

Administrando o vRealize Automation

21 de julho de 2021
vRealize Automation 8.2

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

Conteúdo

- 1 Administrando o vRealize Automation 4**
- 2 Administrando usuários 5**
 - [Como habilitar grupos do Active Directory no vRealize Automation para projetos 6](#)
 - [Como remover usuários no vRealize Automation 7](#)
 - [Como editar funções de usuário no vRealize Automation 8](#)
 - [Como editar atribuições de funções de grupo no vRealize Automation 8](#)
 - [Quais são as funções de usuário do vRealize Automation 9](#)
- 3 Fazendo a manutenção do seu dispositivo 21**
 - [Iniciando e interrompendo o vRealize Automation 21](#)
 - [Dimensionar horizontalmente o vRealize Automation de um a três nós 23](#)
 - [Substituindo um nó de dispositivo 24](#)
 - [Aumentar o espaço em disco do dispositivo vRealize Automation 26](#)
 - [Atualizar a atribuição de DNS para vRealize Automation 26](#)
 - [Como habilitar a sincronização horário 27](#)
 - [Como redefinir a senha root 28](#)
- 4 Usando configurações de tenant de várias organizações no vRealize Automation 31**
 - [Configurar a locação de várias organizações para o vRealize Automation 34](#)
 - [Gerenciando certificados e a configuração de DNS em implantações de várias organizações de nó único 36](#)
 - [Gerenciando o certificado e a configuração de DNS em implantações do vRealize Automation com cluster 38](#)
 - [Fazendo login em tenants e adicionando usuários no vRealize Automation 40](#)
 - [Usando o vRealize Orchestrator com implantações do vRealize Automation em várias organizações 41](#)
- 5 Trabalho com logs 42**
 - [Como trabalhar com logs e pacotes de logs 42](#)
 - [Como configurar o encaminhamento de logs ao vRealize Log Insight 44](#)
 - [Como criar ou atualizar uma integração syslog 49](#)
 - [Como excluir uma integração de syslog para registro em log 50](#)
- 6 Programa de Aperfeiçoamento da Experiência do Cliente 52**
 - [Como entrar ou sair no/do programa 52](#)
 - [Como configurar o tempo de coleta de dados para o programa 53](#)

Administrando o vRealize Automation

1

Este guia descreve como monitorar e gerenciar a infraestrutura crítica e os aspectos de gerenciamento de usuários de uma implantação do vRealize Automation.

As tarefas aqui descritas são vitais para manter uma implantação do vRealize Automation operando de maneira adequada. Essas tarefas incluem o gerenciamento de usuários e grupos e o monitoramento de logs do sistema.

Além disso, ele descreve como configurar e gerenciar implantações em várias organizações.

Embora algumas tarefas de administração do vRealize Automation sejam concluídas no vRealize Automation, outras exigem o uso de produtos relacionados, como o vRealize Suite Lifecycle Manager e o Workspace ONE Access. Os usuários devem se familiarizar com esses produtos e suas funcionalidades antes de concluir as tarefas aplicáveis.

Por exemplo, para obter informações sobre backup, restauração e recuperação de desastres, consulte a seção **Backup e restauração e recuperação de desastres > 2019** da [Documentação do produto vRealize Suite](#).

Observação A recuperação de desastres é compatível no vRealize Automation 8.0.1 e versões posteriores.

Para obter informações sobre como trabalhar com tarefas de instalação, upgrade e gerenciamento do vRealize Suite Lifecycle Manager, consulte a [Documentação do produto Lifecycle Manager](#).

Administrando usuários e grupos no vRealize Automation

2

O vRealize Automation usa o VMware Workspace ONE Access, o aplicativo de gerenciamento de identidade fornecido pela VMware, para importar e gerenciar usuários e grupos. Depois que usuários e grupos são importados ou criados, você pode gerenciar as atribuições de função para implantações de tenant único usando a página Gerenciamento de Identidades e Acessos.

O vRealize Automation é instalado usando o VMware Lifecycle Manager (vRSLCM ou LCM). Ao instalar o vRealize Automation você deve importar uma instância existente do Workspace ONE Access ou implantar uma nova instância para oferecer suporte ao gerenciamento de identidade. Esses dois cenários definem suas opções de gerenciamento.

- Se você implantar uma nova instância do Workspace ONE Access, poderá gerenciar usuários e grupos via LCM. Durante a instalação, você pode configurar uma conexão do Active Directory usando o Workspace ONE Access. Como alternativa, você pode visualizar e editar alguns aspectos de usuários e grupos dentro do vRealize Automation usando a página Gerenciamento de Identidades e Acessos, conforme descrito aqui.
- Se você usar uma instância existente do Workspace ONE Access, importe-a para uso com o vRealize Automation via LCM durante a instalação. Nesse caso, você pode continuar a usar o Workspace ONE Access para gerenciar usuários e grupos ou pode usar as funções de gerenciamento no LCM.

Consulte [Fazendo login em tenants e adicionando usuários no vRealize Automation](#) para obter mais informações sobre como gerenciar usuários em uma implantação de várias organizações.

Os usuários do vRealize Automation devem ter funções atribuídas. As funções definem o acesso aos recursos do aplicativo. Quando o vRealize Automation é instalado com uma instância do Workspace ONE Access, uma organização padrão é criada, e o instalador recebe a função Proprietário da Organização. Todas as outras funções do vRealize Automation são atribuídas pelo Proprietário da Organização.

Existem três tipos de funções no vRealize Automation : funções de organização, funções de serviço e funções de projeto. Para o vRealize Automation Cloud Assembly, o Service Broker e o Code Stream, normalmente, funções em nível de usuário podem usar recursos, enquanto funções em nível de administrador são necessárias para criar e configurar recursos. As funções organizacionais definem permissões dentro do tenant. Os proprietários da organização têm permissões em nível de administrador, enquanto os membros da organização têm permissões em nível de usuário. Os proprietários da organização podem adicionar e gerenciar outros usuários.

Funções de organização	Funções de serviço
■ Proprietário da Organização	■ Administrador do Cloud Assembly
■ Membro da Organização	■ Usuário do Cloud Assembly
	■ Expectador do Cloud Assembly
	■ Administrador do Service Broker
	■ Usuário do Service Broker
	■ Espectador do Service Broker
	■ Administrador do Code Stream
	■ Usuário do Code Stream
	■ Espectador do Code Stream

Além disso, há duas funções principais em nível de projeto não mostradas na tabela: Administrador do Projeto e Usuário do Projeto. Essas funções são atribuídas assystematicamente para cada projeto com o Cloud Assembly. Essas funções são um tanto fluidas. O mesmo usuário pode ser administrador em um projeto e usuário em outro projeto. Para obter mais informações, consulte [Quais são as funções de usuário do vRealize Automation](#).

Para obter mais informações sobre como trabalhar com o LCM e o Workspace ONE Access, consulte [Gerenciamento de usuários com o VMware Identity Manager](#).

Este capítulo inclui os seguintes tópicos:

- [Como habilitar grupos do Active Directory no vRealize Automation para projetos](#)
- [Como remover usuários no vRealize Automation](#)
- [Como editar funções de usuário no vRealize Automation](#)
- [Como editar atribuições de funções de grupo no vRealize Automation](#)
- [Quais são as funções de usuário do vRealize Automation](#)

Como habilitar grupos do Active Directory no vRealize Automation para projetos

Se um grupo não estiver disponível na página Adicionar Grupos quando você adicionar usuários aos projetos, verifique a página Gerenciamento de Identities e Acessos e adicione o grupo, se disponível. Se o grupo não estiver listado na página Gerenciamento de Identities e Acessos no vRealize Automation, talvez ele não esteja sincronizado na sua instância do Workspace One Access. Você pode verificar se ele foi sincronizado e, em seguida, usar este procedimento para adicionar o grupo conforme mostrado aqui.

Para adicionar membros de um grupo do Active Directory a um projeto, você deve garantir que o grupo esteja sincronizado com a sua instância do Workspace One Access e que esse grupo seja adicionado à organização.

Pré-requisitos

Se os grupos não forem sincronizados, eles não ficarão disponíveis quando você tentar adicioná-los a um projeto. Verifique se você sincronizou seus grupos do Active Directory com sua instância do Lifecycle Manager.

Procedimentos

- 1 Faça login no vRealize Automation como um usuário do mesmo domínio do Active Directory que você está adicionando. Por exemplo, @mycompany.com
- 2 No Cloud Assembly, clique em Gerenciamento de Identidades e Acessos no cabeçalho de navegação à direita.
- 3 Clique em **Grupos Empresariais** e depois em **Atribuir Funções**.
- 4 Use a função de pesquisa para encontrar o grupo que você está adicionando e selecione-o.
- 5 Atribua uma função de organização.

No mínimo, o grupo deve ter uma função de Membro da Organização. Consulte [Quais são as funções de usuário do Cloud Assembly](#) para obter mais informações.

- 6 Clique em **Adicionar Acesso ao Serviço**, adicione um ou mais serviços e selecione uma função para cada um.
- 7 Clique em **Atribuir**.

Resultados

Agora, você pode adicionar o grupo do Active Directory a um projeto.

Como remover usuários no vRealize Automation

Você pode remover usuários conforme necessário no vRealize Automation.

Todos os usuários são listados por padrão, e você não pode adicionar usuários com a página Gerenciamento de Identidade e Acesso. Você pode excluir usuários.

Procedimentos

- 1 Selecione a guia Usuários Ativos na página Gerenciamento de Identidades e Acessos.
- 2 Localize e selecione os usuários que você deseja excluir.
- 3 Clique em **Remover Usuários**.

Resultados

Os usuários selecionados são removidos.

Como editar funções de usuário no vRealize Automation

Você pode editar funções atribuídas a usuários do Workspace One Access que foram importados para o vRealize Automation.

Pré-requisitos

Procedimentos

- 1 No Cloud Assembly, clique em Gerenciamento de Identidades e Acessos no cabeçalho de navegação à direita.
- 2 Selecione o usuário desejado na guia Usuários Ativos e clique em **Editar Funções**.
- 3 É possível editar as funções de organização e serviço do usuário.
 - Selecione a lista suspensa ao lado do título Atribuir Funções da Organização para alterar o relacionamento do usuário com a organização.
 - Clique em Adicionar Acesso ao Serviço para adicionar novas funções de serviço para o usuário.
 - Para remover funções de usuário, clique no X ao lado do serviço aplicável.
- 4 Clique em **Salvar**.

Resultados

A atribuição da função do usuário é atualizada conforme especificado.

Como editar atribuições de funções de grupo no vRealize Automation

Você pode editar atribuições de funções para grupos no vRealize Automation

Pré-requisitos

Os usuários e grupos foram importados de uma instância de vIDM válida que está associada à sua implantação do vRealize Automation.

Procedimentos

- 1 No Cloud Assembly, clique em Gerenciamento de Identidades e Acessos no cabeçalho de navegação à direita.
- 2 Selecione a guia Grupos Empresariais.
- 3 Digite o nome do grupo para o qual deseja editar as atribuições de função no campo de pesquisa.
- 4 Edite as atribuições de função para o grupo selecionado. Você tem duas opções.
 - Atribuir Funções da Organização

- Atribuir Funções de Serviço

5 Clique em **Atribuir**.

Resultados

Atribuições de funções são atualizadas conforme especificado.

Quais são as funções de usuário do vRealize Automation

Como proprietário de uma organização, você pode atribuir funções de organização e funções de serviço aos usuários. Essas funções determinam o que os usuários podem fazer ou ver. Em seguida, nos serviços, o administrador de serviços pode atribuir funções de projeto. Para determinar a função que você deseja atribuir, avalie as tarefas nas tabelas a seguir.

Funções de serviço do Cloud Assembly

As funções de serviço do vRealize Automation Cloud Assembly determinam o que você pode ver e fazer no vRealize Automation Cloud Assembly. Essas funções de serviço são definidas no console por um proprietário da organização.

