

Gerenciando o vRealize Automation

21 de julho de 2021

vRealize Automation 7.6

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

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

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

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

Copyright © 2015-2021 VMware, Inc. Todos os direitos reservados. [Informações sobre direitos autorais e marca registrada.](#)

Conteúdo

- 1 Fazendo a manutenção e a personalização de componentes e opções do vRealize Automation 5**
 - [Transmitir uma mensagem para todos os usuários 5](#)
 - [Criar uma lista de permissões de URLs para o quadro de mensagens 7](#)
 - [Iniciando e desligando o vRealize Automation 8](#)
 - [Iniciar o vRealize Automation 8](#)
 - [Reiniciar o vRealize Automation 9](#)
 - [Desligar o vRealize Automation 11](#)
 - [Atualizando certificados do vRealize Automation 12](#)
 - [Extraindo certificados e chaves privadas 14](#)
 - [Substituir certificados no appliance vRealize Automation 14](#)
 - [Substituir o certificado de Infraestrutura como Serviço 17](#)
 - [Substituir o certificado do IaaS Manager Service 19](#)
 - [Atualizar vRealize Orchestrator integrado para confiar em certificados do vRealize Automation 21](#)
 - [Atualizar o vRealize Orchestrator externo para confiar em certificados do vRealize Automation 24](#)
 - [Atualizando o certificado do site de gerenciamento do appliance do vRealize Automation 24](#)
 - [Substituir um certificado do Agente de gerenciamento 29](#)
 - [Alterar o método de sondagem para certificados 32](#)
 - [Gerenciando o banco de dados do appliance do Postgres do vRealize Automation 33](#)
 - [Configurar o Appliance Database 34](#)
 - [Três cenários de failover automático do banco de dados do appliance do nó 36](#)
 - [Cenário: realizar o failover de banco de dados do dispositivo manual 39](#)
 - [Cenário: realizar o failover de banco de dados de manutenção 40](#)
 - [Recupere Manualmente o Banco de Dados do Appliance de Falha Catastrófica 42](#)
 - [Backup e recuperação de instalações do vRealize Automation 44](#)
 - [Programa de Aperfeiçoamento da Experiência do Cliente 44](#)
 - [Participar ou sair do Programa de Aperfeiçoamento da Experiência do Cliente de vRealize Automation 44](#)
 - [Configurar o tempo de coleta de dados 45](#)
 - [Ajustando as configurações do sistema 45](#)
 - [Modificar o ícone Todos os Serviços no catálogo de serviços 46](#)
 - [Personalizar configurações de sobreposição de dados 47](#)
 - [Ajustando configurações no arquivo de configuração do serviço de gerenciador 50](#)
 - [Monitoramento vRealize Automation 55](#)
 - [Monitorando fluxos de trabalho e exibindo registros 55](#)
 - [Monitorando logs e serviços de evento 56](#)

Usar o log de auditoria do vRealize Automation	58
Visualizando informações de host para clusters em ambientes distribuídos	60
Monitorando a integridade do vRealize Automation	62
Configurar testes do sistema para o vRealize Automation	63
Configurar testes de tenant para o vRealize Automation	65
Configurar testes para o vRealize Orchestrator	67
Pacote de testes personalizado	69
Visualizar os resultados do pacote de testes do serviço de integridade do vRealize Automation	71
Solucionando problemas com o serviço de integridade	71
Monitoramento de recursos de ambiente do vRealize Automation usando SNMP	72
Monitorando e gerenciando recursos	73
Escolhendo um cenário de monitoramento de recursos	73
Terminologia de uso de recurso	74
Conectando a uma máquina na nuvem	75
Reduzindo o uso de reserva por atrito	78
Desativando um caminho de armazenamento	78
Coleta de dados	79
Noções básicas sobre a verificação de alocação do vSwap para endpoints do vCenter Server	83
Removendo localizações do datacenter	84
Monitorização de contentores	84
Importação em massa, atualização ou migração de máquinas virtuais	84
Importar uma máquina virtual para um ambiente do vRealize Automation	86
Atualizar uma máquina virtual em um ambiente do vRealize Automation	90
Migrar uma máquina virtual para um ambiente do vRealize Automation diferente	93

Fazendo a manutenção e a personalização de componentes e opções do vRealize Automation

1

Você pode gerenciar máquinas provisionadas e outros aspectos da implantação do vRealize Automation.

Este capítulo inclui os seguintes tópicos:

- [Transmitir uma mensagem para todos os usuários](#)
- [Iniciando e desligando o vRealize Automation](#)
- [Atualizando certificados do vRealize Automation](#)
- [Gerenciando o banco de dados do appliance do Postgres do vRealize Automation](#)
- [Backup e recuperação de instalações do vRealize Automation](#)
- [Programa de Aperfeiçoamento da Experiência do Cliente](#)
- [Ajustando as configurações do sistema](#)
- [Monitoramento vRealize Automation](#)
- [Monitorando a integridade do vRealize Automation](#)
- [Monitoramento de recursos de ambiente do vRealize Automation usando SNMP](#)
- [Monitorando e gerenciando recursos](#)
- [Monitorização de contentores](#)
- [Importação em massa, atualização ou migração de máquinas virtuais](#)

Transmitir uma mensagem para todos os usuários

Como administrador de tenants, você pode transmitir uma mensagem para todos os usuários. A notificação de mensagem é exibida no topo da página do navegador. Seus usuários clicam na notificação para ver a mensagem.

Como usuário, você pode acessar a mensagem pelo banner ou pelo menu suspenso de usuário no cabeçalho.



Você usa o quadro de mensagens para transmitir uma mensagem de texto ou uma página da Web. Dependendo da página da Web, seus usuários podem navegar pelo site no quadro de mensagens.

O quadro de mensagens tem as seguintes limitações.

Tabela 1-1. Limitações do quadro de mensagens

Opção	Limitações
Limitações de mensagens de URL	<ul style="list-style-type: none"> ■ A URL de destino deve ser incluída na lista de permissões do quadro de mensagens. Consulte Criar uma lista de permissões de URLs para o quadro de mensagens. ■ Você só pode publicar conteúdo que esteja hospedado em um site https. ■ Você não pode usar certificados autoassinados. A opção para aceitar o certificado não aparece no quadro de mensagens. ■ A URL do quadro de mensagens está incorporada a um iframe. Alguns sites não funcionam em iframe e exibem um erro. Uma das causas da falha é X-Frame-Options DENY ou SAMEORIGIN no cabeçalho do site de destino. Se o seu site de destino for um site que você controla, será possível definir o cabeçalho X-Frame-Options como X-Frame-Options: ALLOW-FROM https://<vRealizeAutomationApplianceURL>. ■ Alguns sites têm um redirecionamento para uma página de nível superior que pode atualizar a página inteira do vRealize Automation. Esse tipo de site não funciona no quadro de mensagens. A atualização é suprimida e uma mensagem Carregando... aparece no quadro de mensagens. ■ Se você exibir uma página HTML interna, essa página não poderá ter o host do vRealize Automation como a URL.
Limitações de mensagens personalizadas	<ul style="list-style-type: none"> ■ Para manter a segurança, a Mensagem Personalizada permite a marcação simples, mas não é compatível com código HTML. Por exemplo, não é possível usar <href> para criar um link para um site. Você deve usar a opção de mensagem URL.

Pré-requisitos

Faça login no vRealize Automation como **administrador de tenants**.

Procedimentos

- 1 Clique na guia **Administração**.
- 2 Selecione **Notificações > Quadro de Mensagens**
- 3 No menu suspenso **Tipo**, selecione o tipo de mensagem.

Opção	Descrição
Nenhuma	Remove a notificação de mensagem.
Mensagem Personalizada	Insira uma mensagem de texto sem formatação.
URL	<p>Insira a URL da página.</p> <p>A URL deve ser incluída na lista de permissões do quadro de mensagens. Consulte Criar uma lista de permissões de URLs para o quadro de mensagens.</p> <p>Para fazer login do usuário em um site, mais frequentemente seu site interno, com base no ID de usuário do vRealize Automation dele, selecione Incluir ID de usuário. A URL que será transmitida para o site semelhante a <code>http://company.com/internal/message?userID=richard_dawson@company.com</code>. Esse método permite que seu site use a propriedade de JavaScript de <code>window.location.search</code> para fornecer a ID do usuário atual ao seu site.</p>

- 4 Clique em **OK**.

Resultados

A mensagem será transmitida como um banner para todos os seus usuários do tenant.

Para alterar ou remover a mensagem, você deve estar conectado como administrador de tenants. Para alterar a mensagem, repita as mesmas etapas. Para remover a mensagem, selecione Nenhum como o Tipo e clique em **OK**.

Criar uma lista de permissões de URLs para o quadro de mensagens

Como administrador de segurança, você configura uma lista de URLs permitidas que pode ser usada no quadro de mensagens. Essa lista de permissões garante segurança adicional.

Pré-requisitos

Faça login no vRealize Automation como um **administrador de segurança**.

Procedimentos

- 1 Selecione **Administração > Lista de Permissões do Quadro de Mensagens**.
- 2 Clique em **Novo**.

3 Adicione uma URL e clique em **OK**.

As entradas de URL podem incluir o conteúdo a seguir:

- Endereço IP ou FQDN de um site. Por exemplo, <https://docs.vmware.com>.
- Inclui https.
- Pode incluir portas permitidas. Se uma porta não for especificada, as portas permitidas serão 80 e 443.

4 Repita para cada entrada adicional.

Resultados

Um administrador de tenant não pode adicionar uma URL ao quadro de mensagens, a menos que esteja incluída na lista.

Próximo passo

Verifique se você pode adicionar e transmitir uma URL incluída na lista de permissões do quadro de mensagens. Consulte [Transmitir uma mensagem para todos os usuários](#).

Iniciando e desligando o vRealize Automation

O administrador do sistema executa uma inicialização ou desligamento controlado do vRealize Automation para preservar a integridade do sistema e dos dados.

Também é possível usar uma inicialização e desligamento controlado para resolver problemas de comportamento do produto ou de desempenho que podem ser resultado de uma inicialização incipiente incorreta. Use o procedimento de reinicialização quando apenas alguns componentes da implantação falharem.

Iniciar o vRealize Automation

Ao iniciar o vRealize Automation depois que ele for desligado por qualquer motivo esperado ou inesperado, você deverá iniciar os componentes em uma ordem especificada.

Se você estiver gerenciando componentes de implantação no vCenter Server, poderá iniciar seus sistemas operacionais guest a partir daí.

Pré-requisitos

Confirme que os balanceadores de carga que sua implantação usa estão executando.

Procedimentos

- 1 Se você estiver usando um banco de dados PostgreSQL autônomo legado, inicie esse servidor.
- 2 Em qualquer ordem, inicie os servidores vRealize Automation MS SQL autônomos.
- 3 Em uma implantação que usa balanceadores de carga com verificações de integridade, desative todas as verificações de integridade, exceto pings.

- 4 Inicie o dispositivo do vRealize Automation primário.
 - 5 Na interface de gerenciamento de dispositivo do vRealize Automation primário, olhe na guia **Cluster** para verificar se o sistema está no modo síncrono ou assíncrono. Uma implantação de dispositivo único é sempre assíncrona.
 - Se a implantação for síncrona, inicie os dispositivos do vRealize Automation restantes.
 - Se a implantação for assíncrona, vá para a interface de gerenciamento de dispositivo primária do vRealize Automation e aguarde até que o serviço de licenciamento esteja em execução e REGISTRADO.

Em seguida, inicie todos os dispositivos do vRealize Automation restantes.
 - 6 Depois que todos os dispositivos tiverem iniciado, use suas interfaces de gerenciamento para verificar se os serviços estão em execução e REGISTRADOS.
- Pode demorar 15 minutos ou mais para os appliances iniciarem.
- 7 Inicie todos os nós da Web do IaaS e aguarde 5 minutos.
 - 8 Inicie o nó primário do Manager Service e aguarde de 2 a 5 minutos.
 - 9 Em uma implantação distribuída com vários nós do Manager Service, inicie os nós do Manager Service secundário e aguarde de 2 a 5 minutos.
- Em máquinas secundárias, não inicie ou execute o serviço do Windows, a menos que tenha feito a configuração para failover automático do Serviço de Gerenciador.
- 10 Em qualquer ordem, inicie o DEM Orchestrator, os DEM Workers e todos os agentes de proxy do vRealize Automation.
- Você não precisa esperar que uma inicialização termine antes de iniciar outra.
- 11 Se você tiver que desativar as verificações de integridade do balanceador de carga, ative-as novamente.
 - 12 Verifique se os serviços iniciados estão em execução e REGISTRADOS.
 - a Em um navegador, faça login na interface de gerenciamento do dispositivo primário do vRealize Automation.

<https://vrealize-automation-appliance-FQDN:5480>

 - b Clique na guia **Serviços**.
 - c Monitore o andamento da inicialização do serviço clicando em **Atualizar**.

Resultados

Quando todos os serviços estão REGISTRADOS, a implantação está pronta.

Reiniciar o vRealize Automation

Reiniciar os componentes do vRealize Automation pode ajudar a resolver problemas. Você deve reiniciar os componentes em uma ordem especificada.

Se você estiver gerenciando componentes de implantação no vCenter Server, poderá reiniciar seus sistemas operacionais guest a partir daí.

Se você não puder executar uma reinicialização, tente as instruções em [Desligar o vRealize Automation](#) e [Iniciar o vRealize Automation](#).

Pré-requisitos

- Verifique se todos os balanceadores de carga que sua implantação usa estão em execução.

Procedimentos

- 1 Verifique se o banco de dados do dispositivo do vRealize Automation está definido no modo assíncrono. Se necessário, use a interface de gerenciamento para alterá-la para o modo assíncrono.

Você pode retornar ao modo síncrono depois de concluir o procedimento inteiro. Consulte [Gerenciando o banco de dados do appliance do Postgres do vRealize Automation](#) para obter mais informações.

- 2 Reinicie o dispositivo primário do vRealize Automation e aguarde o término da inicialização.
- 3 Use a interface de gerenciamento do dispositivo primário do vRealize Automation para verificar se o serviço de licenciamento está em execução e REGISTRADO.
- 4 Reinicie os dispositivos restantes do vRealize Automation ao mesmo tempo.

- 5 Aguarde até que os dispositivos sejam reiniciados e use suas interfaces de gerenciamento para verificar se os serviços estão em execução e REGISTRADOS.

Pode demorar 15 minutos ou mais para os dispositivos reiniciarem.

- 6 Reinicie o nó primário da Web e aguarde o término da inicialização.
- 7 Se você estiver executando uma implantação distribuída com vários nós da Web, reinicie os nós da Web secundários e aguarde a conclusão das inicializações.
- 8 Reinicie os nós do Serviço de Gerenciador e aguarde o término da inicialização.

Se você estiver executando o failover automático do Serviço de Gerenciador e quiser manter iguais os nós ativos e passivos, reinicie na seguinte ordem:

- a Interrompa os nós passivos do Serviço de Gerenciador sem reiniciá-los.
- b Reinicie o nó ativo do Serviço de Gerenciador completamente.
- c Inicie os nós passivos do Serviço de Gerenciador.

- 9 Em qualquer ordem, reinicie o DEM Orchestrator, os DEM Workers e todos os agentes de proxy do vRealize Automation. Aguarde até que todas as inicializações sejam concluídas.

Você não precisa esperar que uma reinicialização termine antes de reiniciar outra.

10 Verifique se os serviços reiniciados estão em execução e REGISTRADOS.

- a Em um navegador, faça login na interface de gerenciamento do dispositivo primário do vRealize Automation.

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

- b Clique na guia **Serviços**.
- c Monitore o andamento da inicialização do serviço clicando em **Atualizar**.

Resultados

Quando todos os serviços estão REGISTRADOS, a implantação está pronta.

Desligar o vRealize Automation

Para preservar a integridade dos dados, você deve desligar o vRealize Automation em uma ordem especificada.

Se você estiver gerenciando componentes de implantação no vCenter Server, poderá encerrar seus sistemas operacionais guest a partir daí.

Procedimentos

- 1** Em qualquer ordem, encerre o DEM Orchestrator, os DEM Workers e todos os agentes de proxy do vRealize Automation. Aguarde o término do encerramento.
- 2** Encerre os nós do Serviço de Gerenciador e aguarde o término do encerramento.
- 3** Em implantações distribuídas com vários nós da Web, encerre os nós da Web secundários e aguarde o término do encerramento.
- 4** Encerre o nó da Web primário e aguarde o término do encerramento.
- 5** Em implantações distribuídas com vários dispositivos do vRealize Automation no modo síncrono, use a interface de gerenciamento do dispositivo do vRealize Automation para mudar para o modo assíncrono.
- 6** Em implantações distribuídas com vários dispositivos do vRealize Automation, encerre os dispositivos secundários e aguarde o término do encerramento.
- 7** Encerre o dispositivo do vRealize Automation primário e aguarde o término do encerramento.

O dispositivo do vRealize Automation primário é aquele que contém o banco de dados do dispositivo, principal ou gravável. Anote qual dispositivo é primário para que você possa iniciar o backup na ordem correta.
- 8** Em qualquer ordem, encerre todos os servidores vRealize Automation MS SQL autônomos e aguarde o término do encerramento.
- 9** Se você estiver usando um banco de dados PostgreSQL autônomo legado, encerre esse servidor.

Atualizando certificados do vRealize Automation

Um administrador de sistema pode atualizar ou substituir certificados para componentes do vRealize Automation.

O vRealize Automation contém três componentes principais que usam certificados SSL para facilitar a comunicação segura entre si:

- Appliance do vRealize Automation
- Componente de site IaaS
- Componente de serviço de gerenciador IaaS

Além disso, sua implantação pode ter certificados para o site da interface de gerenciamento do Appliance do vRealize Automation. Além disso, cada máquina IaaS executa um Agente de gerenciamento que usa um certificado.

Observação O vRealize Automation usa vários produtos de terceiros, como o Rabbit MQ, para oferecer suporte a uma variedade de funcionalidades. Alguns desses produtos usam seus próprios certificados autoassinados que persistirão mesmo se você substituir os principais certificados do vRealize Automation por certificados fornecidos por uma autoridade de certificação (CA). Devido a essa situação, os usuários não podem controlar efetivamente o uso de certificados em portas específicas, como a porta 5671 que é usada pelo RabbitMQ para comunicação interna.

Com uma exceção, as alterações nos últimos componentes desta lista não afetam os primeiros. A exceção é que um certificado atualizado para componentes do IaaS deve ser registrado no vRealize Automation.

Em geral, certificados autoassinados são gerados e aplicados a esses componentes durante a instalação do produto. Talvez seja necessário substituir um certificado para mudar de certificados autoassinados para certificados fornecidos por uma autoridade de certificação ou quando um certificado expira. Quando você substitui um certificado para um componente do vRealize Automation, relacionamentos de confiança para outros componentes do vRealize Automation são atualizados automaticamente.

Por exemplo, em um sistema distribuído com várias instâncias de um Appliance do vRealize Automation, se você atualizar um certificado para um Appliance do vRealize Automation, todos os outros certificados relacionados serão atualizados automaticamente.

Observação O vRealize Automation oferece suporte para certificados SHA2. Os certificados autoassinados gerados pelo sistema usam Criptografia SHA-256 com RSA. Talvez seja necessário atualizar para certificados SHA2 devido a requisitos de navegador ou sistema operacional.

A interface de gerenciamento de dispositivo do vRealize Automation fornece opções para atualizar ou substituir certificados.

Em uma implantação agrupada em cluster, você deve iniciar alterações a partir da interface do nó primário.

- **Gerar certificado** — O vRealize Automation gera um certificado autoassinado.
- **Importar certificado** — Use seu próprio certificado.
- **Fornecer impressão digital do certificado** — Forneça uma impressão digital do certificado para usar um certificado que já esteja no repositório de certificados em servidores Windows do IaaS.

Usar essa opção não transmite o certificado do dispositivo do vRealize Automation para os servidores Windows do IaaS. A opção permite que os usuários implantem certificados existentes em servidores Windows do IaaS sem carregar os certificados na interface de gerenciamento de dispositivo do vRealize Automation.

- **Manter Existente** — Continue a usar o certificado atual.

Certificados para o site da interface de gerenciamento do dispositivo do vRealize Automation não têm requisitos de registro.

Observação Se o seu certificado usar uma senha para criptografia e você não inseri-la ao substituir seu certificado no dispositivo, a substituição do certificado falhará, e a mensagem `Unable to load private key` será exibida.

Modelos de máquina virtual

Depois de alterar os certificados do dispositivo do vRealize Automation ou do servidor Windows do IaaS, você deve atualizar os agentes de software e convidado do vRealize Automation nos modelos de máquina virtual para que os modelos funcionem novamente no vRealize Automation. Se você não atualizar os agentes, as solicitações de implantação que envolvem componentes de software falharão com um erro semelhante ao exemplo a seguir.

```
The following component requests failed: Linux. Request failed: Machine VM-001:
InstallSoftwareWorkflow. Install software work item timeout.
```

vRealize Orchestrator

Depois de alterar os certificados do vRealize Automation, você deve atualizar o vRealize Orchestrator para confiar nos novos certificados.

O componente do vRealize Orchestrator associado à sua implantação do vRealize Automation tem seus próprios certificados, mas ele também deve confiar nos certificados do vRealize Automation. Por padrão, o componente do vRealize Orchestrator é incorporado no vRealize Automation, embora alguns usuários optem por usar um vRealize Orchestrator externo. Em ambos os casos, consulte a documentação do vRealize Orchestrator para obter mais informações sobre como atualizar certificados do vRealize Orchestrator.

Se você executar uma implantação do vRealize Orchestrator de vários nós atrás de um balanceador de carga, todos os nós do vRealize Orchestrator deverão usar o mesmo certificado.

Para obter mais informações

Para obter mais informações sobre solução de problemas, suporte e requisitos de confiança para certificados, consulte o [artigo da base de dados de conhecimento 2106583 da VMware](#).

Extraindo certificados e chaves privadas

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

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

Tabela 1-2. 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</i> <i>certificate_file</i> -nocerts -out key.pem</code>	Chave privada RSA
Arquivo PEM	<code>openssl pkcs12 -in <i>path_to_.pfx</i> <i>certificate_file</i> -clcerts -nokeys -out cert.pem</code>	Cadeia de certificados
(Opcional) Código de acesso	n/d	Código de acesso

Substituir certificados no appliance vRealize Automation

O administrador de sistema pode atualizar ou substituir um certificado autoassinado por um certificado confiável de uma autoridade de certificação. 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.

Quando você atualiza ou substitui o certificado do dispositivo do vRealize Automation, a confiança com outros componentes relacionados é reiniciada automaticamente. Consulte [Atualizando certificados do vRealize Automation](#) para obter mais informações sobre como atualizar certificados.

Procedimentos

- 1 Faça login na interface de gerenciamento de appliance do vRealize Automation como raiz.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Selecione **vRA > Certificados**.
- 3 Selecione o componente do vRealize Automation para o qual você está atualizando o certificado.
- 4 Selecione a ação adequada no menu **Ação de Certificado**.
Se você estiver usando um certificado codificado por PEM, por exemplo, para um ambiente distribuído, selecione **Importar**.

