

Instalar e configurar VMware vRealize Orchestrator

12 AGOSTO 2021

vRealize Orchestrator 8.5

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 © 2008-2021 VMware, Inc. Todos os direitos reservados. [Informações sobre direitos autorais e marca registrada.](#)

Conteúdo

Instalando e configurando o VMware vRealize Orchestrator 6

1 Introdução ao VMware vRealize Orchestrator 7

Principais recursos da plataforma do Orchestrator 7

Funções de usuário do vRealize Orchestrator 10

Arquitetura do vRealize Orchestrator 11

Plug-ins do vRealize Orchestrator 12

2 Requisitos do sistema vRealize Orchestrator 13

Componentes padrão do dispositivo 13

Requisitos de hardware 14

Máximos de dimensionamento 14

Requisitos de rede 15

Portas e endpoints 15

Suporte a navegador 15

Suporte para internacionalização 16

3 Configurar componentes do vRealize Orchestrator 17

Configuração do vCenter Server 17

Métodos de autenticação 18

4 Instalar o vRealize Orchestrator 19

Baixar e implantar o vRealize Orchestrator Appliance 19

Ligar o vRealize Orchestrator Appliance e abrir a página inicial 21

Ativar ou desativar acesso SSH ao vRealize Orchestrator Appliance 22

5 Configuração inicial 23

Configurando um servidor vRealize Orchestrator autônomo 23

Configurar um servidor vRealize Orchestrator autônomo com autenticação do vRealize Automation 23

Configurar um servidor vRealize Orchestrator autônomo com autenticação do vSphere 25

Capacitação de Recursos do vRealize Orchestrator com Licenças 27

Conexão do banco de dados do vRealize Orchestrator 28

Gerenciar certificados 28

Gerenciar certificados do vRealize Orchestrator 28

Gerar um certificado TLS personalizado para o vRealize Orchestrator 29

Definir um certificado TLS personalizado para vRealize Orchestrator 30

Importar um certificado confiável com o Centro de Controle 32

Configuração dos plug-ins do vRealize Orchestrator	33
Gerenciar plug-ins do vRealize Orchestrator	33
Instalar ou atualizar plug-in do vRealize Orchestrator	33
Excluir um plug-in	34
Alta disponibilidade do vRealize Orchestrator	34
Máximos de dimensionamento	35
Configurar um cluster do vRealize Orchestrator	36
Removendo um nó de cluster do vRealize Orchestrator	37
Dimensionar horizontalmente uma implantação autônoma do vRealize Orchestrator	38
Monitorar um cluster do vRealize Orchestrator	39
Configurando o programa de aperfeiçoamento da experiência do cliente	40
Categorias de informações recebidas pela VMware	40
Participar ou sair do Programa de Aperfeiçoamento da Experiência do Cliente	40
6 Usando os serviços de API do vRealize Orchestrator	42
Gerenciando Certificados SSL por meio da REST API	42
Excluir um certificado TLS usando a REST API	43
Importar certificados TLS usando a REST API	43
Criar um Armazenamento de Chaves usando a REST API	45
Excluir um Armazenamento de Chaves usando a REST API	45
Adicionar uma chave usando a REST API	46
7 Opções adicionais de configuração	47
Reconfigurar a autenticação	47
Mudar o provedor de autenticação	47
Alterar os parâmetros de autenticação	48
Configurando as propriedades de execução do fluxo de trabalho	48
Arquivos de log do vRealize Orchestrator	49
Log de persistência	49
Configuração de logs do vRealize Orchestrator	50
Configurar a integração de log com o vRealize Log Insight	51
Criar ou substituir uma integração de syslog no vRealize Orchestrator	51
Excluir uma integração de syslog no vRealize Orchestrator	52
Ativar logs de depuração do Kerberos	53
Habilitar as extensões do Opentracing e do Wavefront	54
Configurar a extensão do Opentracing	55
Configurar a extensão do Wavefront	55
Habilitar a sincronização de horário para o vRealize Orchestrator	57
Desativar a sincronização de hora para o vRealize Orchestrator	58
Configurar o vRealize Orchestrator Kubernetes CIDR	58
Atualizar as configurações de DNS do vRealize Orchestrator	60

8 Casos de uso de configuração e solução de problemas 61

- Verifique o número da compilação do servidor do vRealize Orchestrator 61
- Configurar o plug-in do vRealize Orchestrator para o vSphere Web Client 62
- Cancelar fluxos de trabalho em execução 63
- Ativar a depuração do servidor do vRealize Orchestrator 63
- Redimensionar os discos do vRealize Orchestrator Appliance 65
- Como dimensionar o tamanho de memória do heap do servidor do vRealize Orchestrator 66
- Recuperação de desastres do vRealize Orchestrator usando o Site Recovery Manager 67
 - Configurar máquinas virtuais para o vSphere Replication 68
 - Criar grupos de proteção 68
 - Criar um plano de recuperação 71
 - Organizar planos de recuperação em pastas 72
 - Editar um plano de recuperação 72

9 Configurar propriedades do sistema 74

- Configurar acesso ao sistema de arquivos do servidor para fluxos de trabalho e ações 74
 - Regras no arquivo js-lo-rights.conf que autorizam acesso de gravação ao sistema vRealize Orchestrator 74
 - Definir acesso do sistema de arquivos do servidor para fluxos de trabalho e ações 75
- Definir acesso a comandos do sistema operacional para fluxos de trabalho e ações 76
- Definir acesso de JavaScript a classes Java 77
- Definir propriedade de tempo limite personalizada 78
- Adicionando um conector JDBC para o plug-in SQL do vRealize Orchestrator. 79

10 Aonde ir a partir daqui 81

Instalando e configurando o VMware vRealize Orchestrator

Instalar e configurar o VMware vRealize Orchestrator fornece informações e instruções sobre como instalar e configurar o VMware[®] vRealize Orchestrator.

Público-alvo

Essas informações foram concebidas para administradores avançados do vSphere e administradores de sistema experientes que estão familiarizados com a tecnologia de máquinas virtuais e com as operações de centro de dados.

Introdução ao VMware vRealize Orchestrator

1

O VMware vRealize Orchestrator é uma plataforma de desenvolvimento e automação de processos que fornece uma biblioteca de fluxos de trabalho extensíveis para permitir que você crie e execute processos automatizados e configuráveis para gerenciar produtos VMware, bem como outras tecnologias de terceiros.

O vRealize Orchestrator automatiza as tarefas operacionais e de gerenciamento de aplicativos da VMware e de terceiros, como os departamentos de manutenção, sistemas de gerenciamento de mudanças e sistemas de gerenciamento de ativos de TI.

Este capítulo inclui os seguintes tópicos:

- [Principais recursos da plataforma do Orchestrator](#)
- [Funções de usuário do vRealize Orchestrator](#)
- [Arquitetura do vRealize Orchestrator](#)
- [Plug-ins do vRealize Orchestrator](#)

Principais recursos da plataforma do Orchestrator

O vRealize Orchestrator é composto por três camadas distintas: uma plataforma de orquestração que fornece os recursos comuns necessários para uma ferramenta de orquestração, uma arquitetura de plug-in para integrar o controle de subsistemas e uma biblioteca de fluxos de trabalho. O vRealize Orchestrator é uma plataforma aberta que pode ser estendida com novos plug-ins e conteúdo, podendo ser integrada a arquiteturas maiores por meio de uma REST API.

O vRealize Orchestrator inclui vários recursos importantes que ajudam na execução e no gerenciamento de fluxos de trabalho.

Persistência

Usa-se um banco de dados PostgreSQL de nível de produção para armazenar informações relevantes, como processos, estados de fluxo de trabalho e a configuração do vRealize Orchestrator.

Gerenciamento central

O vRealize Orchestrator fornece uma ferramenta central para gerenciar seus processos. A plataforma baseada em servidor de aplicativo, com o histórico de versão completa, pode armazenar scripts e primitivos relacionados ao processo no mesmo local de armazenamento. Dessa forma, você pode evitar scripts sem controle de versão e alteração adequada nos seus servidores.

Ponto de verificação

Cada etapa de um fluxo de trabalho é salva no banco de dados, o que impedirá a perda de dados se você precisar reiniciar o servidor. Esse recurso é especialmente útil para processos de longa execução.

Centro de Controle

O Centro de Controle é um portal baseado na Web que aumenta a eficiência administrativa das instâncias do vRealize Orchestrator, fornecendo uma interface administrativa centralizada para operações de tempo de execução, monitoramento de fluxo de trabalho e correlação entre as execuções de fluxo de trabalho e os recursos do sistema.

Versão

Todos os objetos da plataforma do vRealize Orchestrator têm um histórico de versão associado. O histórico de versões é útil para o gerenciamento de alterações básico durante a distribuição de processos para estágios ou localizações do projeto.