Tabela 2-1. Descrições das funções de serviço do vRealize Automation Cloud Assembly

Função	Descrição
Administrador do Cloud Assembly	Um usuário que tenha acesso de leitura e gravação para toda a interface do usuário e recursos de API. Essa é a única função de usuário que pode ver e fazer tudo, incluindo adicionar contas de nuvem, criar novos projetos e atribuir um administrador de projeto.
Usuário do Cloud Assembly	Um usuário que não tem a função Administrador do Cloud Assembly. Em um projeto vRealize Automation Cloud Assembly, o administrador adiciona usuários a projetos como membros, administradores ou visualizadores do projeto. O administrador também pode adicionar um administrador de projeto.
Expectador do Cloud Assembly	Um usuário que tem acesso de leitura para ver informações, mas não pode criar, atualizar ou excluir valores. Esta é uma função somente leitura em todos os projetos. Os usuários com a função de visualizador podem ver todas as informações que estão disponíveis para o administrador. Ele não pode realizar nenhuma ação, a menos que você o torne um administrador de projeto ou membro do projeto. Se o usuário for afiliado a um projeto, ele terá as permissões relacionadas à função. A função de visualizador de projeto não abrange as permissões da mesma forma que a função de administrador ou membro.

Além das funções de serviço, o vRealize Automation Cloud Assembly tem funções de projeto. Todos os projetos estão disponíveis em todos os serviços.

As funções de projeto são definidas no vRealize Automation Cloud Assembly e podem variar entre projetos.

Nas tabelas a seguir, que indicam o que as diferentes funções de serviço e projeto podem ver e fazer, lembre-se de que os administradores de serviços têm permissão total em todas as áreas da interface do usuário.

As descrições das funções de projetos ajudarão você a decidir quais permissões conceder aos usuários.

- Os administradores de projetos aproveitam a infraestrutura criada pelo administrador de serviços para garantir que os membros do projeto tenham os recursos necessários para o trabalho de desenvolvimento.
- Os membros do projeto trabalham em seus projetos para projetar e implantar modelos de nuvem.
- Os espectadores de projeto estão restritos ao acesso somente leitura, com exceção de alguns casos em que eles podem realizar ações não destrutivas, como baixar modelos de nuvem.

Tabela 2-2. Funções de serviço e funções de projeto do vRealize Automation Cloud Assembly

Contexto da interface do usuário	Tarefa	Administrador do Cloud Assembly	Expectador do Cloud Assembly	Usuário do Cloud Assembly		
				O usuário deve ser administrador ou membro do projeto para ver e realizar tarefas relacionadas ao projeto.		
				Administrador do projeto	Membro do projeto	Expectador de projeto
Acessar o Cloud Assembly						
Console	No console do vRA, você pode ver e abrir o Cloud Assembly	Sim	Sim	Sim	Sim	Sim
Infraestrutura						
	Visualizar e abrir a guia Infraestrutura	Sim	Sim	Sim	Sim	Sim
Configurar - Projetos	Criar projetos	Sim				

Tabela 2-2. Funções de serviço e funções de projeto do vRealize Automation Cloud Assembly (continuação)

Contexto da interface do usuário	Tarefa	Administrador do Cloud Assembly	Expectador do Cloud Assembly	Usuário do Cloud Assembly O usuário deve ser administrador ou membro do projeto para ver e realizar tarefas relacionadas ao projeto.		
				Administrador do projeto	Membro do projeto	Expectador de projeto
	Atualizar ou excluir valores do resumo do projeto, usuários, provisionamento, Kubernetes, integrações e testar configurações de projeto.	Sim		Sim. Seus projetos		
	Adicionar usuários e atribuir funções em projetos.	Sim		Sim. Seus projetos.		
	Visualizar projetos	Sim	Sim	Sim. Seus projetos	Sim. Seus projetos	Sim. Seus projetos
Configurar - Zonas de Nuvem	Criar, atualizar ou excluir zonas de nuvem	Sim				
	Visualizar zonas de nuvem	Sim	Sim			
Configurar - Zonas do Kubernetes	Criar, atualizar ou excluir zonas do Kubernetes	Sim				
	Exibir zonas do Kubernetes	Sim	Sim			
Configurar - Tipos	Criar, atualizar ou excluir tipos	Sim				
	Exibir tipos	Sim	Sim			
Configurar - Mapeamentos de Imagem	Criar, atualizar ou excluir mapeamentos de imagens	Sim				
	Visualizar mapeamentos de imagem	Sim	Sim			
Configurar - Perfis de Rede	Criar, atualizar ou excluir perfis de rede	Sim				

Tabela 2-2. Funções de serviço e funções de projeto do vRealize Automation Cloud Assembly (continuação)

Contexto da interface do usuário	Tarefa	Administrador do Cloud Assembly	Expectador do Cloud Assembly	Usuário do Cloud Assembly O usuário deve ser administrador ou membro do projeto para ver e realizar tarefas relacionadas ao projeto.		
				Administrador do projeto	Membro do projeto	Expectador de projeto
	Exibir perfis de rede de imagem	Sim	Sim			
Configurar - Perfis de Armazenamento	Criar, atualizar ou excluir perfis de armazenamento	Sim				
	Exibir perfis de armazenamento de imagem	Sim	Sim			
Configurar - Cartões de Preços	Criar, atualizar ou excluir cartões de preços	Sim				
	Exibir cartões de preços	Sim	Sim			
Configurar - Tags	Criar, atualizar ou excluir tags	Sim				
	Exibir tags	Sim	Sim			
Recursos - Processamento	Adicionar tags aos recursos de processamento descobertos	Sim				
	Exibir recursos de processamento descobertos	Sim	Sim			
Recursos - Redes	Modificar tags de rede, intervalos de IP, endereços IP	Sim				
	Exibir recursos de rede descobertos	Sim	Sim			
Recursos - Segurança	Adicionar tags a grupos de segurança descobertos	Sim				
	Exibir grupos de segurança descobertos	Sim	Sim			
Recursos - Armazenamento	Adicionar tags ao armazenamento descoberto	Sim				

Tabela 2-2. Funções de serviço e funções de projeto do vRealize Automation Cloud Assembly (continuação)

Contexto da interface do usuário	Tarefa	Administrador do Cloud Assembly	Expectador do Cloud Assembly	Usuário do Cloud Assembly O usuário deve ser administrador ou membro do projeto para ver e realizar tarefas relacionadas ao projeto.		
				Administrador do projeto	Membro do projeto	Expectador de projeto
	Exibir armazenamento	Sim	Sim			
Recursos - Máquinas	Adicionar e excluir máquinas	Sim				
	Visualizar máquinas	Sim	Sim	Sim. Seus projetos	Sim. Seus projetos	Sim. Seus projetos
Recursos - Volumes	Excluir volumes de armazenamento descobertos	Sim				
	Exibir volumes de armazenamento descobertos	Sim	Sim	Sim. Seus projetos	Sim. Seus projetos	Sim. Seus projetos.
Recursos - Kubernetes	Implantar ou adicionar clusters do Kubernetes e criar ou adicionar namespaces	Sim				
	Exibir clusters e namespaces do Kubernetes	Sim	Sim	Sim. Seus projetos	Sim. Seus projetos	Sim. Seus projetos
Atividade - Solicitações	Excluir registros de solicitação de implantação	Sim				
	Exibir registros de solicitação de implantação	Sim	Sim	Sim. Seus projetos	Sim. Seus projetos	Sim. Seus projetos
Atividade - Logs de Eventos	Exibir logs de eventos	Sim	Sim	Sim. Seus projetos	Sim. Seus projetos	Sim. Seus projetos
Conexões - Contas de Nuvem	Criar, atualizar ou excluir contas de nuvem	Sim				
	Exibir contas de nuvem	Sim	Sim			
Conexões - Integrações	Criar, atualizar ou excluir integrações	Sim				
	Visualizar integrações	Sim	Sim			

Tabela 2-2. Funções de serviço e funções de projeto do vRealize Automation Cloud Assembly (continuação)

Contexto da interface do usuário	Tarefa	Administrador do Cloud Assembly	Expectador do Cloud Assembly	Usuário do Cloud Assembly O usuário deve ser administrador ou membro do projeto para ver e realizar tarefas relacionadas ao projeto.		
				Administrador do projeto	Membro do projeto	Expectador de projeto
Integração	Criar, atualizar ou excluir planos de integração	Sim				
	Visualizar planos de integração	Sim	Sim			Sim. Seus projetos
Marketplace						
	Ver e abrir a guia Marketplace	Sim	Sim			
	Usar os modelo de nuvem baixados na guia Projetar	Sim		Sim. Se associados aos seus projetos.	Sim. Se associados aos seus projetos.	
Marketplace - Modelos de nuvem	Baixar um modelo de nuvem	Sim				
	Exibir os modelos de nuvem	Sim	Sim			
Marketplace - Imagens	Baixar imagens	Sim				
	Exibir imagens	Sim	Sim			
Marketplace - Downloads	Exibir o log de todos os itens baixados	Sim	Sim			
Extensibilidade						
	Ver e abrir a guia Extensibilidade	Sim	Sim			Sim
Eventos	Exibir eventos de extensibilidade	Sim	Sim			
Assinaturas	Criar, atualizar ou excluir assinaturas de extensibilidade	Sim				
	Desativar assinaturas	Sim				
	Exibir assinaturas	Sim	Sim			

Tabela 2-2. Funções de serviço e funções de projeto do vRealize Automation Cloud Assembly (continuação)

Contexto da interface do usuário	Tarefa	Administrador do Cloud Assembly	Expectador do Cloud Assembly	Usuário do Cloud Assembly O usuário deve ser administrador ou membro do projeto para ver e realizar tarefas relacionadas ao projeto.		
				Administrador do projeto	Membro do projeto	Expectador de projeto
Biblioteca - Tópicos de eventos	Exibir tópicos do evento	Sim	Sim			
Biblioteca - Ações	Criar, atualizar ou excluir ações de extensibilidade	Sim				
	Exibir ações de extensibilidade	Sim	Sim			
Biblioteca - Fluxos de trabalho	Exibir fluxos de trabalho de extensibilidade	Sim	Sim			
Atividade - Execuções de ação	Cancelar ou excluir execuções de ação de extensibilidade	Sim				
	Exibir execuções de ação de extensibilidade	Sim	Sim			Sim. Seus projetos
Atividade - Execuções de fluxo de trabalho	Exibir execuções de fluxo de trabalho de extensibilidade	Sim	Sim			
Projetar						
Projetar	Abra a guia Projetar e veja uma lista de modelos de nuvem	Sim	Sim	Sim. Seus projetos	Sim. Seus projetos	Sim. Seus projetos
Modelos de nuvem	Criar, atualizar e excluir modelos de nuvem	Sim		Sim. Seus projetos	Sim. Seus projetos	
	Visualizar modelos de nuvem	Sim	Sim	Sim. Seus projetos	Sim. Seus projetos	Sim. Seus projetos
	Baixar modelos de nuvem	Sim	Sim	Sim. Seus projetos	Sim. Seus projetos	Sim. Seus projetos
	Carregar modelos de nuvem	Sim		Sim. Seus projetos	Sim. Seus projetos	
	Implantar modelos de nuvem	Sim		Sim. Seus projetos	Sim. Seus projetos	

Tabela 2-2. Funções de serviço e funções de projeto do vRealize Automation Cloud Assembly (continuação)

Contexto da interface do usuário	Tarefa	Administrador do Cloud Assembly	Expectador do Cloud Assembly	Usuário do Cloud Assembly O usuário deve ser administrador ou membro do projeto para ver e realizar tarefas relacionadas ao projeto.		
				Administrador do projeto	Membro do projeto	Expectador de projeto
	Versão e restauração de modelos de nuvem	Sim		Sim. Seus projetos	Sim. Seus projetos	
	Lançar modelos de nuvem no catálogo	Sim		Sim. Seus projetos	Sim. Seus projetos	
Recursos Personalizados	Criar, atualizar ou excluir recursos personalizados	Sim				
	Visualizar recursos personalizados	Sim	Sim	Sim. Seus projetos	Sim. Seus projetos	Sim. Seus projetos
Ações Personalizadas	Criar, atualizar ou excluir ações personalizadas	Sim				
	Exibir ações personalizadas	Sim	Sim	Sim. Seus projetos	Sim. Seus projetos	Sim. Seus projetos
Implantações						
	Visualizar e abrir a guia Implantações	Sim	Sim	Sim	Sim	Sim
	Exiba implantações, incluindo detalhes de implantação, histórico de implantações e informações de solução de problemas.	Sim	Sim	Sim. Seus projetos	Sim. Seus projetos	Sim. Seus projetos
	Execute ações do dia 2 em implantações com base em políticas.	Sim		Sim. Seus projetos	Sim. Seus projetos	

Funções de serviço do Service Broker

As funções de serviço do vRealize Automation Service Broker determinam o que você pode ver e fazer no vRealize Automation Service Broker. Essas funções de serviço são definidas no console por um proprietário da organização.