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

Se quiser gerar uma solicitação CSR para um novo certificado que pode ser enviado a uma autoridade de certificação, selecione **Gerar Solicitação de Assinatura**. Uma CSR ajuda sua CA a criar um certificado com os valores corretos para você importar.

Observação Se você usar cadeias de certificados, especifique os certificados na seguinte ordem:

- a Certificado cliente/servidor assinado pelo certificado de autoridade de certificação intermediário
- b Um ou mais certificados intermediários
- c Um certificado de autoridade de certificação raiz

Opção	Ação
Manter Existentes	Mantenha a configuração SSL atual. Selecione essa opção para cancelar as alterações.
Gerar Certificado	<ul style="list-style-type: none"> a O valor exibido na caixa de texto Nome comum é o Nome de host, conforme ele é exibido na parte superior da página. Se todas as instâncias adicionais do appliance do vRealize Automation estiverem disponíveis, os respectivos FQDN serão incluídos no atributo SAN do certificado. b Insira o nome da organização, como o nome da sua empresa, na caixa de texto Organização. c Insira a unidade organizacional, como o nome ou o local do departamento, na caixa de texto Unidade organizacional. d Insira um código de país ISO 3166 de duas letras, como PT_BR, na caixa de texto País.

Opção	Ação
Gerar solicitação de assinatura	<ul style="list-style-type: none"> a Selecione Gerar Solicitação de Assinatura. b Reveja as entradas nas caixas de texto Organização, Unidade Organizacional, Código do País e Nome Comum. Essas entradas são preenchidas do certificado existente. É possível editá-las se necessário. c Clique em Gerar CSR para gerar uma solicitação de assinatura de certificado e depois clique no link Baixar a CSR gerada aqui para abrir uma caixa de diálogo que permite salvar a CSR em um local onde ela pode ser enviada para uma autoridade de certificação. d Quando receber o certificado preparado, clique em Importar e siga as instruções para importar um certificado no vRealize Automation.
Importar	<ul style="list-style-type: none"> a Copie os valores do certificado, de BEGIN PRIVATE KEY até END PRIVATE KEY, incluindo o cabeçalho e o rodapé, e cole-os na caixa de texto Chave Privada RSA. b Copie os valores do certificado, de BEGIN PRIVATE KEY até END PRIVATE KEY, incluindo o cabeçalho e o rodapé, e cole-os na caixa de texto Cadeia de Certificados. Para vários valores de certificado, inclua um cabeçalho BEGIN CERTIFICATE e um rodapé END CERTIFICATE em cada certificado. <hr/> <p>Observação No caso dos certificados encadeados, atributos adicionais podem estar disponíveis.</p> <hr/> <ul style="list-style-type: none"> c (Opcional) Se o seu certificado usar um código de acesso para criptografar a chave do certificado, copie-o e cole-o na caixa de texto Código de Acesso.

5 Clique em **Salvar Configurações**.

Uma atualização de certificado de dispositivo do vRealize Automation requer serviços do vRealize Automation para reiniciar normalmente. A reinicialização pode levar de 15 minutos a uma hora, dependendo do número de dispositivos do vRealize Automation no seu ambiente.

Depois de reiniciar, os detalhes do certificado de todas as instâncias aplicáveis do dispositivo do vRealize Automation são exibidos na página.

6 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**.

7 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 Gerenciamento de diretórios.

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

8 Se você estiver usando um balanceador de carga, configure e ative todas as verificações de integridade aplicáveis.

Resultados

O certificado é atualizado.

Substituir o certificado de Infraestrutura como Serviço

O administrador do sistema pode substituir um certificado expirado ou um certificado autoassinado por um certificado de autoridade para garantir a segurança em um ambiente de implantação distribuída.

É possível usar um certificado de Nome Alternativo Para o Requerente (SAN) em várias máquinas. Os certificados usados para os componentes do IaaS (Website e Manager Service) devem ser emitidos com valores SAN, incluindo FQDNs de todos os hosts do Windows nos quais o componente correspondente é instalado, e com o FQDN do balanceador de carga do mesmo componente.

Procedimentos

- 1** Faça login na interface de gerenciamento de appliance do vRealize Automation como raiz.

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

- 2** Selecione **vRA > Certificados**.

- 3** Clique em **Web IaaS** no menu **Tipo de Componente**.

- 4** Vá até o painel **Certificado Web IaaS**.

- 5** Selecione a opção de substituição de certificado no menu **Ação do Certificado**.

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

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

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	Descrição
Manter Existentes	Mantenha a configuração SSL atual. Selecione essa opção para cancelar as alterações.
Gerar Certificado	<ol style="list-style-type: none"> a O valor exibido na caixa de texto Nome comum é o Nome de host, conforme ele é exibido na parte superior da página. Se todas as instâncias adicionais do appliance do vRealize Automation estiverem disponíveis, os respectivos FQDN serão incluídos no atributo SAN do certificado. b Insira o nome da organização, como o nome da sua empresa, na caixa de texto Organização. c Insira a unidade organizacional, como o nome ou o local do departamento, na caixa de texto Unidade organizacional. d Insira um código de país ISO 3166 de duas letras, como PT_BR, na caixa de texto País.
Importar	<ol style="list-style-type: none"> a Copie os valores do certificado, de BEGIN PRIVATE KEY até END PRIVATE KEY, incluindo o cabeçalho e o rodapé, e cole-os na caixa de texto Chave Privada RSA. b Copie os valores do certificado, de BEGIN PRIVATE KEY até END PRIVATE KEY, incluindo o cabeçalho e o rodapé, e cole-os na caixa de texto Cadeia de Certificados. Para vários valores de certificado, inclua um cabeçalho BEGIN CERTIFICATE e um rodapé END CERTIFICATE em cada certificado. <p>Observação No caso dos certificados encadeados, atributos adicionais podem estar disponíveis.</p> <ol style="list-style-type: none"> c (Opcional) Se o seu certificado usar um código de acesso para criptografar a chave do certificado, copie-o e cole-o na caixa de texto Código de Acesso.
Fornecer impressão digital do certificado	Use essa opção se você deseja fornecer uma impressão digital do certificado para usar um certificado que já está implantado no armazenamento de certificados nos servidores IaaS. Usar essa opção não transmitirá o certificado do appliance virtual para os servidores IaaS. Ele permite que os usuários implantem certificados existentes em servidores IaaS sem carregá-los na interface de gerenciamento.

6 Clique em **Salvar Configurações**.

Uma atualização de certificado do IaaS Windows Server requer que os serviços do vRealize Automation reiniciem normalmente. A reinicialização pode levar de 15 minutos a uma hora, dependendo do número de dispositivos do vRealize Automation no seu ambiente.

Depois de reiniciar, os detalhes do certificado aparecem na página.

Substituir o certificado do IaaS Manager Service

Um administrador de sistema pode substituir um certificado expirado ou autoassinado por uma autoridade de certificação para garantir a segurança em um ambiente de implantação distribuída.

É possível usar um certificado de Nome Alternativo Para o Requerente (SAN) em várias máquinas. Os certificados usados para os componentes do IaaS (Website e Manager Service) devem ser emitidos com valores SAN, incluindo FQDNs de todos os hosts do Windows nos quais o componente correspondente é instalado, e com o FQDN do balanceador de carga do mesmo componente.

O IaaS Manager Service e o IaaS Web Service compartilham um único certificado.

Procedimentos

- 1 Abra um navegador da Web para a URL da interface de gerenciamento do appliance do vRealize Automation.
- 2 Faça login com o nome de usuário **root** e a senha especificada na implantação do Appliance do vRealize Automation.
- 3 Selecione **vRA > Certificados**.
- 4 Clique em **Manager Service** no menu **Tipo de Componente**.
- 5 Selecione o tipo de certificado no menu **Ação de Certificado**.

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

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

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	Descrição
Manter Existentes	Mantenha a configuração SSL atual. Selecione essa opção para cancelar as alterações.
Gerar Certificado	<ol style="list-style-type: none"> a O valor exibido na caixa de texto Nome comum é o Nome de host, conforme ele é exibido na parte superior da página. Se todas as instâncias adicionais do appliance do vRealize Automation estiverem disponíveis, os respectivos FQDN serão incluídos no atributo SAN do certificado. b Insira o nome da organização, como o nome da sua empresa, na caixa de texto Organização. c Insira a unidade organizacional, como o nome ou o local do departamento, na caixa de texto Unidade organizacional. d Insira um código de país ISO 3166 de duas letras, como PT_BR, na caixa de texto País.
Importar	<ol style="list-style-type: none"> a Copie os valores do certificado, de BEGIN PRIVATE KEY até END PRIVATE KEY, incluindo o cabeçalho e o rodapé, e cole-os na caixa de texto Chave Privada RSA. b Copie os valores do certificado, de BEGIN PRIVATE KEY até END PRIVATE KEY, incluindo o cabeçalho e o rodapé, e cole-os na caixa de texto Cadeia de Certificados. Para vários valores de certificado, inclua um cabeçalho BEGIN CERTIFICATE e um rodapé END CERTIFICATE em cada certificado. <p>Observação No caso dos certificados encadeados, atributos adicionais podem estar disponíveis.</p> <ol style="list-style-type: none"> c (Opcional) Se o seu certificado usar um código de acesso para criptografar a chave do certificado, copie-o e cole-o na caixa de texto Código de Acesso.
Fornecer impressão digital do certificado	Use essa opção se você deseja fornecer uma impressão digital do certificado para usar um certificado que já está implantado no armazenamento de certificados nos servidores IaaS. Usar essa opção não transmitirá o certificado do appliance virtual para os servidores IaaS. Ele permite que os usuários implantem certificados existentes em servidores IaaS sem carregá-los na interface de gerenciamento.

6 Clique em **Salvar Configurações**.

Depois de alguns minutos, os detalhes do certificado aparecem na página.

7 Se exigido pela sua rede ou balanceador de carga, copie o certificado importado ou recém-criado para o balanceador de carga.**8** Abra um navegador e navegue até `https://managerServiceAddress/vmpsProvision/` de um servidor executando um trabalhador ou um agente DEM.

Se você estiver usando um balanceador de carga, o nome do host deve ser o nome de domínio totalmente qualificado do balanceador de carga.

9 Se solicitado, continue após os avisos de certificado.**10** Valide se o novo certificado for fornecido e confiável.**11** Se você estiver usando um balanceador de carga, configure e ative todas as verificações de integridade aplicáveis.

Atualizar vRealize Orchestrator integrado para confiar em certificados do vRealize Automation

Se você atualizar ou alterar certificados do Appliance do vRealize Automation ou IaaS, precisará atualizar o vRealize Orchestrator para confiar em certificados novos ou atualizados.

Este procedimento se aplica a todas as implantações do vRealize Automation que usam uma instância integrada do vRealize Orchestrator. Se você usar uma instância externa do vRealize Orchestrator, consulte [Atualizar o vRealize Orchestrator externo para confiar em certificados do vRealize Automation](#).

Observação Esse procedimento redefine a autenticação do tenant e do grupo de volta para as configurações padrão. Se você tiver personalizado a configuração da autenticação, observe as alterações para que possa configurar a autenticação novamente após concluir o procedimento.

Consulte a documentação do vRealize Orchestrator para obter mais informações sobre como atualizar e substituir certificados do vRealize Orchestrator.

Em uma configuração de cluster, você deve concluir esse procedimento no nó do dispositivo primário do vRealize Automation e, em seguida, executar um `join-cluster` em relação ao primário de cada nó do dispositivo de réplica do vRealize Automation.

Observação Em um cluster, pare o serviço do `vco-configurator` em todos os nós de réplica até que o procedimento seja concluído para evitar a sincronização de centro de controle automática indesejada.

Se você substituir ou atualizar certificados do vRealize Automation sem concluir esse procedimento, o Centro de Controle do vRealize Orchestrator poderá ficar inacessível, e erros poderão aparecer nos arquivos de log `vco-server` e `vco-configurator`.

Problemas com certificados de atualização também poderão ocorrer se o vRealize Orchestrator estiver configurado para ser autenticado em relação a um tenant e um grupo do vRealize Automation diferentes. Para obter informações, consulte o artigo de Base de Conhecimento da VMware [Cadeia de certificados não confiáveis de exceção após a substituição do certificado do vRA \(2147612\)](#).

As sintaxes do comando de confiança mostradas aqui são representativas, em vez de definitivas. Embora sejam apropriadas para a maioria das implantações típicas, pode haver situações em que você precise testar com variações nos comandos.

- Se você especificar o `--certificate`, deverá fornecer o caminho para um arquivo de certificado válido no formato PEM.
- Se você especificar o `--uri`, deverá fornecer o URI do qual o comando pode obter um certificado confiável.
- Se você especificar a opção do `--registry-certificate`, indique que o certificado solicitado deve ser tratado como o certificado para o registro de componente e o certificado confiável seja adicionado ao truststore sob um alias específico usado pelo certificado de registro do componente.

Você também pode gerenciar certificados usando fluxos de trabalho do Gerenciador de Confiança SSL no vRealize Orchestrator. Para obter informações, consulte o tópico *Gerenciar certificados do Orchestrator* na [documentação do vRealize Orchestrator](#).

Procedimentos

- 1 Interrompa os serviços do servidor e do Centro de Controle do vRealize Orchestrator.

```
service vco-server stop
service vco-configurator stop
```

- 2 Redefina o provedor de autenticação do vRealize Orchestrator executando o seguinte comando.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh reset-authentication
ls -l /etc/vco/app-server/
mv /etc/vco/app-server/vco-registration-id /etc/vco/app-server/vco-registration-id.old
vcac-vami vco-service-reconfigure
```

- 3 Verifique o certificado confiável do armazenamento confiável para o vRealize Orchestrator usando o utilitário de interface de linha de comandos localizado em `/var/lib/vco/tools/configuration-cli/bin` com o seguinte comando.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh list-trust
```

- Verifique o certificado com o alias a seguir: `vco.cafe.component registry.ssl.certificate`. Isso deve ser o certificado do vRealize Automation que a instância do vRealize Orchestrator usa como um provedor de autenticação.

- Esse certificado deve corresponder ao certificado do vRealize Automation configurado recentemente. Se não corresponder, poderá ser alterado da seguinte maneira:

- 1 Copie o arquivo PEM do certificado do appliance assinado do vRealize Automation para a pasta /tmp no appliance.
- 2 Execute o seguinte comando adicionando o caminho do certificado apropriado.

```
./vro-configure.sh trust --certificate path-to-the-certificate-file-in-PEM-format--registry-certificate
```

Consulte o comando do exemplo a seguir.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh trust --certificate /var/tmp/test.pem --registry-certificate
```

- 4 Pode ser necessário executar os seguintes comandos para confiar no certificado.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh trust --uri https://vra.domain.com  
  
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh trust --registry-certificate --uri https://vra.domain.com
```

- 5 Certifique-se de que o certificado do vRealize Automation agora esteja inserido no armazenamento de confiança do vRealize Orchestrator usando o seguinte comando.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh list-trust
```

- 6 Inicie os serviços do servidor e do centro de controle do vRealize Orchestrator.

```
service vco-server start  
service vco-configurator start
```

Próximo passo

Você pode validar que a confiança foi atualizada em um sistema em cluster.

- 1 Faça login na interface de gerenciamento de appliance como raiz.
- 2 Selecione a página Serviços.
- 3 Certifique-se de que não haja serviços vco duplicados listados.
Se você vir qualquer duplicata dos serviços vco listados, clique em **Cancelar registro** para remover os serviços que não têm um estado de Registered.
- 4 Certifique-se de que vco-configurator seja iniciado em todos os nós do dispositivo virtual.
- 5 Faça login no centro de controle do vRealize Orchestrator e navegue até a página Validar Configuração para validar a configuração.
- 6 Navegue até a página Provedor de Autenticação e verifique se as configurações de autenticação estão corretas.

Você também pode testar as credenciais de login nesta página.

Atualizar o vRealize Orchestrator externo para confiar em certificados do vRealize Automation

Se você atualizar ou alterar certificados do Appliance do vRealize Automation ou IaaS, precisará atualizar o vRealize Orchestrator para confiar em certificados novos ou atualizados.

Este procedimento se aplica a implantações do vRealize Automation que usam uma instância externa do vRealize Orchestrator.

Observação Esse procedimento redefine a autenticação do tenant e do grupo de volta para as configurações padrão. Se você tiver personalizado a configuração da autenticação, observe as alterações para que possa configurar a autenticação novamente após concluir o procedimento.

Consulte a documentação do vRealize Orchestrator para obter mais informações sobre como atualizar e substituir certificados do vRealize Orchestrator.

Se você substituir ou atualizar os certificados do vRealize Automation sem concluir esse procedimento, o Centro de Controle do vRealize Orchestrator poderá estar inacessível e poderão aparecer erros nos arquivos de log do vco-server e do vco-configurator.

Problemas com certificados de atualização também poderão ocorrer se o vRealize Orchestrator estiver configurado para ser autenticado em relação a um tenant e um grupo do vRealize Automation diferentes. Consulte o [artigo 2147612 da Base de Conhecimento](#).

Procedimentos

- 1 Interrompa os serviços do servidor e do Centro de Controle do vRealize Orchestrator.

```
service vco-configurator stop
```

- 2 Redefina o provedor de autenticação do vRealize Orchestrator.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh reset-authentication
```

- 3 Inicie o serviço do Centro de Controle do vRealize Orchestrator.

```
service vco-configurator start
```

- 4 Faça login no Centro de Controle usando as credenciais de raiz da interface de gerenciamento do appliance virtual.

- 5 Cancele o registro e registre novamente o provedor de autenticação.

Atualizando o certificado do site de gerenciamento do appliance do vRealize Automation

O administrador do sistema pode substituir o certificado SSL do serviço do site de gerenciamento quando expirar ou substituir um certificado autoassinado com um documento emitido por uma autoridade de certificação. Você protege o serviço do site de gerenciamento na porta 5480.

O appliance do vRealize Automation usa o lighttpd para executar seu próprio site de gerenciamento. Ao substituir um certificado de site de gerenciamento, você também deve configurar todos os Agentes de gerenciamento para reconhecer o novo certificado.

Se você estiver executando um ambiente distribuído, poderá atualizar os agentes de gerenciamento manual ou automaticamente. Se você estiver executando uma implantação mínima, deverá atualizar o agente de gerenciamento manualmente.

Consulte [Atualizar manualmente o reconhecimento de certificado do agente de gerenciamento](#) para obter mais informações.

Procedimentos

1 Localizar o Identificador do Agente de Gerenciamento

Use o Identificador do Agente de Gerenciamento quando você criar e registrar um novo certificado de servidor de site de gerenciamento.

2 Substituir o certificado do site de gerenciamento do aplicativo do vRealize Automation

Se o certificado SSL do serviço do site de gerenciamento expirar ou se você começou com um certificado autoassinado e as políticas do site exigirem uma diferente, poderá substituir o certificado.

3 Atualizar o reconhecimento de certificado do Agente de Gerenciamento

Depois de substituir um certificado do site de gerenciamento do appliance do vRealize Automation, você deve atualizar todos os agentes de gerenciamento para reconhecer o novo certificado e restabelecer comunicações confiáveis entre o site de gerenciamento do appliance virtual e os Agentes de Gerenciamento nos hosts de IaaS.

Localizar o Identificador do Agente de Gerenciamento

Use o Identificador do Agente de Gerenciamento quando você criar e registrar um novo certificado de servidor de site de gerenciamento.

Procedimentos

- 1 Abra o arquivo de configuração do Agente de gerenciamento localizado em `<vra-installation-dir>\Management Agent\VMware.IaaS.Management.Agent.exe.config`.

- 2 Grave o valor do atributo da ID do elemento agentConfiguration.

```
<agentConfiguration id="0E22046B-9D71-4A2B-BB5D-70817F901B27">
```

Substituir o certificado do site de gerenciamento do aplicativo do vRealize Automation

Se o certificado SSL do serviço do site de gerenciamento expirar ou se você começou com um certificado autoassinado e as políticas do site exigirem uma diferente, poderá substituir o certificado.

Você tem permissão para reutilizar o certificado usado pelo serviço do vRealize Automation na porta 443 ou usar outro. Se você estiver solicitando um novo certificado emitido pela CA para atualizar um certificado existente, uma prática recomendada será reutilizar o Nome Comum do certificado existente.

Observação O appliance do vRealize Automation usa o `lighttpd` para executar seu próprio site de gerenciamento. Você protege o serviço do site de gerenciamento na porta 5480.

Pré-requisitos

- O certificado deve estar no formato PEM.
- O certificado deve incluir os seguintes, em ordem, juntos em um arquivo:
 - a Chave privada RSA
 - b Cadeia de certificados
- A chave privada não pode ser criptografada.
- O local padrão e o nome do arquivo é `/opt/vmware/etc/lighttpd/server.pem`.

Consulte [Extraindo certificados e chaves privadas](#) para obter mais informações sobre como exportar um certificado e uma chave privada a partir de um armazenamento de chave Java para um arquivo PEM.

Procedimentos

- 1 Faça login usando o console do appliance ou SSH.
- 2 Faça backup do arquivo de certificado atual.

```
cp /opt/vmware/etc/lighttpd/server.pem /opt/vmware/etc/lighttpd/server.pem-bak
```

- 3 Copie o novo certificado para seu dispositivo substituindo o conteúdo do arquivo `/opt/vmware/etc/lighttpd/server.pem` pelas informações do novo certificado.
- 4 Execute o comando a seguir para reiniciar o servidor `lighttpd`.

```
service vami-lighttpd restart
```
- 5 Execute o comando a seguir para reiniciar o serviço `haproxy`.

```
service haproxy restart
```
- 6 Faça login no console de gerenciamento e verifique se o certificado foi substituído. Pode ser preciso reiniciar o navegador.

Próximo passo

Atualize todos os agentes de gerenciamento para reconhecer o novo certificado.

Para implantações distribuídas, você pode atualizar agentes de gerenciamento manual ou automaticamente. Para as instalações mínimas, você deve atualizar os agentes manualmente.

- Para obter informações sobre a atualização automática, consulte [Atualizar automaticamente os agentes de gerenciamento em um ambiente distribuído para reconhecer um certificado do site de gerenciamento do appliance do vRealize Automation](#).
- Para obter informações sobre atualização manual, consulte [Atualizar manualmente o reconhecimento de certificado do agente de gerenciamento](#).

Atualizar o reconhecimento de certificado do Agente de Gerenciamento

Depois de substituir um certificado do site de gerenciamento do appliance do vRealize Automation, você deve atualizar todos os agentes de gerenciamento para reconhecer o novo certificado e restabelecer comunicações confiáveis entre o site de gerenciamento do appliance virtual e os Agentes de Gerenciamento nos hosts de IaaS.

Cada host de IaaS executa um agente de gerenciamento e cada agente de gerenciamento deve ser atualizado. Implantações mínimas devem ser atualizadas manualmente, enquanto implantações distribuídas podem ser atualizadas manualmente ou com o uso de um processo automatizado.

■ [Atualizar manualmente o reconhecimento de certificado do agente de gerenciamento](#)

Depois de substituir um certificado do site de gerenciamento do appliance do vRealize Automation, você deve atualizar os Agentes de Gerenciamento manualmente para reconhecer o novo certificado e restabelecer comunicações confiáveis entre o site de gerenciamento do appliance virtual e os Agentes de Gerenciamento nos hosts de IaaS.

