **Iniciar > Ferramentas administrativas > Serviços** e reinicie o serviço vRealize Automation Agente – *nomedoagente*.

### Próximo passo

Para obter alta disponibilidade, você pode instalar e configurar um agente redundante para o endpoint. Instale cada agente redundante em um servidor separado, mas nomeie-os e configure-os de forma idêntica.

## Instalando o agente de proxy do Hyper-V ou do XenServer

Um administrador de sistema instala os agentes de proxy para comunicação com as instâncias de servidor do Hyper-V e do XenServer. Os agentes descobrem trabalhos disponíveis, recuperam informações do host e relatam itens de trabalho concluídos, além de outras alterações de status do host.

### Requisitos do Hyper-V e do XenServer

Os agentes de proxy do Hyper-V Hypervisor exigem credenciais de administrador de sistema para a instalação.

As credenciais sob as quais o serviço do agente é executado devem ter acesso administrativo ao host de instalação.

São exigidas credenciais de nível de administrador para todas as instâncias do XenServer ou do Hyper-V nos hosts a serem gerenciados pelo agente.

Se você estiver usando pools Xen, todos os nós no pool Xen deverão ser identificados pelos respectivos nomes de domínio totalmente qualificados.

---

**OBSERVAÇÃO** Por padrão, o Hyper-V não está configurado para gerenciamento remoto. Um agente de proxy do vRealize Automation Hyper-V não pode comunicar-se com um servidor do Hyper-V, a menos que o gerenciamento remoto tenha sido ativado.

Consulte a documentação do Microsoft Windows Server para obter informações sobre como configurar o Hyper-V para gerenciamento remoto.

---

### Instalar o agente do Hyper-V ou do XenServer

O agente do Hyper-V gerencia as instâncias do servidor do Hyper-V. O agente do XenServer gerencia as instâncias do servidor do XenServer.

#### Pré-requisitos

- Os componentes do IaaS, incluindo Service Manager e Website, estão instalados.
- [“Baixar o Instalador IaaS do vRealize Automation”](#), na página 79.
- Verifique se agentes de proxy do Hyper-V Hypervisor têm credenciais de administrador do sistema.

- Verifique se as credenciais sob as quais o serviço do agente é executado têm acesso administrativo ao host de instalação.
- Verifique se todas as instâncias do XenServer ou do Hyper-V nos hosts a serem gerenciados pelo agente têm credenciais de nível de administrador.
- Se você estiver usando pools Xen, observe que todos os nós no pool Xen deverão ser identificados pelos respectivos nomes de domínio totalmente qualificados.

O vRealize Automation não pode se comunicar com ou gerenciar qualquer nó que não esteja identificado por seu nome de domínio totalmente qualificado no pool Xen.

- Configure o Hyper-V para gerenciamento remoto para ativar a comunicação do servidor do Hyper-V com os agentes de proxy do vRealize Automation Hyper-V.

Consulte a documentação do Microsoft Windows Server para obter informações sobre como configurar o Hyper-V para gerenciamento remoto.

### Procedimentos

- 1 Clique com o botão direito do mouse no arquivo de instalação `setup__vra-va-nomedohost.dominio.nome@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 vRealize Automation appliance 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 vRealize Automation appliance.
  - b Selecione **Aceitar Certificado**.
  - c Clique em **Exibir Certificado**.  
Compare a impressão digital do certificado com a impressão digital definida para o vRealize Automation appliance. Você pode exibir o certificado do vRealize Automation appliance no navegador do cliente quando o console de gerenciamento é acessado na porta 5480.
- 5 Selecione **Instalação Personalizada** na página Tipo de Instalação.
- 6 Selecione **Seleção de Componentes** na página Tipo de Instalação.
- 7 Aceite o local de instalação raiz ou clique em **Alterar** e selecione um caminho de instalação.
- 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
<b>Instalação de agente redundante</b>	Instale agentes redundantes em servidores diferentes. Nomeie e configure agentes redundantes de forma idêntica.
<b>Instalação de agente único</b>	Selecione um nome exclusivo para o 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 componente Service Manager.

Opção	Descrição
<b>Se você estiver usando um balanceador de carga</b>	Insira o nome de domínio totalmente qualificado e o número de porta do balanceador de carga do componente Manager Service. Por exemplo, <b>balanceador-carga-manager.eng.minhaempresa.com:443</b> . Endereços IP não são reconhecidos.
<b>Sem balanceador de carga</b>	Insira o nome de domínio totalmente qualificado e o número de porta da máquina na qual você instalou o componente Manager Service. Por exemplo, <b>manager_service.minhaempresa.com:443</b> . Endereços IP não são reconhecidos.

A porta padrão é 443.

- 15 Configure uma conexão com o componente Manager Website.

Opção	Descrição
<b>Se você estiver usando um balanceador de carga</b>	Insira o nome de domínio totalmente qualificado e o número de porta do balanceador de carga do componente Manager Website. Por exemplo, <b>balanceador-carga-website.eng.minhaempresa.com:443</b> . Endereços IP não são reconhecidos.
<b>Sem balanceador de carga</b>	Insira o nome de domínio totalmente qualificado e o número de porta da máquina na qual você instalou o componente Manager Website. Por exemplo, <b>componente_website.minhaempresa.com:443</b> . Endereços IP não são reconhecidos.

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”, na página 111.

## 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”](#), na página 113 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”](#), na página 102.

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 Dsktop 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

- Os componentes do IaaS, incluindo Service Manager e Website, estão instalados.
- Verifique se o seu ambiente atende aos [“Requisitos do XenDesktop”](#), na página 112.
- [“Baixar o Instalador IaaS do vRealize Automation”](#), na página 79.

### Procedimentos

- 1 Clique com o botão direito do mouse no arquivo de instalação `setup__vra-va-nomedohost.domínio.nome@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 vRealize Automation appliance 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 vRealize Automation appliance.
  - b Selecione **Aceitar Certificado**.
  - c Clique em **Exibir Certificado**.  
Compare a impressão digital do certificado com a impressão digital definida para o vRealize Automation appliance. Você pode exibir o certificado do vRealize Automation appliance no navegador do cliente quando o console de gerenciamento é acessado na porta 5480.
- 5 Clique em **Avançar**.
- 6 Selecione **Instalação Personalizada** na página Tipo de Instalação.
- 7 Selecione **Agentes Proxy** no painel Seleção do Componente.
- 8 Aceite o local de instalação raiz ou clique em **Alterar** e selecione um caminho de instalação.
- 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
<b>Instalação de agente redundante</b>	Instale agentes redundantes em servidores diferentes. Nomeie e configure agentes redundantes de forma idêntica.
<b>Instalação de agente único</b>	Selecione um nome exclusivo para o agente.

- 14 Configure uma conexão com o componente Service Manager.