Tabela 2-3. Descrições de funções de serviço do Service Broker

Função	Descrição
Administrador do Service Broker	É necessário ter acesso de leitura e gravação para toda a interface do usuário e recursos de API. Esta é a única função de usuário que pode executar todas as tarefas, incluindo a criação de um novo projeto e a atribuição de um administrador de projeto.
Usuário do Service Broker	Qualquer usuário que não tenha a função Administrador do vRealize Automation Service Broker. Em um projeto vRealize Automation Service Broker, o administrador adiciona usuários a projetos como membros, administradores ou visualizadores do projeto. O administrador também pode adicionar um administrador de projeto.
Espectador do Service Broker	Um usuário que tem acesso de leitura para ver informações, mas não pode criar, atualizar ou excluir valores. Os usuários com a função de visualizador podem ver todas as informações que estão disponíveis para o administrador. Ele não pode realizar nenhuma ação, a menos que você o torne um administrador de projeto ou membro do projeto. Se o usuário for afiliado a um projeto, ele terá as permissões relacionadas à função. A função de visualizador de projeto não abrange as permissões da mesma forma que a função de administrador ou membro.

Além das funções de serviço, o vRealize Automation Service Broker tem funções de projeto. Todos os projetos estão disponíveis em todos os serviços.

As funções de projeto são definidas no vRealize Automation Service Broker e podem variar entre projetos.

Nas tabelas a seguir, que indicam o que as diferentes funções de serviço e projeto podem ver e fazer, lembre-se de que os administradores de serviços têm permissão total em todas as áreas da interface do usuário.

Use as seguintes descrições de funções de projeto como ajuda para decidir quais permissões dar aos seus usuários.

- Os administradores de projetos aproveitam a infraestrutura criada pelo administrador de serviços para garantir que os membros do projeto tenham os recursos necessários para o trabalho de desenvolvimento.
- Os membros do projeto trabalham em seus projetos para projetar e implantar modelos de nuvem.
- Os espectadores de projeto estão restritos ao acesso somente leitura.

Tabela 2-4. Funções de serviço e funções de projeto do Service Broker

Contexto da interface do usuário	Tarefa	Administrador do Service Broker	Espectador do Service Broker	Usuário do Service Broker		
				O usuário deve ser administrador do projeto para ver e realizar tarefas relacionadas ao projeto.		
				Administrador do projeto	Membro do projeto	Expectador de projeto
Acessar o Service Broker						
Console	No console, você pode ver e abrir o Service Broker	Sim	Sim	Sim	Sim	Sim
Infraestrutura						
	Visualizar e abrir a guia Infraestrutura	Sim	Sim			
Configurar - Projetos	Criar projetos	Sim				
	Atualizar ou excluir valores do resumo do projeto, usuários, provisionamento, Kubernetes e integrações	Sim				
	Visualizar projetos	Sim	Sim			
Configurar - Zonas de Nuvem	Criar, atualizar ou excluir zonas de nuvem	Sim				
	Visualizar zonas de nuvem	Sim	Sim			
Configurar - Zonas do Kubernetes	Criar, atualizar ou excluir zonas do Kubernetes	Sim				
	Exibir zonas do Kubernetes	Sim	Sim			
Conexões - Contas de Nuvem	Criar, atualizar ou excluir contas de nuvem	Sim				
	Exibir contas de nuvem	Sim	Sim			
Conexões - Integrações	Criar, atualizar ou excluir integrações	Sim				
	Visualizar integrações	Sim	Sim			

Tabela 2-4. Funções de serviço e funções de projeto do Service Broker (continuação)

Contexto da interface do usuário	Tarefa	Administrador do Service Broker	Espectador do Service Broker	Usuário do Service Broker O usuário deve ser administrador do projeto para ver e realizar tarefas relacionadas ao projeto.		
				Administrador do projeto	Membro do projeto	Expectador de projeto
Atividade - Solicitações	Excluir registros de solicitação de implantação	Sim				
	Exibir registros de solicitação de implantação	Sim				
Atividade - Logs de Eventos	Exibir logs de eventos	Sim				
Conteúdo e Políticas						
	Ver e abrir a guia Conteúdo e Políticas	Sim	Sim			
Fontes de conteúdo	Criar, atualizar ou excluir fontes de conteúdo	Sim				
	Exibir fontes de conteúdo	Sim	Sim			
Compartilhamento de Conteúdo	Adicionar ou remover conteúdo compartilhado	Sim				
	Exibir conteúdo compartilhado	Sim	Sim			
Conteúdo	Personalizar o formulário e configurar o item	Sim				
	Visualizar conteúdo	Sim	Sim			
Políticas – Definições	Criar, atualizar ou excluir definições de política	Sim				
	Exibir definições de política	Sim	Sim			
Políticas – Aplicação	Exibir log de aplicação	Sim	Sim			
Notificações - Servidor de E-mail	Configure um servidor de e-mail	Sim				

Tabela 2-4. Funções de serviço e funções de projeto do Service Broker (continuação)

Contexto da interface do usuário	Tarefa	Administrador do Service Broker	Espectador do Service Broker	Usuário do Service Broker		
				O usuário deve ser administrador do projeto para ver e realizar tarefas relacionadas ao projeto.		
				Administrador do projeto	Membro do projeto	Expectador de projeto
Catálogo						
	Ver e abrir a guia Catálogo	Sim	Sim	Sim	Sim	Sim
	Exibir itens de catálogo disponíveis	Sim	Sim	Sim. Seus projetos	Sim. Seus projetos	Sim. Seus projetos
	Solicitar um item de catálogo	Sim		Sim. Seus projetos	Sim. Seus projetos	
Implantações						
	Visualizar e abrir a guia Implantações	Sim	Sim	Sim.	Sim	Sim
	Exiba implantações, incluindo detalhes de implantação, histórico de implantações e informações de solução de problemas.	Sim	Sim	Sim. Seus projetos	Sim. Seus projetos	Sim. Seus projetos
	Executar ações de Dia 2 em implantações com base em políticas	Sim		Sim. Seus projetos	Sim. Seus projetos	
Aprovações						
	Ver e abrir a guia Aprovações	Sim	Sim	Sim	Sim	Sim
	Responder a solicitações de aprovação	Sim		Somente função do usuário do Service Broker	Somente função do usuário do Service Broker	Somente função do usuário do Service Broker

Fazendo a manutenção do seu dispositivo vRealize Automation

3

Como administrador do sistema, você pode precisar executar várias tarefas para garantir o bom funcionamento do seu dispositivo vRealize Automation instalado.

Se você está apenas começando com o vRealize Automation, essas tarefas não são necessárias. Saber como realizar essas tarefas é útil quando você precisa resolver problemas de desempenho ou comportamento do produto.

Este capítulo inclui os seguintes tópicos:

- [Iniciando e interrompendo o vRealize Automation](#)
- [Dimensionar horizontalmente o vRealize Automation de um a três nós](#)
- [Substituindo um nó de dispositivo do vRealize Automation](#)
- [Aumentar o espaço em disco do dispositivo vRealize Automation](#)
- [Atualizar a atribuição de DNS para vRealize Automation](#)
- [Como habilitar a sincronização de horário do vRealize Automation](#)
- [Como redefinir a senha root do vRealize Automation](#)

Iniciando e interrompendo o vRealize Automation

Observe os procedimentos adequados ao iniciar ou desligar o vRealize Automation.

A maneira recomendada de desligar e iniciar os componentes do vRealize Automation é usar a funcionalidade de LIGAR e DESLIGAR fornecida em **Operações de Ciclo de Vida > Ambientes**, do vRealize Suite Lifecycle Manager. Os procedimentos a seguir descrevem métodos manuais para desligar e iniciar componentes do vRealize Automation no caso de o vRealize Suite Lifecycle Manager não estar disponível por algum motivo.

Desligar o vRealize Automation

Para preservar a integridade dos dados, desligue os serviços do vRealize Automation antes de desligar os dispositivos virtuais. Usando o SSH ou o VMRC, você pode desligar ou iniciar todos os nós de qualquer dispositivo individual.

Observação Evite usar comandos `vracli reset vidm`, se possível. Esse comando redefine todas as configurações do Workspace ONE Access e interrompe a associação entre usuários e recursos provisionados.

- 1 Faça login no console de qualquer dispositivo vRealize Automation usando SSH ou o VMRC.
- 2 Para desligar os serviços do vRealize Automation em todos os nós do cluster, execute o seguinte conjunto de comandos.

Observação Se você copiar qualquer um desses comandos para execução e eles falharem, cole-os primeiro no bloco de notas e, em seguida, copie-os novamente antes de executá-los. Esse procedimento remove quaisquer caracteres ocultos e outros artefatos que possam existir na origem da documentação.

```
/opt/scripts/svc-stop.sh  
sleep 120  
/opt/scripts/deploy.sh --onlyClean
```

- 3 Desligue os dispositivos vRealize Automation.

Sua implantação do vRealize Automation está agora encerrada.

Iniciar o vRealize Automation

Após um desligamento não planejado, um desligamento controlado ou um procedimento de recuperação, você deve reiniciar os componentes do vRealize Automation em uma ordem específica. O vRLCM é um componente não crítico e, portanto, pode ser iniciado a qualquer momento. Os componentes do VMware Workspace ONE Access, o antigo VMware Identity Management, devem ser iniciados antes de você iniciar o vRealize Automation.

Observação Verifique se os balanceadores de carga aplicáveis estão em execução antes de iniciar os componentes do vRealize Automation.

- 1 Ligue todos os dispositivos vRealize Automation e aguarde sua inicialização.
- 2 Faça login no console para qualquer dispositivo usando SSH ou o VMRC e execute o seguinte comando para restaurar os serviços em todos os nós.

```
/opt/scripts/deploy.sh
```

- 3 Verifique se todos os serviços estão ativos e em execução com o seguinte comando.

```
kubectl get pods --all-namespaces
```

Observação Você deve ver três instâncias de cada serviço, com um status de Em execução ou Concluído.

Quando todos os serviços estiverem listados como Em execução ou Concluídos, o vRealize Automation estará pronto para uso.

Reiniciar o vRealize Automation

Você pode reiniciar todos os serviços do vRealize Automation centralmente a partir de qualquer um dos dispositivos no seu cluster. Siga as instruções anteriores para desligar o vRealize Automation e, em seguida, use as instruções para iniciar o vRealize Automation. Antes de reiniciar o vRealize Automation, verifique se todos os componentes do balanceador de carga e do VMware Workspace ONE Access aplicáveis estão em execução.

Quando todos os serviços estiverem listados como Em execução ou Concluídos, o vRealize Automation estará pronto para uso.

Execute o seguinte comando para verificar se todos os serviços estão em execução:

```
kubectl -n prelude get pods
```

Dimensionar horizontalmente o vRealize Automation de um a três nós

Conforme necessário, você pode dimensionar horizontalmente uma implantação do vRealize Automation de um nó para três nós.

Você deve usar os recursos do vRealize Suite Lifecycle Manager para concluir várias etapas deste procedimento. Para obter informações sobre como trabalhar com tarefas de instalação, upgrade e gerenciamento do vRealize Suite Lifecycle Manager, consulte a [Documentação do produto Lifecycle Manager](#).