■ [Atualizar automaticamente os agentes de gerenciamento em um ambiente distribuído para reconhecer um certificado do site de gerenciamento do appliance do vRealize Automation](#)

Após a atualização do certificado do site de gerenciamento em uma implementação de alta disponibilidade, a configuração do agente de gerenciamento também deve ser atualizada para reconhecer o novo certificado e restabelecer uma comunicação confiável.

Atualizar manualmente o reconhecimento de certificado do agente de gerenciamento

Depois de substituir um certificado do site de gerenciamento do appliance do vRealize Automation, você deve atualizar os Agentes de Gerenciamento manualmente para reconhecer o novo certificado e restabelecer comunicações confiáveis entre o site de gerenciamento do appliance virtual e os Agentes de Gerenciamento nos hosts de IaaS.

Realize estas etapas para cada Agente de gerenciamento em sua implantação depois de substituir um site de gerenciamento do appliance do vRealize Automation.

Para ambientes distribuídos, você pode atualizar os Agentes de gerenciamento manual ou automaticamente. Para obter informações sobre a atualização automática, consulte [Atualizar automaticamente os agentes de gerenciamento em um ambiente distribuído para reconhecer um certificado do site de gerenciamento do appliance do vRealize Automation](#).

Pré-requisitos

Obtenha as impressões digitais SHA1 do novo certificado do site de gerenciamento do appliance do vRealize Automation.

Procedimentos

- 1 Pare o serviço do Agente de gerenciamento do VMware vCloud Automation Center.
- 2 Navegue até o arquivo de configuração do Agente de gerenciamento localizado em `[vcac_installation_folder]\Management Agent\VMware.IaaS.Management.Agent.exe.Config`, geralmente `C:\Arquivos de Programas (x86)\VMware\VCAC\Management Agent\VMware.IaaS.Management.Agent.exe.Config`.
- 3 Abra o arquivo para edição e localize a definição de configuração do endpoint para o antigo certificado do site de gerenciamento, que você pode identificar pelo endereço do endpoint.

Por exemplo:

```
<agentConfiguration id="C816CFBC-4830-4FD2-8951-C17429CEA291" pollingInterval="00:03:00">
  <managementEndpoints>
    <endpoint address="https://vra-va.local:5480"
thumbprint="D1542471C30A9CE694A512C5F0F19E45E6FA32E6" />
  </managementEndpoints>
</agentConfiguration>
```

- 4 Altere a impressão digital para a impressão digital SHA1 do novo certificado.

Por exemplo:

```
<agentConfiguration id="C816CFBC-4830-4FD2-8951-C17429CEA291" pollingInterval="00:03:00">
  <managementEndpoints>
    <endpoint address="https://vra-va.local:5480"
thumbprint="8598B073359BAE7597F04D988AD2F083259F1201" />
  </managementEndpoints>
</agentConfiguration>
```

- 5 Inicie o serviço do Agente de gerenciamento do VMware vCloud Automation Center.
- 6 Faça login no site de gerenciamento de appliance virtual e selecione a guia **Cluster**.
- 7 Verifique a tabela de Informações de Implementação distribuída para verificar se o servidor IaaS teve contato com o appliance virtual recentemente, o que confirma que a atualização foi bem-sucedida.

Atualizar automaticamente os agentes de gerenciamento em um ambiente distribuído para reconhecer um certificado do site de gerenciamento do appliance do vRealize Automation

Após a atualização do certificado do site de gerenciamento em uma implementação de alta disponibilidade, a configuração do agente de gerenciamento também deve ser atualizada para reconhecer o novo certificado e restabelecer uma comunicação confiável.

Você pode atualizar as informações do certificado do site de gerenciamento do appliance do vRealize Automation para sistemas distribuídos manual ou automaticamente. Para obter informações sobre como atualizar manualmente os agentes de gerenciamento, consulte [Atualizar manualmente o reconhecimento de certificado do agente de gerenciamento](#).

Use este procedimento para atualizar as informações do certificado automaticamente.

Procedimentos

- 1 Quando os agentes de gerenciamento estão em execução, substitua o certificado em um único site de gerenciamento do appliance do vRealize Automation na sua implantação.
- 2 Aguarde 15 minutos para que o agente de gerenciamento seja sincronizado com o novo certificado do site de gerenciamento do appliance do vRealize Automation.
- 3 Substitua os certificados em outros sites de gerenciamento do appliance do vRealize Automation na implantação.

Os agentes de gerenciamento são atualizados automaticamente com as novas informações de certificado.

Substituir um certificado do Agente de gerenciamento

O administrador do sistema pode substituir o certificado do Agente de gerenciamento quando expira ou substituir um certificado autoassinado por um certificado emitido por uma autoridade de certificação.

Cada host do IaaS executa o seu próprio Agente de gerenciamento. Repita este procedimento em cada nó do IaaS cujo Agente de gerenciamento você deseja atualizar.

Pré-requisitos

- Copie o identificador do agente de gerenciamento na coluna ID de nó antes de remover o registro. Você usa esse identificador ao criar o novo certificado do Agente de gerenciamento e ao registrá-lo.
- Ao solicitar um novo certificado, verifique se o atributo Nome comum (CN) no campo de assunto do certificado do novo certificado está digitado no seguinte formato:

```
VMware Management Agent 00000000-0000-0000-0000-000000000000
```

Use a cadeia de caracteres do Agente de gerenciamento do VMware, seguida por um único espaço e o GUID para o Agente de gerenciamento no formato numérico mostrado.

Procedimentos

- 1 Pare o serviço do Agente de gerenciamento do snap-in dos serviços do Windows.
 - a Na sua máquina Windows, clique em **Iniciar**.
 - b Na caixa Pesquisar do menu Iniciar Windows, insira **services.msc** e pressione Enter.
 - c Clique com o botão direito do mouse em serviço do **Agente de gerenciamento do VMware vCloud Automation Center** e clique em **Parar** para parar o serviço.
- 2 Remova o certificado atual da máquina. Para obter informações sobre o gerenciamento de certificados no Windows Server 2008 R2, consulte o artigo Microsoft Knowledge Base em <http://technet.microsoft.com/en-us/library/cc772354.aspx> ou o artigo wiki da Microsoft em <http://social.technet.microsoft.com/wiki/contents/articles/2167.how-to-use-the-certificates-console.aspx>.
 - a Abra o Console de Gerenciamento da Microsoft inserindo o comando **mmc.exe**.
 - b Pressione Ctrl + M para adicionar um novo snap-in ao console ou selecione a opção no menu suspenso Arquivo.
 - c Selecione **Certificados** e clique em **Adicionar**.
 - d Selecione **Conta de computador** e clique em **Avançar**.
 - e Selecione **Computador local: (o computador no qual este console está sendo executado)**.
 - f Clique em **OK**.
 - g Expanda **Certificados (Computador Local)** no lado esquerdo do console.
 - h Expanda **Pessoal** e selecione a pasta Certificados.
 - i Selecione o certificado do Agente de Gerenciamento atual e clique em **Excluir**.
 - j Clique em **Sim** para confirmar a ação de exclusão.
- 3 Importe o certificado recém-gerado para o repositório `computer.personal` local ou não importe nada se quiser que o sistema gere automaticamente um novo certificado auto-assinado.

- 4 Registre o certificado do Management Agent no site de gerenciamento de appliances do vRealize Automation.

- a Abra um prompt de comando como administrador e navegue até o diretório Cafe na máquina em que o Agente de Gerenciamento está instalado, em *<vra-installation-dir>*\Management Agent\Tools\Cafe, normalmente C:\Program Files (x86)\VMware\VCAC\Management Agent\Tools\Cafe.
- b Insira o comando `Vcac-Config.exe RegisterNode` com opções para registrar o certificado e o identificador do Agente de gerenciamento em uma só etapa. Inclua o identificador do agente de gerenciamento que você gravou anteriormente como o valor para a opção `-nd`.

Tabela 1-3. Opções e argumentos necessários para Vcac-Config.exe RegisterNode

[illegible]

O exemplo a seguir mostra o formato do comando:

```
Vcac-Config.exe RegisterNode -v -vamih "vra-vam-hostname.domain.name:5480"  
-cu "root" -cp "password" -hn "machine-hostname.domain.name"  
-nd "00000000-0000-0000-0000-000000000000"  
-tp "000000000000000000000000000000000000000000000000"
```

5 Reinicie o Agente de gerenciamento.

Exemplo: Comando para registrar um certificado do Agente de gerenciamento

```
Vcac-Config.exe RegisterNode -v -vamih "vra-va.eng.mycompany:5480" -cu "root" -cp
"secret" -hn "iaas.eng.mycompany" -nd "C816CFBX-4830-4FD2-8951-C17429CEA291" -tp
"70928851D5B72B206E4B1CF9F6ED953EE1103DED"
```

Alterar o método de sondagem para certificados

Caso haja vírgulas na seção OU do certificado Iaas, você pode encontrar erros STOMP WebSocket nos arquivos de log do Manager Service. Além disso, o provisionamento da máquina virtual pode falhar. Você pode remover as vírgulas, ou alterar o método de sondagem de WebSocket para HTTP.

Para alterar o método de sondagem, siga estas etapas.

Procedimientos

- 1** Abra o seguinte arquivo no editor de texto.

C:\\:Arquivos de programas (x86)\\VMware\\vCAC\\Server\\Manager Service.exe.config.

- 2** Adicione as seguintes linhas dentro da seção `<appSettings>`.

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

- 3** Salve e feche o `Manager Service.exe.config`.

- 4** Reinicie o serviço do gerenciador.

Resultados

Para obter mais informações sobre o Manager Service, consulte *Instalando o vRealize Automation*.

Gerenciando o banco de dados do appliance do Postgres do vRealize Automation

O vRealize Automation requer o banco de dados do appliance para a operação do sistema. Você pode gerenciar o banco de dados do appliance por meio da Interface de Gerenciamento de Appliance Virtual do appliance do vRealize Automation.

Observação Essas informações somente se aplicam a implantações que usam um banco de dados de appliance incorporado. Elas não se aplicam a implantações que usam um banco de dados Postgres externo.

Você pode configurar o banco de dados como um nó único ou com vários nós para facilitar a alta disponibilidade por meio de failover. O instalador do vRealize Automation inclui um nó de banco de dados em cada instalação do Appliance do vRealize Automation. Portanto, se você instalar três instâncias de um Appliance do vRealize Automation, terá três nós de banco de dados. O failover automático é implementado nas implantações aplicáveis. O banco de dados do dispositivo não necessita de manutenção, a menos que uma configuração de máquina seja alterada ou, no caso de uma configuração em cluster, você promova um nó diferente como principal.

Observação A configuração de cluster de banco de dados é definida automaticamente quando você une um virtual appliance ao cluster usando a operação Unir cluster. O cluster de banco de dados não depende diretamente do cluster de virtual appliances. Por exemplo, uma máquina virtual unida a um cluster pode operar normalmente, mesmo que o banco de dados de appliance incorporado não esteja iniciado ou tenha falhado.

Para alta disponibilidade, o vRealize Automation usa o modelo de réplica primária do PostgreSQL para oferecer suporte à replicação de dados. Isso significa que todos os nós do banco de dados trabalham em um cluster com um nó principal, conhecido como principal, e vários nós de replicação, conhecidos como réplicas. O nó principal lida com todas as solicitações de banco de dados, e os nós de réplica transmitem e reproduzem transações do principal localmente.

Uma configuração de cluster contém um nó principal e um ou mais nós de réplica. O nó principal é o nó do dispositivo do vRealize Automation com o banco de dados principal que oferece suporte à funcionalidade do sistema. Os nós de réplica contêm cópias do banco de dados que poderão ser levadas ao serviço se o nó principal falhar.

Existem várias opções de banco de dados de appliance de alta disponibilidade. Selecionar o modo de replicação é a opção de configuração de banco de dados mais importante. O modo de replicação determina como a implantação do vRealize Automation mantém a integridade dos dados e, para configurações de alta disponibilidade, como ela faz failover caso o nó principal ou o nó primário apresente falha. Existem dois modos de replicação disponíveis: síncrono e assíncrono.

Ambos os modos de replicação oferecem suporte a failover de banco de dados, embora cada um tenha vantagens e desvantagens. Para dar suporte ao failover de banco de dados de alta disponibilidade, o modo assíncrono requer dois nós, enquanto o modo síncrono requer três nós. O modo síncrono também chama o failover automático.

Modo de Replicação	Vantagens	Desvantagens
Síncrono	<ul style="list-style-type: none"> ■ Minimiza a chance de perda de dados. ■ Invoca o failover automático. 	<ul style="list-style-type: none"> ■ Pode afetar o desempenho do sistema. ■ Requer três nós.
Assíncrono	<ul style="list-style-type: none"> ■ Requer apenas dois nós. ■ Afeta o desempenho do sistema menos do que o modo síncrono. 	Não é tão robusto quanto o modo síncrono na prevenção da perda de dados.

O vRealize Automation tem suporte para ambos os modos, mas opera em modo assíncrono por padrão e oferece alta disponibilidade somente se houver pelo menos dois nós de banco de dados de appliance. A guia **Cluster** na Interface de Gerenciamento de Appliance Virtual permite alternar entre os modos de sincronização e adicionar nós de banco de dados, conforme necessário.

Ao operar no modo síncrono, o vRealize Automation chama o failover automático.

Se você começar com um nó em uma configuração que não seja de alta disponibilidade, poderá adicionar nós mais tarde, conforme necessário para aprimorar a alta disponibilidade. Se você tiver o hardware apropriado e precisar de proteção máxima contra perda de dados, considere configurar a implantação para operar em modo síncrono.

Failover de banco de dados do appliance

Em uma configuração de alta disponibilidade, o primário transmite constantemente transações para os servidores de réplica. Se o primário falhar, a réplica ativa e em funcionamento estará pronta para prosseguir com as solicitações de somente leitura. Quando o novo primário for promovido, manual ou automaticamente, todas as solicitações futuras serão movidas para ele.

Configurar o Appliance Database

É possível usar a página Banco de Dados da Interface de Gerenciamento de Appliance Virtual para monitorar ou atualizar a configuração do banco de dados do appliance. Você também pode usá-la para alterar a designação do nó primário e o modo de sincronização usado pelo banco de dados.

O banco de dados do appliance é instalado e configurado durante a instalação e a configuração do sistema do vRealize Automation, mas você pode monitorar e alterar a configuração na guia **Banco de Dados** da Interface de Gerenciamento de Appliance Virtual.

A caixa de texto **Status da Conexão** indica se o banco de dados está conectado ao sistema do vRealize Automation e está funcionando corretamente.

Se o banco de dados do dispositivo usa vários nós para oferecer suporte de failover, a tabela na parte inferior da página exibe os nós, seus status e indica qual nó é o primário. A caixa de texto **Modo de Replicação** mostra o modo de operação configurado atualmente para o sistema: síncrono ou assíncrono. Use esta página para atualizar a configuração do banco de dados do appliance.

A coluna Estado de Sincronização* na tabela de nós de banco de dados mostra o método de sincronização para o cluster. Essa coluna funciona com a coluna Status para mostrar o estado dos nós do cluster. O status potencial difere de acordo com o uso de replicação assíncrona ou síncrona pelo cluster.

Tabela 1-4. Estado de sincronização para modos de replicação do banco de dados do appliance

Modo	Mensagem de Estado de Sincronização
Replicação síncrona	Nó primário - sem status Nó de réplica - sincronizar Outros nós - potenciais
Replicação assíncrona	Nó primário - sem status Outros nós - potenciais

A coluna Válido indica se as réplicas estão sincronizadas com o nó primário. O nó primário é sempre válido.

A coluna Prioridade mostra a posição dos nós de réplica em relação ao nó primário. O nó primário não apresenta valor de prioridade. Ao promover uma réplica para primária, selecione o nó com o valor de prioridade mais baixo.

Ao operar no modo síncrono, o vRealize Automation chama o failover automático. No caso de uma falha no nó primário, o próximo nó de réplica disponível se tornará automaticamente o novo primário. A operação de failover requer de 10 a 30 segundos em uma implantação típica do vRealize Automation.

Pré-requisitos

- Instale e configure o vRealize Automation de acordo com as instruções apropriadas em *Instalando o vRealize Automation*.
- Faça login no Gerenciamento do Appliance do vRealize Automation como **root** usando a senha que você inseriu quando implantou o appliance do vRealize Automation.
- Configure um cluster de banco de dados de appliance Postgres incorporado apropriado como parte da sua implantação do vRealize Automation.

Procedimentos

- 1 Na Interface de Gerenciamento de Appliance Virtual, selecione **Configurações do vRA > Banco de Dados**.

- 2 Se o banco de dados usar múltiplos nós, consulte a tabela na parte inferior da página e garanta que o sistema esteja funcionando corretamente.
 - Certifique-se de que todos os nós estejam listados.
 - Certifique-se de que o nó apropriado seja o nó primário designado.

Observação Não clique em **Modo de Sincronização** para alterar o modo de sincronização do banco de dados, a menos que você esteja certo de que os dados estão seguros. Alterar o modo de sincronização sem preparação pode causar perda de dados.

- 3 Para promover um dos nós para principal, clique em **Promover** na coluna apropriada.
- 4 Clique em **Salvar configurações** para salvar a configuração se tiver feito quaisquer alterações.

Três cenários de failover automático do banco de dados do appliance do nó

Existem vários cenários de failover de alta disponibilidade do banco de dados do appliance, e o comportamento do vRealize Automation varia dependendo da configuração do banco de dados do appliance e do número de nós que falham.

Cenários de falha em um único nó

Se um dos três nós falhar, o vRealize Automation iniciará um failover automático. Nenhuma operação adicional de failover automático pode ocorrer até que todos os três nós sejam restaurados.

A tabela a seguir descreve o comportamento e as ações relacionadas a uma falha do nó primário em uma implantação de alta disponibilidade.

Tabela 1-5. O nó principal falha

Comportamento esperado	<ul style="list-style-type: none"> ■ O nó de réplica de sincronização configurado se torna o primário e automaticamente seleciona a funcionalidade do banco de dados do dispositivo. ■ A réplica de sincronização potencial se torna o nó de espera de sincronização. ■ A implantação do vRealize Automation funciona no modo somente leitura até que o failover automático seja concluído.
Ação adicional	<ul style="list-style-type: none"> ■ Quando o antigo primário for recuperado, ele será redefinido automaticamente como réplica pela lógica de reparo do agente de failover. Nenhuma ação manual é necessária. ■ Se o antigo primário não puder ser recuperado, defina manualmente o banco de dados do dispositivo para o modo assíncrono.

A tabela a seguir descreve o comportamento e as ações relacionadas a uma falha do nó de réplica de sincronização em uma implantação de alta disponibilidade.

Tabela 1-6. A réplica de sincronização falha

Comportamento esperado	<ul style="list-style-type: none"> ■ Não ocorre um tempo de inatividade na implantação do vRealize Automation. Haverá um atraso de alguns segundos para solicitações do banco de dados até que a réplica potencial se torne a nova réplica de sincronização. O banco de dados do appliance executa essa ação automaticamente.
Ação adicional	<ul style="list-style-type: none"> ■ Quando a antiga réplica de sincronização estiver online, ela se tornará uma réplica potencial automaticamente. Nenhuma ação manual é necessária. ■ Se a antiga réplica de sincronização não puder ser reparada, defina manualmente o banco de dados do appliance para o modo assíncrono.

A tabela a seguir descreve o comportamento e as ações relacionadas a uma falha do nó primário em uma implantação de alta disponibilidade.

Tabela 1-7. A réplica potencial falha

Comportamento esperado	Nenhum tempo de inatividade na implantação.
Ação adicional	<ul style="list-style-type: none"> ■ Quando a antiga réplica potencial estiver online, ela se tornará uma réplica potencial automaticamente. Nenhuma ação manual é necessária. ■ Se a antiga réplica potencial não puder ser reparada, defina o banco de dados do appliance para o modo assíncrono.

Cenários de falha em dois nós

Se dois dos três nós falharem simultaneamente, o vRealize Automation mudará para o modo somente leitura até que um reparo manual seja executado.

A tabela a seguir descreve o comportamento e as ações relacionadas a uma falha do nó primário e do nó de réplica potencial em uma implantação de alta disponibilidade.

Tabela 1-8. O nó primário e a réplica potencial falham

Comportamento esperado	<ul style="list-style-type: none"> ■ A réplica de sincronização não é promovida para primário automaticamente. As funções do vRealize Automation no modo somente leitura, pois podem processar transações somente leitura até que uma promoção manual seja realizada.
Ação adicional	<ul style="list-style-type: none"> ■ A promoção manual é necessária. Defina o banco de dados do appliance para o modo assíncrono. ■ Quando as réplicas primário e potencial forem recuperadas, defina-as manualmente para sincronizar com o novo primário. Nesse ponto, você poderá mudar o vRealize Automation de volta para o modo síncrono. ■ Quando dois dos três nós estiverem inativos simultaneamente, o vRealize Automation mudará para o modo somente leitura até você efetuar um reparo manual. Se apenas um nó do banco de dados estiver disponível, mude sua implantação para o modo assíncrono.

A tabela a seguir descreve o comportamento e as ações relacionadas à falha do nó de Sincronização e Potencial em uma implantação de alta disponibilidade.

Tabela 1-9. As réplicas de sincronização e potenciais falham

Comportamento esperado	<ul style="list-style-type: none"> ■ As funções do vRealize Automation no modo somente leitura, pois podem processar transações somente leitura até que um reparo manual seja realizado.
Ação adicional	<ul style="list-style-type: none"> ■ A promoção manual é necessária. Defina o banco de dados do appliance para o modo assíncrono. ■ Quando as réplicas de sincronização e potenciais são recuperadas, elas devem ser redefinidas manualmente para serem sincronizadas com o primário. Neste ponto, você poderá mudar o vRealize Automation de volta para o modo síncrono. ■ Quando dois dos três nós estiverem inativos simultaneamente, o vRealize Automation mudará para o modo somente leitura até você efetuar um reparo manual. Se apenas um nó do banco de dados estiver disponível, mude sua implantação para o modo assíncrono.

Falhas de links entre os nós

Se ocorrer uma falha de link entre nós em uma implantação distribuída, o agente de failover automático tentará reparar a configuração.

A tabela a seguir descreve o comportamento e as ações relacionadas a uma falha de link entre dois sites em uma implantação de alta disponibilidade com a configuração especificada quando todos os nós permanecem online e ativos.

Site A: réplica primária e potencial

Site B: réplica de sincronização

Tabela 1-10. Falha de link entre dois sites quando todos os nós permanecem ativos e online

Comportamento esperado	Nenhum tempo de inatividade na implantação do vRealize Automation. A réplica potencial se torna automaticamente a réplica de sincronização.
Ação adicional	Nenhuma ação manual é necessária.

A tabela a seguir descreve o comportamento e as ações relacionadas a uma falha de link entre dois sites em uma implantação de alta disponibilidade com a configuração especificada quando todos os nós permanecem online e ativos.