Integração com o Git

Com o vRealize Orchestrator Client, você pode integrar um repositório Git para melhorar ainda mais a versão e o controle de origem do conteúdo do seu vRealize Orchestrator. Com o Git, você pode gerenciar o desenvolvimento de fluxos de trabalho em várias instâncias do vRealize Orchestrator. Consulte *Usar o Git com o Cliente vRealize Orchestrator* no guia *Usar o Cliente VMware vRealize Orchestrator*.

Mecanismo de script

O mecanismo de JavaScript Mozilla Rhino fornece uma maneira de criar blocos de construção para a plataforma vRealize Orchestrator Client. O mecanismo de script é aprimorado com controle de versão básica, verificação de tipo de variável, gerenciamento de espaço de nome e tratamento de exceções. O mecanismo pode ser usado nos seguintes blocos de construção:

- Ações
- Fluxos de trabalho
- Políticas

Mecanismo de fluxo de trabalho

O mecanismo de fluxo de trabalho permite automatizar os processos de negócios. Ele usa os seguintes objetos para criar uma automação de processo passo a passo em fluxos de trabalho:

- Fluxos de trabalho e ações fornecidas pelo vRealize Orchestrator Client.
- Blocos de construção personalizados criados pelo cliente.
- Os objetos que os plug-ins adicionam ao vRealize Orchestrator Client.

Os usuários, os outros fluxos de trabalho, as agendas ou as políticas podem iniciar fluxos de trabalho.

Mecanismo de política

Você pode usar o mecanismo de política para monitorar e gerar eventos para reagir às condições variáveis no servidor do vRealize Orchestrator Client ou em uma tecnologia com plug-in. As políticas podem agregar eventos da plataforma ou dos plug-ins, o que ajuda você a lidar com condições variáveis em qualquer uma das tecnologias integradas.

vRealize Orchestrator Client

Crie, execute, edite e monitore fluxos de trabalho com o vRealize Orchestrator Client. Você também pode usar o vRealize Orchestrator Client para gerenciar elementos de ação, configuração, política e recursos. Consulte *Usar o Cliente vRealize Orchestrator*.

Desenvolvimento e recursos

A página inicial do vRealize Orchestrator fornece acesso rápido aos recursos para ajudá-lo a desenvolver seus próprios plug-ins, para uso no vRealize Orchestrator. Você também encontrará informações sobre como usar a REST API do vRealize Orchestrator para enviar solicitações ao servidor do vRealize Orchestrator.

Segurança

O vRealize Orchestrator fornece as seguintes funções avançadas de segurança:

- Infraestrutura de chave pública (PKI) para assinar e criptografar conteúdo importado e exportado entre servidores.
- Gerenciamento de direitos digitais (DRM) para controlar como o conteúdo exportado pode ser visualizado, editado e redistribuído.
- Segurança de camada de transporte (TLS) para fornecer comunicação criptografada entre o vRealize Orchestrator Client, o servidor do vRealize Orchestrator e o acesso HTTPS ao front-end da Web.
- Gerenciamento de direitos de acesso avançado para fornecer controle sobre o acesso a processos e os objetos manipulados por esses processos.

Criptografia

O vRealize Orchestrator usa um padrão de criptografia avançada (AES) compatível com FIPS com uma chave de codificação de 256 bits para a criptografia de cadeias de caracteres.

A chave de codificação é gerada aleatoriamente e é exclusiva entre os dispositivos que não fazem parte de um cluster. Todos os nós em um cluster compartilham uma chave de codificação.

Funções de usuário do vRealize Orchestrator

O vRealize Orchestrator fornece ferramentas e interfaces diferentes com base nas responsabilidades específicas das funções de usuário global. No vRealize Orchestrator, você pode ter usuários com direitos completos, que fazem parte do grupo de administradores (**administradores**), desenvolvedores (**designers de fluxo de trabalho**), usuários de solução de problemas (**visualizadores**) e usuários com acesso limitado.

As funções de usuário do vRealize Orchestrator são gerenciadas no menu **Gerenciamento de funções** do vRealize Orchestrator Client. Para obter mais informações sobre como configurar as funções de usuário no vRealize Orchestrator Client, consulte *Atribuir funções no Cliente vRealize Orchestrator* no guia *Usar o Cliente VMware vRealize Orchestrator*.

Observação Para implantações do vRealize Orchestrator autenticadas com o vRealize Automation, ou usando uma licença do vRealize Automation, as funções de usuário são atribuídas com o serviço de gerenciamento de identidade e acesso da plataforma do vRealize Automation. Consulte *Configurar funções do Cliente vRealize Orchestrator no vRealize Automation* ao *Usar o Cliente VMware vRealize Orchestrator*.

Função de usuário	Descrição
Administrador	<p>Este usuário tem acesso completo a todos os recursos e conteúdo da plataforma do vRealize Orchestrator, incluindo o conteúdo criado por grupos específicos. As responsabilidades de usuário de administrador principal incluem:</p> <ul style="list-style-type: none"> ■ Instalação e configuração do vRealize Orchestrator. ■ Adicionar usuários ao vRealize Orchestrator Client, atribuir funções e criar e excluir grupos. Consulte <i>Criar grupos no Cliente vRealize Orchestrator</i> ao <i>Usar o Cliente VMware vRealize Orchestrator</i>. ■ Criando uma integração com um repositório Git para os desenvolvedores em seu ambiente do vRealize Orchestrator. Consulte <i>Configurar uma conexão com um repositório Git</i> ao <i>Usar o Cliente VMware vRealize Orchestrator</i>. ■ Solução de problemas do ambiente do vRealize Orchestrator por meio de recursos como validação e depuração de scripts do fluxo de trabalho.
Espectador	<p>Este usuário tem acesso somente leitura a todos os vRealize Orchestrator Client, incluindo todos os grupos e o conteúdo dos grupos. Este usuário pode visualizar, mas não pode criar, editar ou executar conteúdo ou exportar execuções de fluxo de trabalho, logs de execução de fluxo de trabalho ou pacotes. Os visualizadores não são limitados por permissões de grupo.</p> <p>Observação A função de visualizador só tem suporte para instâncias do vRealize Orchestrator autenticadas com o vRealize Automation. Essa função não é mapeada para uma função do vRealize Automation por padrão, portanto ela deve ser atribuída explicitamente aos usuários.</p>

Função de usuário	Descrição
Designer de fluxo de trabalho	<p>Esse usuário pode estender a funcionalidade da plataforma vRealize Orchestrator ao criar e editar objetos. Os designers de fluxo de trabalho não têm acesso aos recursos administrativos e de solução de problemas do vRealize Orchestrator Client. As principais responsabilidades do designer de fluxo de trabalho incluem:</p> <ul style="list-style-type: none"> ■ Criar, editar, executar e excluir objetos do vRealize Orchestrator, como fluxos de trabalho, ações, políticas e elementos de configuração. ■ O fluxo de trabalho de agendamento é executado. Consulte <i>Agendar fluxos de trabalho no Cliente vRealize Orchestrator</i> ao <i>Usar Cliente VMware vRealize Orchestrator</i>. ■ Adicionando conteúdo criado pelo desenvolvedor de fluxo de trabalho aos grupos aos quais eles são atribuídos. ■ Enviar alterações locais para o inventário de conteúdo do vRealize Orchestrator para o repositório Git de conexão. Consulte <i>Enviar alterações para um repositório Git</i> ao <i>Usar Cliente VMware vRealize Orchestrator</i>.
Usuários com direitos limitados	Os usuários sem função atribuída ainda podem fazer login no vRealize Orchestrator Client, mas ter acesso limitado aos recursos e conteúdo do cliente. Se eles forem atribuídos a um grupo, este usuário poderá exibir e executar o conteúdo incluído nesse grupo.

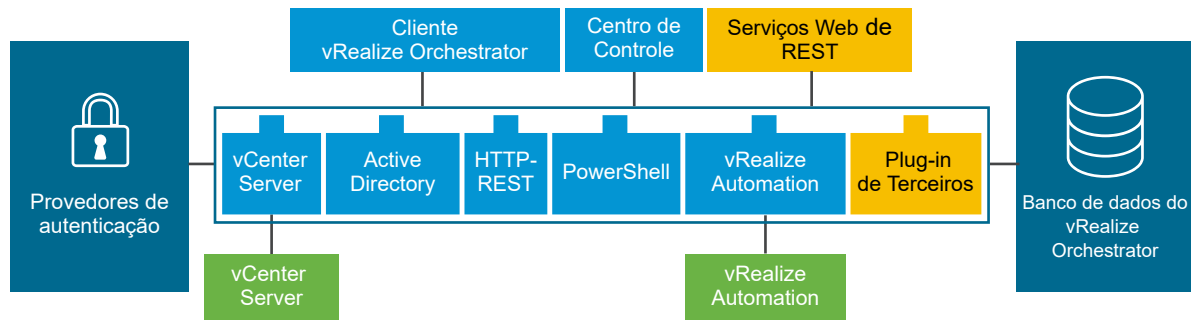
Arquitetura do vRealize Orchestrator

O vRealize Orchestrator contém uma biblioteca de fluxos de trabalho e um mecanismo de fluxo de trabalho para permitir que você crie e execute fluxos de trabalho que automatizam os processos de orquestração. Você poderá executar fluxos de trabalho nos objetos de tecnologias diferentes que o vRealize Orchestrator acessa por meio de uma série de plug-ins.