Opção	Descrição
<b>Se você estiver usando um balanceador de carga</b>	Insira o nome de domínio totalmente qualificado e o número de porta do balanceador de carga do componente Manager Service. Por exemplo, <b>balanceador-carga-manager.eng.minhaempresa.com:443</b> . Endereços IP não são reconhecidos.
<b>Sem balanceador de carga</b>	Insira o nome de domínio totalmente qualificado e o número de porta da máquina na qual você instalou o componente Manager Service. Por exemplo, <b>manager_service.minhaempresa.com:443</b> . Endereços IP não são reconhecidos.

A porta padrão é 443.

- 15 Configure uma conexão com o componente Manager Website.

Opção	Descrição
<b>Se você estiver usando um balanceador de carga</b>	Insira o nome de domínio totalmente qualificado e o número de porta do balanceador de carga do componente Manager Website. Por exemplo, <b>balanceador-carga-website.eng.minhaempresa.com:443</b> . Endereços IP não são reconhecidos.
<b>Sem balanceador de carga</b>	Insira o nome de domínio totalmente qualificado e o número de porta da máquina na qual você instalou o componente Manager Website. Por exemplo, <b>componente_website.minhaempresa.com:443</b> . Endereços IP não são reconhecidos.

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”](#), na página 115 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”](#), na página 102.

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

- Os componentes do IaaS, incluindo Service Manager e Website, estão instalados.
- Verifique se você atendeu a todos os [“Requisitos do servidor de provisionamento Citrix”](#), na página 115.
- [“Baixar o Instalador IaaS do vRealize Automation”](#), na página 79.

### Procedimentos

- 1 Clique com o botão direito do mouse no arquivo de instalação `setup_vra-va-nomedohost.domínio.nome@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 vRealize Automation appliance 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 vRealize Automation appliance.
  - b Selecione **Aceitar Certificado**.
  - c Clique em **Exibir Certificado**.  
Compare a impressão digital do certificado com a impressão digital definida para o vRealize Automation appliance. Você pode exibir o certificado do vRealize Automation appliance no navegador do cliente quando o console de gerenciamento é acessado na porta 5480.
- 5 Selecione **Instalação Personalizada** na página Tipo de Instalação.
- 6 Selecione **Seleção de Componentes** na página Tipo de Instalação.
- 7 Aceite o local de instalação raiz ou clique em **Alterar** e selecione um caminho de instalação.
- 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
<b>Instalação de agente redundante</b>	Instale agentes redundantes em servidores diferentes. Nomeie e configure agentes redundantes de forma idêntica.
<b>Instalação de agente único</b>	Selecione um nome exclusivo para o agente.

- 13 Configure uma conexão com o componente Service Manager.

Opção	Descrição
<b>Se você estiver usando um balanceador de carga</b>	Insira o nome de domínio totalmente qualificado e o número de porta do balanceador de carga do componente Manager Service. Por exemplo, <b>balanceador-carga-manager.eng.minhaempresa.com:443</b> . Endereços IP não são reconhecidos.
<b>Sem balanceador de carga</b>	Insira o nome de domínio totalmente qualificado e o número de porta da máquina na qual você instalou o componente Manager Service. Por exemplo, <b>manager_service.minhaempresa.com:443</b> . Endereços IP não são reconhecidos.

A porta padrão é 443.

- 14 Configure uma conexão com o componente Manager Website.

Opção	Descrição
<b>Se você estiver usando um balanceador de carga</b>	Insira o nome de domínio totalmente qualificado e o número de porta do balanceador de carga do componente Manager Website. Por exemplo, <b>balanceador-carga-website.eng.minhaempresa.com:443</b> . Endereços IP não são reconhecidos.
<b>Sem balanceador de carga</b>	Insira o nome de domínio totalmente qualificado e o número de porta da máquina na qual você instalou o componente Manager Website. Por exemplo, <b>componente_website.minhaempresa.com:443</b> . Endereços IP não são reconhecidos.

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 4-18.** 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. Visite <a href="http://support.microsoft.com">http://support.microsoft.com</a> para obter mais informações.
Política de execução do MS PowerShell	<p>A Política de execução do MS PowerShell deve ser definida como <b>RemoteSigned</b> ou <b>Unrestricted</b>.</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

- Os componentes do IaaS, incluindo Service Manager e Website, estão instalados.
- Verifique se você atendeu a todos os [“Requisitos dos scripts do Visual Basic”](#), na página 118.
- [“Baixar o Instalador IaaS do vRealize Automation”](#), na página 79.

### Procedimentos

- 1 Clique com o botão direito do mouse no arquivo de instalação `setup__vra-va-nomedohost.domínio.nome@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 vRealize Automation appliance 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 vRealize Automation appliance.
  - b Selecione **Aceitar Certificado**.
  - c Clique em **Exibir Certificado**.  
Compare a impressão digital do certificado com a impressão digital definida para o vRealize Automation appliance. Você pode exibir o certificado do vRealize Automation appliance no navegador do cliente quando o console de gerenciamento é acessado na porta 5480.
- 5 Selecione **Instalação Personalizada** na página Tipo de Instalação.
- 6 Selecione **Seleção de Componentes** na página Tipo de Instalação.
- 7 Aceite o local de instalação raiz ou clique em **Alterar** e selecione um caminho de instalação.
- 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
<b>Instalação de agente redundante</b>	Instale agentes redundantes em servidores diferentes. Nomeie e configure agentes redundantes de forma idêntica.
<b>Instalação de agente único</b>	Selecione um nome exclusivo para o agente.

- 13 Configure uma conexão com o componente Service Manager.

Opção	Descrição
<b>Se você estiver usando um balanceador de carga</b>	Insira o nome de domínio totalmente qualificado e o número de porta do balanceador de carga do componente Manager Service. Por exemplo, <b>balanceador-carga-manager.eng.minhaempresa.com:443</b> . Endereços IP não são reconhecidos.
<b>Sem balanceador de carga</b>	Insira o nome de domínio totalmente qualificado e o número de porta da máquina na qual você instalou o componente Manager Service. Por exemplo, <b>manager_service.minhaempresa.com:443</b> . Endereços IP não são reconhecidos.

A porta padrão é 443.

- 14 Configure uma conexão com o componente Manager Website.

Opção	Descrição
<b>Se você estiver usando um balanceador de carga</b>	Insira o nome de domínio totalmente qualificado e o número de porta do balanceador de carga do componente Manager Website. Por exemplo, <b>balanceador-carga-website.eng.minhaempresa.com:443</b> . Endereços IP não são reconhecidos.
<b>Sem balanceador de carga</b>	Insira o nome de domínio totalmente qualificado e o número de porta da máquina na qual você instalou o componente Manager Website. Por exemplo, <b>componente_website.minhaempresa.com:443</b> . Endereços IP não são reconhecidos.

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

- Os componentes do IaaS, incluindo Service Manager e Website, estão instalados.
- Verifique se você atendeu a todos os requisitos. Consulte [“Ativar solicitações WMI remotas em máquinas Windows”](#), na página 121.
- [“Baixar o Instalador IaaS do vRealize Automation”](#), na página 79.