Site A: primário

Site B: réplica de sincronização e potencial

Tabela 1-11. Falha de link entre dois sites quando todos os nós permanecem ativos e online - Configuração alternada

Comportamento esperado	A réplica de sincronização se torna o primário e automaticamente seleciona a funcionalidade do banco de dados do dispositivo. O agente de failover automático promove a réplica potencial para se tornar a nova réplica de sincronização. A implantação do vRealize Automation opera em modo somente leitura até que esta promoção seja concluída.
Ação adicional	Nenhuma ação manual é necessária. Quando o link é recuperado, o agente de failover automático redefine o antigo primário como réplica.

Cenário: realizar o failover de banco de dados do dispositivo vRealize Automation manual

Quando existe um problema com o banco de dados Postgres do appliance do vRealize Automation, você faz o failover manualmente para uma réplica do nó do appliance do vRealize Automation no cluster.

Siga esses passos quando o banco de dados Postgres no nó do dispositivo do vRealize Automation primário falhar ou deixar de ser executado.

Observação Quando um nó entrar em um estado não íntegro, não tente usar sua interface de gerenciamento do appliance virtual para operações, incluindo failover.

Pré-requisitos

- Configurar um cluster dos nós do appliance do vRealize Automation. Cada nó hospeda uma cópia do banco de dados do dispositivo Postgres incorporado.

Procedimentos

- 1 Remova o endereço IP do nó primário do balanceador de carga externo.
- 2 Faça login na interface de gerenciamento de appliance do vRealize Automation como raiz.
`https://vrealize-automation-appliance-FQDN:5480`
- 3 Selecione **Cluster**.
- 4 Da lista dos nós do banco de dados, localize o nó de réplica com a prioridade mais baixa.
Os nós de réplica aparecem em ordem de prioridade ascendente.
- 5 Clique em **Promover** e espere que a operação termine.
Quando finalizado, o nó de réplica é listado como o novo nó primário.
- 6 Corrija problemas com o nó primário antigo e adicione-o de volta ao cluster:
 - a Isole o antigo nó primário.

Desconecte o nó da sua atual rede, aquele que está sendo roteado aos nós remanescentes do appliance do vRealize Automation. Selecione outro NIC para o gestor ou gerencie-o diretamente do console gestor da máquina virtual.

- b Recupere o antigo nó primário.

Ligue o nó ou, caso contrário, corrija o problema. Por exemplo, você deve reinicializar a máquina virtual se essa não responde.

- c A partir de uma sessão de console como raiz, pare o serviço vpostgres.

```
service vpostgres stop
```

- d Adicione novamente o antigo nó primário à sua rede original, aquele que está sendo roteado aos outros nós do dispositivo do vRealize Automation.

- e A partir de uma sessão de console como raiz, pare o serviço haproxy.

```
service haproxy restart
```

- f Faça login na nova interface de gerenciamento do nó primário do dispositivo do vRealize Automation como root.

- g Selecione **Cluster**.

- h Localize o antigo nó primário e clique em **Redefinir**.

- i Após uma reinicialização sucedida, reinicie o antigo nó primário.

- j Com o antigo nó primário ligado, verifique se os seguintes serviços são executados.

```
haproxy horizon-workspace rabbitmq-server vami-lighttpd vcac-server vco-server
```

- k Adicione novamente o antigo nó primário ao balanceador de carga externo.

Observação Se um nó primário que foi rebaixado para réplica ainda estiver elencado como primário, você talvez precise reuní-lo manualmente ao cluster para corrigir o problema.

Cenário: realizar o failover de banco de dados de manutenção

Como administrador do sistema do vRealize Automation, você deve executar uma operação de failover de manutenção de banco de dados do appliance.

Este cenário assume que o nó primário atual está instalado e funcionando normalmente. Há duas etapas de manutenção de failover de banco de dados: manutenção do nó primário e manutenção do nó de réplica. Quando um nó primário tiver sido substituído para se tornar uma réplica, você deve executar a manutenção do mesmo para que ele seja adequado para tornar-se primário de novo caso haja necessidade.

Observação Não interrompa ou reinicie o serviço HAProxy na máquina do host aplicável enquanto realiza um failover de manutenção.

Pré-requisitos

- O vRealize Automation é instalado e configurado de acordo com as devidas instruções no *Instalando o vRealize Automation*.
- Faça login no Gerenciamento do Appliance do vRealize Automation como **root** usando a senha que você inseriu quando implantou o appliance do vRealize Automation.
- Instale e configure um cluster de banco de dados de dispositivo Postgres incorporado apropriado.
- Se o banco de dados usa o modo de replicação síncrona, verifique se há três nós ativos no cluster.

Procedimentos

- 1 Remova o endereço IP do nó primário do balanceador de carga externo.

- 2 Isole o nó primário.

Desconecte o nó de sua rede atual. Esta deve ser a rede que está roteando para os nós Appliance do vRealize Automation restantes.

- 3 Selecione outra NIC para gerenciamento ou gerencie-a diretamente na Interface de gerenciamento de appliances virtuais.

- 4 Selecione **Cluster** na Interface de Gerenciamento do Appliance Virtual.

- 5 Selecione o nó de réplica com a prioridade mais baixa para promoção para primário e clique em **Promover**.

Os nós de réplica aparecem em ordem de prioridade ascendente.

O antigo primário é rebaixado ao status de réplica, e o novo primário é promovido.

- 6 Realize a manutenção de réplica adequada.

- 7 Quando a manutenção estiver concluída, confirme que o dispositivo virtual está executando com conectividade de rede e que seu serviço HAProxy está executando.

a Faça login no console de gerenciamento do vRealize Automation como **raiz**.

b Certifique-se de que possa ser executado um ping no nó da réplica, resolvido pelo nome e tenha um status recente na guia **Cluster** da Interface de Gerenciamento do Appliance Virtual.

- 8 Clique em **Redefinir** para o nó de réplica.

Essa operação redefine o banco de dados, para que ele seja configurado para replicar no primário atual, e repete a sincronização do nó de réplica com a configuração do proxy de alta disponibilidade mais recente no nó primário.

- 9 Após a redefinição de sucesso, retorne o endereço IP de nó de appliance virtual de réplica para o pool de endereço IP do balanceador de carga do virtual appliance externo.

- 10 Certifique-se de que o nó da réplica aparece como íntegro na tabela do banco de dados e que pode ser pingado e resolvido pelo nome.

Próximo passo

Corrija problemas com o nó primário antigo e adicione-o de volta ao cluster.

Recupere Manualmente o Banco de Dados do Appliance de Falha Catastrófica

Se o banco de dados do dispositivo falhar e nenhum dos nós de banco de dados estiver funcionando e em execução ou se todos os nós de réplica estiverem fora de sincronia quando o primário falhar, utilize o procedimento a seguir para tentar recuperar o banco de dados.

Esse procedimento se aplica a situações em que nenhum nó de banco de dados está operacional em um cluster que está sendo executado no modo assíncrono. Neste cenário, você normalmente verá erros semelhantes aos seguintes na página da Interface de Gerenciamento do Appliance Virtual durante a tentativa de carregar ou atualizar a página:

Erro ao inicializar o serviço do banco de dados: não foi possível abrir a Conexão JDBC para a transação; a exceção aninhada é org.postgresql.util.PSQLException: Falha na tentativa de conexão.

Procedimentos

- 1 Tente recuperar o banco de dados usando a Interface de Gerenciamento do Appliance Virtual de um de nós do banco de dados.
 - a Se possível, abra a página do **Cluster** da Interface de Gerenciamento do Appliance Virtual do nó com o estado mais atual. Normalmente, esse nó é aquele que era o nó primário antes do banco de dados falhar.
 - b Se a Interface de Gerenciamento do Dispositivo Virtual para o nó primário falhar ao abrir, tente abrir a Interface para outros nós de réplica.
 - c Se você puder encontrar um nó de banco de dados com uma Interface de Gerenciamento do Appliance Virtual em funcionamento, tente recuperá-la realizando um failover manual.
 Consulte [Cenário: realizar o failover de banco de dados do dispositivo vRealize Automation manual](#).
- 2 Se o procedimento na etapa 1 falhar, inicie uma sessão shell e tente determinar o nó com o estado mais recente. Inicie uma sessão shell para todos os nós disponíveis do cluster e tente iniciar seus bancos de dados executando o seguinte comando shell: `service vpostgres start`

- 3 Use o procedimento a seguir para cada nó que tenha um banco de dados local em execução para determinar o nó com o estado mais recente.

- a Execute o seguinte comando para determinar o nó com o estado mais recente. Se o comando retornar como f, ele será o nó com o estado mais recente e você poderá prosseguir para a etapa 4.

```
su - postgres
psql vcac
vcac=# select pg_is_in_recovery();
pg_is_in_recovery
```

- Se esse comando retornar como f, esse nó terá o estado mais recente.
- Caso o nó retorne um t, execute o seguinte comando no nó:

```
SELECT pg_last_xlog_receive_location() as receive_loc, pg_last_xlog_replay_location() as
replay_loc, extract(epoch from pg_last_xact_replay_timestamp()) as replay_timestamp;
```

Esse comando deve retornar um resultado semelhante ao seguinte.

```
vcac=# SELECT pg_last_xlog_receive_location() as receive_loc, pg_last_xlog_replay_location()
as replay_loc, extract(epoch from pg_last_xact_replay_timestamp()) as replay_timestamp;
 receive_loc | replay_loc | replay_timestamp
-----+-----+-----
 0/20000000 | 0/203228A0 | 1491577215.68858
(1 row)
```

- 4 Compare os resultados para cada nó para determinar qual deles tem o estado mais recente.

Selecione o nó com o maior valor na coluna `receive_loc`. Se for igual, selecione o maior da coluna `replay_loc` e, em seguida, se for igual novamente, selecione o nó com o maior valor da coluna `replay_timestamp`.

- 5 Execute o seguinte comando no nó com o estado mais recente: `vcac-vami psql-promote-master -force`
- 6 Abra o arquivo `/etc/haproxy/conf.d/10-psql.cfg` em um editor de texto e atualize a seguinte linha.

```
server masterserver sc-rdops-vm06-dhcp-170-156.eng.vmware.com:5432 check on-marked-up shutdown-
backup-sessions
```

Para ficar da seguinte maneira com o nó FQDN atual:

```
server masterserver current-node-fqdn:5432 check on-marked-up shutdown-backup-sessions
```

- 7 Salve o arquivo.
- 8 Execute o comando `service haproxy restart`.

- 9 Abra a página do **Cluster** da Interface de Gerenciamento do Appliance Virtual para o nó mais recente.

Este nó deve aparecer como o nó primário e os outros nós devem ser réplicas inválidas. Além disso, o botão **Redefinir** para as réplicas está habilitado.

- 10 Clique em **Redefinir** para cada réplica sucessivamente até que o estado do cluster seja reparado.

Backup e recuperação de instalações do vRealize Automation

Para minimizar o tempo de inatividade do sistema e a perda de dados quando ocorrem falhas, os administradores fazem backup de toda as instalações do vRealize Automation regularmente. Se ocorrer falha no sistema, você poderá fazer a recuperação restaurando o último backup e reinstalando alguns componentes.

Para fazer backup e restaurar o vRealize Automation, consulte os seguintes tópicos na [documentação do vRealize Suite](#):

- Preparações para fazer backup do vRealize Automation
- Recuperação do sistema vRealize Automation

Programa de Aperfeiçoamento da Experiência do Cliente

Este produto participa do Programa de Aperfeiçoamento da Experiência do Cliente (CEIP) da VMware. O CEIP fornece a VMware as informações que permitem VMware melhorar seus produtos e serviços, resolver problemas e aconselhar sobre a melhor forma de implantar e usar nossos produtos. É possível escolher em fazer parte ou deixar o CEIP por vRealize Automation em qualquer momento.

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>.

Participar ou sair do Programa de Aperfeiçoamento da Experiência do Cliente de vRealize Automation

Você pode participar ou sair do Programa de Aperfeiçoamento da Experiência do Cliente (CEIP) por vRealize Automation em qualquer momento.

vRealize Automation lhe dá a oportunidade de participar do Programa de Aperfeiçoamento da Experiência do Cliente (CEIP) ao instalar inicialmente e configurar o produto. Após a instalação, é possível participar ou sair do CEIP seguindo esses passos.

Procedimentos

- 1 Faça login como raiz na interface de gerenciamento do appliance do vRealize Automation.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Clique na guia **Telemetria**.
- 3 Marque ou desmarque a opção **Participar do Programa de Aperfeiçoamento da Experiência do Cliente VMware**.
Quando selecionada, a opção ativa o Programa e envia os dados para `https://vmware.com`.
- 4 Clique em **Salvar Configurações**.

Configurar o tempo de coleta de dados

É possível definir o dia e hora quando o Programa de Aperfeiçoamento da Experiência do Cliente (PAEC) envia dados para VMware.

Procedimentos

- 1 Faça login em uma sessão de console no appliance do vRealize Automation como raiz.
- 2 Abra o seguinte arquivo no editor de texto.
`/etc/telemetry/telemetry-collector-vami.properties`
- 3 Edite as propriedades para o dia da semana (dow) e hora do dia (hod).

Propriedade	Descrição
<code>frequency.dow=<dia da semana></code>	Dia quando a coleta de dados ocorre.
<code>frequency.hod=<hora do dia></code>	Horário local do dia quando a coleta de dados ocorre. Os valores possíveis são 0-23.

- 4 Salve e feche `telemetry-collector-vami.properties`.
- 5 Aplique as configurações digitando o seguinte comando.
`vcac-config telemetry-config-update --update-info`
Mudanças são aplicadas a todos os nós em sua implantação.

Ajustando as configurações do sistema

Como administrador de sistema, ajuste o registro em log e personalize modelos de e-mail IaaS. Você também pode gerenciar configurações que aparecem como padrões para cada tenant, como servidores de e-mail para lidar com notificações. Os administradores de tenant podem optar por substituir esses padrões se o seu tenant solicita diferentes configurações.

Modificar o ícone Todos os Serviços no catálogo de serviços

Você pode modificar o ícone padrão no catálogo de serviços para exibir uma imagem personalizada. Quando o ícone é modificado, a alteração é válida para todos os tenants. Não é possível configurar ícones específicos de tenant para o catálogo.

São fornecidos comandos para Linux ou Mac e Windows, para que você possa executar os comandos do cURL em qualquer um desses sistemas operacionais.

Pré-requisitos

- Converta a imagem em uma cadeia de caracteres de codificação base64.
- O cURL deve estar instalado na máquina em que os comandos são executados.
- Você deve ter as credenciais de um usuário do vRealize Automation com a função de administrador do sistema.

Procedimentos

- 1 Defina a variável VCAC na sessão de terminal para os comandos do cURL.

Sistema Operacional	Comando
Linux/Mac	<code>export VCAC=<VA URL></code>
Windows	<code>set VCAC=<VA URL></code>

- 2 Recupere o token de autenticação para o usuário administrador do sistema.

Sistema Operacional	Comando
Linux/Mac	<code>curl https://\$VCAC/identity/api/tokens --insecure -H "Accept: application/json" -H 'Content-Type: application/json' --data '{"username":"<Catalog Administrator User>","password":"<password>","tenant":"vsphere.local"}'</code>
Windows	<code>curl https://%VCAC%/identity/api/tokens --insecure -H "Accept:application/json" -H "Content-Type:application/json" --data "{\"username\":\"<Catalog Administrator User>\",\"password\":\"<password>\",\"tenant\":\"vsphere.local\"}"</code>

Um token de autenticação é gerado.

- 3 Defina a variável de token de autenticação substituindo <Auth Token> pela cadeia de caracteres de token gerada na etapa anterior.

Sistema Operacional	Comando
Linux/Mac	<code>export AUTH="Bearer <Auth Token>"</code>
Windows	<code>set AUTH=Bearer <Auth Token></code>

4 Adicione a cadeia de caracteres com codificação base64 para a imagem.

Sistema Operacional	Comando
Linux/Mac	<pre>curl https://\$VCAC/catalog-service/api/icons --insecure -H "Accept: application/json" -H 'Content-Type: application/json' -H "Authorization: \$AUTH" --data '{"id":"cafe_default_icon_genericAllServices","fileName":"<filename>","contentType":"image/png","image":"<IMAGE DATA as base64 string>"}'</pre>
Windows	<pre>curl https://%VCAC%/catalog-service/api/icons --insecure -H "Accept: application/json" -H "Content-Type: application/json" -H "Authorization: %AUTH%" --data "{\"id\":\"cafe_default_icon_genericAllServices\",\"fileName\":\"<filename>\",\"contentType\":\"image/png\",\"image\":\"<IMAGE DATA as base64 string>\"}"</pre>

Resultados

O novo ícone de serviços aparece no catálogo de serviços depois de aproximadamente cinco minutos.

Se quiser reverter para o ícone padrão, você poderá executar o seguinte comando depois de seguir as etapas de 1 a 3.

Sistema Operacional	Comando
Linux/Mac	<pre>curl https://\$VCAC/catalog-service/api/icons/cafe_default_icon_genericAllServices --insecure -H "Authorization: \$AUTH" --request DELETE</pre>
Windows	<pre>curl https://%VCAC%/catalog-service/api/icons/cafe_default_icon_genericAllServices --insecure -H "Authorization: %AUTH%" --request DELETE</pre>

Personalizar configurações de sobreposição de dados

Você pode definir as configurações de sobreposição de dados do vRealize Automation para controlar como o sistema mantém, arquiva e exclui dados legados.

Use o recurso de sobreposição de dados para ativar a sobreposição, definir o número máximo de dias para o vRealize Automation manter dados no banco de dados IaaS do SQL Server antes de os arquivar ou excluir, e outros controles de sobreposição de dados.

Por padrão, o recurso de sobreposição de dados está desativado.

Defina as configurações de sobreposição de dados na página **Configurações Globais** do vRealize Automation. Quando ativado, esse recurso consulta e remove dados das seguintes tabelas de banco de dados do SQL Server:

- UserLog
- Audit
- CategoryLog
- VirtualMachineHistory
- VirtualMachineHistoryProp

- AuditLogItems
- AuditLogItemsProperties
- TrackingLogItems
- WorkflowHistoryInstances
- WorkflowHistoryResults

Se você definir `DataRolloverIsArchiveEnabled` como `True`, versões de arquivamento das tabelas serão criadas no esquema `dbo`. Por exemplo, a versão de arquivamento do `UserLog` seria `UserLogArchive`, enquanto a versão de arquivamento do `VirtualMachineHistory` seria `VirtualMachineHistoryArchive`.

Quando habilitado, o recurso de sobreposição de dados é executado uma vez por dia em um horário predeterminado, 3h da manhã, de acordo com a configuração de fuso horário do appliance do vRealize Automation. Usando a configuração `DataRollover MaximumAgeInDays`, você pode definir o número máximo de dias que deseja manter os dados. Observe que esse processo geralmente é executado rapidamente dentro de alguns minutos a uma hora. No entanto, quando esse recurso é ativado pela primeira vez, o processo pode ter muitos dados para arquivar/excluir, e isso pode levar muito mais tempo para ser concluído. Este processo é projetado para ser executado até que seja concluído. Ele executa seu trabalho em pequenos e rápidos trechos transacionais de tamanho de lotes, para não causar problemas de simultaneidade. Observe que esse processo pode ser interrompido normalmente como descrito abaixo.

Observação Você pode interromper o processo de `DataRollover` alterando a configuração do `DataRollover Status` de `Em execução` para `Desativado` ou `Ativado`. Isso faz com que o processo em execução no momento encerre normalmente. Nenhum trabalho é perdido. Todos os dados arquivados ou excluídos até o ponto do processo de interrupção são salvos.

Se `DataRollover IsArchiveEnabled` for definido como `True`, os dados mais antigos que o período especificado na configuração do `DataRollover MaximumAgeInDays` serão movidos para as tabelas de arquivamento. Se a configuração `DataRollover IsArchiveEnabled` for definida como `False`, os dados serão permanentemente excluídos e nenhum arquivamento de dados ocorrerá. Dados excluídos não são recuperáveis.

Procedimentos

- 1 Faça login no console do vRealize Automation como um **administrador do sistema**.
- 2 Selecione **Infraestrutura > Administração > Configurações globais**.

- 3 Na página **Configurações Globais**, localize a seção **Sobreposição de Dados** da tabela e revise e defina as configurações.

Configuração	Descrição
DataRollover BatchSize	Isso é padronizado como 2000 e provavelmente não precisa ser alterado. No entanto, se parecem ser alguns impactos de desempenho, um BatchSize menor poderá ajudar. Um BatchSize maior pode obter o trabalho realizado de forma mais rápida, mas será colocado mais pressão no processamento simultâneo. O intervalo válido é de 100 a 20000.
DataRollover IsArchiveEnabled	Especifica se os dados de sobreposição devem ou não ser movidos para tabelas de arquivamento depois que o número máximo de dias tiver sido atingido. Esse valor está definido como True por padrão. Se você definir esse valor como False, todos os dados mais antigos que o período especificado na configuração DataRollover MaximumAgeInDays serão excluídos permanentemente.
DataRollover MaximumAgeInDays	Especifica o número máximo de dias durante os quais o sistema mantém dados no banco de dados antes de os mover para arquivamento ou de os excluir permanentemente. Esse valor está definido como 90 dias por padrão.
DataRollover Status	Especifica se a sobreposição de dados deve ou não ser habilitada. Esse valor está definido como Desabilitado por padrão. Para habilitar a sobreposição de dados, defina o valor como Habilitado.
DataRollover VirtualMachineHistory BatchSize	Especifica o tamanho do lote na tabela do VirtualMachineHistory no intervalo de 1 a 5 registros. A padrão é 1.
DataRollover UpdateStatistics	O UpdateStatistics está desativado por padrão, mas é altamente recomendável que seja ativado (definido como 1), pois as estatísticas atualizadas são boas para o desempenho da consulta. Isso causa o [dbo].O procedimento armazenado [usp_DataRollover] para executar o comando de estatísticas de atualização nas tabelas após o processo de arquivamento ter sido executado.

- 4 Clique no ícone **Editar** (✎) na primeira coluna da tabela para editar uma configuração.
A área de **Valor** para a configuração aplicável fica editável.
- 5 Clique no ícone **Salvar** (✔) na primeira coluna da tabela para salvar suas alterações.

Ajustando configurações no arquivo de configuração do serviço de gerenciador

Você pode usar o arquivo de configuração de serviço de gerenciador (`managerService.exe.config`) para ajustar configurações comuns para implantações de máquina.

O arquivo `managerService.exe.config` normalmente está no diretório `%Unidade-do-Sistema%\Arquivos de Programas x86\VMware\vCAC\Servidor`. Sempre faça uma cópia do arquivo antes de editá-lo.

Você pode usar as seguintes configurações de arquivo do `managerService.exe.config` para controlar vários aspectos de implantações de máquina. Os valores padrão aparecem.

- `<add key="ProcessLeaseWorkflowTimerCallbackIntervalMilliseconds" value="3600000"/>`
- `<add key="BulkRequestWorkflowTimerCallbackMilliseconds" value="10000"/>`
- `<add key="MachineRequestTimerCallbackMilliseconds" value="10000"/>`
- `<add key="MachineWorkflowCreationTimerCallbackMilliseconds" value="10000"/>`
- `<add key="RepositoryConnectionMaxRetryCount" value="100"/>`
- `<add key="MachineCatalogRegistrationRetryTimerCallbackMilliseconds" value="120000"/>`
- `<add key="MachineCatalogUnregistrationRetryTimerCallbackMilliseconds" value="120000"/>`
- `<add key="MachineCatalogUpdateMaxRetryCount" value="15"/>`

Definindo limites de simultaneidade com muitos recursos

Para conservar os recursos, o vRealize Automation limita o número de instâncias em execução simultânea do provisionamento da máquina e da coleta de dados. Você pode alterar os limites.