O vRealize Orchestrator fornece um conjunto padrão de plug-ins, incluindo um plug-ins para o vCenter Server e o vRealize Automation, para permitir que você orquestre tarefas nos ambientes diferentes que os plug-ins expõem.

O vRealize Orchestrator também apresenta uma arquitetura aberta para conectar aplicativos externos de terceiros à plataforma de orquestração. Você pode executar fluxos de trabalho nos objetos das tecnologias conectadas que você mesmo define. O vRealize Orchestrator se conecta a um provedor de autenticação para gerenciar contas de usuário e a um banco de dados PostgreSQL pré-configurado para armazenar informações dos fluxos de trabalho que ele executa. Você pode acessar o vRealize Orchestrator, os objetos que ele expõe e os fluxos de trabalho do vRealize Orchestrator por meio da interface do cliente do vRealize Orchestrator Client ou por meio de serviços da Web. O monitoramento e a configuração de fluxos de trabalho e serviços do vRealize Orchestrator são feitos por meio do vRealize Orchestrator Client e do Centro de Controle.

Figura 1-1. Arquitetura do VMware vRealize Orchestrator



Plug-ins do vRealize Orchestrator

Os plug-ins lhe permitem usar o vRealize Orchestrator para acessar e controlar tecnologias e aplicativos externos. Ao expor uma tecnologia externa em um plug-in do vRealize Orchestrator, você pode incorporar objetos e funções em fluxos de trabalho que acessam os objetos e as funções dessa tecnologia externa.

As tecnologias externas que você pode acessar usando plug-ins incluem ferramentas de gerenciamento de virtualização, sistemas de e-mail, bancos de dados, serviços de diretório e interfaces de controle remoto.

O vRealize Orchestrator fornece um conjunto de plug-ins padrão que você pode usar para incorporar em fluxos de trabalho essas tecnologias como a API e os recursos de e-mail do VMware vCenter Server. Ao usar os plug-ins, você pode automatizar a entrega de novos serviços de TI ou adaptar os recursos de infraestrutura e serviços de aplicativos existentes. Além disso, você pode usar a arquitetura aberta de plug-ins do vRealize Orchestrator para desenvolver plug-ins de acesso a outros aplicativos.

Os plug-ins do vRealize Orchestrator que a VMware desenvolve são distribuídos como arquivos `.vmoapp`.

Para obter mais informações sobre os plug-ins do vRealize Orchestrator, consulte [Usar plug-ins do VMware vRealize Orchestrator](#).

Para obter mais informações sobre plug-ins do vRealize Orchestrator de terceiros, consulte [VMware Marketplace](#).

Requisitos do sistema vRealize Orchestrator

2

Seu sistema deve atender aos requisitos técnicos necessários para que o vRealize Orchestrator funcione corretamente.

Para obter uma lista das versões compatíveis do vCenter Server, do vSphere Web Client, do vRealize Automation e de outras soluções da VMware, consulte [Matriz de interoperabilidade de produto do VMware](#).

Este capítulo inclui os seguintes tópicos:

- [Componentes do vRealize Orchestrator Appliance](#)
- [Requisitos de hardware para o vRealize Orchestrator Appliance](#)
- [Máximos de dimensionamento do vRealize Orchestrator](#)
- [Requisitos de rede para o vRealize Orchestrator](#)
- [Portas e endpoints do vRealize Orchestrator](#)
- [Navegadores compatíveis com o vRealize Orchestrator](#)
- [Nível de suporte de internacionalização e localização](#)

Componentes do vRealize Orchestrator Appliance

O vRealize Orchestrator Appliance é um dispositivo virtual baseado em Photon em execução nos contêineres.

O vRealize Orchestrator Appliance inclui os seguintes componentes:

- Uma camada Kubernetes ao nível da infraestrutura.
- Um banco de dados PostgreSQL pré-configurado.
- Os principais serviços do vRealize Orchestrator: o serviço do servidor, o serviço do Centro de Controle e o serviço da UI de orquestração.

A configuração padrão do banco de dados do vRealize Orchestrator Appliance está pronta para produção.

Observação Para usar o vRealize Orchestrator Appliance em um ambiente de produção, você deve configurar o servidor do vRealize Orchestrator para fazer a autenticação pelo vRealize Automation ou pelo vSphere. Consulte [Configurando um servidor vRealize Orchestrator autônomo](#).

Requisitos de hardware para o vRealize Orchestrator Appliance

O vRealize Orchestrator Appliance é uma máquina virtual pré-configurada baseada em Photon que é executada em contêineres. Antes de implantar o dispositivo, verifique se o seu sistema atende aos requisitos mínimos de hardware.

O vRealize Orchestrator Appliance tem os seguintes requisitos de hardware:

- 4 CPUs
- 12 GB de memória
- 200 GB de disco rígido

Não reduza o tamanho de memória padrão porque o servidor do vRealize Orchestrator requer pelo menos 8 GB de memória livre.

Máximos de dimensionamento do vRealize Orchestrator

A tabela de limites de dimensionamento descreve os máximos recomendados em implantações do vRealize Orchestrator 8.x.

Componente	Dimensionar destinos	Mais informações
Máquinas virtuais	35.000	
Conexões do vCenter Server	10	Consulte Configuração do vCenter Server
Nós ativos em um cluster	3	Consulte Configurar um cluster do vRealize Orchestrator
Fluxos de trabalho em execução simultaneamente	300 por nó	Consulte Configurando as propriedades de execução do fluxo de trabalho
Fluxos de trabalho em execução na fila	10.000 por nó	
Execuções de fluxo de trabalho preservadas	100 por nó	
Dias de expiração de evento do log	15	

Requisitos de rede para o vRealize Orchestrator

Cada nó do vRealize Orchestrator requer uma configuração de rede.

Os requisitos de rede para o vRealize Orchestrator são:

- Endereço de rede e IPv4 estáticos únicos
- Servidor DNS acessível definido manualmente
- Nome de domínio totalmente qualificado (FQDN) válido definido manualmente que pode ser resolvido de forma direta e inversa por meio do servidor DNS

Observação Não há suporte para a alteração do endereço IP ou a alteração do nome do host após a instalação e isso resulta em uma configuração interrompida que não é recuperável.

Portas e endpoints do vRealize Orchestrator

O serviço Kubernetes do vRealize Orchestrator inclui dois endpoints e várias portas de rede principais.

Portas de rede do vRealize Orchestrator

Você pode acessar o vRealize Orchestrator pela porta 443. A porta 443 é protegida com um certificado autoassinado gerado durante a instalação e não pode ser substituída pelo usuário. Ao usar um balanceador de carga externo, ele deve ser configurado para balancear na porta 443.

Para visualizar todas as portas do vRealize Orchestrator, consulte a ferramenta [Portas e Protocolos](#).

Endpoints do vRealize Orchestrator

Você pode acessar os serviços do Centro de Controle e do Cliente vRealize Orchestrator nos seguintes endpoints:

Serviço	Endpoint
Cliente vRealize Orchestrator	<code>https://your_orchestrator_FQDN/orchestration-ui</code>
Centro de Controle	<code>https://your_orchestrator_FQDN/vco-controlcenter</code>

Navegadores compatíveis com o vRealize Orchestrator

Confirme se os navegadores suportam o vRealize Orchestrator.

Para acessar o vRealize Orchestrator Client e o Centro de Controle, você deve usar um dos seguintes navegadores:

- Microsoft Edge

- Mozilla Firefox
- Google Chrome

Nível de suporte de internacionalização e localização

O Centro de Controle do vRealize Orchestrator e o vRealize Orchestrator Client incluem suporte para sistemas operacionais que não estejam em inglês, formatação de dados que não estejam em inglês e suporte a vários idiomas para o centro de controle e a interface de usuário do cliente.

O Centro de Controle do vRealize Orchestrator e o vRealize Orchestrator Client oferecem suporte ao uso de sistemas operacionais que não estejam em inglês, entrada e saída não em inglês e suporte para a formatação de dados que não estão em inglês, como datas, horas e números.