#### Procedimentos

- 1 Clique com o botão direito do mouse no arquivo de instalação `setup__vra-va-nomedohost.domínio.nome@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 vRealize Automation appliance 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 vRealize Automation appliance.
  - b Selecione **Aceitar Certificado**.
  - c Clique em **Exibir Certificado**.  
Compare a impressão digital do certificado com a impressão digital definida para o vRealize Automation appliance. Você pode exibir o certificado do vRealize Automation appliance no navegador do cliente quando o console de gerenciamento é acessado na porta 5480.
- 5 Selecione **Instalação Personalizada** na página Tipo de Instalação.
- 6 Selecione **Seleção de Componentes** na página Tipo de Instalação.

- 7 Aceite o local de instalação raiz ou clique em **Alterar** e selecione um caminho de instalação.
- 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
<b>Instalação de agente redundante</b>	Instale agentes redundantes em servidores diferentes. Nomeie e configure agentes redundantes de forma idêntica.
<b>Instalação de agente único</b>	Selecione um nome exclusivo para o agente.

- 13 Configure uma conexão com o componente Service Manager.

Opção	Descrição
<b>Se você estiver usando um balanceador de carga</b>	Insira o nome de domínio totalmente qualificado e o número de porta do balanceador de carga do componente Manager Service. Por exemplo, <b>balanceador-carga-manager.eng.minhaempresa.com:443</b> . Endereços IP não são reconhecidos.
<b>Sem balanceador de carga</b>	Insira o nome de domínio totalmente qualificado e o número de porta da máquina na qual você instalou o componente Manager Service. Por exemplo, <b>manager_service.minhaempresa.com:443</b> . Endereços IP não são reconhecidos.

A porta padrão é 443.

- 14 Configure uma conexão com o componente Manager Website.

Opção	Descrição
<b>Se você estiver usando um balanceador de carga</b>	Insira o nome de domínio totalmente qualificado e o número de porta do balanceador de carga do componente Manager Website. Por exemplo, <b>balanceador-carga-website.eng.minhaempresa.com:443</b> . Endereços IP não são reconhecidos.
<b>Sem balanceador de carga</b>	Insira o nome de domínio totalmente qualificado e o número de porta da máquina na qual você instalou o componente Manager Website. Por exemplo, <b>componente_website.minhaempresa.com:443</b> . Endereços IP não são reconhecidos.

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.



# Tarefas pós instalação do vRealize Automation

# 5

Após a instalação do vRealize Automation, existem tarefas que podem exigir a sua atenção.

Este capítulo inclui os seguintes tópicos:

- [“Substituindo certificados autoassinados por certificados fornecidos por uma autoridade”](#), na página 125
- [“Instalando o agente do vRealize Log Insight em servidores IaaS”](#), na página 125
- [“Configurar o acesso ao tenant padrão”](#), na página 125

## 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*.

## 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. Consulte o *Guia de Administração de Agentes do VMware vRealize Log Insight*.

vRealize Automation appliances incluem o agente do vRealize Log Insight por padrão.

## 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 console do vRealize Automation como administrador do sistema do tenant padrão.
  - a Navegue até o console do vRealize Automation.

Opção	Descrição
<b>Sem balanceador de carga</b>	<code>https://vrealize-appliance-hostname.domain.name/vcac</code>

- b Faça login com o nome de usuário **administrator** e a senha que você definiu para esse usuário quando configurou o SSO.
- 2 Selecione **Administração > Tenants**.
- 3 Clique no nome do tenant padrão, **vsphere.local**.
- 4 Clique na guia **Usuários locais**.
- 5 Crie contas de usuário local para o tenant padrão do vRealize Automation.  
Os usuários locais são específicos do tenant e só podem acessar o tenant no qual você os criou.
  - a Clique no ícone Adicionar (+).
  - b Insira os detalhes do usuário responsável pela administração da sua infraestrutura.
  - c Clique em **Adicionar**.
  - d Repita essa etapa para adicionar um ou mais usuários responsáveis pela configuração do tenant padrão.
- 6 Clique na guia **Administradores**.
- 7 Atribua seus usuários locais ao administrador de tenant e às funções de administrador do IaaS.
  - a Insira um nome de usuário na caixa de pesquisa **Administradores de tenant** e pressione Enter.
  - b Insira um nome de usuário na caixa de pesquisa **Administradores do IaaS** e pressione Enter.  
O administrador do IaaS é responsável pela criação e gerenciamento dos seus endpoints de infraestrutura no vRealize Automation. Somente o administrador do sistema pode conceder essa função.
- 8 Clique em **Atualizar**.

## Próximo passo

Forneça à sua equipe a URL de acesso e as informações de login das contas de usuário que você criou para que possam começar a configuração do vRealize Automation.

- Os administradores de tenant configuram definições, como a autenticação do usuário, incluindo a configuração de Gerenciamento de diretórios para alta disponibilidade. Consulte *Configurando o vRealize Automation*.
- Os administradores do IaaS preparam recursos externos para o provisionamento. Consulte *Configurando o vRealize Automation*.
- Se você tiver configurado a Criação de conteúdo inicial durante a instalação, o administrador de configuração poderá solicitar o item de catálogo Conteúdo inicial para preencher rapidamente uma prova de conceito. Para obter um exemplo de como solicitar o item e concluir a ação manual do usuário, consulte *Instalando e configurando o vRealize Automation para o cenário do Rainpole*.

# Solucionando problemas com uma instalação do vRealize Automation

# 6

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:

- [“Localidades do log padrão”](#), na página 127
- [“Revertendo uma instalação com falha”](#), na página 128
- [“Criar um pacote de suporte do vRealize Automation”](#), na página 130
- [“Solução de problemas gerais com a instalação”](#), na página 131
- [“Solucionando problemas com o appliance do vRealize Automation”](#), na página 134
- [“Solucionando problemas de componentes do IaaS”](#), na página 137
- [“Solução de erros de login”](#), na página 143

## Localidades do log padrão

Consulte os arquivos de registro do sistema e do produto para obter informações sobre uma falha na instalação.

Os caminhos de arquivo mostrados são os caminhos padrão. Se você instalou o IaaS em outro diretório, navegue até o diretório de instalação personalizado.

**OBSERVAÇÃO** Para a coleta de logs, considere tirar proveito dos vRealize Automation e vRealize Orchestrator Content Packs para o vRealize Log Insight. Os Content Packs e o Log Insight fornecem um resumo consolidado de eventos de log para componentes no vRealize Suite. Para obter mais informações, visite o [VMware Solution Exchange](#).

## Registros do Windows

Use o seguinte para encontrar arquivos de log para eventos do Windows.

Registro	Localização
Registros do visualizador de eventos do Windows	Iniciar > Painel de Controle > Ferramentas Administrativas > Visualizador de Eventos

## Registros de instalação

Os registros de instalação estão nas localizações a seguir.

Registro	Localização padrão
Registros de instalação	C:\Arquivos de programas (x86)\vCAC\InstallLogs C:\Arquivos de programas (x86)\VMware\vCAC\Server\ConfigTool\Log
Registros de instalação do WAPI	C:\Arquivos de programas (x86)\VMware\vCAC\Web API\ConfigTool\Logfilename WapiConfiguration-<XXX>

## Registros do IaaS

Os registros do IaaS estão nas localizações a seguir.