Configurando o provisionamento simultâneo de máquinas

Várias solicitações simultâneas de provisionamento de máquina podem impactar o desempenho do vRealize Automation. Você pode fazer algumas alterações nos limites dos agentes de proxy e das atividades do fluxo de trabalho para alterar o desempenho.

Dependendo das necessidades dos proprietários das máquinas, o servidor do vRealize Automation pode receber várias solicitações simultâneas de provisionamento de máquinas. Isso pode ocorrer nas seguintes circunstâncias:

- Um único usuário envia uma solicitação para várias máquinas
- Vários usuários solicitam máquinas ao mesmo tempo
- Um ou mais gerenciadores de grupos aprovam várias solicitações de máquinas pendentes um após o outro

O tempo necessário para o vRealize Automation provisionar uma máquina geralmente aumenta com grandes números de solicitações simultâneas. O aumento no tempo de provisionamento depende de três fatores importantes:

- O efeito do desempenho de atividades com uso intensivo de recursos do fluxo de trabalho do vRealize Automation, incluindo a atividade SetupOS (para máquinas criadas na plataforma de virtualização, como no provisionamento baseado em WIM) e a atividade Clone (para máquinas clonadas na plataforma de virtualização).
- O limite configurado para o vRealize Automation em relação ao número de atividades de provisionamento com uso intensivo de recursos (geralmente longas) que podem ser executadas simultaneamente. Por padrão, esse limite é oito. Atividades simultâneas além do limite configurado são colocadas em fila.
- Qualquer limite na plataforma de virtualização ou na conta de serviço na nuvem em relação ao número de itens de trabalho do vRealize Automation (com uso intensivo de recursos ou não) que podem ser executados simultaneamente. Por exemplo, o limite padrão no vCenter Server é quatro, sendo que os itens de trabalho que ultrapassam esse valor são colocados em fila.

Por padrão, o vRealize Automation limita atividades de provisionamento virtual simultâneas para hipervisores que usam agentes de proxy até oito por endpoint. Isso garante que a plataforma de virtualização gerenciada por um determinado agente nunca receba um número suficiente de itens de trabalho com uso intensivo de recursos que impeça a execução de outros itens. Planeje um teste cuidadoso dos efeitos da alteração do limite antes de fazer qualquer alteração.

Determinar o melhor limite para o seu local pode exigir que você investigue a execução de itens de trabalho na plataforma de virtualização e também a execução de atividades de fluxo de trabalho no vRealize Automation.

Se você aumentar o limite do vRealize Automation configurado por agente, talvez seja necessário fazer ajustes extras de configuração no vRealize Automation, como a seguir:

- Os intervalos de tempo limite de execução padrão para as atividades SetupOS e Clone do fluxo de trabalho são de duas horas para cada. Se o tempo necessário para executar uma dessas atividades exceder o limite, a atividade será cancelada e ocorrerá falha no provisionamento. Para impedir essa falha, aumente um ou ambos os intervalos de tempo limite de execução.
- Os intervalos de tempo limite de entrega padrão para as atividades SetupOS e Clone do fluxo de trabalho são de 20 horas para cada. Assim que uma dessas atividades é iniciada, se a máquina resultante da atividade não tiver sido provisionado dentro de 20 horas, a atividade será cancelada e ocorrerá falha no provisionamento. Sendo assim, se você tiver aumentado o limite para o ponto em que isso costuma ocorrer, talvez você queira aumentar um ou ambos os intervalos de tempo limite de entrega.

Configurando coletas de dados simultâneas

Por padrão, o vRealize Automation limita as atividades de coleta de dados simultâneas. Se você alterar esse limite, poderá evitar tempos limites desnecessários alterando os intervalos de tempo limite de execução padrão para os diferentes tipos de coleta de dados.

O vRealize Automation coleta regularmente dados de recursos de processamento de virtualização por meio de seus agentes de proxy e a partir de contas de serviço na nuvem e de máquinas físicas por meio dos endpoints que as representam. Dependendo do número de recursos de processamento de virtualização, agentes e endpoints em seu site, operações de coleta de dados simultâneas podem ocorrer com frequência.

O tempo de execução da coleta de dados depende do número de objetos nos endpoints, incluindo máquinas virtuais, repositórios de dados, modelos e recursos de processamento. Dependendo de várias condições, uma única coleta de dados pode exigir uma quantidade significativa de tempo. Assim como ocorre com o provisionamento de máquinas, as operações simultâneas aumentam o tempo necessário para concluir a coleta de dados.

Por padrão, as atividades simultâneas de coleta de dados são limitadas a duas por agente, sendo que as atividades que ultrapassam esse valor são colocadas em fila. Isso garante que cada coleta de dados seja concluída de forma relativamente rápida e é improvável que as atividades simultâneas de coleta de dados afetem o desempenho do IaaS.

Porém, dependendo dos recursos e das circunstâncias do seu site, é possível aumentar o limite configurado e ao mesmo tempo manter um desempenho suficientemente rápido para tirar proveito da simultaneidade na coleta de dados de proxy. Embora o aumento no limite possa aumentar o tempo necessário para a realização de uma única coleta de dados, isso pode ser compensado pela capacidade de coletar mais informações de mais recursos de processamento e de mais máquinas ao mesmo tempo.

Se você aumentar o limite configurado por agente, será preciso ajustar também os intervalos de tempo limite de execução padrão para os diferentes tipos de coleta de dados que usam um agente de proxy: inventário, desempenho, estado e WMI. Se o tempo necessário para executar uma dessas atividades exceder o intervalo de tempo limite configurado, a atividade será cancelada e reiniciada. Para impedir o cancelamento da atividade, aumente um ou mais desses intervalos de tempo limite de execução.

Ajustar limites de simultaneidade e intervalos de tempo limite

Você pode alterar os limites por agente referentes a provisionamento simultâneo, atividades de coleta de dados e intervalos de tempo limite padrão.

Ao inserir um valor de tempo para essas variáveis, use o formato hh:mm:ss (hh=horas, mm=minutos e ss=segundos).

Pré-requisitos

Faça login como administrador no servidor que hospeda o IaaS Manager Service. Para instalações distribuídas, esse é o servidor em que o Manager Service foi instalado.

Procedimentos

- 1 Abra o arquivo `ManagerService.exe.config` em um editor. O arquivo está localizado no diretório de instalação do servidor do vRealize Automation, geralmente `%SystemDrive%\Program Files x86\VMware\VCAC\Server`.
- 2 Localize a seção chamada `workflowTimeoutConfigurationSection`.
- 3 Atualize as variáveis a seguir, conforme necessário.

Parâmetro	Descrição
<i>MaxOutstandingResourceIntensive WorkItems</i>	Limite de provisionamento simultâneo (o padrão é 8)
<i>CloneExecutionTimeout</i>	Intervalo de tempo limite de execução de provisionamento virtual
<i>SetupOSExecutionTimeout</i>	Intervalo de tempo limite de execução de provisionamento virtual
<i>CloneTimeout</i>	Intervalo de tempo limite de entrega de clone de provisionamento virtual
<i>SetupOSTimeout</i>	Intervalo de tempo limite de entrega do sistema operacional de configuração de provisionamento virtual
<i>CloudInitializeProvisioning</i>	Intervalo de tempo limite de inicialização de provisionamento na nuvem
<i>MaxOutstandingDataCollectionWorkItems</i>	Limite de coleta de dados simultânea
<i>InventoryTimeout</i>	Intervalo de tempo limite de execução de coleta de dados de inventário
<i>PerformanceTimeout</i>	Intervalo de tempo limite de execução de coleta de dados de desempenho
<i>StateTimeout</i>	Intervalo de tempo limite de execução de coleta de dados de estado

- 4 Salve e feche o arquivo.
- 5 Selecione **Iniciar > Ferramentas administrativas > Serviços**.
- 6 Pare e depois reinicie o serviço do vRealize Automation.
- 7 (Opcional) Se o vRealize Automation estiver sendo executado no modo de alta disponibilidade, as alterações feitas no arquivo `ManagerService.exe.config` após a instalação deverão ser feitas no servidor principal e no servidor de failover.

Ajustar a frequência de execução de retornos de chamada da máquina

Você pode alterar a frequência de diversos procedimentos de retorno de chamada, incluindo a frequência com a qual o procedimento de retorno de chamada do vRealize Automation é executado para concessões de máquinas alteradas.

O vRealize Automation usa um intervalo de tempo configurado para executar diferentes procedimentos de retorno de chamada no serviço do Model Manager, como `ProcessLeaseWorkflowTimerCallbackIntervalMiliSeconds` que pesquisa por máquinas cujas concessões foram alteradas. Você pode alterar esses intervalos de tempo para verificar com maior ou menor frequência.

O valor de tempo para essas variáveis deve ser inserido em milissegundos. Por exemplo, 10000 milissegundos = 10 segundos e 3600000 milissegundos = 60 minutos = 1 hora.

Pré-requisitos

Faça login como administrador no servidor que hospeda o IaaS Manager Service. Para instalações distribuídas, esse é o servidor em que o Manager Service foi instalado.

Procedimentos

- 1 Abra o arquivo `ManagerService.exe.config` em um editor. O arquivo está localizado no diretório de instalação do servidor do vRealize Automation, geralmente `%SystemDrive%\Program Files x86\VMware\VCAC\Server`.
- 2 Atualize as variáveis a seguir, conforme desejado.

Parâmetro	Descrição
<i>RepositoryWorkflowTimerCallbackMiliSeconds</i>	Verifica a atividade do serviço do repositório ou Model Manager Web Service. O valor padrão é 10000.
<i>ProcessLeaseWorkflowTimerCallbackIntervalMiliSeconds</i>	Verifica se há concessões de máquinas expiradas. O valor padrão é 3600000.
<i>BulkRequestWorkflowTimerCallbackMiliSeconds</i>	Verifica solicitações em massa. O valor padrão é 10000.
<i>MachineRequestTimerCallbackMiliSeconds</i>	Verifica solicitações de máquina. O valor padrão é 10000.
<i>MachineWorkflowCreationTimerCallbackMiliSeconds</i>	Verifica se há novas máquinas. O valor padrão é 10000.

- 3 Salve e feche o arquivo.
- 4 Selecione **Iniciar > Ferramentas administrativas > Serviços**.
- 5 Interrompa e, em seguida, reinicie o serviço do vCloud Automation Center.
- 6 (Opcional) Se o vRealize Automation estiver sendo executado no modo de alta disponibilidade, as alterações feitas no arquivo `ManagerService.exe.config` após a instalação deverão ser feitas no servidor principal e no servidor de failover.

Ajustar as configurações de log do IaaS

É possível ajustar o vRealize Automation para registrar apenas as informações que você quer ver no log do Service Manager.

Se o vRealize Automation for executado no modo de alta disponibilidade e você alterar o arquivo `ManagerService.exe.config` após a instalação, você deverá fazer as alterações nos servidores primário e de failover do vRealize Automation.

Procedimentos

- 1 Faça login no servidor do vRealize Automation usando as credenciais com acesso administrativo.

- 2 Edite o arquivo `ManagerService.exe.config` em `%SystemDrive%\Program Files x86\VMware\VCAC\Server` ou no diretório de instalação do servidor do vRealize Automation, case ele esteja em um local diferente.
- 3 Edite as chaves do `RepositoryLogSeverity` e do `RepositoryLogCategory` para configurar quais tipos de eventos são gravados em seus arquivos de log.

Opção	Descrição
RepositoryLogSeverity	<p>Especifique um nível de gravidade para ignorar os eventos abaixo dessa gravidade.</p> <ul style="list-style-type: none"> ■ <i>Erro</i> registra apenas erros recuperáveis e superiores ■ <i>Aviso</i> registra avisos não críticos e superiores ■ <i>Informação</i> registra todas as mensagens informativas e superiores ■ <i>Detalhado</i> registra um rastreo de depuração e pode prejudicar o desempenho <p>Por exemplo, <code><add key="RepositoryLogSeverity" value="Warning" /></code>.</p>
RepositoryLogCategory	<p>Especifique uma categoria para registrar todos os eventos para essa categoria, independente da gravidade. Por exemplos, <code><add key="RepositoryLogCategory" value="MissingMachines,UnregisteredMachines,AcceptMachineRequest,RejectMachineRequest" /></code> registra todos os eventos para máquinas em falta ou não registradas, e cada solicitação de máquina aceita ou rejeitada.</p>

- 4 Salve e feche o arquivo.
- 5 Selecione **Iniciar > Ferramentas Administrativas > Serviços** e reinicie o serviço do vCloud Automation Center.

Resultados

É possível ver como as alterações afetam o log exibindo o arquivo de log do Manager Service localizado em `%SystemDrive%\Program Files (x86)\VMware\VCAC\Server\Logs` na máquina em que o Manager Service está instalado ou no diretório de instalação do servidor do vRealize Automation, se você tiver instalado em uma localização diferente.

Monitoramento vRealize Automation

Dependendo da sua função, você pode monitorar os fluxos de trabalho ou serviços, exibir logs de eventos ou auditoria ou coletar logs para todos os hosts em uma implantação distribuída.

Monitorando fluxos de trabalho e exibindo registros

Dependendo de sua função, você pode monitorar os fluxos de trabalho e exibir os registros de atividade.

Tabela 1-12. Opções de monitoramento e exibição de registros

Objetivo	Função	Sequência de menus e descrição
Exibir informações sobre ações que ocorreram, como o tipo de ação, a data e a hora da ação, e assim por diante.	Administrador do IaaS	Exiba as informações de registro padrão ou controle a exibição de conteúdo usando opções de coluna e de filtro. Selecione Infraestrutura > Monitoramento > Registro de auditoria . O registro de auditoria fornece detalhes sobre o status das máquinas virtuais gerenciadas e das atividades realizadas nessas máquinas durante a reconfiguração. O log inclui informações sobre provisionamento de máquina, NSX, reclamação e ações de reconfiguração.
Exibir o status de Distributed Execution Manager e outros fluxos de trabalho programados e disponíveis.	Administrador do IaaS	Exibir o status do fluxo de trabalho e, opcionalmente, abrir um fluxo de trabalho específico para exibir os respectivos detalhes. Selecione Infraestrutura > Monitoramento > Status do DEM .
Exibir e, opcionalmente, exportar dados de registro.	Administrador do IaaS	Exiba as informações de registro padrão ou controle a exibição de conteúdo usando opções de coluna e de filtro. Selecione Infraestrutura > Monitoramento > Registro .
Exibir o status e o histórico de Distributed Execution Manager e outros fluxos de trabalho.	Administrador do IaaS	Exibir o histórico do fluxo de trabalho e, opcionalmente, abrir um fluxo de trabalho específico para exibir os respectivos detalhes de execução. Selecione Infraestrutura > Monitoramento > Histórico de fluxos de trabalho .
Exibir uma lista de eventos, incluindo o tipo de evento, a hora, o ID do usuário e assim por diante, e, opcionalmente, exibir uma página de detalhes do evento.	Administrador de sistema	Exibir uma lista de eventos e respectivos atributos associados, como o tempo de execução, a descrição do evento, o nome do tenant, o tipo e o ID de destino, além outras características. Selecione Administração > Eventos > Logs de evento .
Monitorar o status das suas solicitações e exibir os respectivos detalhes.	Administrador de tenant ou gerente de grupo de negócios	Exibir o status das solicitações pelas quais você é responsável ou proprietário. Clique em Solicitações .
Visualize informações sobre eventos recentes.	Administrador do IaaS ou administrador de tenants	Exiba eventos recentes para o usuário atualmente conectado. Selecione Infraestrutura > Eventos Recentes

Monitorando logs e serviços de evento

É possível monitorar serviços e logs de evento do vRealize Automation para determinar seus estados atuais e históricos.

O período de retenção padrão para os logs de eventos é de 90 dias. Você pode alterar o período no arquivo `/etc/vcac/vcac.properties`.

Para obter informações sobre como limpar os logs personalizando as configurações de sobreposição de dados, consulte *Configurando o vRealize Automation*.

Serviços do vRealize Automation

Um administrador do sistema pode visualizar o status dos serviços do vRealize Automation a partir do Log de eventos no console do administrador do sistema.

São necessários subconjuntos de serviços para executar os componentes de produto individuais. Por exemplo, os serviços de identidade e serviços de núcleo de interface do usuário devem estar em execução antes que você possa configurar um tenant.

As tabelas a seguir indicam quais serviços estão associados a áreas de funcionalidade do vRealize Automation.

Tabela 1-13. Grupo do Serviço de identidade

Serviço	Descrição
management-service	Grupo do Serviço de identidade
sts-service	Appliance do Single Sign-on
authorization	Serviço de autorização
autenticação	Autenticação
eventlog-service	Serviço do log de eventos
licensing-service	Serviço de licença

Tabela 1-14. Serviços de núcleo de interface do usuário

Serviço	Descrição
shel-ui-app	Serviço do Shell
branding-service	Serviço de identidade visual
plugin-service	Serviço de extensibilidade (plug-in)
portal-service	Serviço do portal

Todos os seguintes serviços são necessários para executar o componente do IaaS.

Tabela 1-15. Grupo de catálogo de serviços (serviços de controle)

Serviço	Descrição
notification-service	Serviço de notificação
workitem-service	Serviço do item de trabalho

Tabela 1-15. Grupo de catálogo de serviços (serviços de controle) (continuação)

Serviço	Descrição
approval-service	Serviço de aprovação
catalog-service	Catálogo de serviços

Tabela 1-16. Grupo de serviços do IaaS

Serviço	Descrição
iaas-proxy-provider	Proxy do IaaS
iaas-server	Máquina do Windows do IaaS

Tabela 1-17. XaaS

Serviço	Descrição
vco	vRealize Orchestrator
advanced-designer-service	ações de recurso e blueprints do XaaS

Usar o log de auditoria do vRealize Automation

O vRealize Automation oferece o log de auditoria para dar suporte à coleta e à retenção de eventos importantes do sistema.

Atualmente, o vRealize Automation dá suporte ao log de auditoria como uma extensão do log de eventos. Essa funcionalidade fornece informações básicas de auditoria e as configurações de retenção são configuráveis usando apenas as chamadas de serviço de agente da REST API do vRealize Automation. O log de auditoria está disponível para os administradores de tenant e os administradores de sistema que podem fazer login em tenants. Ele fornece recursos de pesquisa e de filtro para eventos.

Por padrão, o vRealize Automation dá suporte ao log de auditoria para a assinatura de fluxo de trabalho, o endpoint e os eventos de criação, atualização e exclusão de grupos de estrutura. O vRealize Automation também dá suporte à personalização de registro em log de auditoria para uma variedade de eventos do IaaS.

O log de auditoria do vRealize Automation está desativado por padrão. Você pode ativá-lo ou desativá-lo ao acionar a caixa de seleção **Habilitado** na seção Integração do Log de Auditoria na página **vRA > Logs** da interface de gerenciamento do dispositivo virtual.

As informações de log de auditoria aparecem na página padrão Logs de Evento. Como um administrador de tenant, selecione **Administração > Logs de Evento** para exibir esta página. Os eventos de auditoria são identificados na tabela de logs de evento com a designação Auditoria no campo Tipo de Evento. Cada entrada mostra uma Descrição do Evento para cada evento como, bem como para Tenant, Tempo, Usuário e Nome do Serviço relacionado.

Habilitar o log de auditoria para todos os outros eventos do IaaS exige um arquivo de configuração personalizado e a execução dos comandos apropriados na sua máquina do host do IaaS. Entre em contato com os Serviços Profissionais da VMware para obter assistência.

Você pode configurar o vRealize Automation para exportar eventos para um servidor syslog externo, especificamente o VMware Log Insight.

Configure o vRealize Automation para Log de Auditoria do Log Insight

Você pode configurar o vRealize Automation para exportar eventos de auditoria para o VMware Log Insight para facilitar a visualização de eventos de auditoria.

O registro em log de auditoria está desativado por padrão, e você deve ativá-lo para gerar e visualizar eventos de registro em log de auditoria.

Se usado, o SSL será configurado no Appliance do vRealize Automation em que o agente do Log Insight reside e diz respeito à conexão com o servidor Syslog do Log Insight. Para usar o SSL, você deve configurar os certificados apropriados e a conectividade entre o vRealize Automation e o servidor do Log Insight instalado na sua implantação.

Pré-requisitos

O vRealize Automation usa o Agente do Log Insight instalado por padrão em uma implantação do vRealize Automation para ler entradas de log para visualização no Log Insight.

Procedimentos

- 1 Faça login na interface de Gerenciamento do appliance virtual como um administrador de sistema.
- 2 Selecione **Logs > do vRA**.
- 3 Verifique se a caixa de seleção **Habilitado** para o log de auditoria está selecionada no título Integração do Log de Auditoria.
- 4 Insira o nome da máquina do **Host** para o servidor do Log Insight no título Configuração do Agente do Log Insight.
 - a Insira o nome da máquina **Host** do agente do Log Insight.
 - b Insira a **Porta** a ser usada para comunicação com o agente do Log Insight.
 - c Selecione o protocolo de comunicação apropriado.
 - d Use a caixa de seleção **SSL Habilitado** para indicar se o SSL será usado para comunicação entre o agente do Log Insight e o servidor.

Se você optar por não usar o SSL, poderá ignorar o restante das configurações na página. Se o SSL for usado, você deverá definir essas configurações.

- 5 Faça as seleções adequadas na seção Certificados de Raiz Confiável SSL se estiver usando o SSL.

Por padrão, o Appliance do vRealize Automation usa um certificado autoassinado. Se você quiser usar um certificado de Raiz Confiável, deverá importá-lo.

- a Marque a caixa de seleção apropriada para indicar se deseja usar um novo certificado ou um certificado existente.

Para obter mais informações, consulte as observações na página Configurar Registro em Log do vRealize Automation da Interface de Gerenciamento do Appliance Virtual.

- 6 Clique em **Salvar Configurações**.

- 7 Faça as seleções apropriadas na seção Certificados de Servidor SSL.

- 8 Use a seção Configuração do Comportamento do Agente para configurar como o agente funciona com arquivos de log.

Resultados

Os eventos de log de auditoria do vRealize Automation são visíveis da interface do Log Insight.

Visualizando informações de host para clusters em ambientes distribuídos

Você pode coletar logs de todos os nós que estejam clusterizados em uma implantação distribuída do console de gerenciamento do appliance do vRealize Automation.

Você também pode visualizar informações para cada host na implantação. A guia **Cluster** no console de gerenciamento do vRealize Automation inclui uma tabela de Informações de implantação distribuída que exibe as seguintes informações:

- Uma lista de todos os nós na implantação.
- O nome de host do nó. O nome de host dado como um nome de domínio inteiramente qualificado.
- O horário desde que o host respondeu ao console de gerenciamento pela última vez. Os nós para componentes do IaaS relatam a disponibilidade a cada três minutos e os nós para dispositivos virtuais relatam a cada nove minutos.
- O tipo de componente do vRealize Automation. Identifica se o nó é um appliance virtual ou um servidor de IaaS.