As interfaces de usuário do vRealize Orchestrator e o vRealize Orchestrator Client estão traduzidas para os seguintes idiomas:

- Espanhol
- Francês
- Alemão
- Chinês tradicional
- Chinês simplificado
- Coreano
- Japonês
- Italiano
- Holandês
- Português (Brasil)
- Russo

Configurar componentes do vRealize Orchestrator

3

Quando você baixa e implanta o vRealize Orchestrator Appliance, o servidor do vRealize Orchestrator é pré-configurado. Após a implantação, os serviços são iniciados automaticamente.

Para melhorar a disponibilidade e o dimensionamento da configuração do seu vRealize Orchestrator, siga estas diretrizes:

- Instale e configure um provedor de autenticação e configure o vRealize Orchestrator para trabalhar com o provedor. Consulte o [Configurando um servidor vRealize Orchestrator autônomo](#).
- Para ambientes agrupados em cluster do vRealize Orchestrator, instale e configure um servidor de balanceamento de carga e configure-o para distribuir a carga de trabalho entre os servidores do vRealize Orchestrator.

Este capítulo inclui os seguintes tópicos:

- [Configuração do vCenter Server](#)
- [Métodos de autenticação](#)

Configuração do vCenter Server

Aumentar o número de instâncias do vCenter Server na instalação do seu vRealize Orchestrator faz com que o vRealize Orchestrator gerencie mais sessões. Muitas sessões ativas podem fazer com que o vRealize Orchestrator experimente tempos limites quando ocorrerem mais de 10 conexões do vCenter Server.

Para obter uma lista das versões compatíveis do vCenter Server, consulte a [Matriz de interoperabilidade de produto do VMware](#).

Observação Se a sua rede tiver largura de banda e latência suficientes, você poderá executar várias instâncias do vCenter Server em diferentes máquinas virtuais na configuração do vRealize Orchestrator. Se você estiver usando a LAN para melhorar a comunicação entre o vRealize Orchestrator e o vCenter Server, uma linha de 100 MB será obrigatória.

Métodos de autenticação

Para autenticar e gerenciar permissões de usuário, o vRealize Orchestrator requer uma conexão com o vRealize Automation ou com uma instância do servidor vSphere.

Ao baixar e implantar o vRealize Orchestrator Appliance, você deve configurar o servidor com uma autenticação do vRealize Automation ou vSphere. Consulte o [Configurando um servidor vRealize Orchestrator autônomo](#).

Observação A autenticação do vRealize Orchestrator 8.x com o vRealize Automation só tem suporte com o vRealize Automation 8.x.

Instalar o vRealize Orchestrator

4

O vRealize Orchestrator consiste em um componente de servidor e um componente de cliente.

Para usar o vRealize Orchestrator, você deve implantar o vRealize Orchestrator Appliance e configurar o servidor do vRealize Orchestrator.

Você pode alterar as definições de configuração padrão do vRealize Orchestrator usando o Centro de Controle do vRealize Orchestrator.

Este capítulo inclui os seguintes tópicos:

- [Baixar e implantar o vRealize Orchestrator Appliance](#)

Baixar e implantar o vRealize Orchestrator Appliance

Antes de poder acessar o conteúdo e os serviços do vRealize Orchestrator, você deve baixar e implantar o vRealize Orchestrator Appliance.

Pré-requisitos

- Verifique se você tem uma instância do vCenter Server em execução. A versão do vCenter Server deve ser 6.0 ou posterior.
- Verifique se o host no qual você está implantando o vRealize Orchestrator Appliance atende aos requisitos mínimos de hardware. Consulte o [Requisitos de hardware para o vRealize Orchestrator Appliance](#).
- Se o sistema estiver isolado e sem acesso à Internet, você deverá baixar o arquivo .ova para o dispositivo no site da VMware.

Procedimentos

- 1 Efetue login no vSphere Web Client como um **administrador**.
- 2 Selecione um objeto do inventário que seja um objeto principal válido de uma máquina virtual, como um centro de dados, pasta, cluster, pool de recursos ou host.
- 3 Selecione **Ações > Implantar Modelo OVF**.
- 4 Insira o caminho do arquivo ou a URL para o arquivo .ova e clique em **Avançar**.

- 5 Insira um nome e uma localização para o vRealize Orchestrator Appliance e clique em **Avançar**.
- 6 Selecione um host, cluster, pool de recursos ou vApp como um destino no qual você deseja que o dispositivo seja executado e clique em **Avançar**.
- 7 Analise os detalhes da implantação e clique em **Avançar**.
- 8 Aceite os termos do contrato de licença e clique em **Avançar**.
- 9 Selecione o formato de armazenamento que você deseja usar para o vRealize Orchestrator Appliance.

Formato	Descrição
Thick Provisioned Lazy Zeroed	Cria um disco virtual em um formato completo padrão. O espaço necessário para o disco virtual é alocado quando o disco virtual é criado. Se qualquer dado permanecer no dispositivo físico, ele não será apagado durante a criação, mas será zerado sob demanda mais tarde na primeira gravação da máquina virtual.
Thick Provisioned Eager Zeroed	Oferece suporte a recursos de cluster, como Tolerância a Falhas. O espaço necessário para o disco virtual é alocado quando o disco virtual é criado. Se qualquer dado permanecer no dispositivo físico, ele será zerado quando o disco virtual for criado. Pode demorar muito mais tempo para criar discos nesse formato do que para criar discos em outros formatos.
Thin Provisioned Format	Economiza espaço no disco rígido. Para o disco dinâmico, você provisiona o máximo de espaço de repositório de dados que o disco exige com base no valor selecionado para o tamanho do disco. O disco fino começa pequeno e, a princípio, usa apenas o espaço de repositório de dados que o disco precisa para suas operações iniciais.

- 10 Clique em **Avançar**.
- 11 Defina as configurações de rede e insira a senha **raiz**.

Ao definir as configurações de rede do vRealize Orchestrator Appliance, você deve usar o protocolo IPv4. Para as configurações de rede DHCP e Estática, você deve adicionar um nome de domínio totalmente qualificado (FQDN) para o seu vRealize Orchestrator Appliance.

Se o nome do host exibido no shell do vRealize Orchestrator Appliance implantado for *photon-machine*, os requisitos de configuração de rede anteriores não serão atendidos.

- 12 (Opcional) Defina as configurações de rede adicionais para o vRealize Orchestrator Appliance, como ativar o acesso SSH.

Observação Ao configurar uma rede do Kubernetes, os valores do CIDR do cluster interno e do CIDR de serviço interno devem permitir pelo menos 1024 hosts. Devido a esse requisito, o valor da máscara de rede deve ser 22 ou menos. Os valores de máscara de rede superiores a 22 são inválidos. As propriedades de rede do Kubernetes têm os seguintes valores padrão:

Kubernetes network property	Default value	Property description
CIDR do cluster interno do Kubernetes	10.244.0.0/22	O CIDR usado para pods em execução no cluster do Kubernetes.
CIDR do serviço interno do Kubernetes	10.244.4.0/22	O CIDR usado para serviços do Kubernetes no cluster do Kubernetes.

Observação Você também pode alterar as propriedades de rede do CIDR do Kubernetes após a implantação. Consulte o [Configurar o vRealize Orchestrator Kubernetes CIDR](#).

- (Opcional) Para ativar o modo FIPS para o vRealize Orchestrator Appliance, defina o **Modo FIPS** como **strict**.

Observação A adoção do FIPS 140-2 tem suporte apenas para novos ambientes do vRealize Orchestrator. Se você quiser ativar o modo FIPS no seu ambiente, deverá fazê-lo durante a instalação.

- Clique em **Avançar**.

- Análise a página **Pronto para ser concluído** e clique em **Concluir**.

Resultados

O vRealize Orchestrator Appliance é implantado com êxito.

Próximo passo

Faça login na linha de comando do vRealize Orchestrator Appliance como **raiz** e confirme que você pode realizar uma pesquisa direta ou reversa de DNS.

- Para realizar uma pesquisa de DNS direta, execute o comando `nslookup your_orchestrator_FQDN`. O comando deve retornar o endereço IP do vRealize Orchestrator Appliance.
- Para realizar uma pesquisa de DNS reversa, execute o comando `nslookup your_orchestrator_IP`. O comando deve retornar o FQDN do vRealize Orchestrator Appliance.

Observação Se você não tiver ativado o SSH durante a implantação, também poderá realizar pesquisas de DNS no console da máquina virtual no vSphere Web Client.

Ligar o vRealize Orchestrator Appliance e abrir a página inicial

Para usar o vRealize Orchestrator Appliance autônomo, primeiro você deve ligá-lo.

Procedimentos

- Faça login no vSphere Web Client como **administrador**.
- Clique com o botão direito do mouse no vRealize Orchestrator Appliance e selecione **Energia > Ligar**.

- 3 Em um navegador, vá até o endereço do host da sua máquina virtual do vRealize Orchestrator Appliance que você configurou durante a implantação do OVA.