Se você estiver usando uma implantação clusterizada de três nós, o vRealize Automation geralmente poderá resistir à falha de um nó e ainda funcionar. A falha de dois nós em um cluster de três nós resultará em um vRealize Automation não funcional.

Pré-requisitos

Esse procedimento pressupõe que você já tenha uma implantação de único nó do vRealize Automation em funcionamento.

Procedimentos

- 1 Desligue todos os dispositivos do vRealize Automation.

Para encerrar os serviços de vRealize Automation em todos os nós do cluster, execute o seguinte conjunto de comandos.

```
/opt/scripts/svc-stop.sh
sleep 120
/opt/scripts/deploy.sh --onlyClean
```

Agora você pode desligar os dispositivos do vRealize Automation.

- 2 Tire um instantâneo de implantação.

Use a opção Criar Instantâneo no vRealize Suite Lifecycle Manager **Operações de Ciclo de Vida > Ambientes > vRA > Exibir Detalhes**.

Observação Instantâneos online, obtidos sem desligar os nós do vRealize Automation, são compatíveis com a 8.0.1. Para ambientes do vRealize Automation 8.0, você deve parar primeiro os nós do vRealize Automation.

- 3 Ligue o dispositivo do vRealize Automation e abra todos os contêineres.
- 4 Usando a funcionalidade de Locker localizada em **LCM > Locker > Certificados** no vRealize Suite Lifecycle Manager, gere ou importe certificados do vRealize Automation para todos os componentes, incluindo FQDNs de nó do vRealize Suite Lifecycle Manager e o nome de domínio completo do Balanceador de Carga do vRealize Automation.
Adicione os nomes dos três dispositivos nos Nomes Alternativos da Entidade.
- 5 Importe o novo certificado para o vRealize Suite Lifecycle Manager.
- 6 Substitua o certificado existente do vRealize Suite Lifecycle Manager pelo que foi gerado na etapa anterior usando a opção LCM **Operações de Ciclo de Vida > Ambientes > vRA > Exibir Detalhes** Substituir Certificado.
- 7 Dimensione horizontalmente o vRealize Automation para três nós usando a seleção Adicionar Componentes em **LCM > Operações de Ciclo de Vida > Ambientes > vRA > Exibir Detalhes**.

Resultados

O vRealize Automation foi dimensionada para uma implantação de três nós.

Substituindo um nó de dispositivo do vRealize Automation

Quando um dispositivo do vRealize Automation em uma configuração de vários nós de alta disponibilidade (HA) apresenta uma falha, pode ser necessário substituir o nó com falha.

Cuidado Antes de continuar, a VMware recomenda que você entre em contato com o suporte técnico para solucionar o problema de HA e verificar se o problema está isolado em um único nó.

Se o suporte técnico determinar que é necessário substituir o nó, tome as seguintes medidas.

- 1 No vCenter, faça snapshots de backup de cada dispositivo na configuração de HA.

Nos snapshots de backup, não inclua a memória da máquina virtual.

- 2 Desligue o nó com falha.

- 3 Anote o número de compilação de software do vRealize Automation do nó com falha e as configurações de rede.

Anote o FQDN, o endereço IP, o gateway, os servidores DNS e, especialmente, o endereço MAC. Mais tarde, você atribuirá os mesmos valores ao nó de substituição.

- 4 O nó do banco de dados primário deve ser um dos nós íntegros. Siga estas etapas:

- a Faça login como raiz na linha de comando de um nó íntegro.

- b Encontre o nome do nó do banco de dados primário executando o seguinte comando.

```
vracli status | grep primary -B 1
```

O resultado deve ser semelhante a este exemplo, em que postgres-1 é o nó primário do banco de dados.

```
"Conninfo":
"host=postgres-1.postgres.prelude.svc.cluster.local
dbname=repmgr-db user=repmgr-db passfile=/scratch/repmgr-db.cred
connect_timeout=10",
"Role": "primary",
```

- c Verifique se o nó do banco de dados primário está íntegro, executando o comando a seguir.

```
kubectll -n prelude get pods -o wide | grep postgres
```

O resultado deve ser semelhante a este exemplo, em que postgres-1 está na lista como em execução e íntegro.

```
postgres-1 1/1 Running 0 39h 12.123.2.14 vc-vm-224-84.company.com <none> <none>
postgres-2 1/1 Running 0 39h 12.123.1.14 vc-vm-224-85.company.com <none> <none>
```

Importante Se o nó do banco de dados primário estiver com falha, entre em contato com o suporte técnico em vez de prosseguir.

- 5 Na linha de comando raiz do nó íntegro, remova o nó com falha.

```
vracli cluster remove faulty-node-FQDN
```

- 6 Use o vCenter para implantar um nó novo de substituição do vRealize Automation.

Implante o mesmo número de compilação de software do vRealize Automation e aplique as configurações de rede do nó com falha. Inclua o FQDN, o endereço IP, o gateway, os servidores DNS e, especialmente, o endereço MAC que você anotou anteriormente.

- 7 Ligue o nó de substituição.

- 8 Faça login como raiz na linha de comando do nó de substituição.
- 9 Verifique se a sequência de inicialização inicial foi concluída, executando o seguinte comando.

```
vracli status first-boot
```

Procure uma mensagem `First boot complete`.

- 10 No nó de substituição, ingresse o cluster do vRealize Automation.

```
vracli cluster join primary-DB-node-FQDN
```

- 11 Faça login como raiz na linha de comando do nó de banco de dados primário.

- 12 Implante o cluster reparado, executando o seguinte script.

```
/opt/scripts/deploy.sh
```

Aumentar o espaço em disco do dispositivo vRealize Automation

Você pode precisar aumentar o espaço em disco do dispositivo vRealize Automation para finalidades específicas, como armazenamento de arquivos de log.

Procedimentos

- 1 Use o vSphere para expandir o VMDK no dispositivo vRealize Automation.
- 2 Faça login na linha de comando do dispositivo vRealize Automation como um usuário raiz.
- 3 No prompt de comando, execute o seguinte comando do vRealize Automation:

```
vracli disk-mgr resize
```

Se o redimensionamento do vRealize Automation falhar, consulte o [Artigo 79925 da Base de Conhecimento](#).

Atualizar a atribuição de DNS para vRealize Automation

Um administrador pode atualizar as atribuições de DNS para vRealize Automation.

Procedimentos

- 1 Faça login no console de qualquer dispositivo vRealize Automation usando SSH ou VMRC.
- 2 Para encerrar os serviços de vRealize Automation em todos os nós do cluster, execute o seguinte conjunto de comandos.

```
/opt/scripts/svc-stop.sh
sleep 120
/opt/scripts/deploy.sh --onlyClean
```

- 3 Faça login no vCenter e desligue todos os nós vRealize Automation usando o comando `Shut Down Guest OS`.
- 4 Atualize a propriedade DNS do OVF de cada nó vRealize Automation.
 - a Navegue até o nó do vRealize Automation do inventário do vCenter.
 - b Selecione a guia Configurar e expanda Configurações.
 - c Selecione as opções de vApp.
 - d Na lista de propriedades do OVF, localize e selecione `vami.DNS.vRealize_Automation`.
 - e Clique em **Definir valor** e insira as novas entradas DNS na caixa de texto Valor da propriedade.
 - f Clique em **OK**.
- 5 Inicie todos os nós do vRealize Automation e aguarde para que eles iniciem completamente, o que será indicado por uma tela azul no console.
- 6 Reinicie os nós do vRealize Automation novamente e aguarde para que eles iniciem completamente.
- 7 Faça login em cada nó do vRealize Automation com SSH e verifique se os novos servidores DNS estão listados em `/etc/resolve.conf`.
- 8 Em um dos nós do vRealize Automation, execute o seguinte comando para iniciar os serviços vRealize Automation: `/opt/scripts/deploy.sh`

Resultados

As configurações de DNS vRealize Automation são alteradas conforme especificado.

Como habilitar a sincronização de horário do vRealize Automation

Você pode habilitar a sincronização de horário na sua implantação do vRealize Automation usando a linha de comando do dispositivo vRealize Automation.

Você pode configurar a sincronização de horário para sua implantação do vRealize Automation independente ou em cluster usando o protocolo de rede NTP. O vRealize Automation oferece suporte a duas configurações NTP mutuamente exclusivas:

Configuração NTP	Descrição
ESXi	<p>Você pode usar essa configuração quando o servidor ESXi que hospeda o dispositivo vRealize Automation é sincronizado com um servidor NTP. Se estiver usando uma implantação em cluster, todos os hosts ESXi deverão ser sincronizados com um servidor NTP.</p> <p>Observação Poderá ocorrer um desvio de relógio se a sua implantação do vRealize Automation for migrada para um host ESXi não sincronizado com um servidor NTP.</p> <p>Para obter mais informações sobre como configurar o NTP para o ESXi, consulte o artigo KB 57147 Configurando o protocolo NTP em um host ESXi usando o vSphere Web Client.</p>
systemd	<p>Essa configuração usa o daemon systemd-timesyncd para sincronizar os relógios da sua implantação do vRealize Automation.</p> <p>Observação Por padrão, o daemon systemd-timesyncd está habilitado, mas configurado sem servidores NTP. Se o dispositivo vRealize Automation usar uma configuração de IP dinâmico, ele poderá usar qualquer servidor NTP recebido pelo protocolo DHCP.</p>

Procedimentos

1 Faça login na linha de comando do dispositivo vRealize Automation como **root**.

2 Habilite o NTP com o ESXi.

- a Execute o comando `vracli ntp esxi`.
- b Execute o comando `vracli ntp apply`.

A configuração NTP do ESXi é aplicada à implantação do vRealize Automation.

3 Habilite o NTP com o systemd.

- a Execute o comando `vracli ntp systemd --set FQDN_ou_IP_do_servidor_systemd`.

Observação Você pode adicionar vários servidores NTP systemd, separando seus endereços de rede com uma vírgula.

- b Execute o comando `vracli ntp apply`.

A configuração NTP do systemd é aplicada à implantação do vRealize Automation.

4 (Opcional) Para confirmar o status da configuração NTP, execute o comando `vracli ntp status`.

A configuração NTP poderá falhar se houver uma diferença de horário de mais de 10 minutos entre o servidor NTP e a implantação do vRealize Automation. Para resolver esse problema, reinicie o dispositivo vRealize Automation que está sincronizado com o servidor NTP.

Como redefinir a senha root do vRealize Automation

Você pode redefinir uma senha root perdida ou esquecida do vRealize Automation.

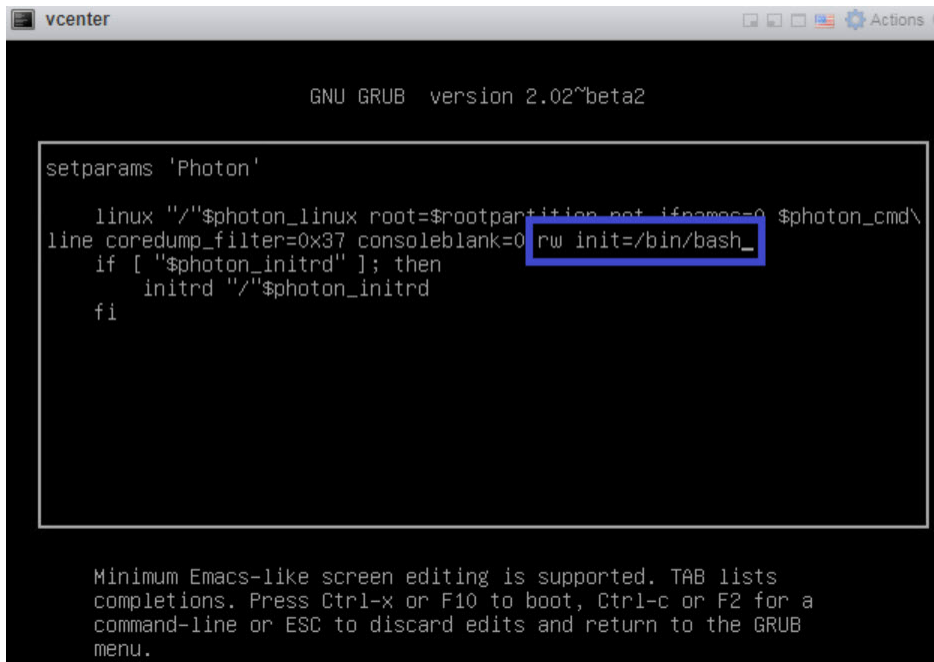
Neste procedimento, você usa uma janela de linha de comando no dispositivo vCenter do host para redefinir a senha raiz do vRealize Automation da sua organização.