Figura 1-1. Tabela de informações de implantação distribuída

	Host / Node Name	Version	Last Connected	Type	State*	Valid*
▶	cava-n-80-175.eng.vmware.com	7.5.0.378	7 minutes ago	MASTER	Up	Delete
▶	cava-n-85-043.eng.vmware.com	7.5.0.14528	14 seconds ago	IAAS		Delete

Você pode usar essa tabela para monitorar a atividade na implantação. Por exemplo, se a coluna Conectado pela última vez em indicar que um host não se conectou recentemente, isso poderá indicar um problema com o servidor do host.

Coleta de logs

É possível criar um arquivo zip que contenha arquivos de log para todos os hosts em sua implantação usando o botão Criar Pacote de Suporte na página **vRA > Logs**. Para obter mais informações, consulte [Coletar logs de implantações distribuídas e clusters](#).

Removendo nós da tabela

Ao remover um host da implantação, remova o nó correspondente da tabela de informações de implantação distribuída para otimizar os tempos de coleta de logs. Clique no botão **Excluir** para remover um nó da tabela.

Coletar logs de implantações distribuídas e clusters

Para oferecer suporte à solução de problemas e a atividades de manutenção de registros, você pode criar um arquivo zip que inclua todos os arquivos de log para servidores na sua implantação.

A tabela de informações de implantação distribuída na guia Cluster da interface de gerenciamento do appliance virtual lista os nós para os quais os arquivos de log são coletados. Você também pode excluir os nós desta tabela.

Para obter informações relacionadas sobre a configuração de implantação do appliance do vRealize Automation, consulte *Instalando o vRealize Automation*.

Procedimentos

- 1 Faça login na interface de Gerenciamento do appliance virtual como um administrador de sistema.
- 2 Clique em **vRA > Registros**.
- 3 Clique em **Criar Pacote de Suporte**.

Os arquivos de log de cada nó são coletados e copiados em um arquivo zip.

Remover um nó da tabela de Informações de Implantação distribuída

Exclua um nó quando quiser removê-lo do seu cluster de implantação ou quando você estiver substituindo um certificado de agente de gerenciamento.

A tabela de informações de implantação distribuída na guia Cluster da interface de gerenciamento do appliance virtual lista os nós para o cluster aplicável. Você pode clicar no botão **Excluir** de qualquer nó na tabela para remover esse nó do cluster, ou você pode usar o procedimento a seguir.

Procedimentos

- 1 Faça login no appliance do vRealize Automation usando o nome de usuário **raiz** e a senha especificados ao implantar o appliance.

- 2 Clique na guia **Cluster**.

A tabela Informações de implantação distribuída lista os nós para a implantação distribuída.

- 3 Localize o ID do nó a ser excluído, abrindo um prompt de comando e executando o seguinte comando:

```
/usr/sbin/vcac-config cluster-config-node --action list
```

- 4 Localize o ID do nó, por exemplo `cafe.node.46686239.17144`, na saída JSON.

- 5 Abra um prompt de comando e digite um comando com o seguinte formato, usando o ID do nó obtido na etapa anterior.

```
/usr/sbin/vcac-config cluster-config-node  
--action delete --id UID do nó
```

Por exemplo, insira o seguinte comando para o ID do nó de exemplo `cafe.node.46686239.17144`:

```
/usr/sbin/vcac-config cluster-config-node --action delete --id cafe.node.46686239.17144
```

- 6 Clique em **Atualizar**.

O nó já não aparece na tela.

Monitorando a integridade do vRealize Automation

O serviço de Integridade do vRealize Automation avalia a integridade funcional de um ambiente do vRealize Automation.

Os administradores do IaaS configuram o Serviço de Integridade para executar pacotes de teste que determinam se os componentes estão registrados e se os recursos necessários estão disponíveis. Esta tabela mostra os pacotes de teste fornecidos pelo Serviço de Integridade e alguns testes de exemplo em cada pacote.

Kis de teste de serviço de integridade	Testes de exemplo
Testes do sistema para o vRealize Automation	<ul style="list-style-type: none"> ■ Teste de conexão de VA de identidade/SSO ■ Verificação de licença do vRealize Automation - A licença expirou? ■ Verificação de senha raiz do appliance virtual do vRealize Automation - A senha expirará em breve?
Testes de tenant para o vRealize Automation	<ul style="list-style-type: none"> ■ Verificar caminhos de armazenamento de reserva do vSphere ■ Verificar atribuições de política de reserva a reservas ■ Verificar status do serviço do portal
Testes para o vRealize Orchestrator	<ul style="list-style-type: none"> ■ Verificar o número de nós vRO ativos ■ Verificar a utilização do heap de memória Java nos nós do vRO ■ Verificar o status do serviço vro-server nos nós do vRO

Depois de executar um pacote de testes em uma máquina virtual, o Serviço de Integridade relata o número de testes que foram aprovados ou reprovados. Para cada teste reprovado, o Serviço de Integridade fornece estes links:

Link	Conteúdo
Causa	Explicação da causa da reprovação.
Correção	Informações que você pode usar para corrigir o problema.

Você pode configurar o Serviço de Integridade para executar testes com base em uma programação ou sob demanda.

Você também pode usar o Python para criar testes personalizados. Consulte o *Guia de extensibilidade do Serviço de Integridade do vRealize Automation*.

Os administradores de tenants com uma função de Consumidor de Integridade podem visualizar resultados de testes para suas locações, mas não podem configurar ou executar um teste.

Configurar testes do sistema para o vRealize Automation

Um **administrador do IaaS** configura o Serviço de Integridade para executar testes de sistema em um appliance virtual do vRealize Automation selecionado. Esses testes determinam se os componentes, como a licença do vRealize Automation, estão registrados e se os recursos necessários, como a memória, estão disponíveis no appliance virtual. Quando você configura os testes de sistema, a página Integridade exibe os testes como um cartão de teste.

Para configurar o Serviço de Integridade de modo a executar testes de sistema para o vRealize Automation, siga este procedimento.

Pré-requisitos

Faça login no vRealize Automation como **administrador do IaaS**.

Procedimentos

- 1 Selecione **Administração > Integridade**.
- 2 Clique em **Nova Configuração**.
- 3 Na página Detalhes da Configuração, forneça as informações solicitadas.

Opção	Descrição
Nome	Seu título para essa configuração. Esse título é exibido no cartão de teste.
Descrição	Uma descrição do pacote de testes.
Produto	Selecione vRealize Automation.
Programação	Selecione com que frequência o pacote de testes é executado.

- 4 Clique em **Avançar**.
- 5 Na página Selecionar Pacotes de Teste, escolha **Testes do Sistema para o vRealize Automation**.
- 6 Clique em **Avançar**.
- 7 Na página Parâmetros da Configuração, forneça as informações solicitadas.

Tabela 1-18. Appliance virtual vRealize Automation

Opção	Descrição
Endereço do Servidor Web Público	<ul style="list-style-type: none"> ■ Para uma implantação mínima, a URL base para o host do appliance do vRealize Automation. Por exemplo, <code>https://va-host.domain/</code>. ■ Para uma implantação de alta disponibilidade, a URL base para o balanceador de carga do vRealize Automation. Por exemplo, <code>https://load-balancer-host.domain/</code>.
Endereço do Console SSH	Nome do domínio totalmente qualificado do appliance vRealize Automation. Por exemplo, <code>va-host.domain</code> .
Usuário do Console SSH	raiz
Senha do Console SSH	A senha raiz.

Tabela 1-19. Tenant do Sistema vRealize Automation

Opção	Descrição
Administrador de Tenants do Sistema	administrador
Senha do Tenant do Sistema	A senha do administrador.

Tabela 1-20. Monitoramento do Espaço em Disco do vRealize Automation

Opção	Descrição
Porcentagem de Limite de Aviso	Porcentagem aceitável do espaço em disco do appliance virtual que é usada antes de o teste de aviso falhar.
Porcentagem de Limite Crítico	Porcentagem aceitável do espaço em disco do appliance virtual que é usada antes de o teste crítico falhar.

8 Clique em **Avançar**.

9 Na página Resumo, reveja as informações.

10 Clique em **Concluir**.

Os testes são executados segundo a programação selecionada.

Próximo passo

[Visualizar os resultados do pacote de testes do serviço de integridade do vRealize Automation](#)

Configurar testes de tenant para o vRealize Automation

Um **administrador do IaaS** configura o Serviço de Integridade para executar testes de tenant em um appliance virtual do vRealize Automation selecionado. Esses testes determinam se os componentes relacionados ao tenant, como o software-serviço, estão registrados e se os recursos necessários, como as máquinas virtuais do vSphere, estão disponíveis no appliance virtual. Quando você configura os testes de tenant, a página Integridade exibe os testes como um cartão de teste.

Para configurar o Serviço de Integridade de modo a executar testes de tenant para o vRealize Automation, siga este procedimento.

Pré-requisitos

Faça login no vRealize Automation como **administrador do IaaS**.

Procedimentos

1 Selecione **Administração > Integridade**.

2 Clique em **Nova Configuração**.

3 Na página Detalhes da Configuração, forneça as informações solicitadas.

Opção	Descrição
Nome	Seu título para essa configuração. Esse título é exibido no cartão de teste.
Descrição	Uma descrição dos testes.

Opção	Descrição
Produto	Selecione vRealize Automation.
Programação	Selecione a frequência da execução dos testes.

- 4 Clique em **Avançar**.
- 5 Na página Selecionar Pacotes de Teste, escolha **Testes de Tenant para o vRealize Automation**.
- 6 Clique em **Avançar**.
- 7 Na página Parâmetros da Configuração, forneça as informações solicitadas.

Tabela 1-21. Appliance virtual vRealize Automation

Opção	Descrição
Endereço Web do vRealize Automation	<ul style="list-style-type: none"> ■ Para uma implantação mínima, a URL base para o host do appliance do vRealize Automation. Por exemplo, <code>https://va-host.domain/</code>. ■ Para uma implantação de alta disponibilidade, a URL base para o balanceador de carga do vRealize Automation. Por exemplo, <code>https://load-balancer-host.domain/</code>.
Endereço do Console SSH	Nome do domínio totalmente qualificado do host SSH. Por exemplo, <code>ssh-host.domain</code> .
Usuário do Console SSH	raiz
Senha do Console SSH	Senha para a raiz.
Tempo máximo de resposta do serviço (ms)	Quantidade máxima de tempo em milissegundos que o sistema aguarda uma resposta.

Tabela 1-22. Tenant do vRealize Automation

Opção	Descrição
Tenant em Teste	qe
Nome de Usuário do Administrador da Estrutura	<p>Nome de usuário do administrador da estrutura.</p> <p>Observação O administrador da estrutura também deve ter um administrador de locatário e uma função de administrador de IaaS para que todos os testes sejam executados.</p>
Senha do Administrador da Estrutura	Senha para o administrador da estrutura.

Tabela 1-23. Tenant do Sistema vRealize Automation

Opção	Descrição
Administrador de Tenants do Sistema	administrador
Senha do Tenant do Sistema	Senha para o administrador.

Tabela 1-24. Monitoramento do Espaço em Disco do vRealize Automation

Opção	Descrição
Porcentagem de Limite Crítico	Porcentagem aceitável do espaço em disco do appliance virtual que é usada antes de o teste crítico falhar.

- 8 Clique em **Avançar**.
- 9 Na página Resumo, reveja as informações.
- 10 Clique em **Concluir**.
Os testes são executados segundo a programação selecionada.

Próximo passo

[Visualizar os resultados do pacote de testes do serviço de integridade do vRealize Automation](#)

Configurar testes para o vRealize Orchestrator

Um **administrador do IaaS** configura o serviço de integridade para executar testes para o vRealize Orchestrator no host do vRealize Orchestrator. Esses testes confirmam se os componentes, como o serviço vro-server, estão registrados e se os recursos necessários, como heap de memória Java suficiente, estão disponíveis na máquina do host. Quando você configura os testes vRealize Orchestrator, a página Integridade exibe os testes como um cartão de teste.

Pré-requisitos

Faça login no vRealize Automation como **administrador do IaaS**.

Procedimentos

- 1 Selecione **Administração > Integridade**.
- 2 Clique em **Nova Configuração**.
- 3 Na página Detalhes da Configuração, forneça as informações solicitadas.

Opção	Descrição
Nome	Seu título para essa configuração. Esse título é exibido no cartão de teste.
Descrição	Uma descrição dos testes.

Opção	Descrição
Produto	Selecione vRealize Orchestrator.
Programação	Selecione a frequência de execução dos testes.

- 4 Clique em **Avançar**.
- 5 Na página Selecionar Pacotes de Teste, escolha **Testes para o vRealize Orchestrator**.
- 6 Clique em **Avançar**.
- 7 Na página Parâmetros da Configuração, forneça as informações solicitadas.

Tabela 1-25. Host/Balanceador de Carga do vRealize Orchestrator

Opção	Descrição
Endereço do Cliente	<ul style="list-style-type: none"> ■ Para uma implantação mínima, o nome de domínio totalmente qualificado do host vRealize Orchestrator . Por exemplo, <i>vro-host.domain</i>. ■ Para uma implantação de alta disponibilidade, a URL base para o balanceador de carga do vRealize Orchestrator, <i>https://load-balancer-host.domain/</i>.
Nome de Usuário do Cliente	administrador
Senha do Cliente	A senha do administrador.
Nome de Usuário do Console SSH	raiz
Senha do Console SSH	A senha raiz.
Limite de Utilização do Heap	Porcentagem aceitável do espaço do heap que é usada antes de o teste de aviso falhar.

Tabela 1-26. Instâncias do vRealize Orchestrator atrás do balanceador de carga

Opção	Descrição
Endereço do Console SSH	Endereço IP ou URL da instância do vRealize Orchestrator atrás do balanceador de carga.
Nome de Usuário do Console SSH	Nome de usuário com acesso a essa instância.
Senha do Console SSH	A senha do nome do usuário.

- Clique em **ADICIONAR** para adicionar outra instância do vRealize Orchestrator à lista.
- Clique em **REMOVER** para remover uma instância selecionada do vRealize Orchestrator da lista de instâncias atrás do balanceador de carga.

- 8 Clique em **Avançar**.
- 9 Na página Resumo, reveja as informações.

10 Clique em **Concluir**.

Os testes são executados segundo a programação selecionada.

Próximo passo

[Visualizar os resultados do pacote de testes do serviço de integridade do vRealize Automation](#)

Pacote de testes personalizado

Você pode usar o Python para criar um pacote de testes personalizado para o Serviço de Integridade do vRealize Automation .

A criação de um pacote de testes personalizado permite estender os testes fornecidos para o serviço de integridade, adicionando um pacote de testes para determinar a integridade dos componentes adicionais do vRealize Automation. Para obter informações sobre como criar um pacote de testes personalizado, consulte o *vRealize Automation Guia de extensibilidade do serviço de integridade*.

Adicionar um pacote de testes personalizado

Um **Administrador do IaaS** deve adicionar um pacote de testes personalizado ao serviço de integridade do vRealize Automation antes de executar o pacote de testes.

Para adicionar um pacote de testes personalizado a um ativo do vRealize Automation, execute este procedimento.

Pré-requisitos

- Crie um indicador Python para os arquivos do pacote de testes personalizado. Para obter informações, consulte o *vRealize Automation Guia de extensibilidade do serviço de integridade*.
- Faça login no vRealize Automation como **administrador do IaaS**.

Procedimentos

- 1** Clique em **Administração > Integridade**.
- 2** No canto superior direito, clique no ícone de engrenagem e selecione **Extensibilidade**.
- 3** Clique em **Novo ativo**.
- 4** Na caixa de diálogo Adicionar Ativo, forneça as informações solicitadas.

Opção	Descrição
Título do ativo	O número de versão e o nome do pacote de testes que você estiver executando, por exemplo, Infoblox 1.0.
Descrição do ativo	Uma descrição dos testes contidos no indicador Python.

Opção	Descrição
Versão do ativo	Número de versão do pacote de teste.
Arquivo do ativo	Clique em Escolher arquivo e selecione o arquivo do seu pacote de teste personalizado.

5 Clique em **Adicionar**.

Uma nova linha é adicionada à tabela de ativos com o status **UPLOADED**. Quando o status muda para **INSTALLED**, o pacote de testes está pronto para uso. Se o processo de instalação falhar, você verá um pop-up com um motivo.

Observação Se a página não for atualizada, clique no ícone de atualização.

Próximo passo

[Executar um pacote de testes personalizado.](#)

Executar um pacote de testes personalizado

Um **administrador do IaaS** configura o serviço de integridade para um pacote de testes personalizado no ambiente do vRealize Automation. Quando você configura o pacote de testes personalizado, a página Integridade exibe o pacote de testes como cartão de teste.

Para configurar o serviço de integridade de modo a executar um pacote de testes personalizado para o vRealize Automation, siga este procedimento.

Pré-requisitos

- [Adicionar um pacote de testes personalizado.](#)
- Faça login no vRealize Automation como **administrador do IaaS**.

Procedimentos

- 1 Selecione **Administração > Integridade**.
- 2 Clique em **Nova Configuração**.
- 3 Na página Detalhes da Configuração, forneça as informações solicitadas.

Opção	Descrição
Nome	Seu título para essa configuração. Esse título é exibido no cartão de teste.
Descrição	Uma descrição do pacote de testes.
Produto	Selecione o produto que deseja testar no menu suspenso Produto .
Programação	Selecione com que frequência você deseja executar esse pacote de testes.

4 Clique em **Avançar**.

- 5 Na página Selecionar Pacotes de Teste, selecione o pacote de teste personalizado e clique em **Avançar**.
- 6 Na página Configurar Parâmetros, insira as informações solicitadas e clique em **Avançar**.
- 7 Na página Resumo, revise as informações e clique em **Concluir**.

O pacote de testes personalizado é executado segundo a programação selecionada.

Próximo passo

[Visualizar os resultados do pacote de testes do serviço de integridade do vRealize Automation](#)

Visualizar os resultados do pacote de testes do serviço de integridade do vRealize Automation

Você pode visualizar os resultados do pacote de teste do serviço de integridade após executá-los.

A página Integridade exibe cada pacote de testes configurado como um cartão de teste. Quando um pacote de testes é executado, o resultado aparece no meio do cartão de teste.

Os cartões de teste que você vê na página Integridade são filtrados de acordo com o seu privilégio.

- Os administradores do IaaS podem ver todos os cartões de teste.
- Os administradores de tenants com a função de Consumidor de Integridade podem ver apenas o cartão de teste de suas locações.

Pré-requisitos

- O pacote de teste configurado foi executado na programação.
- Faça login no console do vRealize Automation como **administrador do IaaS** ou **administrador de tenants**.

Procedimentos

- 1 Selecione **Administração > Integridade**.
- 2 Se um teste não está programado para execução, clique em **Executar** no cartão de teste.
- 3 Clique no centro de um cartão de teste depois que os testes forem concluídos.

Aparece uma página que exibe o status de cada teste. Para ver por que um teste foi reprovado, clique em **Causa**. Para abrir um tópico que explica como corrigir o problema, clique no link de **Correção**, caso haja um disponível.

Solucionando problemas com o serviço de integridade

Os tópicos de solução de problemas com o Serviço de Integridade fornecem soluções para problemas que você pode enfrentar ao usar o Serviço de Integridade.

O teste do status de serviço falha

Você pode corrigir um teste de serviço com falha alterando a configuração da programação de teste.

Problema

Se um teste de status de serviço falhar e você clicar em **Causa**, verá esta mensagem: Não é possível estabelecer uma conexão SSH; Mensagem de exceção:[Falha de autenticação].

Causa

Quando o pacote de testes está programado para execução a cada 15 minutos, o login do sistema bloqueia a conta do usuário raiz.

Solução

- ◆ Altere a programação de teste para **Nenhum**, aguarde 15 minutos e execute o conjunto de testes novamente.

Após atualizar a Página de Integridade no Console do Appliance está vazia

Após atualizar o vRealize Automation, a Página de Integridade no Console do Appliance está vazia.

Problema

O serviço de integridade não inicia após atualizar.

Solução

- ◆ Em cada appliance virtual do vRealize Automation, abra um prompt de comando como **root** e execute estes comandos.
 - a Para configurar o serviço de integridade para iniciar automaticamente, execute este comando.

```
chkconfig vrhb-service on
```
 - b Para iniciar o serviço de integridade neste appliance virtual, execute este comando.

```
service vrhb-service start
```

Monitoramento de recursos de ambiente do vRealize Automation usando SNMP

Como administrador de sistema familiarizado com o SNMP, você deseja usar a REST API do vRealize Automation para vSNMP para facilitar a forma como você monitora seus nós do vRealize Automation. Usando o vSNMP, você pode usar o SNMP para atuar como um sistema de aviso de início criptografado quando o vRealize Automation está prestes a ficar sem CPU, RAM ou espaço em disco, para evitar quedas de memória.

Você pode monitorar manualmente os OIDs SNMP ou pode monitorar os recursos ativamente ao configurar interceptações SNMP.

Por exemplo, se o vSNMP enviar um evento, como "uso excessivo de CPU detectado", você poderá começar a coletar informações sobre os processos que consomem a CPU e determinar qual deles está usando recursos excessivos. Em seguida, você poderá correlacionar a CPU, a memória e outros usos para solucionar problemas adicionais.

Usando o vRealize Automation vSNMP, você pode expor toda a árvore do Linux para monitoramento e recuperação de dados usando a REST API ou usando o daemon vSNMPD que está sendo executado em suas instâncias do vRealize Automation.

O vRealize Automation SNMP não tem uma interface de uso geral. Você deve usar os comandos da REST API ou do daemon.

Para obter mais informações, consulte "Usando o SNMP para monitorar o vRealize Automation" no Guia de Programação do vRealize Automation. Para localizar o Guia de Programação, consulte [Documentação da API do vRealize Automation](#) e selecione o link da versão.

Monitorando e gerenciando recursos

Diferentes funções do vRealize Automation monitoram o uso de recursos e gerenciam a infraestrutura de maneiras diferentes.

Escolhendo um cenário de monitoramento de recursos

Os administradores de estrutura, administradores de tenant e gerenciadores de grupos de negócios possuem diferentes interesses no que diz respeito ao monitoramento de recursos. Por isso, o vRealize Automation permite que você monitore diferentes aspectos da utilização de recursos.

Por exemplo, um administrador de estrutura se preocupa em monitorar o consumo de recursos de reservas e de recursos de processamento, já um administrador de tenant se preocupa com a utilização de recursos dos grupos de provisionamento em um tenant. O vRealize Automation possibilita diferentes maneiras de controlar o consumo de recursos, dependendo da sua função e da utilização de recursos em específico que você deseja monitorar.