`https://FQDN_seu_orquestrador/vco.`

Ativar ou desativar acesso SSH ao vRealize Orchestrator Appliance

Você pode ativar ou desativar o acesso SSH ao vRealize Orchestrator Appliance.

Pré-requisitos

- Baixe e implante o vRealize Orchestrator Appliance.
- Verifique se o vRealize Orchestrator Appliance está instalado e em execução.

Procedimentos

- 1 Faça login na linha de comando do vRealize Orchestrator Appliance como **raiz**.
- 2 Para ativar o acesso SSH, execute o comando `/usr/bin/toggle-ssh enable`.
- 3 Para desativar o acesso SSH, execute o comando `/usr/bin/toggle-ssh disable`.

Configuração inicial

5

Antes de começar a automatizar tarefas e gerenciar sistemas e aplicativos com o vRealize Orchestrator, você deve usar o Centro de Controle do vRealize Orchestrator para configurar um provedor de autenticação externo. Você também pode usar o Centro de Controle do vRealize Orchestrator para tarefas adicionais de configuração, como gerenciar informações de licença e certificado, instalar plug-ins e monitorar o estado do cluster do seu vRealize Orchestrator.

Este capítulo inclui os seguintes tópicos:

- [Configurando um servidor vRealize Orchestrator autônomo](#)
- [Capacitação de Recursos do vRealize Orchestrator com Licenças](#)
- [Conexão do banco de dados do vRealize Orchestrator](#)
- [Gerenciar certificados](#)
- [Configuração dos plug-ins do vRealize Orchestrator](#)
- [Alta disponibilidade do vRealize Orchestrator](#)
- [Configurando o programa de aperfeiçoamento da experiência do cliente](#)

Configurando um servidor vRealize Orchestrator autônomo

Embora o vRealize Orchestrator Appliance seja uma máquina virtual pré-configurada baseada em Photon, você deve configurar um provedor de autenticação antes de acessar a funcionalidade completa do Centro de Controle do vRealize Orchestrator e do vRealize Orchestrator Client.

Configurar um servidor vRealize Orchestrator autônomo com autenticação do vRealize Automation

Para preparar o vRealize Orchestrator Appliance para uso, você deve definir as configurações do host e o provedor de autenticação. Você pode configurar o vRealize Orchestrator para autenticar com o vRealize Automation. Use a autenticação vRealize Automation com o vRealize Automation 8.x.

Pré-requisitos

- Baixe e implante a versão mais recente do vRealize Orchestrator Appliance. Consulte o [Baixar e implantar o vRealize Orchestrator Appliance](#).
- Instale e configure o vRealize Automation 8.x e verifique se o seu servidor vRealize Automation está em execução. Consulte a documentação do vRealize Automation.

Importante A versão do produto do provedor de autenticação do vRealize Automation deve corresponder à versão do produto de sua implantação do vRealize Orchestrator. Por exemplo, para autenticar uma implantação do vRealize Orchestrator 8.5, você deve usar uma implantação do vRealize Automation 8.5.

Se você planeja criar um cluster:

- Configure um balanceador de carga para distribuir o tráfego entre as várias instâncias do vRealize Orchestrator. Consulte o [Guia de Balanceamento de Carga do VMware vRealize Orchestrator 8.x](#).

Procedimentos

1 Acesse o Centro de Controle para iniciar o assistente de configuração.

- a Vá para `https://your_orchestrator_FQDN/vco-controlcenter`.
- b Faça login como **raiz** com a senha que você inseriu durante a implantação OVA.

2 Configure o provedor de autenticação.

- a Na página **Configurar provedor de autenticação**, selecione **vRealize Automation** no menu suspenso **Modo de autenticação**.
- b Na caixa de texto **Endereço do host**, insira seu endereço de host do vRealize Automation e clique em **CONECTAR**.

O formato do endereço do host vRealize Automation deve ser `https://your_vra_hostname`.
- c Clique em **Aceitar certificado**.
- d Insira as credenciais do proprietário da organização vRealize Automation sob o qual será configurado o vRealize Orchestrator. Clique em **REGISTRAR**.
- e Clique em **SALVAR ALTERAÇÕES**.

Uma mensagem indica que sua configuração foi salva com êxito.

Resultados

Você concluiu com êxito a configuração do servidor vRealize Orchestrator.

Próximo passo

- Verifique se o **CSP** é o provedor de licença configurado na página de **Licenciamento**.

- Verifique se o nó está configurado corretamente na página **Validar Configuração**.

Observação Após a configuração do provedor de autenticação, o servidor vRealize Orchestrator é reiniciado automaticamente após 2 minutos. Verificar a configuração imediatamente após a autenticação pode retornar um status de configuração inválido.

Configurar um servidor vRealize Orchestrator autônomo com autenticação do vSphere

Você registra o servidor vRealize Orchestrator com um servidor vCenter Single Sign-On usando o modo de autenticação do vSphere. Use a autenticação do vCenter Single Sign-On com o vCenter Server 6.0 e versões posteriores.

Pré-requisitos

- Baixe e implante a versão mais recente do vRealize Orchestrator Appliance. Consulte o [Baixar e implantar o vRealize Orchestrator Appliance](#).
- Instale e configure um vCenter Server com o vCenter Single Sign-On em execução. Consulte a documentação do vSphere.

Se você planeja criar um cluster:

- Configure um balanceador de carga para distribuir o tráfego entre as várias instâncias do vRealize Orchestrator. Consulte o [Guia de Balanceamento de Carga do VMware vRealize Orchestrator 8.x](#).

Procedimentos

- 1 Acesse o Centro de Controle para iniciar o assistente de configuração.
 - a Vá para `https://your_orchestrator_FQDN/vco-controlcenter`.
 - b Faça login como **raiz** com a senha que você inseriu durante a implantação OVA.

2 Configure o provedor de autenticação.

- a Na página **Configurar Provedor de Autenticação**, selecione **vSphere** no menu suspenso **Modo de autenticação**.
- b Na caixa de texto **Endereço do host**, insira o nome de domínio totalmente qualificado ou o endereço IP da instância do Platform Services Controller que contém o vCenter Single Sign-On e clique em **Conectar**.

Observação Se você usar um Platform Services Controller externo ou várias instâncias do Platform Services Controller atrás de um balanceador de carga, deverá importar manualmente os certificados de todos os Platform Services Controllers que compartilham um domínio vCenter Single Sign-On.

Observação Para integrar um vSphere Client diferente ao seu ambiente configurado vRealize Orchestrator, você deve configurar o vSphere para usar o mesmo Platform Services Controller registrado para o vRealize Orchestrator. Para ambientes de alta disponibilidade do vRealize Orchestrator, você deve replicar as instâncias de PCS atrás do servidor do balanceador de carga do vRealize Orchestrator.

- c Revise a informação de certificado do provedor de autenticação e clique em **Aceitar Certificado**.
- d Insira as credenciais da conta de administrador local para o domínio vCenter Single Sign-On. Clique em **REGISTRAR**.

Por padrão, essa conta é **administrator@vsphere.local** e o nome do tenant padrão é **vsphere.local**.

- e Na caixa de texto **Grupo de administradores**, insira o nome de um grupo de administradores e clique em **PESQUISAR**.

Por exemplo, **vsphere.local\vcadmins**

- f Selecione o grupo de administração que você deseja usar.
- g Clique em **SALVAR ALTERAÇÕES**.

Uma mensagem indica que sua configuração foi salva com êxito.

Resultados

Você concluiu com êxito a configuração do servidor vRealize Orchestrator.

Próximo passo

- Verifique se **CIS** é o provedor de licença configurado na página **Licenciamento**.
- Verifique se o nó está configurado corretamente na página **Validar Configuração**.

Observação Após a configuração do provedor de autenticação, o servidor vRealize Orchestrator é reiniciado automaticamente após 2 minutos. Verificar a configuração imediatamente após a autenticação pode retornar um status de configuração inválido.

Capacitação de Recursos do vRealize Orchestrator com Licenças

O acesso a certos recursos do vRealize Orchestrator se baseia na licença aplicada à sua implantação do vRealize Orchestrator.

Após a autenticação, a instância do vRealize Orchestrator é atribuída a uma licença baseada no provedor de autenticação. As licenças controlam o acesso aos seguintes recursos do vRealize Orchestrator:

- Integração com o Git
- Gerenciamento de funções
- Suporte a vários idiomas (Python, Node.js e PowerShell)

Você pode alterar manualmente a licença do servidor do vRealize Orchestrator na página **Licenças** do centro de controle.

Observação Não há limite para o número de implantações do vRealize Orchestrator às quais você pode aplicar a mesma licença, independentemente do tipo de licença. Para licenças do vRealize Automation, não é necessário ter um ambiente de vRealize Automation implantado e configurado.