Pré-requisitos

Esse processo é para administradores do vRealize Automation e requer as credenciais necessárias para acessar o dispositivo vCenter host.

Procedimentos

- 1 Desligue e inicie o vRealize Automation usando o procedimento descrito em [Iniciando e interrompendo o vRealize Automation](#).
- 2 Quando a janela da linha de comando do sistema operacional Photon for exibida, insira e pressione a tecla **Enter** para abrir o editor do menu de inicialização GNU GRUB.
- 3 No editor GNU GRUB, insira `rw init=/bin/bash` no final da linha que começa com `linux "/"` `$photon_linux root=rootpartition`, conforme mostrado abaixo:



```
GNU GRUB version 2.02~beta2

setparams 'Photon'

linux "/"$photon_linux root=$rootpartition rw init=/bin/bash $photon_cmd\
line coredump_filter=0x37 consoleblank=0
if [ "$photon_initrd" ]; then
  initrd "/"$photon_initrd
fi

Minimum Emacs-like screen editing is supported. TAB lists
completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a
command-line or ESC to discard edits and return to the GRUB
menu.
```

- 4 Pressione a tecla **F10** para aplicar a alteração e reiniciar o vRealize Automation.
- 5 Aguarde a reinicialização do vRealize Automation.
- 6 No prompt `root [/]#`, insira `passwd` e pressione a tecla **Enter**.
- 7 No prompt `New password:`, insira sua nova senha e pressione a tecla **Enter**.
- 8 No prompt `Retype new password:`, reinsira sua nova senha e pressione a tecla **Enter**.

- 9 No prompt root [/]#, insira `reboot -f` e pressione a tecla **Enter** para concluir o processo de redefinição da senha root.

```
root [ / ]# passwd
New password:
Retype new password:
passwd: password updated successfully
root [ / ]# reboot -f_
```

Próximo passo

Como administrador do vRealize Automation, agora você pode fazer login no vRealize Automation com a nova senha root.

Usando configurações de tenant de várias organizações no vRealize Automation

4

O vRealize Automation permite que os provedores de TI do cliente configurem vários tenants, ou organizações, em cada implantação. Os provedores podem configurar várias organizações de tenants e alocar infraestrutura em cada implantação. Os provedores também podem gerenciar usuários para tenants. Cada tenant gerencia seus próprios projetos, recursos e implantações.

Em uma configuração de várias organizações do vRealize Automation, os provedores podem criar várias organizações. e cada organização de tenant usa seus próprios projetos, recursos e implantações. Embora os provedores não possam gerenciar a infraestrutura de tenants remotamente, eles podem fazer login nos tenants e gerenciar a infraestrutura dentro de seus tenants.

A multilocação depende da coordenação e configuração de três produtos da VMware diferentes, conforme descrito abaixo:

- Workspace ONE Access - Este produto fornece o suporte de infraestrutura para multilocação e as conexões de domínios do Active Directory que fornecem gerenciamento de usuários e grupos em organizações de tenants.
- vRealize Suite Lifecycle Manager - Este produto oferece suporte à criação e à configuração de tenants para produtos com suporte, como o vRealize Automation. Além disso, ele fornece alguns recursos de gerenciamento de certificados.
- vRealize Automation - Provedores e usuários fazem login no vRealize Automation para acessar tenants nos quais eles criam e gerenciam implantações.

Ao configurar a multilocação, os usuários devem estar familiarizados com todos esses três produtos e com a documentação associada.

Para obter mais informações sobre como trabalhar com o Lifecycle Manager e o Workspace ONE Access, consulte o [Gerenciamento de usuários com o VMware Identity Manager](#) e [Gerenciando usuários e grupos](#).

Administradores com privilégios do vRealize Suite Lifecycle Manager criam e gerenciam tenants usando a página Tenants do Lifecycle Manager, localizada no serviço Gerenciamento de Identidades e Tenants. Tenants são construídos usando uma conexão IWA ou LDAP do Active Directory e têm suporte pelo instância associada do VMware Workspace ONE Access que é necessária para implantações do vRealize Automation. Consulte a documentação associada para obter informações sobre como usar o Lifecycle Manager.

Ao configurar a multilocalização, você começa com uma base, ou tenant mestre. Esse tenant é o tenant padrão criado quando o aplicativo Workspace ONE Access subjacente é implantado. Outros tenants, conhecidos como subtenants, podem ser baseados no tenant mestre. Atualmente, o vRealize Automation oferece suporte a até 20 organizações de tenant com a implantação padrão de três nós.

Ao configurar o vRealize Automation para multilocalização, você deve primeiro instalar o aplicativo em uma configuração de organização única e, em seguida, usar o Lifecycle Manager para definir uma configuração de várias organizações. Uma implantação do Workspace ONE Access oferece suporte ao gerenciamento de tenants e as conexões de domínios do Active Directory associadas.

Quando a multilocalização é configurada inicialmente, um administrador de provedor é designado no Lifecycle Manager. Você pode alterar essa designação ou adicionar administradores posteriormente, se desejar. Em configurações de várias organizações, os usuários e grupos do vRealize Automation são gerenciados principalmente por meio do Workspace ONE Access.

Depois que as organizações são criadas, os usuários autorizados podem fazer login em seus aplicativos para criar ou trabalhar com projetos e recursos e criar implantações. Os administradores podem gerenciar funções de usuário no vRealize Automation.

Definindo uma configuração de várias organizações

Você pode habilitar uma implantação de várias organizações depois de concluir uma instalação do vRealize Automation. Ao definir uma configuração de várias organizações, você deve configurar seu Workspace ONE Access para uso de multilocalização e, em seguida, usar o Lifecycle Manager para criar e configurar tenants. Isso se aplica a implantações novas e existentes. Como etapa inicial para configurar tenants, você deve usar o Lifecycle Manager para definir um alias para o tenant mestre que foi criado por padrão no Workspace ONE Access. Os subtenants criados com base nesse tenant mestre herdam as configurações de domínio do Active Directory do tenant mestre.

No Lifecycle Manager, você atribui tenants a um produto, como o vRealize Automation, e a um ambiente específico. Ao configurar um tenant, você também deve designar um administrador de tenants. Por padrão, a multilocalização é habilitada com base no nome de host do tenant. Os usuários podem optar por configurar manualmente o nome do tenant pelo nome de DNS. Durante esse procedimento, você deve definir vários sinalizadores para oferecer suporte a multilocalização e também deve configurar o balanceador de carga.

Se você usar uma instância em cluster, os nomes de host baseados em tenants do Workspace ONE Access e do vRealize Automation apontarão para o balanceador de carga.

Se os seus balanceadores de carga do vRealize Automation e do Workspace ONE Access em cluster não usarem certificados curinga, os usuários deverão adicionar nomes de host de tenants como entradas SAN nos certificados para cada novo tenant criado.

Você não pode excluir tenants no vRealize Automation ou no Lifecycle Manager. Se precisar adicionar tenants a uma implantação de multilocalização existente, poderá usar o Lifecycle Manager, mas isso exigirá um tempo de inatividade de três a quatro horas.

Nomes de host e multilocalização

Em versões anteriores do vRealize Automation, os usuários acessavam tenants com URLs baseadas no caminho do diretório. Na implementação atual de multilocalização, os usuários acessam os tenants com base no nome do host.

Além disso, o formato de nome do host que os usuários do vRealize Automation usarão para acessar tenants difere do formato usado para acessar tenants no Workspace ONE Access. Por exemplo, um nome de host válido seria assim: *tenant1.example.eng.vmware.com* em oposição a *vidm-node1.eng.vmware.com*.

Multilocalização e certificados

Você deve criar certificados para todos os componentes envolvidos em uma configuração de várias organizações. Você precisará de um ou mais certificados para o Workspace ONE Access, o Lifecycle Manager e o vRealize Automation, dependendo de você estar usando uma configuração de nó único ou uma configuração em cluster.

Ao configurar certificados, você pode usar curingas com os nomes de SAN ou nomes dedicados. O uso de curingas simplificará um pouco o gerenciamento de certificados, pois estes deverão ser atualizados sempre que você adicionar novos tenants. Se o seu balanceador de carga do vRealize Automation e do Workspace ONE Access não usar certificados curinga, você deverá adicionar nomes de host de tenants como entradas SAN nesses certificados para cada novo tenant criado. Além disso, se você usar o SAN, os certificados deverão ser atualizados manualmente se você adicionar ou excluir hosts ou alterar um nome de host. Você também deve atualizar as entradas DNS para tenants.

Observe que o Lifecycle Manager não cria certificados separados para cada tenant.

Em vez disso, ele cria um único certificado com cada nome de host do tenant listado. Para configurações básicas, o CNAME do tenant usa o seguinte formato: *tenantname.vrahostname.domain*. Para configurações de alta disponibilidade, o nome usa o seguinte formato: *tenantname.vraLBhostname.domain*.

Se você estiver usando uma configuração em cluster do Workspace ONE Access, observe que o Lifecycle Manager não poderá atualizar o certificado do balanceador de carga e, portanto, você deverá atualizá-lo manualmente. Além disso, se você precisar registrar novamente produtos ou serviços externos ao Lifecycle Manager, este será um processo manual.

Este capítulo inclui os seguintes tópicos:

- [Configurar a localização de várias organizações para o vRealize Automation](#)
- [Fazendo login em tenants e adicionando usuários no vRealize Automation](#)

- Usando o vRealize Orchestrator com implantações do vRealize Automation em várias organizações

Configurar a locação de várias organizações para o vRealize Automation

É possível configurar a locação de várias organizações para o vRealize Automation usando o vRealize Suite Lifecycle Manager.

Veja a seguir uma descrição genérica do procedimento para configurar a multilocação para o vRealize Automation, incluindo a configuração de DNS e certificados. Ela se concentra na implantação de um único nó, mas inclui notas para uma configuração em cluster.

Consulte <https://vmwarelab.org/2020/04/14/vrealize-automation-8-1-multi-tenancy-setup-with-vrealize-suite-lifecycle-manager-8-1/> para obter mais informações e assistir a um vídeo de demonstração sobre como concluir uma configuração do vRealize Automation em várias organizações.

Pré-requisitos

- Instale e configure o Workspace ONE Access versão 3.3.2.
- Instale e configure o vRealize Suite Lifecycle Manager versão 8.2.

Procedimentos

- 1 Crie os registros DNS de tipos A e CNAME necessários.
 - Para seu tenant mestre e cada subtenant, você deve criar e aplicar um certificado SAN.
 - Para implantações de nó único, o FQDN do vRealize Automation aponta para o dispositivo vRealize Automation, enquanto o FQDN do Workspace ONE Access aponta para o dispositivo Workspace ONE Access.
 - Para implantações em cluster, os FQDNs baseados em tenant Workspace ONE Access e vRealize Automation devem apontar para os respectivos balanceadores de carga. Como o Workspace ONE Access está configurado com terminação SSL, o certificado é aplicado ao cluster e ao balanceador de carga do Workspace ONE Access. Como o balanceador de carga do vRealize Automation usa passagem SSL, o certificado é aplicado apenas ao cluster do vRealize Automation.

Consulte [Gerenciando certificados e a configuração de DNS em implantações de várias organizações de nó único](#) e [Gerenciando o certificado e a configuração de DNS em implantações do vRealize Automation com cluster](#) para obter mais detalhes.

- 2 Crie ou importe os certificados de vários domínios (SAN) necessários para o Workspace One 3.3.2 e o vRA 8.2.