Tabela 1-27. Escolher um cenário de monitoramento de recursos

Cenário de monitoramento de recursos	Privilégios necessários	Localização
Monitore a quantidade de memória e armazenamento físico atualmente consumida pelos recursos de processamento e determine a quantidade que permanece disponível. Você também pode monitorar o número de máquinas reservadas e alocadas que são provisionadas em cada recurso de processamento.	Administrador de estrutura (monitorar a utilização dos recursos de processamento no grupo de estrutura)	Infraestrutura > Recursos de processamento > Recursos de processamento
Monitore as máquinas atualmente provisionadas e sob gerenciamento do vRealize Automation.	Administrador de estrutura	Infraestrutura > Máquinas > Máquinas gerenciadas
Monitore a quantidade de armazenamento, memória e cota de máquina da reserva que está atualmente alocada e determine a capacidade que continua disponível.	Administrador de estrutura (monitorar a utilização dos recursos para reservas nos recursos de processamento e em máquinas físicas)	Infraestrutura > Reservas > Reservas
Monitore a quantidade de armazenamento, memória e cota de máquina atualmente consumida pelos grupos de negócios e determine a capacidade que continua disponível.	<ul style="list-style-type: none"> ■ Administrador de tenant (monitorar a utilização de recursos para todos os grupos no tenant) ■ Gerenciador de grupos de negócios (monitorar a utilização de recursos para os grupos que você gerencia) 	Administração > Usuários e grupos > Grupos de negócios

Terminologia de uso de recurso

O vRealize Automation usa uma terminologia explícita para distinguir entre os recursos que estão disponíveis, os recursos que foram separados para usos específicos e os recursos que estão sendo consumidos ativamente por máquinas provisionadas.

A tabela de Terminologia de uso de recursos explica a terminologia que o vRealize Automation usa para exibir o uso de recursos.

Tabela 1-28. Terminologia de uso de recurso

Termo	Descrição
Físico	Indica a memória real ou capacidade de armazenamento de um recurso de computação.
Reservado	Indica a cota, a memória e a capacidade de armazenamento de uma máquina separadas para uma reserva. Por exemplo, se um recurso de computação tiver uma capacidade física de 600 GB e houver três reservas de 100 GB em cada, o armazenamento reservado do recurso de computação será de 300 GB e o armazenamento reservado será de 50%.
Gerenciado	Indica que a máquina está provisionada e sob gerenciamento do vRealize Automation.
Alocado	Indica os recursos de cota, memória ou armazenamento que estão sendo consumidos ativamente pelas máquinas provisionadas. Por exemplo, considere uma reserva com uma cota de máquina igual a dez. Se houver 15 máquinas provisionadas nessa cota, mas apenas seis delas estiverem ligadas no momento, a taxa de alocação da cota da máquina será de 60%.
Usado	O valor da coluna Usado sempre é igual ao valor da coluna Alocado .
Disponível	Indica a capacidade física não utilizada em um caminho de armazenamento.

Conectando a uma máquina na nuvem

Na primeira vez que se conectar a uma máquina na nuvem, faça login como Administrador.

Em seguida, você poderá adicionar as credenciais com as quais faz login no console do vRealize Automation como usuário na máquina e fazer login com as credenciais do vRealize Automation a partir daí.

Importante Se você estiver usando o Amazon Web Services, o RDP ou o SSH deverá estar habilitado na instância da máquina Amazon e as máquinas deverão estar em um grupo de segurança no qual as portas corretas estejam abertas.

Coletar credenciais do usuário para uma máquina do Amazon

Para fazer login como administrador em uma máquina Amazon, você deve obter a senha de administrador da máquina.

A senha de administrador está disponível na página Detalhes de informações da máquina. Se a imagem da máquina Amazon a partir da qual a máquina foi provisionada não estiver configurada para gerar a senha de administrador em cada inicialização, você precisará obter a senha usando uma técnica alternativa. Para obter informações sobre como obter a senha de administrador de outra maneira, pesquise nos tópicos *Conectar-se à instância Amazon EC2* na documentação Amazon.

Se necessário, você pode criar as credenciais de usuário necessárias do vRealize Automation. As credenciais do usuário serão válidas para futuros logins nessa máquina.

Pré-requisitos

- A máquina Amazon já foi provisionada.
- Faça login no vRealize Automation como proprietário da máquina, **gerente de grupos de negócios** ou **usuário de suporte**.
- O RDP ou SSH está ativo na imagem de máquina Amazon que será usada para provisionamento
- As máquinas estão em um grupo de segurança no qual as portas corretas estão abertas.

Procedimentos

- 1 Vá para a página **Itens** e filtre por grupos gerenciados ou por um grupo específico.
- 2 Selecione a máquina Amazon na lista de máquinas.
Clique em **Exibir detalhes** no menu suspenso **Ações** para exibir detalhes, como o tipo de máquina.
- 3 Selecione **Editar** no menu suspenso **Ações**.
- 4 Clique em **Mostrar senha do administrador** para obter a senha do administrador da máquina.
Como alternativa, é possível obter a senha usando um procedimento externo da Amazon.
- 5 Clique em **Conectar usando RDP** no menu suspenso **Ações**.
- 6 Clique em **Usar outra conta** quando forem solicitadas as credenciais de login.
- 7 Digite **LOCAL\Administrador** quando for solicitado o nome de usuário.
- 8 Digite a senha de administrador quando solicitada.
- 9 Clique em **OK**.
Agora, você está conectado à máquina como administrador.
- 10 Adicione as credenciais do vRealize Automation conforme apropriado. Por exemplo, em uma máquina de servidor do Windows, abra o gerenciador de servidores e selecione **Configuração > Usuários e grupos locais** e adicione as credenciais, usando um formato **DOMÍNIO\nome de usuário**, ao grupo **Usuários da área de trabalho remota**.
Seu nome de usuário e senha do vRealize Automation agora são credenciais válidas para futuros logins nessa máquina.
- 11 Faça logout da máquina Amazon.
- 12 Clique em **Conectar usando RDP** no menu suspenso **Ações**.
- 13 Quando solicitado o login, digite as credenciais de senha e nome de usuário do vRealize Automation para fazer login na máquina.

Resultados

Os proprietários de máquina agora podem fazer login na máquina usando suas credenciais do vRealize Automation.

Coletar credenciais do usuário para uma máquina do vCloud

Para fazer login em uma máquina do vCloud Air ou do vCloud Director como administrador, você deve obter a senha de administrador da máquina.

A senha de administrador está disponível na página Detalhes de informações da máquina. Se a imagem de máquina a partir da qual a máquina foi provisionada não estiver configurada para gerar a senha de administrador em cada inicialização, você pode encontrar a senha usando uma técnica alternativa. Para informações sobre como obter a senha de administrador de outra maneira, consulte a documentação do vCloud Air ou do vCloud Director.

Se necessário, você pode criar as credenciais de usuário necessárias do vRealize Automation. As credenciais do usuário serão válidas para futuros logins nessa máquina.

Pré-requisitos

- A máquina do vCloud Air ou vCloud Director já foi provisionada.
- Faça login no vRealize Automation como proprietário da máquina, **gerente de grupos de negócios** ou **usuário de suporte**.
- O RDP ou SSH está ativo na imagem de máquina do vCloud Air ou vCloud Director, que será usada para provisionamento
- As máquinas estão em um grupo de segurança no qual as portas corretas estão abertas.

Procedimentos

- 1 Vá para a página **Itens** e filtre por grupos gerenciados ou por um grupo específico.
- 2 Selecione a máquina do vCloud Air ou do vCloud Director na lista de máquinas.
Clique em **Exibir detalhes** no menu suspenso **Ações** para exibir detalhes, como o tipo de máquina.
- 3 Selecione **Editar** no menu suspenso **Ações**.
- 4 Clique em **Mostrar senha do administrador** para obter a senha do administrador da máquina.
Como alternativa, é possível obter a senha usando um procedimento externo do vCloud Air ou do vCloud Director.
- 5 Clique em **Conectar usando RDP** no menu suspenso **Ações**.
- 6 Clique em **Usar outra conta** quando forem solicitadas as credenciais de login.
- 7 Digite **LOCAL\Administrador** quando for solicitado o nome de usuário.
- 8 Digite a senha de administrador quando solicitada.
- 9 Clique em **OK**.

Agora, você está conectado à máquina como administrador.

- 10 Adicione as credenciais do vRealize Automation conforme apropriado. Por exemplo, em uma máquina de servidor do Windows, abra o gerenciador de servidores e selecione **Configuração > Usuários e grupos locais** e adicione as credenciais, usando um formato **DOMÍNIO\nome de usuário**, ao grupo **Usuários da área de trabalho remota**.

Seu nome de usuário e senha do vRealize Automation agora são credenciais válidas para futuros logins nessa máquina.

- 11 Faça logout da máquina do vCloud Air ou do vCloud Director.
- 12 Clique em **Conectar usando RDP** no menu suspenso **Ações**.
- 13 Quando solicitado o login, digite as credenciais de senha e nome de usuário do vRealize Automation para fazer login na máquina.

Resultados

Os proprietários de máquina agora podem fazer login na máquina usando suas credenciais do vRealize Automation.

Reduzindo o uso de reserva por atrito

Os administradores de malha podem reduzir o número de máquinas em uma reserva particular, a longo prazo, mantendo a reserva e as máquinas existentes provisionadas em ativo.

É possível reduzir a cota de máquina reservada, memória e armazenamento de uma reserva virtual abaixo do valor atualmente afetado. Isso permite o gerenciamento de máquinas existentes para continuar sem mudança, evitando o provisionamento de novas máquinas até a alocação cair abaixo do novo valor reservado.

Observação Como as máquinas virtuais desligadas não estão incluídas nos totais de cota de memória e de máquina, reduzir a alocação de memória ou da máquina de uma reserva pode impedir que as máquinas que estão atualmente desligadas sejam novamente ligadas.

Por exemplo, considere um grupo de negócios com uma reserva que contém 20 máquinas provisionadas que estão definidas para expirar nos próximos 90 dias. Se você quiser reduzir essa reserva pelo atrito para não mais de 15 máquinas, é possível editar a reserva para reduzir a cota de 20 máquinas para 15. Nenhuma máquina pode ser provisionada na reserva até que o número de máquinas na reserva seja naturalmente reduzido pelas próximas expirações.

Desativando um caminho de armazenamento

Se você estiver desativando um caminho de armazenamento e movendo máquinas para um novo, um administrador de estrutura deverá desativar o caminho de armazenamento no vRealize Automation.

Esta é uma visão geral de alto nível da sequência de etapas necessárias para desativar um caminho de armazenamento:

- 1 Um administrador de estrutura desativa o caminho de armazenamento em todas as reservas que o utilizam. Consulte [Desativar um caminho de armazenamento](#).

- 2 Mova as máquinas para um novo caminho de armazenamento fora do vRealize Automation.
- 3 Aguarde que o vRealize Automation execute automaticamente a coleta de dados de inventário ou inicie a coleta de dados de inventário manualmente. Consulte [Configurar a coleta de dados de recursos de processamento](#).

Desativar um caminho de armazenamento

Os administradores de malha podem desativar os caminhos de armazenamento em reservas quando eles são desativados.

Observação Em cada reserva na qual você desativar um caminho de armazenamento, verifique se há espaço suficiente restante nos outros caminhos de armazenamento ativados.

Pré-requisitos

Faça login no vRealize Automation como **administrador de estrutura**.

Procedimentos

- 1 Selecione **Infraestrutura > Reservas > Reservas**.
- 2 Aponte para a reserva na qual o caminho de armazenamento que você está desativando é usado e clique em **Editar**.
- 3 Clique na guia **Recursos**.
- 4 Localize o caminho de armazenamento que você está desativando.
- 5 Clique no ícone **Editar** (✎).
- 6 Marque a caixa de seleção na coluna Desativado para desativar esse caminho de armazenamento.
- 7 Clique no ícone **Salvar** (✓).
- 8 Clique em **OK**.
- 9 Repita esse procedimento para todas as reservas que usam o caminho de armazenamento que você está desativando.

Coleta de dados

O vRealize Automation coleta dados de endpoints de origens de infraestrutura e de seus recursos de computação.

A coleta de dados ocorre em intervalos regulares. Cada tipo de coleta de dados tem um intervalo padrão que você pode substituir ou modificar. Cada tipo de coleta de dados tem também um intervalo de tempo limite padrão que você pode substituir ou modificar.

Os administradores do IaaS podem iniciar a coleta de dados manualmente para endpoints de origens de infraestrutura, enquanto os administradores de malha podem iniciar a coleta de dados manualmente para recursos de processamento.

Tabela 1-29. Tipos de coleta de dados

Tipo de coleta de dados	Descrição
Coleta de dados de endpoint da origem de infraestrutura	<p>Atualiza informações sobre hosts de virtualização, modelos e imagens ISO para ambientes de virtualização. Atualiza os centros de dados virtuais e modelos para vCloud Director. Atualiza regiões do Amazon e máquinas provisionadas em regiões do Amazon.</p> <p>A coleta de dados de endpoint é executada a cada 4 horas.</p>
Coleta de dados de inventário	<p>Atualiza o registro das máquinas virtuais cujo uso de recursos está vinculado a um determinado recurso de processamento, incluindo informações detalhadas sobre as redes, o armazenamento e as máquinas virtuais. Esse registro também inclui informações sobre máquinas virtuais não gerenciadas, que são provisionadas fora do vRealize Automation.</p> <p>A coleta de dados de inventário é executada a cada 24 horas.</p> <p>O intervalo de tempo limite padrão para coleta de dados de inventário é de 2 horas.</p>
Coleta de dados de estado	<p>Atualiza o registro do estado de energia de cada máquina descoberta através da coleta de dados de inventário. A coleta de dados de estado também registra máquinas ausentes gerenciadas pelo vRealize Automation, mas que não podem ser detectadas no recurso de processamento de virtualização ou no endpoint de nuvem.</p> <p>A coleta de dados de estado é executada a cada 15 minutos.</p> <p>O intervalo de tempo limite padrão para a coleta de dados de estado é de 1 hora.</p>
Coleta de dados de desempenho (apenas recursos de processamento do vSphere)	<p>Atualiza o registro da utilização média de CPU, armazenamento, memória e rede para cada máquina virtual descoberta através da coleta de dados de inventário.</p> <p>A coleta de dados de desempenho é executada a cada 24 horas.</p> <p>O intervalo de tempo limite padrão para a coleta de dados de desempenho é de 2 horas.</p>
Coleta de dados de inventário de rede e segurança (apenas para recursos de computação do vSphere)	<p>Atualiza o registro de dados de rede e segurança relacionado ao vCloud Networking and Security e ao NSX, em particular informações sobre grupos de segurança e balanceamento de carga, para cada máquina após a coleta de dados de inventário.</p>
Coleta de dados do WMI (somente para recursos de processamento do Windows)	<p>Atualiza o registro dos dados de gerenciamento para cada máquina Windows. Um agente WMI deve ser instalado, geralmente no host do Manager Service, e habilitado para coletar dados de máquinas Windows.</p>

Iniciar a coleta de dados do endpoint manualmente

A coleta de dados do endpoint é executada automaticamente a cada 4 horas, mas os administradores do IaaS podem iniciar manualmente a coleta de dados do endpoint a qualquer momento para endpoints que não exigem agentes de proxy.

A página **Coleta de dados** fornece informações sobre o status e a idade da coleta de dados e permite que você inicie manualmente uma nova coleta de dados do endpoint.

Pré-requisitos

Faça login no vRealize Automation como **administrador do IaaS**.

Procedimentos

- 1 Selecione **Infraestrutura > Pontos de extremidade > Pontos de extremidade**.
- 2 Clique na linha do endpoint que você deseja coletar dados.
- 3 Selecione uma ação de coleta de dados disponível.

Configurar a coleta de dados de recursos de processamento

Você pode ativar ou desativar a coleta de dados, configurar a frequência da coleta de dados ou solicitar manualmente a coleta de dados.

A página **Coleta de dados** oferece informações sobre o status e a data das coletas de dados. Ela também permite que você configure a coleta de dados para os seus recursos de processamento.

Pré-requisitos

Faça login no vRealize Automation como **administrador de estrutura**.

Procedimentos

- 1 Selecione **Infraestrutura > Recursos de processamento > Recursos de processamento**.
- 2 Aponte para o recurso de processamento para o qual você deseja configurar a coleta de dados e clique em **Coleta de dados**.
- 3 Configure as especificações da coleta de dados do **Recurso de processamento**.
 - Selecione **Ativado** para ativar a coleta de dados.
 - Selecione **Desativado** para desativar a coleta de dados.
- 4 Configure a coleta de dados de **Inventário**.
 - Selecione **Ativado** para ativar a coleta de dados.
 - Selecione **Desativado** para desativar a coleta de dados.
 - Insira um número na caixa de texto **Frequência** para configurar o intervalo de tempo (em horas) entre as coletas de dados de inventário.
 - Clique em **Solicitar agora** para iniciar manualmente a coleta de dados.

5 Configure a coleta de dados de **Estado**.

- Selecione **Ativado** para ativar a coleta de dados.
- Selecione **Desativado** para desativar a coleta de dados.
- Insira um número na caixa de texto **Frequência** para configurar o intervalo de tempo (em minutos) entre as coletas de dados de estado.
- Clique em **Solicitar agora** para iniciar manualmente a coleta de dados.

6 Configure a coleta de dados de **Desempenho**.

Essa opção está disponível apenas para integrações do vSphere.

- Selecione **Ativado** para ativar a coleta de dados.
- Selecione **Desativado** para desativar a coleta de dados.
- Insira um número na caixa de texto **Frequência** para configurar o intervalo de tempo (em horas) entre as coletas de dados de desempenho.
- Clique em **Solicitar agora** para iniciar manualmente a coleta de dados.

7 Configure a coleta de dados de **Inventário de snapshot**.

Essa opção está disponível para recursos de processamento gerenciados pelo vRealize Business for Cloud.

- Selecione **Ativado** para ativar a coleta de dados.
- Selecione **Desativado** para desativar a coleta de dados.
- Insira um número na caixa de texto **Frequência** para configurar o intervalo de tempo (em horas) entre as coletas de dados de snapshot.
- Clique em **Solicitar agora** para iniciar manualmente a coleta de dados.

8 Clique em **OK**.

Atualizar dados de custo para todos os recursos de processamento

Os administradores de malha podem atualizar manualmente as informações de custo de todos os recursos de processamento gerenciados pelo vRealize Business for Cloud.

Pré-requisitos

Faça login no vRealize Automation como **administrador de estrutura**.

Procedimentos

- 1** Selecione **Infraestrutura > Recursos de processamento > Recursos de processamento**.
- 2** Clique em **Atualizar custo**.
- 3** Clique em **Solicitar agora**.

Resultados

Quando a atualização de custo for concluída, o status será alterado para bem-sucedido.

Noções básicas sobre a verificação de alocação do vSwap para endpoints do vCenter Server

Você pode usar o vSwap para determinar a disponibilidade do espaço de permuta para o arquivo de permuta de tamanho máximo em uma máquina de destino. A verificação do vSwap ocorre quando você cria ou reconfigura uma máquina virtual a partir do vRealize Automation. A verificação de alocação do vSwap está disponível apenas para endpoints do vCenter Server.

A alocação de armazenamento do vRealize Automation verifica se há espaço disponível suficiente no repositório de dados para acomodar discos de máquinas virtuais durante uma solicitação de criação ou reconfiguração. Porém, quando a máquina é ligada, se não houver espaço disponível suficiente para criar arquivos de permuta no endpoint do vCenter Server, a máquina não será ligada. Quando ocorre falha ao ligar a máquina, todas as personalizações que dependem da máquina também falham. A máquina também pode ser descartada. Dependendo do tamanho da solicitação, o feedback dizendo que a máquina não está ligando ou não está provisionando não é imediatamente evidente.

Você pode usar a verificação de alocação do vSwap para ajudar a superar essas limitações verificando a disponibilidade de espaço de permuta para o arquivo de permuta de tamanho máximo como parte do processo de criação e reconfiguração do vRealize Automation para endpoints do vCenter Server. Para habilitar a verificação de alocação do vSwap, defina a propriedade personalizada `VirtualMachine.Storage.ReserveMemory` como `True` no componente da máquina ou blueprint geral.

Considere estes comportamentos para as verificações de alocação do vSwap:

- O arquivo de permuta está localizado no repositório de dados que contém a máquina virtual. Não há suporte para configurações alternativas do vCenter Server para localização de arquivos de permuta em um repositório de dados dedicado ou diferente.
- O tamanho de permuta é considerado ao criar ou reconfigurar uma máquina virtual. O tamanho de permuta máximo corresponde ao tamanho da memória da máquina virtual.
- Os valores das reservas de armazenamento do vRealize Automation em um host não devem exceder a capacidade física do recurso de processamento.
- Ao criar uma reserva, a soma dos valores reservados não deve exceder o espaço de armazenamento disponível.
- As reservas de memória no nível da máquina virtual ou do host ou pool de recursos no vSphere não são coletadas no endpoint do vSphere e não são consideradas durante os cálculos no vRealize Automation.
- O vSwap não valida o espaço de permuta que está disponível durante as operações de ativação das máquinas existentes.

- Você deve executar novamente a coleta de dados para capturar as alterações feitas no endpoint do vSphere em relação ao vSwap.

Removendo localizações do datacenter

Para remover uma localização do datacenter de um menu de usuário, um administrador do sistema deve remover as informações de localização do arquivo de localizações e um administrador de malha deve remover informações de localização do recurso de processamento.

Por exemplo, se adicionar Londres ao arquivo de localizações, associe dez recursos de processamento com essa localização e, em seguida, remova Londres do arquivo. Os recursos de processamento ainda estão associados à localização Londres, e Londres ainda está incluído na lista suspensa de localização na página Confirmar solicitação de máquina. Para remover a localização da lista suspensa, um administrador de malha deve editar o recurso de processamento e redefinir a Localização para em branco para todos os recursos de processamento que estão associados à localização.

O seguinte é uma visão geral de alto nível da sequência de etapas necessárias para remover uma localização de datacenter:

- 1 O administrador do sistema remove as informações de localização do datacenter do arquivo de localizações.
- 2 Um administrador de malha remove todas as associações de recursos de processamento para a localização, editando as localizações de cada recurso de processamento associado.

Monitorização de contentores

Você pode monitorar o status de um contentor que você cria em Contentores para vRealize Automation.

Após a criação dos contentores com base em um modelo, você pode monitorar seu estado. Clicando em **Detalhes** em um contentor, você pode monitorar a largura da banda de rede, o uso da CPU e da memória, registros e propriedades do contentor.

Importação em massa, atualização ou migração de máquinas virtuais

Você pode usar o recurso Importações em Massa para importar, atualizar ou migrar máquinas virtuais para o vRealize Automation. O recurso Importações em Massa otimiza o gerenciamento de várias máquinas em diversos ambientes.

O Importações em Massa cria um arquivo CSV que contém dados de definição da máquina virtual, como reserva, caminho de armazenamento, blueprint, proprietário e quaisquer propriedades personalizadas. Você pode usar o arquivo CSV para importar máquinas virtuais para seu ambiente do vRealize Automation. O Importações em Massa oferece suporte às seguintes tarefas administrativas:

- Importe uma ou mais máquinas virtuais não gerenciadas de modo que elas possam ser gerenciadas em um ambiente do vRealize Automation.
- Faça uma mudança global em uma propriedade de máquina virtual, como um caminho de armazenamento.
- Migre uma máquina virtual de um ambiente do vRealize Automation a outro.