Autenticação	Licença	Integração com o Git	Gerenciamento de funções	Suporte a vários idiomas
vSphere	vSphere vCloud Suite Standard	Não	Não	Não
vSphere	vRealize Automation vRealize Suite Advanced ou Enterprise vCloud Suite Advanced ou Enterprise	Sim	Sim	Sim
vRealize Automation	vRealize Automation vRealize Suite Advanced ou Enterprise vCloud Suite Advanced ou Enterprise	Sim	As funções são gerenciadas da instância do vRealize Automation usada para autenticar o vRealize Orchestrator.	Sim

Observação As licenças do vRealize Suite Standard não incluem o vRealize Automation e, portanto, não oferecem suporte ao acesso aos recursos do vRealize Orchestrator.

Conexão do banco de dados do vRealize Orchestrator

O servidor vRealize Orchestrator requer um banco de dados para o armazenamento de dados.

O vRealize Orchestrator Appliance implantado inclui um banco de dados PostgreSQL pré-configurado usado pelo servidor vRealize Orchestrator para armazenar dados.

O banco de dados PostgreSQL não está acessível para os usuários.

Gerenciar certificados

Emitido para um determinado servidor e contendo informações sobre sua chave pública, o certificado permite que você assine todos os elementos criados no vRealize Orchestrator e garanta a autenticidade. Quando o cliente recebe um elemento do seu servidor, normalmente um pacote, o cliente verifica sua identidade e decide se deseja confiar na sua assinatura.

■ Gerenciar certificados do vRealize Orchestrator

Você pode gerenciar os certificados do vRealize Orchestrator na página **Certificados** no Centro de Controle do vRealize Orchestrator ou com o vRealize Orchestrator Client, usando os fluxos de trabalho marcados do *ssl_trust_manager*.

Gerenciar certificados do vRealize Orchestrator

Você pode gerenciar os certificados do vRealize Orchestrator na página **Certificados** no Centro de Controle do vRealize Orchestrator ou com o vRealize Orchestrator Client, usando os fluxos de trabalho marcados do *ssl_trust_manager*.

Importar um certificado para o repositório de confiança do Orchestrator

O Centro de Controle do vRealize Orchestrator usa uma conexão segura para se comunicar com o vCenter Server, com o sistema de gerenciamento de banco de dados relacional (RDBMS), o LDAP, o Single Sign-on e outros servidores. Você pode importar o certificado TLS obrigatório de uma URL ou de um arquivo codificado por PEM. Toda vez que você quiser usar uma conexão TLS para uma instância do servidor, deverá importar o certificado correspondente na guia **Certificados Confiáveis** na página **Certificados** e importar o certificado TLS correspondente.

Você pode carregar o certificado TLS no vRealize Orchestrator de um endereço de URL ou um arquivo codificado por PEM.

Opção	Descrição
Importar da URL ou URL do proxy	A URL do servidor remoto: <code>https://seu_endereco_IP_servidor</code> ou <code>seu_endereco_IP_servidor:porta</code>
Importar do arquivo	Caminho para o arquivo de certificado codificado pelo PEM. Observação Você também pode importar um certificado confiável executando o fluxo de trabalho Importar um certificado confiável de um arquivo no vRealize Orchestrator Client. O arquivo importado por meio deste fluxo de trabalho deve ser codificado por DER.

Para obter mais informações sobre como importar um certificado, consulte [Importar um certificado confiável com o Centro de Controle](#).

Certificado de assinatura de pacote

Os pacotes exportados de um servidor do vRealize Orchestrator são assinados digitalmente. Importe, exporte ou gere um novo certificado para ser usado para a assinatura de pacotes. Os certificados de assinatura do pacote são uma forma de identificação digital que é usada para garantir a comunicação criptografada e uma assinatura para seus pacotes do Orchestrator.

O vRealize Orchestrator Appliance inclui um certificado de assinatura de pacote que é gerado automaticamente, com base nas configurações de rede do dispositivo. Se as configurações de rede do dispositivo mudarem, você deverá gerar um novo certificado de assinatura de pacote manualmente. Depois de gerar um novo certificado de assinatura de pacote, todos os pacotes exportados futuros serão assinados com o novo certificado.

Gerar um certificado TLS personalizado para o vRealize Orchestrator

Você pode usar o vRealize Orchestrator Appliance para gerar um novo certificado TLS para o seu ambiente ou definir um certificado personalizado existente.

O vRealize Orchestrator Appliance inclui um certificado Trusted Layer Security (TLS) gerado automaticamente, com base nas configurações de rede do dispositivo. Se as configurações de rede do dispositivo mudarem, você deverá gerar um novo certificado manualmente. Você pode criar uma cadeia de certificados para garantir a comunicação criptografada e fornecer uma assinatura para seus pacotes. No entanto, o destinatário não pode ter certeza de que o pacote autoassinado é um pacote emitido pelo seu servidor e não um terceiro alegando ser você. Para provar a identidade do seu servidor, use um certificado assinado por uma Autoridade de Certificação (CA).

O vRealize Orchestrator gera um certificado de servidor exclusivo para o seu ambiente. A chave privada é armazenada na tabela `vmo_keystore` do banco de dados do vRealize Orchestrator.

Observação Para configurar o vRealize Orchestrator Appliance para usar um certificado TLS personalizado existente, consulte [Definir um certificado TLS personalizado para vRealize Orchestrator](#).

Pré-requisitos

Verifique se o acesso SSH para o vRealize Orchestrator Appliance está ativado. Consulte o [Ativar ou desativar acesso SSH ao vRealize Orchestrator Appliance](#).

Procedimentos

- 1 Faça login na linha de comando do vRealize Orchestrator Appliance pelo SSH como **raiz**.
- 2 Execute o comando `vracli certificate ingress --generate auto --set stdin`.

- 3 Para aplicar o certificado personalizado ao seu vRealize Orchestrator Appliance, execute o script de implantação.

- a Navegue até o diretório `/opt/scripts/`.

```
cd /opt/scripts/
```

- b Execute o script `./deploy.sh`.

Importante Não interrompa o script de implantação. Você recebe a seguinte mensagem quando o script termina de ser executado:

```
O Prelude foi implantado com êxito. Para acessar, acesse seu_endereco_orquestrador.
```

Próximo passo

Para confirmar que a nova cadeia de certificados foi aplicada, execute o comando `vracli certificate ingress --list`.

Definir um certificado TLS personalizado para vRealize Orchestrator

Defina um certificado TLS personalizado para o seu vRealize Orchestrator Appliance.

O vRealize Orchestrator Appliance inclui um certificado Trusted Layer Security (TLS) gerado automaticamente, com base nas configurações de rede do dispositivo.

Você pode configurar o vRealize Orchestrator Appliance para usar um certificado TLS personalizado existente. Você pode definir o certificado importando o arquivo PEM relevante da sua máquina local para o vRealize Orchestrator Appliance. Você também pode definir o certificado TLS personalizado copiando a cadeia de certificados diretamente para o vRealize Orchestrator Appliance. Ambos os procedimentos exigem que você execute o script `./deploy.sh` antes que o novo certificado TLS possa ser usado na sua implantação do vRealize Orchestrator.

Para obter informações sobre como gerar um novo certificado TLS personalizado, consulte [Gerar um certificado TLS personalizado para o vRealize Orchestrator](#).

Pré-requisitos

- Verifique se o acesso SSH para o vRealize Orchestrator Appliance está ativado. Consulte o [Ativar ou desativar acesso SSH ao vRealize Orchestrator Appliance](#).
- Certifique-se de que o arquivo PEM que contém o certificado TLS contenha os seguintes componentes na ordem definida:
 - a A chave privada para o certificado.
 - b O certificado principal.
 - c Se aplicável, o(s) certificado(s) intermediário(s) da Autoridade de Certificação (CA).
 - d O certificado CA raiz.

Por exemplo, o certificado TLS pode ter a seguinte estrutura:

```
-----BEGIN RSA PRIVATE KEY-----
<Private Key>
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
<Primary TLS certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root CA certificate>
-----END CERTIFICATE-----
```

Procedimentos

- 1 Defina o certificado importando o arquivo PEM para o vRealize Orchestrator Appliance.

- a Importe o PEM do certificado da sua máquina local executando um comando Secure Copy (SCP) a partir de um shell SSH.

Para Linux, você pode usar um comando SCP de terminal:

```
scp ~/PEM_local_filepath/your_cert_file.PEM root@orchestrator_FQDN_or_IP:/
PEM_orchestrator_filepath/your_cert_file.PEM
```

Para o Windows, você pode usar um comando PSCP do cliente PuTTY:

```
pscp C:\PEM_local_filepath\your_cert_file.PEM root@<orchestrator_FQDN_or_IP>:/
PEM_orchestrator_filepath/your_cert_file.PEM
```

- b Faça login na linha de comando do vRealize Orchestrator Appliance pelo SSH como **raiz**.
 - c Execute o comando `vracli certificate ingress --set your_cert_file.PEM`.
- 2 (Opcional) Defina o certificado copiando a cadeia de certificados diretamente para o dispositivo.
 - a Faça login na linha de comando do vRealize Orchestrator Appliance pelo SSH como **raiz**.
 - b Execute o comando `vracli certificate ingress --set stdin`.
 - c Copie e cole a cadeia de certificados e pressione Ctrl+D.