Registro	Localização padrão
Registros de site	C:\Arquivos de programas (x86)\VMware\vCAC\Server\Website\Logs
Registro do repositório	C:\Arquivos de programas (x86)\VMware\vCAC\Server\Model Manager Web\Logs
Registros do Manager Service	C:\Arquivos de programas (x86)\VMware\vCAC\Server\Logs
Registros do DEM Orchestrator	C:\Users\<nome do usuário>\AppData\Local\Temp\VMware\vCAC\Distributed Execution Manager\<nome do sistema> DEO \Logs
Registros do agente	C:\Users\<nome do usuário>\AppData\Local\Temp\VMware\vCAC\Agents\<nome do agente>\logs

## Registros de estrutura do vRealize Automation

As entradas de registro para Estruturas do vRealize Automation encontram-se na localização a seguir.

Registro	Localização padrão
Registros de estrutura	/var/log/vmware

## Registros de provisionamento de componentes de software

Registros de provisionamento de componentes de software encontram-se na localização a seguir.

Registro	Localização padrão
Registro de bootstrap do agente do software	/opt/vmware-appdirector (para Linux) ou \opt\vmware-appdirector (para Windows)
Registros de script do ciclo de vida do software	/tmp/taskId (para Linux) \Users\darwin\AppData\Local\Temp\taskId (para Windows)

## Coleção de registros para implantações distribuídas

Você pode criar um arquivo zip que agrupa todos os registros dos componentes de uma implantação distribuída. .

## Revertendo uma instalação com falha

Quando uma instalação falha e reverte, o administrador de sistema deve verificar se todos os arquivos necessários foram desinstalados antes de iniciar outra instalação. Alguns arquivos devem ser desinstalados manualmente.



## Reverter uma instalação mínima

Um administrador de sistema deve remover manualmente alguns arquivos e reverter o banco de dados para desinstalar completamente uma instalação do IaaS do vRealize Automation com falha.

### Procedimentos

- 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.

A instalação é completamente removida.

## Reverter uma instalação distribuída

Um administrador de sistema deve remover manualmente alguns arquivos e reverter o banco de dados para desinstalar completamente uma instalação do IaaS com falha.

### Procedimentos

- 1 Se os seguintes componentes estão presentes, desinstale-os com o desinstalador do Windows.

- Servidor do vRealize Automation
- WAPI do vRealize Automation

---

**OBSERVAÇÃO** Se você vir a seguinte mensagem, reinicie a máquina e, em seguida, siga este procedimento: Erro ao abrir o arquivo de registro de instalação. Verifique se a localização do arquivo de registro especificado existe e é gravável.

---



---

**OBSERVAÇÃO** Se o sistema Windows foi revertido ou o IaaS foi desinstalado, você deve executar o comando `iisreset` antes de reinstalar o IaaS do vRealize Automation.

---

- 2 Reverta o seu banco de dados para o estado em que estava antes da instalação ser iniciada. O método usado depende do modo de instalação do banco de dados original.

- 3 No IIS (Internet Information Services Manager), selecione o Site padrão (no site personalizado) e clique em **Associações**. Remova a associação de https (padrões para 443).
- 4 Verifique se o Repositório de aplicativos, vCAC e WAPI foram excluídos e se os pools de aplicativos RepositoryAppPool, vCACAppPool, WapiAppPool também foram excluídos.

**Tabela 6-1.** 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 o DEM-Worker.
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 vRealize Automation appliance. Os pacotes de suporte coletam logs e ajudam a você ou o suporte técnico do VMware a resolver problemas do vRealize Automation.

### Procedimentos

- 1 Em um navegador da Web, abra a interface de gerenciamento do vRealize Automation appliance.  
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Faça login como raiz e clique em **Configurações do vRA > Cluster**.
- 3 Clique em **Criar Pacote de Suporte**.
- 4 Clique em **Download** e salve o arquivo de pacote de suporte no seu sistema.

Os pacotes de suporte incluem informações do vRealize Automation appliance e dos servidores Windows do IaaS. Se você perder a conectividade entre os componentes do vRealize Automation appliance e do IaaS, o pacote de suporte poderá ter os logs do componente do IaaS ausentes.

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 do IaaS que aparecem em vermelho.

Para que um procedimento de backup colete pacotes de log do componente do IaaS, consulte o [Artigo da base de conhecimento da VMware 2078179](#).

## 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. Por exemplo, dependendo do balanceador de carga que você está usando, edite a configuração do tempo limite do balanceador de carga no seu arquivo `ssl.conf`, `httpd.conf` ou em outro arquivo de configuração da Web.
- 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 vRealize Automation appliance.

#### 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

Para cada servidor do vRealize Automation appliance e todos os servidores do Windows em que os componentes do IaaS serão instalados, habilite a sincronização de hora, conforme descrito nos seguintes tópicos:

- [“Ativar a sincronização data/hora no appliance do vRealize Automation”](#), na página 54
- [“Ativar a sincronização de horário no servidor Windows”](#), na página 58

Para obter uma visão geral da pontualidade do vRealize Automation, consulte [“Sincronização de hora”](#), na página 31.

## Podem aparecer páginas em branco ao usar o Internet Explorer 9 ou 10 no Windows 7

Quando você usa o Internet Explorer 9 ou 10 no Windows 7 e o modo de compatibilidade está habilitado, aparecem algumas páginas sem conteúdo.

### Problema

Ao usar o Internet Explorer 9 ou 10 no Windows 7, as seguintes páginas não têm conteúdo:

- Infraestrutura
- Página da pasta de tenant padrão no Orchestrator
- Página de configuração do servidor no Orchestrator

### Causa

O problema pode estar relacionado ao fato de o modo de compatibilidade estar habilitado. Você pode desabilitar o modo de compatibilidade para o Internet Explorer seguindo as etapas abaixo.

### Solução

#### Pré-requisitos

Certifique-se de que a barra de menus seja exibida. Se você estiver usando o Internet Explorer 9 ou 10, pressione Alt para exibir a barra de menus (ou clique com o botão direito do mouse na barra de endereços e selecione **Barra de menus**).

#### Procedimentos

- 1 Selecione **Ferramentas > Configurações do Modo de Exibição de Compatibilidade**.
- 2 Desmarque **Exibir sites da intranet no Modo de Exibição de Compatibilidade**.
- 3 Clique em **Fechar**.

## Não é possível estabelecer uma relação confiável para o canal seguro de SSL/TLS

Talvez você receba a mensagem "Não é possível estabelecer uma relação confiável para o canal seguro de SSL/TLS ao atualizar certificados de segurança para o vCloud Automation Center".

### Problema

Se ocorrer um problema de certificado com o arquivo vcac-config.exe ao atualizar um certificado de segurança, talvez apareça a seguinte mensagem:

A conexão subjacente foi fechada: não foi possível estabelecer uma relação confiável para o canal seguro de SSL/TLS.

Você pode obter mais informações sobre a causa do problema seguindo o procedimento abaixo.