Observação Somente o vCloud Director e o vSphere são compatíveis para importação em massa. A configuração do filtro para outro tipo de endpoint não gera dados no arquivo CSV.

Você pode executar os comandos de recurso do Importações em Massa usando o console do vRealize Automation ou a interface de linha de comando CloudUtil. Para obter mais informações sobre como usar a interface de linha de comando CloudUtil, consulte a documentação *Extensibilidade do ciclo de vida*.

Observação A importação em massa de máquinas não ignora as etapas normais de provisionamento. Todos os fluxos de trabalho externos existentes acionados pelo agente de eventos durante o provisionamento são executados para máquinas importadas. Você pode desativar temporariamente os fluxos de trabalho para máquinas importadas executando um dos seguintes procedimentos:

- Desative todas as assinaturas do Agente de Eventos. Se você estiver desativando assinaturas, deverá agendar uma interrupção de serviço para o seu cluster do vRealize Automation, pois a extensibilidade não será aplicada a nenhuma máquina normal provisionada durante esse período.
 - Adicione uma condição a assinaturas de eventos para não disparar quando uma máquina for importada. Para adicionar essa condição, navegue até Assinaturas de Eventos, selecione a assinatura a ser desativada e adicione uma propriedade personalizada `VirtualMachine.Imported.ConvergedBlueprint` diferente de `<Id do blueprint de importação>`. Essa condição não afeta as máquinas normalmente provisionadas e, em vez disso, é aplicada apenas às máquinas importadas.
-

Pré-requisitos

- Faça login no vRealize Automation como **administrador de estrutura** e como **gerente de grupos de negócios**.
- Se você estiver importando máquinas virtuais que usam endereços IP estáticos, prepare um pool de endereços configurados corretamente.

Importar uma máquina virtual para um ambiente do vRealize Automation

Você pode importar uma máquina virtual não gerenciada para um ambiente do vRealize Automation.

Uma máquina virtual não gerenciada existe em um hipervisor, mas não é gerenciada em um ambiente do vRealize Automation e não pode ser exibida no console. Após a importação de uma máquina virtual não gerenciada, ela passa a ser gerenciada com o uso da interface de gerenciamento do vRealize Automation. Dependendo dos seus privilégios, você pode ver essa máquina virtual na guia **Máquinas Gerenciadas** ou na guia **Implantações**.

A opção de importações em massa não é compatível com implantações provisionadas a partir de um blueprint que contenha um componente de rede e segurança NSX ou um componente de software.

Pré-requisitos

- Faça login no vRealize Automation como **administrador de estrutura** e como **gerente de grupos de negócios**.
- Se você estiver importando máquinas virtuais que usam endereços IP estáticos, prepare um pool de endereços configurados corretamente. Para obter mais informações sobre como usar um perfil de rede para controlar intervalos de endereço IP, consulte *Configurando o vRealize Automation*.
- Se você usar a importação em massa para importar uma máquina virtual com um endereço IP estático que esteja alocado a outra máquina virtual, a importação falhará.

Procedimentos

- 1 Desative temporariamente todas as Assinaturas do Agente de Eventos.

Observação Se estiver desativando assinaturas, você deverá agendar uma interrupção de serviço para o seu cluster do vRealize Automation. Durante esse processo, a extensibilidade não é aplicada a qualquer máquina provisionada normalmente. A falha na desativação das assinaturas pode resultar em perda de dados e exclusão permanente de máquinas da infraestrutura de apoio.

- 2 Gere um arquivo de dados CSV da máquina virtual.
 - a Selecione **Infraestrutura > Administração > Importações em massa**.
 - b Clique em **Gerar Arquivo CSV**.
 - c Selecione **Não Gerenciadas** no menu suspenso **Máquinas**.
 - d Selecione o valor padrão de **Grupo de negócios** no menu suspenso.
 - e Insira o valor padrão de **Proprietário**.

- f Selecione o valor padrão de **Blueprint** no menu suspenso.

O blueprint deve ser publicado e adicionado a um direito para que a importação seja bem-sucedida.

- g Selecione o valor padrão de **Máquina componente** no menu suspenso.

Se você selecionar um valor para **Grupo de negócios** e **Blueprint**, poderá ver os seguintes resultados no arquivo de dados CSV:

- Host Reservation (Name or ID) = INVALID_RESERVATION
- Host To Storage (Name or ID) = INVALID_HOST_RESERVATION_TO_STORAGE

Essas mensagens aparecerão se você não tiver uma reserva no grupo de negócios selecionado para a máquina virtual host que também hospeda a máquina virtual não gerenciada. Se você tiver uma reserva nesse grupo de negócios para o host da máquina virtual não gerenciada, os valores de Reserva de Host e de Host para Armazenar serão preenchidos apropriadamente.

- h Selecione um dos tipos de recursos disponíveis no menu suspenso **Recurso**.

Item de Menu	Descrição
Endpoint	Informações necessárias para acessar um host de virtualização.
Recurso de processamento	Informações necessárias para acessar um grupo de máquinas virtuais que estejam desempenhando uma função semelhante.

- i Selecione o nome do recurso de máquina virtual do menu suspenso **Nome**.
- j Clique em **OK**.

3 Edite seu arquivo de dados CSV da máquina virtual.

- a Abra o arquivo CSV e edite as categorias de dados para que correspondam às categorias existentes no ambiente de destino do vRealize Automation.

Para importar as máquinas virtuais contidas em um arquivo de dados CSV, cada máquina virtual deve ser associada aos seguintes itens:

- Reserva
- Localização de armazenamento
- Blueprint
- Componente de máquina virtual
- Proprietário existente na implantação de destino

Todos os valores de cada máquina virtual devem estar presentes no ambiente de destino do vRealize Automation para que a importação seja bem-sucedida. Você pode alterar os valores da reserva, do local de armazenamento, do blueprint e do proprietário, ou adicionar um endereço IP estático a máquinas virtuais individuais ao editar o arquivo CSV.

Título	Comentário
# Import—Yes or No	Selecione Não para evitar que uma máquina virtual específica seja importada.
Nome da máquina virtual	Não altere.
ID da máquina virtual	Não altere.
Reserva de host (nome ou ID)	Insira o nome ou a ID de uma reserva no ambiente de destino do vRealize Automation.
Host de armazenamento (nome ou ID)	Insira o nome ou a ID de um local de armazenamento no ambiente de destino do vRealize Automation.
Nome da implantação	<p>Insira um novo nome para a implantação (por exemplo, o nome da máquina virtual) que você está criando no ambiente de destino do vRealize Automation.</p> <p>Observação Cada máquina virtual deve ser importada para sua própria implantação. Não é possível importar uma única máquina virtual para uma implantação existente. Não é possível importar várias máquinas virtuais para uma única implantação.</p>
ID do blueprint	<p>Insira a ID do blueprint no ambiente de destino do vRealize Automation que você usa para importar a máquina virtual.</p> <p>Observação Insira apenas a ID do blueprint, não o nome do blueprint. Você deve selecionar um blueprint que contenha apenas um componente de máquina virtual. O blueprint deve ser publicado e adicionado a um direito.</p> <p>Para máquinas virtuais importadas, não associe um blueprint que inclui perfis de componente. As configurações existentes nas máquinas virtuais importadas, como o tamanho da memória ou do armazenamento, podem estar fora dos limites do perfil. Quando isso acontece, a validação falha para qualquer reconfiguração futura baseada em blueprint das máquinas virtuais.</p>

Título	Comentário
ID da máquina componente	Insira o nome do componente de uma máquina virtual que esteja contido no blueprint selecionado. Não é possível importar uma máquina virtual para um blueprint que tenha mais de um componente.
Nome do proprietário	Insira um usuário no ambiente de destino do vRealize Automation que tenha direito ao blueprint.

Se você importar uma máquina virtual com uma ou mais propriedades personalizadas, identifique cada propriedade personalizada usando três valores separados por vírgulas anexados à linha com os valores para essa máquina. Use esse formato para cada propriedade personalizada.

,Custom.Property.Name, Value, FLAGS

FLAGS (Sinalizadores) são três caracteres que descrevem como a propriedade é tratada pelo vRealize Automation. Na ordem de uso, os sinalizadores são:

- 1 H ou N = oculto ou não oculto
- 2 E ou O = criptografado ou não criptografado
- 3 R ou P = tempo de execução ou sem tempo de execução

Por exemplo, é possível anexar uma propriedade personalizada para configurar um endereço IP estático para uma máquina. Usando o seguinte formato, essa propriedade personalizada aloca um endereço IP estático disponível a partir de um perfil de rede.

,VirtualMachine.Network#.Address, w.x.y.z, HOP

Altere as variáveis com as informações apropriadas na máquina virtual.

- Troque # pelo número da interface de rede que está sendo configurada com esse endereço IP estático. Por exemplo, `VirtualMachine.Network0.Address`.
- Troque *w.x.y.z* pelo endereço IP estático da máquina virtual. Por exemplo, `11.27.42.57`.

A cadeia de caracteres de sinalizador de HOP—oculta, não criptografada, sem tempo de execução—define a visibilidade da propriedade. Como essa propriedade particular é usada somente pela importação em massa, ela é removida da máquina virtual após a importação bem-sucedida.

Para essa propriedade personalizada funcionar, o endereço IP deve estar disponível em um pool de endereços configurado corretamente. Se o endereço não puder ser encontrado ou já estiver em uso, a importação ocorrerá sem a definição de um endereço IP estático e um erro será registrado.

- b Salve o arquivo CSV.
- 4 Use a interface de gerenciamento do vRealize Automation para importar sua máquina virtual para um ambiente do vRealize Automation.
 - a Selecione **Infraestrutura > Administração > Importações em massa**.
 - b Clique em **Novo**.

- c Insira um nome exclusivo para essa tarefa na caixa de texto **Nome**, por exemplo, importação não gerenciada 10.
- d Insira o nome de arquivo CSV na caixa de texto **Arquivo CSV** procurando pelo nome de arquivo CSV.
- e Selecione as opções de importação.

Opção	Descrição
Hora de início	Define uma data de início futura. A hora de início escolhida será a hora local do servidor, e não a hora local da estação de trabalho do usuário.
Agora	Inicia o processo de importação imediatamente.
Atraso (segundos)	Se você estiver importando muitas máquinas virtuais, selecione a quantidade de segundos de atraso que deseja atribuir ao registro de cada máquina virtual. Selecionar esse item de menu reduz a velocidade do processo de importação. Deixe em branco para selecionar nenhum atraso.
Tamanho do lote	Se você estiver importando muitas máquinas virtuais, selecione o número de máquinas virtuais a serem registradas em um dado momento. Selecionar esse item de menu reduz a velocidade do processo de importação. Deixe em branco para selecionar nenhum limite.
Ignorar máquinas gerenciadas	Deixe essa opção desmarcada.
Ignorar validação do usuário	Selecionar essa item de menu define o proprietário da máquina virtual como o valor listado na coluna Proprietário do arquivo de dados CSV sem verificar se o usuário existe ou não. Selecionar esse item de menu pode reduzir o tempo de importação.
Testar importação	Testa o processo de importação sem importar as máquinas virtuais para que você possa verificar se houve erros no arquivo CSV.

- f Clique em **OK**.

O progresso da operação é exibido na página Importações em Massa.

Atualizar uma máquina virtual em um ambiente do vRealize Automation

Você pode fazer uma alteração em uma propriedade da máquina virtual, como um caminho de armazenamento, para atualizar uma ou mais máquinas virtuais gerenciadas em um ambiente do vRealize Automation.

Uma máquina virtual gerenciada é uma máquina gerenciada em um ambiente do vRealize Automation e pode ser visualizada no console.

Pré-requisitos

- Faça login no vRealize Automation como **administrador de estrutura** e como **gerente de grupos de negócios**.

Procedimentos

- 1 Gere um arquivo de dados CSV da máquina virtual.
 - a Selecione **Infraestrutura > Administração > Importações em massa**.
 - b Clique em **Gerar Arquivo CSV**.
 - c Selecione **Gerenciadas** no menu suspenso **Máquinas**.
 - d Selecione um dos tipos de recursos disponíveis no menu suspenso **Recurso**.

Opção	Descrição
Endpoint	Informações necessárias para acessar um host de virtualização.
Recurso de processamento	Informações necessárias para acessar um grupo de máquinas virtuais que estejam desempenhando uma função semelhante.

- e Selecione o nome do recurso de máquina virtual do menu suspenso **Nome**.
- f (Opcional) Selecione **Incluir propriedades personalizadas** se quiser migrar as propriedades personalizadas da máquina virtual.
- g Clique em **OK**.

2 Edite seu arquivo de dados CSV da máquina virtual.

- a Abra o arquivo CSV com um editor de texto e edite as categorias de dados que você deseja alterar globalmente.

Para atualizar as máquinas virtuais contidas em um arquivo de dados CSV, cada máquina deve ser associada aos seguintes itens:

- Reserva
- Localização de armazenamento
- Blueprint
- Componente de máquina
- Proprietário existente na implantação de destino

Todos os valores de cada máquina devem estar presentes no ambiente de destino do vRealize Automation para que a atualização seja bem-sucedida. Você pode alterar os valores da reserva, do local de armazenamento, do blueprint e do proprietário, ou adicionar um endereço IP estático a máquinas individuais ao editar o arquivo CSV.

- b Se você estiver alterando o endereço IP estático de uma máquina virtual, acrescente um comando ao arquivo CSV no seguinte formato.

```
,VirtualMachine.Network#.Address, w.x.y.z, HOP
```

Configure o comando com as informações apropriadas na máquina virtual.

- Troque # pelo número da interface de rede que está sendo configurada com esse endereço IP estático. Por exemplo, VirtualMachineNetwork0.Address.
- Troque w.x.y.z pelo endereço IP estático da máquina virtual. Por exemplo, 11.27.42.57.
- A cadeia de caracteres *HOP*, Oculta, Não criptografada, Sem tempo de execução, define a visibilidade da propriedade. Essa propriedade padrão é removida da máquina virtual após uma importação bem-sucedida.

Para que uma atualização seja bem-sucedida, o endereço IP deve estar disponível em um grupo de endereços configurado corretamente. Se o endereço não puder ser encontrado ou já estiver em uso, a atualização ocorrerá sem a definição de um endereço IP estático, e um erro será registrado.

- c Salve o arquivo CSV e feche o editor de texto.

3 Use a interface de gerenciamento do vRealize Automation para atualizar uma ou mais máquinas virtuais em um ambiente do vRealize Automation.

- a Selecione **Infraestrutura > Administração > Importações em massa**.
- b Clique em **Novo**.
- c Insira um nome exclusivo para essa tarefa na caixa de texto **Nome**, por exemplo, atualização global gerenciada 10.

- d Insira o nome de arquivo CSV na caixa de texto **Arquivo CSV** procurando pelo nome de arquivo CSV.
- e Selecione as opções de importação.

Opção	Descrição
Hora de início	Define uma data de início futura. A hora de início especificada será a hora local do servidor e não a hora local da estação de trabalho do usuário.
Agora	Inicia o processo de importação imediatamente.
Atraso (segundos)	Se você estiver atualizando muitas máquinas virtuais, selecione o número de segundos de atraso que deseja atribuir a cada atualização de máquina virtual. Selecionar essa opção reduzirá a velocidade do processo de atualização. Deixe em branco para não especificar nenhum atraso.
Tamanho do lote	Se você estiver atualizando muitas máquinas virtuais, selecione o número total de máquinas a serem atualizadas em um determinado momento. Selecionar essa opção reduzirá a velocidade do processo de atualização. Deixe em branco para não especificar limite.
Ignorar máquinas gerenciadas	Deixe essa opção desmarcada.
Ignorar validação do usuário	Selecionar essa opção define o proprietário da máquina como o valor listado na coluna Proprietário do arquivo de dados CSV sem verificar se o usuário existe ou não. Selecionar essa opção pode reduzir o tempo de atualização.
Testar importação	Deixe essa opção desmarcada.

- f Clique em **OK**.

O progresso da operação é exibido na página Importações em Massa.

Migrar uma máquina virtual para um ambiente do vRealize Automation diferente

Você pode migrar uma ou mais máquinas virtuais gerenciadas em um ambiente do VMware vRealize™ Automation para um ambiente diferente do vRealize Automation.

Uma máquina virtual gerenciada é uma máquina virtual gerenciada em um ambiente do vRealize Automation e pode ser visualizada no console.

Pré-requisitos

- Faça login no vRealize Automation como **administrador de estrutura** e como **gerente de grupos de negócios**.
- Se você estiver importando máquinas virtuais que usam endereços IP estáticos, prepare um pool de endereços configurados corretamente. Para obter mais informações sobre como usar um perfil de rede para controlar intervalos de endereço IP, consulte *Configurando o vRealize Automation*.

Procedimentos

- 1 Gere um arquivo de dados CSV da máquina virtual.
 - a Selecione **Infraestrutura > Administração > Importações em massa**.
 - b Clique em **Gerar Arquivo CSV**.
 - c Selecione **Gerenciadas** no menu suspenso **Máquinas**.
 - d Selecione um dos tipos de recursos disponíveis no menu suspenso **Recurso**.

Opção	Descrição
Endpoint	Informações necessárias para acessar um host de virtualização.
Recurso de processamento	Informações necessárias para acessar um grupo de máquinas virtuais que estejam desempenhando uma função semelhante.

- e Selecione o nome do recurso de máquina virtual do menu suspenso **Nome**.
- f (Opcional) Selecione **Incluir propriedades personalizadas**.

Você inclui propriedades personalizadas ao importar uma máquina virtual para uma nova implantação com as mesmas propriedades.
- g Clique em **OK**.

2 Edite seu arquivo de dados CSV da máquina virtual.

A necessidade ou não de editar o arquivo de dados CSV depende da semelhança dos ambientes de origem e de destino. Se os valores de configuração no ambiente de origem não corresponderem aos valores no ambiente de destino, você deverá editar o arquivo de dados CSV para que esses valores correspondam antes de iniciar a migração.

- a Abra o arquivo CSV e edite as categorias de dados para que correspondam às categorias existentes no ambiente de destino do vRealize Automation.

Para migrar máquinas virtuais contidas em um arquivo de dados CSV, cada máquina virtual deve ser associada a uma reserva, um local de armazenamento, um blueprint, um componente de máquina e um proprietário existente no ambiente de destino do vRealize Automation. Todos os valores de cada máquina virtual devem estar presentes no ambiente de destino do vRealize Automation para que a migração seja bem-sucedida. Você pode alterar os valores da reserva, do local de armazenamento, do blueprint e do proprietário, ou adicionar um endereço IP estático a máquinas virtuais individuais ao editar o arquivo CSV.

Título	Comentário	Exemplo
# Importar--Sim ou Não	Selecione Não para evitar que uma máquina virtual específica seja importada.	Sim
Nome da máquina virtual	Não altere.	MyMachine
ID da máquina virtual	Não altere.	a6e05812-0b06-4d4e-a84a-fed242340426a
Reserva de host (nome ou ID)	Insira o nome ou a ID de uma reserva no ambiente de destino do vRealize Automation.	DevReservation
Host de armazenamento (nome ou ID)	Insira o nome ou a ID de um local de armazenamento no ambiente de destino do vRealize Automation.	ce-san-1:custom-nfs-2
Nome da implantação	Insira um novo nome para a implantação que você está criando no ambiente de destino do vRealize Automation. Cada máquina virtual deve ser migrada para sua própria implantação. Não é possível importar uma única máquina virtual para uma implantação existente. Você não pode importar várias máquinas virtuais em um único ambiente.	ImportedDeployment0001
ID do blueprint convergido	Insira a ID do blueprint no ambiente de destino do vRealize Automation que você usa para importar a máquina virtual. Certifique-se de inserir apenas o ID do blueprint. Não insira o nome do blueprint. Você deve selecionar um blueprint que contenha apenas um componente de máquina virtual. O blueprint deve ser publicado e adicionado a um direito.	ImportBlueprint

Título	Comentário	Exemplo
ID do blueprint de componente	Insira o nome do componente de uma máquina virtual que esteja contido no blueprint selecionado. Não é possível importar uma máquina virtual para um blueprint que tenha mais de um componente.	ImportedMachine
Nome do proprietário	Insira um usuário no ambiente de destino do vRealize Automation.	user@tenant

Exemplo de uma linha de CSV completa e devidamente formatada: Yes, MyMachine, a6e05812-0b06-4d4e-a84a-fed242340426, DevReservation, ce-san-1:custom-nfs-2, Imported Deployment 0001, ImportBlueprint, ImportedMachine, user@tenant

- b Se você estiver migrando uma máquina virtual com um endereço IP estático, acrescente um comando no seguinte formato ao arquivo CSV.

```
,VirtualMachine.Network#.Address, w.x.y.z, HOP
```

Configure o comando com as informações apropriadas na máquina virtual.

- Troque # pelo número da interface de rede que está sendo configurada com esse endereço IP estático. Por exemplo, VirtualMachineNetwork0.Address.
- Troque w.x.y.z pelo endereço IP estático da máquina virtual. Por exemplo, 11.27.42.57.
- A cadeia de caracteres HOP, Oculta, Não criptografada, Sem tempo de execução, define a visibilidade da propriedade. Essa propriedade padrão é removida da máquina virtual após uma importação bem-sucedida.

Para que uma migração seja bem-sucedida, o endereço IP deve estar disponível em um grupo de endereços configurado corretamente. Se o endereço não puder ser encontrado ou já estiver em uso, a migração ocorrerá sem a definição de um endereço IP estático, e um erro será registrado.

- c Salve o arquivo CSV.
- 3 Use a interface de gerenciamento do vRealize Automation para migrar sua máquina virtual para um ambiente do vRealize Automation.
- a Selecione **Infraestrutura > Administração > Importações em massa**.
 - b Clique em **Novo**.
 - c Insira um nome exclusivo para essa tarefa na caixa de texto **Nome**, por exemplo, migração gerenciada 10.
 - d Insira o nome de arquivo CSV na caixa de texto **Arquivo CSV** procurando pelo nome de arquivo CSV.

- e Selecione as opções de importação.

Opção	Descrição
Hora de início	Define uma data de início futura. A hora de início escolhida será a hora local do servidor, e não a hora local da estação de trabalho do usuário.
Agora	Inicia o processo de migração imediatamente.
Atraso (segundos)	Se você estiver migrando muitas máquinas virtuais, selecione a quantidade de segundos de atraso que deseja atribuir ao registro de cada máquina virtual. Selecionar essa opção reduzirá a velocidade do processo de migração. Deixe em branco para selecionar nenhum atraso.
Tamanho do lote	Se você estiver migrando muitas máquinas virtuais, selecione o número de máquinas virtuais a serem registradas em um dado momento. Selecionar essa opção reduzirá a velocidade do processo de migração. Deixe em branco para selecionar nenhum limite.
Ignorar máquinas gerenciadas	Deixe essa opção desmarcada.
Ignorar validação do usuário	Selecionar essa opção define o proprietário da máquina virtual como o valor listado na coluna Proprietário do arquivo de dados CSV sem verificar se o usuário existe ou não. Selecionar essa opção pode reduzir o tempo de migração.
Testar importação	Teste o processo de migração sem migrar as máquinas virtuais, para que você possa verificar se há erros no arquivo CSV.

- f Clique em **OK**.

O progresso da operação é exibido na página Importações em Massa.