Você pode criar certificados no Lifecycle Manager usando o serviço Locker, que permite criar licenças de certificados e senhas. Como alternativa, você pode usar um servidor de CA ou algum outro mecanismo para gerar certificados.

Se precisar adicionar ou criar tenants adicionais, você deverá recriar e aplicar seus tenants do vRealize Automation e do Workspace ONE Access.

Depois de criar seus certificados, você poderá aplicá-los no Lifecycle Manager usando o recurso Lifecycle Operations. Você deve selecionar o ambiente e o produto e, em seguida, a opção Substituir Certificado no menu à direita. Em seguida, é possível selecionar o produto. Ao substituir um certificado, você deve confiar novamente em todos os produtos associados no seu ambiente.

É necessário aguardar a aplicação do certificado e a reinicialização de todos os serviços antes de prosseguir para a próxima etapa.

Consulte [Gerenciando certificados e a configuração de DNS em implantações de várias organizações de nó único](#) e [Gerenciando o certificado e a configuração de DNS em implantações do vRealize Automation com cluster](#) para obter mais detalhes.

- 3 Aplique o certificado SAN do Workspace One à instância ou ao cluster do Workspace ONE Access.
- 4 No vRealize Suite Lifecycle Manager, execute o assistente para Habilitar Locação para habilitar a multilocação e criar um alias para o tenant mestre padrão.

Habilitar a locação requer que você crie um alias para o tenant padrão ou o tenant mestre da organização do provedor. Depois de habilitar a locação, será possível acessar o Workspace ONE Access por meio do FQDN do tenant mestre.

Por exemplo, se o FQDN existente do Workspace ONE Access for `idm.example.local` e você criar um alias de default-tenant, depois que a locação for habilitada, o FQDN do Workspace ONE Access mudará para `default-tenant.example.local`, e todos os clientes que estiverem se comunicando com o Workspace ONE Access agora se comunicarão por meio de `default-tenant.example.local`.

- 5 Aplique os certificados SAN vRealize Automation na instância vRealize Automation ou no cluster.

Você pode aplicar certificados SAN por meio do serviço Lifecycle Manager Lifecycle Operations. Você precisa visualizar os detalhes do ambiente e depois selecionar Substituir Certificados no menu à direita. É necessário aguardar a conclusão da tarefa de substituição de certificado antes de adicionar tenants. Como parte da substituição do certificado, os serviços do vRealize Automation serão reiniciados.

- 6 No Lifecycle Manager, execute o assistente Adicionar Tenants para configurar os tenants desejados.

Você adiciona tenants usando a página Gerenciamento de Tenants do Lifecycle Manager, localizada em Gerenciamento de Identidade e Tenants. Você só poderá adicionar tenants para os quais já tiver definido certificados e configurações de DNS.

Ao criar um tenant, você deve designar um administrador de tenants e pode selecionar as conexões do Active Directory para esse tenant. As conexões disponíveis são baseadas naquelas configuradas no seu tenant padrão ou mestre. Você também deve selecionar o produto ou a instância do produto ao qual o tenant será associado.

Próximo passo

Depois de criar tenants, você pode usar a página Gerenciamento de Tenants do Lifecycle Manager, localizada em Gerenciamento de Identidade e Tenants, para alterar ou adicionar administradores de tenants, adicionar diretórios do Active Directory ao tenant e alterar associações de produtos para o tenant.

Você também pode fazer login na sua instância do Workspace ONE Access para visualizar e validar sua configuração de tenant.

Gerenciando certificados e a configuração de DNS em implantações de várias organizações de nó único

As configurações do vRealize Automation de locação em várias organizações dependem de uma configuração coordenada entre vários produtos, e você deve garantir que as configurações de DNS e os certificados estejam definidos corretamente para que a sua configuração de locação em várias organizações funcione.

Essa configuração em várias organizações assume implantações de nó único para os seguintes componentes:

- Lifecycle Manager
- Workspace ONE Access Identity Manager
- vRealize Automation

Além disso, ela presume-se que você esteja começando com um tenant padrão, que é sua organização de provedor, e criando dois subtenants, denominados tenant-1 e tenant-2.

Você pode criar e aplicar certificados usando o serviço Locker no vRealize Suite Lifecycle Manager ou pode usar outro mecanismo. O Lifecycle Manager também permite que você substitua ou confie novamente em certificados no vRealize Automation ou Workspace ONE Access.

Requisitos de DNS

Você deve criar registros principais de tipo A e registros de tipo CNAME para os componentes do sistema, conforme descrito a seguir.

- Crie registros principais de tipo A para cada componente do sistema e para cada um dos tenants que você criará ao habilitar a multilocação.
- Crie registros de tipo A de multilocação para cada um dos tenants que você criará, bem como para o tenant mestre.

- Crie registros de tipo CNAME de multilocalização para cada um dos tenants que você criar, sem incluir o tenant mestre.

Requisitos de certificado para a implantação da multilocalização de nó único

Você deve criar dois certificados de Nome alternativo de requerente (SAN), um para o Workspace ONE Access e outro para o vRealize Automation.

- O certificado do vRealize Automation lista o nome do host do servidor vRealize Automation e os nomes dos tenants que você criará.
- O certificado do Workspace ONE Access lista o nome do host do servidor Workspace ONE Access e os nomes dos tenants que você está criando.
- Se você usar nomes de SAN dedicados, os certificados deverão ser atualizados manualmente quando você adicionar ou exclui hosts ou alterar um nome de host. Você também deve atualizar as entradas DNS para tenants. Como uma opção para simplificar a configuração, você pode usar curingas para os certificados do Workspace ONE Access e do vRealize Automation. Por exemplo, *.example.com e *.vra.example.com.

Observação O vRealize Automation 8.x oferece suporte a certificados curinga apenas para nomes DNS que correspondem às especificações na lista de Sufixos Públicos em <https://publicsuffix.org>. Por exemplo, *.myorg.com é um nome válido enquanto *.myorg.local é inválido.

Observe que o Lifecycle Manager não cria certificados separados para cada tenant.

Em vez disso, ele cria um único certificado com cada nome de host do tenant

listado. Para configurações básicas, o CNAME do tenant usa o seguinte formato:

tenantname.vrahostname.domain. Para configurações de alta disponibilidade, o nome usa o seguinte formato: *tenantname.vraLBhostname.domain*.

Resumo

A tabela a seguir resume os requisitos de DNS e certificado para uma implantação do Workspace ONE Access e do vRealize Automation de nó único.

Requisitos de DNS	Requisitos de certificado SAN
Main A Type Records lcm.example.local WorkspaceOne.example.local vra.example.local	Workspace One Certificate Nome do host: WorkspaceOne.example.local, default-tenant.example.local, tenant-1.vra.example.local, tenant-2.vra.example.local
Multi-tenancy A Type Records default-tenant.example.local tenant-1.example.local tenant-2.example.local	
Multi-Tenancy CNAME Type Records tenant-1.vra.example.local tenant-2.vra.example.local	vRealize Automation Certificate Nome do host: vra.example.local, tenant-1.vra.example.local, tenant-2.vra.example.local

Gerenciando o certificado e a configuração de DNS em implantações do vRealize Automation com cluster

Você deve coordenar o certificado e a configuração de DNS entre todos os componentes aplicáveis para configurar uma implantação do vRealize Automation com cluster de várias organizações.

Em uma configuração típica com cluster, existem três dispositivos Workspace ONE Access e três dispositivos vRealize Automation, bem como um único dispositivo Lifecycle Manager.

Essa configuração pressupõe implantações com cluster para os seguintes componentes:

- Dispositivos Workspace ONE Access Identity Manager:

- idm1.example.local
- idm2.example.local
- idm3.example.local
- idm-lb.example.local

- Dispositivos vRealize Automation:

- vra1.example.local
- vra2.example.local
- vra3.example.local
- vra-lb.example.local

- Dispositivo Lifecycle Manager

Requisitos de DNS

Você deve criar os dois registros principais de tipo A para cada componente e para cada um dos tenants que você criará ao habilitar a multilocalização. Além disso, você deve criar registros de tipo CNAME de multilocalização para cada um dos tenants que criar, sem incluir o tenant mestre. Por fim, você também deve criar registros de tipo A principais para os balanceadores de carga do Workspace ONE Access e do vRealize Automation.

- Crie registros de tipo A para os três dispositivos Workspace ONE Access e para os dispositivos vRealize Automation que apontam para seus respectivos FQDNs.
- Além disso, crie registros de tipo A para o balanceador de carga do Workspace ONE Access e o balanceador de carga vRealize Automation que apontem para seus respectivos FQDNs.
- Crie registros de Tipo A de multilocalização para o tenant padrão e para tenant-1 e tenant-2 que apontem para o endereço IP do balanceador de carga do Workspace ONE Access.
- Crie registros CNAME para tenant-1 e tenant-2 que apontem para o endereço IP do balanceador de carga do vRealize Automation.

Requisitos de certificado de Nome alternativo do requerente (SAN)

Você deve criar dois certificados do Workspace ONE Access, um aplicável aos dispositivos de cluster e outro aplicável ao balanceador de carga. Além disso, crie um certificado que se aplique aos dispositivos vRealize Automation, aos tenants que você está criando, excluindo o tenant padrão, e ao balanceador de carga.

- Crie um certificado para os dispositivos Workspace ONE Access que liste os FQDNs dos dispositivos Workspace ONE Access, bem como o tenant padrão e outros tenants que você criar. Esse certificado deve incluir os endereços IP dos dispositivos Workspace ONE Access.
- Como prática recomendada, crie uma terminação SSL no balanceador de carga. Para oferecer suporte a essa terminação, crie um certificado para o balanceador de carga do Workspace ONE Access que liste o FQDN do balanceador de carga do Workspace ONE Access, bem como o tenant padrão e todos os outros tenants que você criar. Esse certificado deve incluir o endereço IP do balanceador de carga.
- Você deve criar um certificado para o vRealize Automation que liste os nomes de host dos três dispositivos vRealize Automation, bem como o balanceador de carga relacionado e os tenants que você está criando. Além disso, ele deve listar os endereços IP dos três dispositivos vRealize Automation.
- Como uma opção para simplificar a configuração, você pode usar curingas para os certificados do Workspace ONE Access e do vRealize Automation. Por exemplo, *.example.com, *.vra.example.com e *.vra-lb.example.com.

Observação O vRealize Automation 8.x oferece suporte a certificados curinga apenas para nomes DNS que correspondem às especificações na lista de Sufixos Públicos em <https://publicsuffix.org>. Por exemplo, *.myorg.com é um nome válido enquanto *.myorg.local é inválido.

Se você estiver usando uma configuração em cluster do Workspace ONE Access, observe que o Lifecycle Manager não poderá atualizar os certificados do balanceador de carga e, portanto, você deverá atualizá-los manualmente. Além disso, se você precisar registrar novamente produtos ou serviços externos ao Lifecycle Manager, este será um processo manual.

Resumo das entradas de DNS e dos certificados para uma configuração de cluster de várias organizações

A tabela a seguir descreve os requisitos de DNS e certificado para uma implantação do Workspace ONE Access e do vRealize Automation com cluster de várias organizações.

Requisitos de DNS	Requisitos de certificado SAN
Main A Type Records lcm.example.local WorkspaceOne-1.example.local WorkspaceOne-2.example.local WorkspaceOne-3.example.local vra.example-1.local vra.example-2.local vra.example-3.local	Workspace One Certificate Nome do host: WorkspaceOne.example.local, default-tenant.example.local, tenant-1.example.local, tenant-2.example.local
Multi-Tenancy A Type Records default-tenant.example.local tenant-1.vra.example.local tenant-2.vra.example.local	Workspace One LB Certificate (LB Terminated) Nome do host: WorkSpaceOne-lb.example.local, default-tenant.example.local, vra.example.local, tenant-1.example.local, tenant-2.example.local
Multi-Tenancy CNAME Type Records tenant-1.vra-lb.example.local - vra-lb.example.local tenant-2.vra-lb.example.local - vra-lb.exmple.local	vRealize Automation Certificate Nome do host: vra-1.example.local, vra-2.example.local, vra-3.example.local, vra- lb.example.local, tenant-1.example.local, tenant-2.example.local Nenhum certificado é exigido no balanceador de carga do vRealize Automation, pois ele usa a passagem SSL.