### Solução

- 1 Abra o arquivo vcac-config.exe.config e localize o endereço do repositório: <add key="repositoryAddress" value="https://[IaaS address]:443/repository/" />
- 2 Navegue para esse endereço usando o Internet Explorer.
- 3 Prossiga pelas mensagens de erro sobre problemas com certificados não confiáveis.

- 4 Obtenha um relatório de segurança do Internet Explorer e use-o para solucionar os problemas com certificados não confiáveis.

Se os problemas persistirem, repita o procedimento navegando com o endereço que precisa ser registrado, o endereço de Endpoint que você usou para registrar o vcac-config.exe.

## Conectar-se à rede por meio de um servidor proxy

Alguns sites podem se conectar à Internet por meio de um servidor proxy.

### Problema

Sua implantação não pode se conectar à Internet aberta. Por exemplo, não é possível acessar sites, nuvens públicas que você gerencia ou endereços de fornecedores dos qual você baixa softwares ou atualizações.

### Causa

Seu site se conecta à Internet por meio de um servidor proxy.

### Solução

#### Pré-requisitos

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

#### Procedimentos

- 1 Aponte um navegador da Web para o console de gerenciamento do vRealize Automation appliance:  
`https://FQDN-ou-endereço-IP-de-appliance:5480`
- 2 Faça login com o nome de usuário **root** e a senha que você definiu quando implantou o appliance.
- 3 Clique na guia **Rede**.
- 4 Insira o FQDN ou endereço IP do servidor proxy local e o número da porta.
- 5 Se o servidor proxy exigir credenciais, insira o nome do usuário e a senha.
- 6 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 o login do usuário do VMware Identity Manager”](#), na página 144.

## Etapas do console para a configuração de conteúdo inicial

Há uma alternativa para usar a interface de instalação do vRealize Automation para criar a conta do administrador de configuração e o conteúdo inicial.

### Problema

Como última parte da instalação do vRealize Automation, você segue o processo para inserir uma nova senha, criar a conta de usuário local configurationadmin e criar o conteúdo inicial. Ocorre um erro, e a interface entra em um estado irreversível.

### Solução

Em vez de usar a interface, insira comandos de console para criar o usuário configurationadmin e o conteúdo inicial. Observe que a interface pode falhar após a conclusão bem-sucedida de uma parte do processo e que, portanto, talvez você apenas precise de alguns dos comandos.

Por exemplo, você pode inspecionar os registros e a execução de fluxos de trabalho do vRealize Orchestrator e determinar que a configuração baseada em interface criou o usuário configurationadmin, mas não o conteúdo inicial. Nesse caso, basta inserir os dois últimos comandos de console para concluir o processo.

### Procedimentos

- 1 Faça login no console do vRealize Automation appliance como root.

- 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.p
y --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.p
y --host $CURRENT_VA_HOSTNAME --username $SSO_ADMIN_USERNAME --password
$SSO_ADMIN_PASSWORD --workflowid ef00fce2-80ef-4b48-96b5-fdee36981770 --
configurationAdminPassword $CONFIGURATIONADMIN_PASSWORD
```

## 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 de vRealize Automation appliance.

#### Problema

O download dos instaladores não ocorre durante a execução de `setup__vra-va-nomedohost.domínio.nome.exe`.

#### Causa

- Ocorrem problemas de conectividade de rede durante a conexão com a máquina vRealize Automation appliance.
- Impossível conectar à máquina do vRealize Automation appliance porque ela não pode ser acessada ou não consegue responder antes que a conexão expire.

#### Solução

- 1 Verifique se você consegue se conectar ao vRealize Automation appliance digitando a seguinte URL em um navegador da Web.

`https://vra-va-nomedohost.domínio.nome`

- 2 Confira os outros tópicos de solução de problemas do vRealize Automation appliance.

- 3 Faça download do arquivo de instalação e reconecte-se ao vRealize Automation appliance.

## O arquivo Encryption.key tem permissões incorretas

Um erro do sistema pode ocorrer quando permissões incorretas são atribuídas ao arquivo Encryption.key de um appliance virtual.

### Problema

Faça login no vRealize Automation appliance e a página Tenants será exibida. Depois que a página tiver começado a carregar, você verá a mensagem **Erro do Sistema**.

### Causa

O arquivo Encryption.key tem permissões incorretas ou o grupo ou o nível do usuário do proprietário foi atribuído incorretamente.

### Solução

#### Pré-requisitos

Faça login no appliance virtual que exibe o erro.

---

**OBSERVAÇÃO** Se os appliances virtuais estiverem sendo executados sob um balanceador de carga, você deverá verificar cada appliance virtual.

---

#### Procedimentos

- 1 Exiba o arquivo de log `/var/log/vcac/catalina.out` e procure a mensagem `Não é possível gravar em /etc/vcac/Encryption.key`.
- 2 Vá até o diretório `/etc/vcac/` e verifique as permissões e a propriedade do arquivo Encryption.key. Você deverá ver uma linha semelhante à seguinte:
 