3 Para aplicar o novo certificado TLS, execute o script de implantação.

a Navegue até o diretório `/opt/scripts/`.

```
cd /opt/scripts/
```

b Execute o script `./deploy.sh`.

Importante Não interrompa o script de implantação. Você recebe a seguinte mensagem quando o script termina de ser executado:

```
O Prelude foi implantado com êxito. Para acessar, acesse https://FQDN_seu_orquestrador.
```

Resultados

Você definiu um certificado TLS personalizado para o seu vRealize Orchestrator Appliance.

Próximo passo

Para confirmar que a nova cadeia de certificados foi aplicada, execute o comando `vrac li certificate ingress --list`.

Importar um certificado confiável com o Centro de Controle

Para se comunicar com outros servidores com segurança, o servidor do vRealize Orchestrator deve conseguir verificar sua identidade. Para esse propósito, pode ser necessário importar o certificado TLS da entidade remota para o armazenamento de confiança do vRealize Orchestrator. Para confiar em um certificado, você pode importá-lo para o armazenamento de confiança, estabelecendo uma conexão com uma URL específica ou diretamente como um arquivo codificado por PEM.

Procedimentos

- 1** Faça login no Centro de Controle como **root**.
- 2** Vá para a página **Certificados**.
- 3** Selecione **Certificados Confiáveis** e clique em **Importar**.
- 4** Para importar o certificado de um arquivo, selecione **Importar de um arquivo codificado em PEM**.
- 5** Acesse o arquivo de certificado e clique em **Importar**.
- 6** Para importar o certificado de um endereço de URL, selecione **Importar da URL**.
- 7** Digite o endereço de URL em que o seu certificado está armazenado e clique em **Importar**.

Resultados

Você importou com êxito um certificado de servidor remoto para o armazenamento de confiança do vRealize Orchestrator.

Configuração dos plug-ins do vRealize Orchestrator

O vRealize Orchestrator Appliance fornece acesso a uma biblioteca pré instalada de plug-ins padrão. Os plug-ins do vRealize Orchestrator padrão são configurados com fluxos de trabalho específicos do plug-in executados no Cliente do vRealize Orchestrator.

Os plug-ins padrão do vRealize Orchestrator vêm com fluxos de trabalho de configuração. Você pode executar esses fluxos de trabalho a partir do Cliente do vRealize Orchestrator para registrar endpoints para gerenciamento.

Os fluxos de trabalho de configuração têm a tag *configuration*. Por exemplo, para acessar fluxos de trabalho usados para gerenciar brokers e assinaturas AMQP, insira as tags *AMQP* e *Configuração* na caixa de texto de pesquisa da biblioteca de fluxos de trabalho.

Gerenciar plug-ins do vRealize Orchestrator

Na página **Gerenciar Plug-Ins** do Centro de Controle do vRealize Orchestrator, você pode exibir uma lista de todos os plug-ins que são instalados no vRealize Orchestrator e executar ações básicas de gerenciamento.

Instalar ou atualizar um plug-in

Com os plug-ins do vRealize Orchestrator, o servidor do vRealize Orchestrator pode ser integrado a outros produtos de software. O vRealize Orchestrator vem com um conjunto de plug-ins padrão pré-instalados. Você pode ampliar ainda mais os recursos da plataforma do vRealize Orchestrator instalando plug-ins personalizados.

Você pode instalar ou atualizar plug-ins na página **Gerenciar Plug-ins** do vRealize Orchestrator. A extensão de arquivo que pode ser usada é `.vmoapp`.

Para obter mais informações sobre como instalar ou atualizar os plug-ins do vRealize Orchestrator, consulte [Instalar ou atualizar plug-in do vRealize Orchestrator](#).

Alterar o nível de log do plug-in

Em vez de alterar o nível de log do vRealize Orchestrator, você pode alterá-lo apenas para plug-ins específicos.

Desativar um plug-in

Você pode desativar um plug-in desmarcando a opção **Ativar plug-in** ao lado do nome do plug-in.

Essa ação não remove o arquivo de plug-in. Para obter mais informações sobre como desinstalar um plug-in do vRealize Orchestrator, consulte [Excluir um plug-in](#).

Instalar ou atualizar plug-in do vRealize Orchestrator

Você pode instalar ou atualizar plug-ins de terceiros no Centro de Controle do vRealize Orchestrator.

Pré-requisitos

Baixe o arquivo `.dar` ou `.vmoapp` do plug-in.

Observação O formato de arquivo preferido para plug-ins do vRealize Orchestrator é `.vmoapp`.

Procedimentos

- 1 Faça login no Centro de Controle como **raiz**.
- 2 Selecione a página **Gerenciar Plug-ins**.
- 3 Clique em **Procurar** e selecione o arquivo `.dar` ou `.vmoapp` do plug-in que você deseja instalar ou atualizar.
- 4 Clique em **Carregar**.
- 5 Revise as informações de plug-in, se aplicável, aceite o contrato de licença do usuário final e clique em **Instalar**.

O plug-in é instalado ou atualizado, e o serviço do servidor do vRealize Orchestrator é reiniciado.

Próximo passo


Verifique se as informações de plug-in corretas estão listadas na página **Gerenciar Plug-ins**.

Excluir um plug-in

Você pode excluir plug-ins de terceiros do vRealize Orchestrator Appliance por meio do Centro de Controle.

Observação A partir do vRealize Orchestrator 8.0, não é mais possível excluir o pacote de plug-ins manualmente do vRealize Orchestrator Client.

Procedimentos

- 1 Faça login no Centro de Controle como **raiz**.
- 2 Selecione **Gerenciar plug-ins**.
- 3 Localize o plug-in que você deseja excluir e clique no ícone para excluir ().
- 4 Confirme que você deseja excluir o plug-in e clique em **Excluir**.

Resultados

Você excluiu o plug-in do vRealize Orchestrator Appliance.

Alta disponibilidade do vRealize Orchestrator

Para aumentar a disponibilidade dos serviços do vRealize Orchestrator, inicie várias instâncias do servidor do vRealize Orchestrator em um cluster com um banco de dados compartilhado.

O vRealize Orchestrator funciona como uma única instância até que esteja configurada para funcionar como parte de um cluster.

Várias instâncias do servidor do vRealize Orchestrator com configurações idênticas de servidor e plug-ins funcionam juntas em um cluster e compartilham um banco de dados.

Todas as instâncias do servidor do vRealize Orchestrator se comunicam umas com as outras por meio da troca de heartbeats. Cada heartbeat é um carimbo de data/hora que o nó grava no banco de dados compartilhado do cluster em um determinado intervalo de tempo. Problemas de rede, um servidor de banco de dados sem resposta ou sobrecarregamento podem fazer com que um nó do cluster do vRealize Orchestrator pare de responder. Se uma instância do servidor do vRealize Orchestrator ativo não conseguir enviar heartbeats dentro do período de tempo limite do failover, ela será considerada não responsiva. O tempo limite de failover é igual ao valor do intervalo de heartbeat multiplicado pelo número de heartbeats do failover. Ele serve como definição para um nó não confiável e pode ser personalizado de acordo com os recursos disponíveis e com a carga de produção.

Um nó do vRealize Orchestrator entra no modo de espera quando perde a conexão com o banco de dados e permanece neste modo até que a conexão de banco de dados seja restaurada. Os outros nós no cluster assumem o controle do trabalho ativo, reiniciando todos os fluxos de trabalho interrompidos de seus últimos itens não finalizados, como tarefas programáveis ou invocações de fluxo de trabalho.

Você pode monitorar o estado do seu cluster do vRealize Orchestrator na página

Gerenciamento de Cluster do Orchestrator do Centro de Controle do vRealize Orchestrator.

Você também pode usar esta página para configurar o heartbeat do cluster, o número de heartbeats de failover e o número de nós ativos do vRealize Orchestrator.

Máximos de dimensionamento do vRealize Orchestrator

A tabela de limites de dimensionamento descreve os máximos recomendados em implantações do vRealize Orchestrator 8.x.