Fazendo login em tenants e adicionando usuários no vRealize Automation

Depois de criar tenants para o vRealize Automation no Lifecycle Manager, você pode fazer login no Workspace ONE Access para visualizar seus tenants e adicionar usuários.

Você pode ver os tenants criados para uma implantação do vRealize Automation fazendo login na instância do Workspace ONE Access associada. A URL a ser usada é `https://nome do tenant padrão.domainname.local` ou, para uma implantação sem cluster, `https://idm.domainname.local`, o que o direcionará de volta à URL do Workspace ONE Access do tenant padrão.

Você pode validar tenants específicos no Workspace ONE Access usando a seguinte URL: `https://tenant-1.domainname.local`. Essa URL abre uma página que mostra os usuários do tenant especificado. Você pode clicar em **Adicionar Usuário** para criar usuários adicionais sistematicamente.

Os usuários autorizados podem fazer login na organização do provedor principal no vRealize Automation usando `https://vra.domainname.local`. Esta visão fornece acesso a todos serviços relacionados do vRealize Automation.

Os usuários autorizados podem fazer login nos tenants aplicáveis no vRealize Automation usando `https://nome do tenant.vra.domainname.local`.

Para obter mais informações sobre como gerenciar usuários no Workspace ONE Access, consulte [href=../..../VMware-Workspace-ONE-Access/3.3/idm-administrator/GUID-234FC22E-1292-4EA2-AAF1-346719573FBA.html](https://docs.vmware.com/en/VMware-Workspace-ONE-Access/3.3/idm-administrator/GUID-234FC22E-1292-4EA2-AAF1-346719573FBA.html)

Adicionando usuários locais

Você pode adicionar usuários locais à sua implantação usando a instância do Workspace ONE Access associada. Usuários locais são aqueles que não estão armazenados em nenhum provedor de identidade externo.

Usando o vRealize Orchestrator com implantações do vRealize Automation em várias organizações

Você pode usar o vRealize Orchestrator com implantações de locação do vRealize Automation em várias organizações.

O tenant padrão oferece suporte direto para a integração do vRealize Orchestrator. O vRealize Orchestrator está disponível em estado pré-configurado na página Integrações. Os subtenants não têm uma integração do vRealize Orchestrator pré-registrada. Eles têm várias opções para adicionar a integração do vRealize Orchestrator.

- Eles podem adicionar integração com o vRealize Orchestrator incorporado navegando até Configurar Provedor de Autenticação no vRealize Orchestrator e conectando-se com o uso do endereço de host do tenant do vRealize Automation aplicável. Em seguida, eles podem selecionar **Infraestrutura > Conexões > Integrações** e adicionar o vRO incorporado como uma integração.
- Eles podem adicionar uma instância externa do vRealize Orchestrator que usa o vRealize Automation em várias organizações como provedor de autenticação.

Qualquer instância do vRealize Orchestrator que usar uma implantação do vRealize Automation em várias organizações como provedor de autenticação poderá ser registrada em qualquer um dos tenants, criando uma nova integração e fornecendo o FQDN do vRealize Orchestrator sem fornecer credenciais.

Trabalhando com logs no vRealize Automation

5

Você pode usar o utilitário de linha de comando do `vraccli` fornecido para criar e usar logs no vRealize Automation .

É possível usar os logs diretamente no vRealize Automation ou encaminhar todos os logs ao vRealize Log Insight .

Este capítulo inclui os seguintes tópicos:

- [Como trabalhar com logs e pacotes de logs no vRealize Automation](#)
- [Como configurar o encaminhamento de logs ao vRealize Log Insight](#)
- [Como criar ou atualizar uma integração de syslog no vRealize Automation](#)

Como trabalhar com logs e pacotes de logs no vRealize Automation

Logs são gerados automaticamente pelos vários serviços. Você pode gerar pacotes de log no vRealize Automation. Também pode configurar seu ambiente para encaminhar logs automaticamente ao vRealize Log Insight.

Informações sobre como usar o utilitário de linha de comando `vraccli` para gerar pacotes de logs estão disponíveis usando o argumento `--help` na linha de comando `vraccli` (por exemplo, `vraccli log-bundle --help`).

Para obter informações relacionadas sobre como usar o vRealize Log Insight, consulte [Como configurar o encaminhamento de logs ao vRealize Log Insight](#) .

Comandos de pacotes de logs

É possível criar um pacote de logs para conter todos os logs que são gerados pelos serviços que você executa. Um pacote de logs contém todos os logs de serviço e é necessário para a solução de problemas.

Em um ambiente em cluster (modo de alta disponibilidade), execute o comando `vracli log-bundle` em apenas um nó. Logs são extraídos de todos os nós do ambiente. No entanto, no caso de um problema de rede ou outro problema de cluster, os logs serão extraídos de quantos nós puderem ser alcançados. Por exemplo, se um nó for desconectado em um cluster de três nós, logs serão coletados apenas dos dois nós íntegros. A saída do comando `vracli log-bundle` contém informações sobre quaisquer problemas encontrados e suas etapas de solução alternativa.

- Para criar um pacote de logs, aplique SSH a qualquer nó e execute o seguinte comando `vracli`:

```
vracli log-bundle
```

- Para alterar o valor de tempo limite para a coleta de logs de cada nó, execute o seguinte comando `vracli`:

```
vracli log-bundle --collector-timeout $CUSTOM_TIMEOUT_IN_SECONDS
```

Por exemplo, se o seu ambiente contiver arquivos de log grandes, rede lenta ou alto uso de CPU, você poderá definir o tempo limite para mais do que o valor padrão de 1000 segundos.

- Para configurar outras opções, como tempo limite de assembly e local do buffer, use o seguinte de ajuda `vracli`:

```
vracli log-bundle --help
```

Estrutura do pacote de logs

O pacote de logs é um arquivo tar com carimbo de data/hora. O nome do pacote corresponde ao formato de arquivo padrão `log-bundle-<date>T<time>.tar`, por exemplo `log-bundle-20200629T131312.tar`. Normalmente, o pacote de logs configurável contém logs de todos os nós no ambiente. Em caso de erro, ele conterá o máximo de logs possível. Ele contém pelo menos os logs do nó local.

O pacote de logs inclui o seguinte conteúdo:

- Arquivo de ambiente

O arquivo de ambiente contém a saída de vários comandos de manutenção do Kubernetes. Ele fornece informações sobre o uso atual de recursos por nó e por pod. Ele também contém informações de cluster e a descrição de todas as entidades Kubernetes disponíveis.

- Logs e configuração de host

A configuração de cada host (por exemplo, seu diretório `/etc`) e os logs específicos do host (por exemplo, `journald`) são coletados em um único diretório para cada nó ou host do cluster. O nome do diretório corresponde ao nome do host do nó. O conteúdo interno do diretório corresponde ao sistema de arquivos do host. O número desses diretórios corresponde ao número de nós do cluster.

- Logs de serviços

Logs dos serviços Kubernetes em execução estão disponíveis em `<hostname>/services-logs/<namespace>/<app-name>/<container-name>.log`. Um exemplo de nome de arquivo é `my-host-01/services-logs/prelude/vco-app/vco-server-app.log`.

- *hostname* é o nome do host do nó no qual o contêiner do aplicativo está ou estava em execução. Normalmente, há uma instância para cada nó de cada serviço. Por exemplo, 3 nós = 3 instâncias.
- *namespace* é o namespace Kubernetes no qual o aplicativo está ou foi implantado. Para serviços voltados para o usuário, esse valor é `prelude`.
- *app-name* é o nome do aplicativo Kubernetes que produziu os logs, por exemplo `provisioning-service-app`.
- *container-name* é o nome do contêiner que produziu os logs. Alguns aplicativos consistem em vários contêineres. Por exemplo, `vco-app` inclui os contêineres `vco-server-app` e `vco-controlcenter-app`.
- Logs de pod (legados)
Antes das alterações na arquitetura de registro feitas no vRealize Automation 8.2, os logs de serviços (descritos no marcador anterior) estavam localizados no diretório de cada pod do pacote de logs. Embora você possa continuar a gerar logs de pods no pacote usando a linha de comando `vracli log-bundle --include-legacy-pod-logs`, isso não é aconselhável, pois todas as informações de logs já residem nos logs de cada serviço. Incluir logs de pod pode aumentar desnecessariamente o tempo e o espaço necessários para gerar o pacote de logs.

Como configurar o encaminhamento de logs ao vRealize Log Insight

Você pode encaminhar logs do vRealize Automation para vRealize Log Insight para aproveitar as vantagens de uma análise de log e geração de relatórios mais avançadas.

O vRealize Automation acompanha um agente de registro em [log baseado em fluentd](#). Esse agente coleta e armazena logs para que estes possam ser incluídos em um pacote de logs e examinados posteriormente. Você pode configurar o agente para encaminhar uma cópia dos logs para um servidor vRealize Log Insight usando a REST API do vRealize Log Insight. A API permite que outros programas se comuniquem com o vRealize Log Insight.

Para obter mais informações sobre o vRealize Log Insight, incluindo a documentação da REST API do vRealize Log Insight, consulte [Documentação do vRealize Log Insight](#).

Configure o agente de registro em log para encaminhar continuamente logs do vRealize Automation ao vRealize Log Insight usando o utilitário de linha de comando do `vracli` fornecido.

Todas as linhas de log são marcadas com um nome de host, e a tag de ambiente e pode ser examinada no vRealize Log Insight. Em um ambiente de alta disponibilidade (HA), os logs são marcados com nomes de host diferentes, dependendo do nó em que foram originados. A tag de ambiente é configurável usando a opção `--environment ENV`, conforme descrito abaixo na seção *Configurar ou atualizar a integração do vRealize Log Insight*. Em um ambiente de HA, a tag de ambiente tem o mesmo valor para todas as linhas de log, independentemente do nó em que se originaram.

Informações sobre como usar o utilitário de linha de comando `vrcli` estão disponíveis usando o argumento `--help` na linha de comando `vrcli`. Por exemplo: `vrcli vrli --help`.

Verificar a configuração existente do vRealize Log Insight

Command

```
vrcli vrli
```

Arguments

Não há argumentos de linha de comando.

Output

A configuração atual para a integração do vRealize Log Insight é gerada no formato JSON.

Exit codes

Os seguintes códigos de saída são possíveis:

- 0 - A integração com o vRealize Log Insight está configurada.
- 1 - Ocorreu uma exceção como parte da execução do comando. Examine a mensagem de erro para obter detalhes.
- 61 (ENODATA) -A integração com o vRealize Log Insight não está configurada. Examine a mensagem de erro para obter detalhes.

Example – check integration configuration

```
$ vrcli vrli
No vRLI integration configured

$ vrcli vrli
{
  "agentId": "0",
  "environment": "prod",
  "host": "my-vrli.local",
  "port": 9543,
  "scheme": "https",
  "sslVerify": false
}
```

Configurar ou atualizar a integração do vRealize Log Insight

Command

```
vracli vrli set [options] FQDN_OR_URL
```

Observação Depois de executar o comando, pode levar até 2 minutos para o agente de registro em log aplicar a configuração especificada.

Arguments

■ FQDN_OR_URL

Especifica o FQDN ou endereço IP do servidor vRealize Log Insight a ser usado para publicar logs. A porta 9543 e o https são usados por padrão. Se alguma dessas configurações precisar ser alterada, você poderá usar uma URL em vez disso.

Observação Você pode definir um esquema de host diferente (o padrão é https) e uma porta diferente (o padrão para https é 9543, o padrão para http é 9000) a serem usados para enviar os logs, conforme mostrado nos seguintes exemplos:

```
vracli vrli set some-host
vracli vrli set some-host:9543
vracli vrli set http://some-host:9000
```

As portas 9543 para https e 9000 para http são usadas pela REST API de ingestão do vRealize Log Insight, conforme descrito em *Administrando o vRealize Log Insight*, tópico *Portas e interfaces externas*, na documentação do [vRealize Log Insight](#).