```
-rw----- 1 vcac vcac 48 Dec 4 06:48 encryption.key
```

A permissão de leitura e gravação é necessária, e o proprietário e grupo do arquivo devem ser `vcac`.
- 3 Se a saída que você vir for diferente, altere as permissões ou a propriedade do arquivo, conforme necessário.

### Próximo passo

Faça login na página Tenant para verificar se você pode fazer login sem erros.

## O Identity Manager não inicia após o reinício do espaço de trabalho do Horizon

Em um ambiente de alta disponibilidade vRealize Automation, o Identity Manager pode não iniciar 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:

Erro ao criar o bean com o nome "liquibase" definido no recurso de caminho de classe [spring/datastore-wireup.xml]: a invocação de método init falhou; a exceção aninhada é liquibase.exception.LockException: não foi possível adquirir o bloqueio do log de alteração. Atualmente bloqueado por fe80:0:0:0:250:56ff:fea8:7d0c%eth0 (fe80:0:0:0:250:56ff:fea8:7d0c%eth0) desde 29/10/15

### Causa

O Identity Manager pode não iniciar 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 no vRealize Automation appliance usando o SSH.
- 2 Execute o comando `service horizon-workspace` para interromper o serviço do espaço de trabalho do Horizon.
- 3 Execute o comando `su postgres` para se tornar um usuário Postgres.
- 4 Execute o comando `psql vcac`.
- 5 Execute esta consulta SQL: `"update "databasechangelock" set locked=FALSE, lockgranted=NULL, lockedby=NULL where id=1;"`
- 6 Execute a consulta SQL `select *` do `databasechangelock`.  
A saída deve mostrar um valor de "f" para bloqueado.
- 7 Inicie o serviço do espaço de trabalho do Horizon usando o comando `service horizon-workspace start`.

## Atribuições de funções de appliance incorretas após o failover

Após um failover, os nós mestre e de réplica do vRealize Automation appliance 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 vRealize Automation appliances, você encerra o nó do banco de dados mestre ou o torna inacessível. Você pode usar o console de gerenciamento em outro nó para promover esse nó como o novo mestre, o que restaura o acesso de gravação ao banco de dados do vRealize Automation.

Mais tarde, você recoloca o velho nó mestre online, mas a guia Banco de Dados em seu console de gerenciamento ainda lista o nó como o nó mestre, mesmo ele não sendo. Há falhas nas tentativas de usar qualquer console de gerenciamento de nós para resolver o problema promovendo oficialmente o nó antigo de volta como mestre.

### Solução

Quando o failover ocorrer, siga estas diretrizes ao configurar os nós mestres antigos versus novos.

- Antes de promover outro nó como mestre, remova o nó mestre anterior do pool de balanceadores de carga de nós do vRealize Automation appliance.
- Para que o vRealize Automation recoloca um nó mestre antigo no cluster, deixe a máquina antiga ficar online. Em seguida, abra o console de gerenciamento do novo mestre. Olhe para o nó antigo listado como `invalid` na guia Banco de Dados e clique em seu botão **Redefinir**.

Após uma restauração bem-sucedida, você pode restaurar o nó antigo para o pool de balanceadores de carga de nós do vRealize Automation appliance.

- Para recolocar um nó mestre antigo ao 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 vRealize Automation appliance.

- Até que você faça a redefinição ou a nova união do nó mestre antigo corretamente no cluster, não use seu console de gerenciamento para operações de gerenciamento de cluster, mesmo se o nó tiver voltado a ficar online.
- Depois de realizar a redefinição ou a nova união corretamente, você poderá promover um nó antigo de volta como mestre.



## 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.

### 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 appliance e do 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 vRealize Automation appliance 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 vRealize Automation appliance falhou devido a parâmetros msiexec 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 vRealize Automation appliance ou problemas de conectividade entre os dispositivos. Falha em uma tentativa de conexão porque não houve resposta ou a conexão não pôde ser realizada.
- Problemas com certificados confiáveis em um IaaS usando 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 ao vRealize Automation appliance digitando a seguinte URL em um navegador da Web: `https://vra-va-nomedohost.domínio.nome`.

- 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, acesse `https://<ip-web>/repository/data/MetaModel.svc` e verifique se nenhum erro de certificado é exibido no navegador.

- 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, verifique o status do serviço MetaModel acessando `https://<ip-web>/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 o [artigo 2564571 da Base de Dados de Conhecimento Microsoft](#).

### 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 no vRealize Automation appliance.  
`https://nomedoappliancevirtual/vcac/nomedotenant`
  - 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 Manager Service

Os nós de IaaS que são clonados de um modelo no qual o MS DTC está instalado contêm identificadores duplicados para MS DTC, o que impede a comunicação entre os nós.

### Problema

O IaaS Manager Service falha e exibe 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

Quando você clona um nó do IaaS com o MS DTC instalado, ambos os clones usam o mesmo identificador exclusivo para o MS DTC. A comunicação entre os nós falha.

### Solução

- 1 Abra um prompt de comando do Administrador.
- 2 Execute o seguinte comando: **msdtc -uninstall**
- 3 Reinicie a máquina virtual.
- 4 Abra um prompt de comando separado e execute o seguinte comando:  
**msdtc -install <manager-service-host>**.

## 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 `<em>@seudomínio</em>` do nome do usuário, você será desconectado do SSO imediatamente e redirecionado para a página de login sem explicação. </li>

#### 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 `@seudominio` 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 vRealize Automation appliance, os appliances devem ser capazes de se identificar uns aos outros com um nome de host curto. Caso contrário, você não poderá fazer login.

### Problema

Você configura o vRealize Automation para alta disponibilidade instalando um vRealize Automation appliance adicional. 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 vRealize Automation appliance não formarão corretamente um cluster de alta disponibilidade até poderem resolver os nomes de host curtos dos nós no cluster.

## Solução

Para permitir que um cluster de alta disponibilidade vRealize Automation appliances resolva nomes de host curtos, siga qualquer uma destas abordagens. Você deve modificar todos os appliances do cluster.

### Procedimentos

- Edite ou crie uma linha de pesquisa em `/etc/resolv.conf`. A linha deve conter domínios que comportam vRealize Automation appliances. Separe vários domínios com espaços. Por exemplo:

```
search eng.mycompany.com tech.mycompany.com
```

- Edite ou crie linhas de domínio em `/etc/resolv.conf`. Cada linha deve conter um domínio que comporta vRealize Automation appliances. Por exemplo:

```
domain eng.mycompany.com
```

- Adicione linhas ao arquivo `/etc/hosts` para que cada nome curto do vRealize Automation appliance seja mapeado para seu nome de domínio totalmente qualificado. Por exemplo:

```
node1    node1.eng.mycompany.com
node2    node2.eng.mycompany.com
```

## O proxy impede o login do usuário do VMware Identity Manager

A configuração para usar um proxy pode impedir que os usuários do VMware Identity Manager façam login.

### Problema

Você configura o vRealize Automation para acessar a rede por meio de um servidor proxy, e os usuários do VMware Identity Manager visualizam o seguinte erro quando tentam fazer login.

```
Error Unable to get metadata
```

## Solução

### Pré-requisitos

Configure o vRealize Automation para acessar a rede por meio de um servidor proxy. Consulte [“Conectar-se à rede por meio de um servidor proxy”](#), na página 133.



**Procedimentos**

- 1 Faça login no console do vRealize Automation appliance 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=vra-hostname`  
Por exemplo: `NO_PROXY="localhost, 127.0.0.1, vra.system.mycompany.com"`
- 4 Salve e feche proxy.
- 5 Reinicie o serviço de espaço de trabalho Horizon inserindo o seguinte comando.  
`service horizon-workspace restart`



# Instalação silenciosa do vRealize Automation

# 7

O vRealize Automation inclui uma opção para instalação silenciosa com script.

A instalação silenciosa usa um executável que faz referência a um arquivo de resposta baseado em texto, no qual você predefine FQDNs do sistema, credenciais de contas e outras configurações que são normalmente adicionadas ao longo de uma instalação convencional manual ou baseada em assistente. 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

Este capítulo inclui os seguintes tópicos:

- [“Realizar uma instalação silenciosa do vRealize Automation”](#), na página 147
- [“Realizar uma instalação silenciosa do Agente de Gerenciamento do vRealize Automation”](#), na página 148
- [“Arquivo de resposta de instalação silenciosa do vRealize Automation”](#), na página 149
- [“A linha de comando de instalação do vRealize Automation”](#), na página 150

## Realizar uma instalação silenciosa do vRealize Automation

Você pode realizar uma instalação autônoma e silenciosa do vRealize Automation a partir do console de um vRealize Automation appliance recém-implantado.

### Pré-requisitos

- Implante um vRealize Automation appliance, mas não faça login nem inicie o Assistente de Instalação.
- 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”](#), na página 148.

### Procedimentos

- 1 Faça login no console do vRealize Automation appliance como root.

- 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

- Implante o vRealize Automation appliance.
- Crie ou identifique seus servidores Windows IaaS e configure seus pré-requisitos.

### Procedimentos

- 1 No servidor Windows IaaS, aponte um navegador da Web para a seguinte URL no vRealize Automation appliance.

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

- 2 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.

- 3 Abra `InstallManagementAgent.ps1` em um editor de texto.

- 4 Próximo do início do arquivo de script, adicione as configurações específicas da implantação.

- A URL do vRealize Automation appliance

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

- Credenciais da conta do usuário root do vRealize Automation appliance

- 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
- 5 Salve e feche `InstallManagementAgent.ps1`.
  - 6 Para instalar silenciosamente o Agente de Gerenciamento, clique duas vezes em `InstallManagementAgent.ps1`.
  - 7 (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 vRealize Automation appliances 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 vRealize Automation appliance
- Credenciais da conta do usuário root do vRealize Automation appliance
- 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 a linha de comando de instalação do vRealize Automation

A interface de linha de comando de instalação do vRealize Automation tem três operações básicas.

As operações básicas exibem IDs de nó do vRealize Automation, executam comandos ou exibem as informações de ajuda. Para mostrar essas operações na exibição do console, insira o seguinte comando sem opções ou qualificadores.

```
vra-command
```

#### Exibir IDs de nó

Você precisa conhecer os IDs de nó do vRealize Automation para executar comandos nos sistemas de destino corretos. Para exibir IDs de nó, insira o seguinte comando.

```
vra-command list-nodes
```

Anotar os IDs de nó antes de executar comandos.

#### Executar comandos

A maioria das funções de linha de comando envolve executar um comando em um nó no cluster do vRealize Automation. Para executar um comando, use a seguinte sintaxe.

```
vra-command execute --node ID-do-nó nome-do-comando --nome-do-parâmetro valor-do-parâmetro
```

Como mostra a sintaxe anterior, muitos comandos exigem parâmetros e valores de parâmetros escolhidos pelo usuário.

#### Exibir a ajuda

Para exibir informações de ajuda para 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 vRealize Automation appliance 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, acesse o console do vRealize Automation appliance 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
```





# Índice

## A

- acesso ao banco de dados do IaaS, habilitando do usuário de serviço **99**
- Administradores do IaaS, criando **125**
- Agente de gerenciamento
  - desinstalar **37, 44**
  - instalação silenciosa **148**
  - instalando **36, 43**
  - instalar **37, 44**
- agente de proxy, falha na instalação **141**
- agente do VDI para XenDesktop, instalando **112**
- Agente do vSphere
  - configuração compatível para simultaneidade **103**
  - permissões necessárias **103**
- agentes
  - agentes de integração **17**
  - agentes de WMI **17**
  - ativando solicitações WMI remotas **121**
  - configurando agentes do vSphere **107**
  - configurando o Hyper-V **111**
  - configurando o XenServer **111**
  - escolhendo o cenário de instalação **102**
  - Hyper-V **108**
  - instalando **101**
  - instalando a WMI **121**
  - instalando agentes do Citrix **116**
  - instalando agentes do vSphere **105**
  - instalando o agente do EPI para Citrix **115**
  - instalando o agente do EPI para scripts do VB **118**
  - instalando o XenDesktop **113**
  - instalando para scripts do Visual Basic **119**
  - localização e requisitos de instalação **103**
  - PowerShell de EPI **17**
  - PowerShell de VDI **17**
  - requisitos de script do Visual Basic **118**
  - XenServer **108**
- agentes de proxy, instalando e configurando para vSphere **103**
- agentes de proxy de virtualização **17**
- agentes de proxy do vSphere, instalando e configurando **103**
- agentes de WMI
  - ativando solicitações remotas **121**
  - instalando **121**
- agentes do Citrix, instalando **116**

- agentes do EPI, instalando para scripts do Visual Basic **118, 119**
- agentes do Hyper-V, instalando **108**
- agentes do vSphere
  - configurando **107**
  - exigindo um certificado confiável **107**
  - instalando **105**
- agentes do XenServer, instalando **108**
- appliance do vRealize Automation, implantando **68**
- Appliances do vRealize Automation, solucionando problemas **134**
- arquivo de resposta, instalação silenciosa **149**
- arquivo Encryption.key, definindo permissões **135**
- arquivos PEM, comando para extração **31**
- arquivos pfx, configurar a confiança de certificado **66**
- assistente de instalação, implantação corporativa **42**
- Assistente de Instalação, visão geral **33**
- autenticação **100**
- Autenticação do IaaS, falha **138**
- Autenticação do Windows **100**
- autenticação em tempo de execução **100**
- Autenticação SQL **100**

## B

- balanceadores de carga
  - configurando **70**
  - verificações de integridade **65**
- banco de dados do IaaS
  - configurando o Windows Service para acesso **99**
  - configurando para SSL seguro **60, 80–83**
  - criando o banco de dados **82**
  - criando o banco de dados manualmente **81**
  - criando o banco de dados usando o assistente **83**
  - especificando o banco de dados SQL **60**
- banco de dados
  - criando usando o assistente **83**
  - preparando o banco de dados do IaaS **80**
  - requisitos **21**

## C

- cadeia de certificados, ordem **30**
- caminho de implantação
  - instalação distribuída **11**
  - selecionando **11**
- casos de uso, instalação silenciosa **147**
- cenário de implantação
  - instalação distribuída **63**
  - instalação mínima **51**
  - instalação mínima **11**
- cenários, escolhendo a instalação do agente **102**
- certificados
  - mudando de autoassinado **125**
  - relações confiáveis **65**
- certificados encadeados, ordem **30**
- certificados SSL, extraindo **31**
- chaves privadas RSA, comando para extração **31**
- Citrix, instalando o agente do EPI **115**
- clusters do vRealize Appliance;unindo **76**
- clusters; unindo **76**
- componente Website, instalando **85, 87, 89**
- componentes da instalação
  - Appliance do VMware vRealize Automation **15**
  - escolhendo o caminho de implantação **11**
  - Infraestrutura como Serviço (IaaS) da VMware **15**
  - SSO **14**
  - verificando pré-requisitos **60**
- componentes de infraestrutura, instalando **58**
- Componentes do IaaS
  - instalando **57**
  - instalando em uma configuração distribuída **77**
  - registrando **62**
  - solucionando problemas **137**
- componentes do IaaS, definições **64**
- Configuração de conteúdo inicial, criar senha **42, 49**
- configurações da conta, especificando **60**
- configurações de hora do appliance virtual, com o assistente de instalação **39, 46**
- configurações do servidor, especificando **60**
- configurar, appliance do vRealize Automation **71**
- Coordenador de Transações Distribuídas (DTC) **21**
- criação do conteúdo inicial, solucionando problemas **133**

## D

- DEM
  - instalando **97**
  - requisitos **23**

- requisitos do Openstack **25**
- requisitos do PowerVC **25**
- sobre a instalação **96**
- DEM Worker, conectando ao SCVMM **98**
- dems
  - Requisitos do Amazon Web Services EC2 **24**
  - Requisitos do Red Hat **25**
  - requisitos do SCVMM **25**
- DEMs, falha na instalação **138**
- desinstalar, instalação falhou **129**
- Desinstalar, instalação falhou **129**
- dispositivo do vRealize Automation **70**
- dispositivos, configurando instâncias adicionais **75**
- Distributed Execution Manager, *Consulte* DEM
- Distributed Execution Managers, *Consulte também* DEM
- download da instalação, solução de problemas **134**
- DTC (Coordenador de Transações Distribuídas) **21**