■ Opções

■ --agent-id SOME_ID

Define o ID do agente de registro em log para esse dispositivo. O padrão é 0. Usado para identificar o agente ao publicar logs no vRealize Log Insight usando a REST API vRealize Log Insight.

■ --environment ENV

Define um identificador para o ambiente atual. Ele estará disponível nos logs do vRealize Log Insight como uma tag para entrada de log. O padrão é prod.

■ --ca-file /path/to/server-ca.crt

Especifica um arquivo que contém o certificado da autoridade de certificação (CA) que foi usado para assinar o certificado do servidor vRealize Log Insight. Isso força o agente de registro em log a confiar na CA especificada e permite que ele verifique se o certificado do servidor vRealize Log Insight foi assinado por uma autoridade não confiável. O arquivo pode conter uma cadeia de certificados inteira para verificar o certificado. No caso de um certificado autoassinado, transmita o certificado propriamente dito.

- `--ca-cert CA_CERT`

A definição é idêntica à de `--ca-file`, como acima, mas, em vez disso, transmite o certificado (cadeia) em linha como uma string.

- `--insecure`

Desativa a verificação SSL do certificado do servidor. Isso força o agente de registro em log a aceitar qualquer certificado SSL ao publicar logs.

- Opções avançadas

- `--request-max-size BYTES`

Vários eventos de log são ingeridos com uma única chamada de API. Esse argumento controla o tamanho máximo da carga útil, em bytes, para cada solicitação. Os valores válidos estão entre 4000 e 4000000. O valor padrão é 256000. Para obter informações relacionadas aos valores permitidos, consulte o tópico sobre ingestão de eventos do vRealize Log Insight na documentação da REST API do vRealize Log Insight. Definir esse valor como um nível muito baixo pode fazer com que os eventos de log maiores que o tamanho permitido sejam descartados.

- `--request-timeout SECONDS`

Uma chamada para a API pode travar por vários motivos, incluindo problemas com o aspectos remotos, problemas de rede e assim por diante. Esse parâmetro controla o número de segundos de espera para a conclusão de cada operação, como abrir uma conexão, gravar dados ou aguardar uma resposta, antes que a chamada seja reconhecida como falha. O valor não pode ser inferior a 1 segundo. O padrão é 30.

- `--request-immediate-retries RETRIES`

Os logs são armazenados em blocos agregados antes de serem enviados ao vRealize Log Insight (consulte `--buffer-flush-thread-count` abaixo). Se uma solicitação de API falhar, o log será repetido imediatamente. O número padrão de novas tentativas imediatas é 3. Se nenhuma das novas tentativas for bem-sucedida, o fragmento inteiro de log será revertido e repetido novamente mais tarde.

- `--buffer-flush-thread-count THREADS`

Para melhorar o desempenho e limitar o tráfego de rede, os logs são armazenados em buffer localmente em fragmentos antes de serem liberados e enviados ao servidor de log. Cada fragmento contém logs de um único serviço. Dependendo do seu ambiente, esses fragmentos podem ficar grandes e demorados de liberar. Esse argumento controla o número de fragmentos que podem ser liberados simultaneamente. O padrão é 2.

Observação Ao configurar a integração por https, se o servidor do vRealize Log Insight estiver configurado para usar um certificado não confiável, como um certificado autoassinado ou um certificado que foi assinado por uma autoridade não confiável, você deverá usar uma das opções `--ca-file`, `--ca-cert` ou `--insecure`. Caso contrário, o agente de log falhará ao validar a identidade do servidor e não enviará logs. Ao usar `--ca-file` ou `--ca-cert`, o certificado do servidor do vRealize Log Insight deve ser válido para o nome do host do servidor. Em todos os casos, verifique a integração, permitindo alguns minutos para o processamento e, em seguida, verificando se o vRealize Log Insight recebeu os logs.

Output

Nenhuma saída é esperada.

Exit codes

Os seguintes códigos de saída são possíveis:

- 0 - A configuração foi atualizada.
- 1 - Ocorreu uma exceção como parte da execução. Examine a mensagem de erro para obter detalhes.

Examples – Configure or update integration configuration

```
$ vracli vrli set my-vrli.local

$ vracli vrli set 10.20.30.40

$ vracli vrli set --ca-file /etc/ssl/certs/ca.crt 10.20.30.40

$ vracli vrli set --ca-cert "$(cat /etc/ssl/certs/ca.crt)" 10.20.30.40

$ vracli vrli set --insecure http://my-vrli.local:8080

$ vracli vrli set --agent-id my-vrli-agent my-vrli.local

$ vracli vrli set --environment staging my-vrli.local

$ vracli vrli set --environment staging --request-max-size 10000 --request-timeout 120 --request-immediate-retries 5 --buffer-flush-thread-count 4 my-vrli.local
```

Apagar a integração do vRealize Log Insight

Command


```
vracli vrli unset
```

Observação Depois de executar o comando, pode levar até 2 minutos para o agente de registro em log aplicar a configuração especificada.

Arguments

Não há argumentos de linha de comando.

Output

A confirmação é emitida em formato de texto simples.

Exit codes

Os seguintes códigos de saída estão disponíveis:

- 0 - A configuração foi apagada ou não existia uma configuração.
- 1 - Ocorreu uma exceção como parte da execução. Examine a mensagem de erro para obter detalhes.

Examples – Clear integration

```
$ vracli vrli unset
Clearing vRLI integration configuration

$ vracli vrli unset
No vRLI integration configured
```

Como criar ou atualizar uma integração de syslog no vRealize Automation

Você pode configurar o vRealize Automation para enviar suas informações de log a servidores syslog remotos.

O comando `vracli remote-syslog set` é usado para criar uma integração de syslog ou sobrescrever integrações existentes.

A integração de syslog remota do vRealize Automation oferece suporte aos seguintes tipos de conexão:

- Por UDP.
- Por TCP sem TLS.

Observação Para criar uma integração de syslog sem usar TLS, adicione o sinalizador `--disable-ssl` para o comando `vracli remote-syslog set`.

- Por TCP com TLS.

Para obter informações sobre como configurar a integração de log com o vRealize Log Insight, consulte [Como configurar o encaminhamento de logs ao vRealize Log Insight](#).

Pré-requisitos

Configure um ou mais servidores syslog remotos.

Procedimentos

- 1 Faça login na linha de comando do dispositivo vRealize Automation como **root**.
- 2 Para criar uma integração com um servidor de syslog, execute o comando `vracli remote-syslog set`.

```
vracli remote-syslog set -id name_of_integration protocol_type://syslog_URL_or_FQDN:syslog_port
```

Observação Se você não inserir uma porta no comando `vracli remote-syslog set`, o valor padrão da porta será 514.

Observação É possível adicionar um certificado à configuração de syslog. Para adicionar um arquivo de certificado, use o sinalizador `--ca-file`. Para adicionar um certificado como texto simples, use o sinalizador `--ca-cert`.

- 3 (Opcional) Para substituir uma integração de syslog existente, execute o `vracli remote-syslog set` e defina o sinalizador `-id` como o valor para o nome da integração que você deseja sobrescrever.

Observação Por padrão, o dispositivo vRealize Automation solicita que você confirme que deseja sobrescrever a integração de syslog. Para pular a solicitação de confirmação, adicione o sinalizador `-f` ou `--force` ao comando `vracli remote-syslog set`.

Próximo passo

Para revisar as integrações de syslog atuais no dispositivo, execute o comando `vracli remote-syslog`.

Como excluir uma integração de syslog para registro em log no vRealize Automation

Você pode excluir integrações de syslog do seu dispositivo vRealize Automation executando o comando `vracli remote-syslog unset`.

Pré-requisitos

Crie uma ou mais integrações de syslog no dispositivo vRealize Automation. Consulte [Como criar ou atualizar uma integração de syslog no vRealize Automation](#).

Procedimentos

- 1 Faça login na linha de comando do dispositivo vRealize Automation como **root**.

2 Exclua integrações de syslog do dispositivo vRealize Automation usando um dos seguintes métodos:

- Para excluir uma integração de syslog específica, execute o comando `vraccli remote-syslog unset -id nome_integração`.
- Para excluir todas as integrações de syslog no dispositivo vRealize Automation, execute o comando `vraccli remote-syslog unset` sem o sinalizador `-id`.

Observação Por padrão, o dispositivo vRealize Automation solicita que você confirme que deseja excluir todas as integrações de syslog. Para pular a solicitação de confirmação, adicione o sinalizador `-f` ou `--force` ao comando `vraccli remote-syslog unset`.

Participando do Programa de Aperfeiçoamento da Experiência do Cliente do vRealize Automation

6

Este produto participa do Programa de Aperfeiçoamento da Experiência do Cliente (CEIP) da VMware. O CEIP oferece informações à VMware que a permitem melhorar seus produtos e serviços, corrigir problemas e lhe recomendar como implantar e utilizar nossos produtos da melhor forma.

Detalhes sobre os dados coletados pelo CEIP e as finalidades para as quais eles são usados pela VMware são apresentados na Central de Confiança e Garantia, em <http://www.vmware.com/trustvmware/ceip.html>.

Este capítulo inclui os seguintes tópicos:

- [Como entrar ou sair no/do Programa de Aperfeiçoamento da Experiência do Cliente do vRealize Automation](#)
- [Como configurar o tempo de coleta de dados para o Programa de Aperfeiçoamento da Experiência do Cliente do vRealize Automation](#)

Como entrar ou sair no/do Programa de Aperfeiçoamento da Experiência do Cliente do vRealize Automation

Para entrar ou sair no/do Programa de Aperfeiçoamento da Experiência do Cliente (CEIP), use a linha de comando do dispositivo vRealize Automation.

Você pode entrar no programa CEIP ao instalar o vRealize Automation e com o vRealize Lifecycle Manager (LCM). Também pode entrar ou sair no/do programa usando as opções de linha de comando após a instalação.

Para entrar no Programa de Aperfeiçoamento da Experiência do Cliente usando as opções da linha de comando:

- 1 Faça login no linha de comando do dispositivo vRealize Automation como **root**.
- 2 Execute o comando `vracli ceip on`.
- 3 Revise as informações do Programa de Aperfeiçoamento da Experiência do Cliente e execute o comando `vracli ceip on --acknowledge-ceip`.

- 4 Para reiniciar os serviços do vRealize Automation, execute o comando `/opt/scripts/deploy.sh`.

Para sair do Programa de Aperfeiçoamento da Experiência do Cliente usando opções da linha de comando:

- 1 Faça login no linha de comando do dispositivo vRealize Automation como **root**.
- 2 Execute o comando `vracli ceip off`.
- 3 Para reiniciar os serviços do vRealize Automation, execute o comando `/opt/scripts/deploy.sh`.

Como configurar o tempo de coleta de dados para o Programa de Aperfeiçoamento da Experiência do Cliente do vRealize Automation

Você pode definir o dia e a hora em que o Programa de Aperfeiçoamento da Experiência do Cliente (CEIP) envia dados para a VMware.

Procedimentos

- 1 Faça login no linha de comando do dispositivo vRealize Automation como **root**.
- 2 Abra o seguinte arquivo em um editor de texto.
`/etc/telemetry/telemetry-collector-vami.properties`
- 3 Edite as propriedades para o dia da semana (dow) e a hora do dia (hod).

Propriedade	Descrição
<code>frequency.dow=<day-of-week></code>	Dia em que ocorre a coleta de dados.
<code>frequency.hod=<hour-of-day></code>	Hora local do dia em que ocorre a coleta de dados. Os valores possíveis são 0–23.

- 4 Salve e feche `telemetry-collector-vami.properties`.
- 5 Aplique as configurações inserindo o seguinte comando.

```
vcac-config telemetry-config-update --update-info
```

As alterações são aplicadas a todos os nós na sua implantação.