## E

- Endpoints
  - requisitos de DEM do Openstack **25**
  - requisitos de DEM do PowerVC **25**
- erro interno, adicionando o endpoint do XaaS **140**
- Erros de login, solução de problemas **143**

## F

- falha na instalação, servidores fora de sincronia **131**
- falha nas solicitações de máquina **141**
- falha no login
  - servidores fora de sincronia **131**
  - solucionando problemas **144**
- falha no login do administrador do IaaS **143**
- Federal Information Processing Standard (FIPS) **140**
- FIPS (Federal Information Processing Standard) **140**

## H

- Hipervisor, requisitos **108**
- Hyper-V
  - agente **108**
  - agente de proxy **108**
  - requisitos **108**

## I

- IaaS
  - agentes **17**
  - fazer download do instalador **79**
- IaaS Manager Service, requisitos **23**

- identity manager, não inicia **135**
- IDs de nó **150**
- Implantação corporativa, instalar com assistente **43**
- implantação distribuída
  - desabilitar serviços não utilizados **77**
  - instalar com assistente **43**
  - validando **77**
  - visão geral da instalação **13**
- implantação mínima, visão geral da instalação **12**
- Implantações mínimas, instalar com o assistente de instalação **35**
- Impressão digital do SSL de agente de gerenciamento, localizando **36, 43**
- incompatibilidade entre nomes de certificado **139**
- informações atualizadas **9**
- instalação
  - appliance do vRealize Automation **52**
  - concluindo **40, 47, 62**
  - dispositivo do vRealize Automation **70**
  - DNS e resolução de nome de host **19**
  - especificando agentes **61**
  - especificando gerentes **61**
  - pós-instalação **125**
  - preparação **19**
  - solucionando problemas **127**
  - visão geral **11**
  - visão geral da implantação distribuída **13**
  - visão geral da implantação mínima **12**
  - visão geral da instalação mínima **52**
- Instalação, usando o console de gerenciamento **51**
- instalação distribuída
  - desinstalando **129**
  - visão geral **63**
- instalação distribuída do IaaS **64**
- instalação falhou, registros **127**
- instalação mínima, desinstalando **129**
- instalação silenciosa
  - Agente de gerenciamento **148**
  - arquivo de resposta **149**
  - casos de uso **147**
  - vRealize Automation **147**
- Instalador do IaaS
  - baixando **59**
  - solução de problemas **137**
- instalando
  - configurando dispositivos para o vCloud Automation Center **70**
  - considerações sobre o navegador **20**
  - fazer download do instalador do IaaS **79**
  - planilha **66**

## L

- linha de comando **150**
- Log Insight **125**

## M

- Manager Service
  - definição **64**
  - instalando **91, 94**
  - requisitos **23**
- mensagem de erro do sistema **135**
- Model Manager
  - definição **64**
  - lógica de negócios editável **15**
  - modelo de dados unificado **15**
  - políticas de execução **15**
  - solução de problemas causados por falhas de instalação **139**
  - vários tenants protegidos **15**
- Model Manager Data, instalando **85, 87, 89**
- Model Manager Web **15**

## N

- nó mestre incorreto **136**
- Nome do Host do XenServer, definindo **113**
- Nós de IaaS clonados **142**

## O

- Openstack, requisitos de DEM **25**

## P

- pacote de suporte, criando **130**
- parâmetro de instalação, validação **41, 48**
- parâmetros de implantação, especificando **40, 47**
- Personalizações de e-mail **143**
- pós-instalação **125**
- PowerShell, definindo como RemoteSigned **102**
- PowerVC, requisitos de DEM **25**
- pré-requisitos
  - considerações sobre o navegador **20**
  - verificando **60**
- preparação da instalação, sincronização de hora **31**
- problemas com certificados confiáveis **139**
- proxy **144**

## R

- registros
  - coletando **130**
  - localizações **127**
- Registros
  - IaaS **127**
  - solucionando problemas **127**
- repositório de identidades, requisitos do domínio **29**

## requisitos

- bancos de dados **21**
- DEM **23**
- SQL **21**
- requisitos de instalação
  - ambientes de implantação **20**
  - credenciais **29**
  - hardware **20**
  - máquina virtual **20**
  - requisitos de porta **26**
  - requisitos do IaaS **22**
  - segurança **30**
  - sistema operacional **20**
  - usuários **29**
  - Windows Server **21**
  - XenDesktop **112**
- requisitos de servidor, servidor do IaaS ou Windows **22**
- requisitos Java, do banco de dados MSSQL **22**

## S

- scripts do Visual Basic
  - instalando agentes do EPI **119**
  - instalando o agente do EPI **118**
- segurança
  - certificados **30**
  - certificados do IaaS **58, 79**
  - relações confiáveis **65**
  - senha **31**
  - software de terceiros **31**
- senha, restrições **21**
- serviço de gerenciador, confiança de certificado **66**
- Serviços do IaaS, verificando **101**
- servidor de provisionamento **115**
- sincronização de horário, servidores **54, 75**
- sincronização de horas, ativando na máquina Windows **58**
- snapshots, criando **40, 47**
- solução de problemas
  - horas de servidor fora de sincronia **131**
  - Instalador do IaaS **137**
  - nós de IaaS clonados **142**
  - páginas em branco exibidas **132**
- solução de problemas com a instalação **131**
- solucionando problemas
  - localizações de registro **127**
  - nó mestre incorreto **136**
  - solicitações de máquina **141**
- solucionando problemas, instalação **127**
- SQL, requisitos **21**

## T

- tarefas pós instalação, configurando o Windows Service para acessar o banco de dados do IaaS **99**
- tempo limite atingido do balanceador de carga antes da conclusão, alterando a configuração de tempo limite do balanceador de carga **131**
- tenants, configurando o tenant padrão **125**
- tipo de instalação
  - fazendo login **59**
  - selecioneando **59**

## V

- validação de certificado **137**
- vCloud Suite, licenciamento **7**
- verificações de integridade **65**
- Verificador de pré-requisitos, executar o assistente de instalação **39, 46**
- Visual Basic, requisitos de script **118**
- VMware IaaS
  - distributed execution manager **16**
  - manager service **16**
- Vmware IaaS, banco de dados **16**
- VMware IaaS, Model Manager **15**
- VMware IaaS, Site do IaaS **15**
- VMware Identity Manager **144**
- vRealize Appliance
  - configurando **55**
  - implantando **33, 52**
- vRealize Orchestrator, usar externo para implantações de alta disponibilidade **63**

## W

- WAPI, falha na instalação **138**

## X

- XenDesktop
  - instalando o agente **113**
  - instalando um agente do VDI **112**
  - requisitos de instalação **112**
- XenServer
  - agente **108**
  - agente de proxy **108**