Componente	Dimensionar destinos	Mais informações
Máquinas virtuais	35.000	
Conexões do vCenter Server	10	Consulte Configuração do vCenter Server
Nós ativos em um cluster	3	Consulte Configurar um cluster do vRealize Orchestrator
Fluxos de trabalho em execução simultaneamente	300 por nó	Consulte Configurando as propriedades de execução do fluxo de trabalho
Fluxos de trabalho em execução na fila	10.000 por nó	
Execuções de fluxo de trabalho preservadas	100 por nó	
Dias de expiração de evento do log	15	

Configurar um cluster do vRealize Orchestrator

Você pode configurar sua nova implantação do vRealize Orchestrator para executar em alta disponibilidade implantando três nós e conectando-os como um cluster.

Um cluster do vRealize Orchestrator consiste em três instâncias do vRealize Orchestrator que compartilham um banco de dados PostgreSQL comum. O banco de dados do cluster do vRealize Orchestrator configurado só pode ser executado no modo assíncrono.

Para criar um cluster do vRealize Orchestrator, você deve selecionar uma instância do vRealize Orchestrator para ser o nó primário do cluster. Depois de configurar o nó primário, você une os nós secundários a ele.

O cluster criado do vRealize Orchestrator é pré-configurado com failover automático.

Observação A falha do failover automático pode levar à perda de dados do banco de dados.

Pré-requisitos

- Baixe e implante três instâncias autônomas do vRealize Orchestrator. Consulte o [Baixar e implantar o vRealize Orchestrator Appliance](#).

Observação O número recomendado de nós que podem ser usados para criar um ambiente do vRealize Orchestrator agrupado em cluster é três.

- Verifique se o acesso SSH está ativado para todos os nós do vRealize Orchestrator. Consulte o [Ativar ou desativar acesso SSH ao vRealize Orchestrator Appliance](#).
- Configure um servidor do balanceador de carga. Consulte o [Guia de Balanceamento de Carga do VMware vRealize Orchestrator 8.x](#).

Procedimentos

- 1 Configure o nó primário.
 - a Faça login no vRealize Orchestrator Appliance do nó primário pelo SSH como **raiz**.
 - b Para configurar o servidor do balanceador de carga do cluster, execute o comando `vraccli load-balancer set load_balancer_FQDN`.
 - c Faça login no Centro de Controle do nó primário e selecione **Configurações do Host**.
 - d Clique em **Alterar** e defina o endereço do host do servidor do balanceador de carga conectado.
 - e Configure o provedor de autenticação. Consulte o [Configurando um servidor vRealize Orchestrator autônomo](#).
- 2 Associe nós secundários ao nó primário.
 - a Faça login no vRealize Orchestrator Appliance do nó secundário pelo SSH como **raiz**.
 - b Para unir o nó secundário ao nó primário, execute o comando `vraccli cluster join primary_node_hostname_or_IP`.

- c Insira a senha raiz do nó primário.
 - d Repita o procedimento para outro nó secundário.
- 3** (Opcional) Se o seu nó primário usar um certificado personalizado, você deverá definir o certificado no dispositivo ou gerar um novo certificado. Consulte o [Gerar um certificado TLS personalizado para o vRealize Orchestrator](#).

Observação O arquivo que contém a cadeia de certificados deve ser codificado por PEM.

- 4** Conclua a implantação do cluster.
- a Faça login no vRealize Orchestrator Appliance do nó primário pelo SSH como **raiz**.
 - b Para confirmar que todos os nós estão em um estado pronto, execute o comando `kubect1 -n prelude get nodes`.
 - c Execute o script `/opt/scripts/deploy.sh` e aguarde a conclusão da implantação.

Resultados

Você criou um cluster do vRealize Orchestrator. Após criar o cluster, você pode acessar seu ambiente do vRealize Orchestrator apenas a partir do endereço FQDN do seu servidor do balanceador de carga.

Observação Como você pode acessar apenas o Centro de Controle do cluster com a senha raiz do balanceador de carga, não poderá editar a configuração de um nó do cluster se ele tiver uma senha raiz diferente. Para editar a configuração desse nó, remova-o do balanceador de carga, edite a configuração no Centro de Controle e inclua o nó novamente no balanceador de carga.

Próximo passo

Para monitorar o estado do cluster vRealize Orchestrator, faça login no Centro de Controle e selecione a página **Gerenciamento de Cluster do Orchestrator**. Consulte o [Monitorar um cluster do vRealize Orchestrator](#).

Removendo um nó de cluster do vRealize Orchestrator

Você pode excluir um vRealize Orchestrator para poder reduzir a capacidade do cluster.

Após a remoção de um nó do cluster do vRealize Orchestrator, esse nó não funcionará mais. Se quiser usar esse nó novamente, você deverá excluir seu vRealize Orchestrator Appliance do seu vCenter Server e implantá-lo novamente. Consulte o [Baixar e implantar o vRealize Orchestrator Appliance](#).

Pré-requisitos

Crie um cluster do vRealize Orchestrator. Consulte o [Configurar um cluster do vRealize Orchestrator](#).

Procedimentos

- 1 Faça login na linha de comando do vRealize Orchestrator Appliance do nó que você deseja remover como **raiz**.
- 2 Para remover o nó do seu vRealize Orchestrator, execute o comando `vracli cluster leave`.
- 3 Faça login na linha de comando do vRealize Orchestrator Appliance de um dos nós restantes como **raiz**.
- 4 Execute o comando `kubectl -n prelude get nodes` e confirme se o nó removido não faz mais parte do cluster.

Dimensionar horizontalmente uma implantação autônoma do vRealize Orchestrator

Você pode aumentar a disponibilidade e o dimensionamento da sua implantação configurada do vRealize Orchestrator ao dimensioná-la.

Pré-requisitos

- Baixe, implante e configure uma instância do vRealize Orchestrator. Consulte [Baixar e implantar o vRealize Orchestrator Appliance](#) e [Configurando um servidor vRealize Orchestrator autônomo](#).
- Baixe e implante duas instâncias extras do vRealize Orchestrator. Consulte o [Baixar e implantar o vRealize Orchestrator Appliance](#).
- Configure um servidor do balanceador de carga. Consulte o [Guia de Balanceamento de Carga do VMware vRealize Orchestrator 8.x](#).

Procedimentos

- 1 Configure o nó primário.
 - a Faça login no Centro de Controle de sua implantação do vRealize Orchestrator configurada como **raiz**.
 - b Selecione **Configurar Provedor de Autenticação** e cancele o registro do provedor de autenticação.
 - c Selecione **Configurações do Host** e insira o nome do host do servidor do balanceador de carga.
 - d Selecione **Configurar Provedor de Autenticação** e registre o provedor de autenticação novamente.
 - e Faça login na linha de comando do vRealize Orchestrator Appliance da instância configurada como **raiz**.
 - f Para interromper todos os serviços da instância do vRealize Orchestrator, execute o comando `/opt/scripts/deploy.sh --onlyClean`.

- g Para definir o balanceador de carga, execute `vracli load-balancer set load_balancer_FQDN`.
- h (Opcional) Se a instância do vRealize Orchestrator usar um certificado personalizado, execute o comando `vracli certificate ingress --set seu_arquivo_cert.pem`.

Observação O arquivo que contém a cadeia de certificados deve ser codificado por PEM.

- 2 Associe os nós secundários à instância configurada.
 - a Faça login na linha de comando do vRealize Orchestrator Appliance do nó secundário como **raiz**.
 - b Para unir o nó secundário à instância configurada, execute o comando `vracli cluster join nó_primario_nomedohost_ou_IP`.
 - c Repita o procedimento para o outro nó secundário.
- 3 Conclua o processo de dimensionamento horizontal.
 - a Faça login na linha de comando do vRealize Orchestrator Appliance da instância configurada como **raiz**.
 - b Execute `/opt/scripts/deploy.sh` e espere que o script termine.

Resultados

Você dimensionou horizontalmente a implantação do vRealize Orchestrator.

Monitorar um cluster do vRealize Orchestrator

Você pode monitorar o cluster do seu vRealize Orchestrator por meio do Centro de Controle do vRealize Orchestrator.

Você pode monitorar os estados de sincronização de configuração das instâncias do vRealize Orchestrator que ingressaram em um cluster da página **Gerenciamento de cluster do Orchestrator** no Centro de Controle.

Estado de sincronização de configuração	Descrição
EM EXECUÇÃO	O serviço do vRealize Orchestrator está disponível e pode aceitar solicitações.
ESPERA	<p>O serviço do vRealize Orchestrator não pode processar solicitações porque:</p> <ul style="list-style-type: none"> ■ O nó faz parte de um cluster de Alta Disponibilidade (HA) e permanece em modo de espera até que o nó principal apresente falha. ■ O serviço não pode verificar os pré-requisitos de configuração, como uma conexão válida com o banco de dados, o provedor de autenticação e a licença de instância do vRealize Orchestrator.

Estado de sincronização de configuração	Descrição
Falha ao recuperar o status de integridade do serviço	Não é possível entrar em contato com o serviço do servidor do vRealize Orchestrator porque está parado ou há um problema de rede.
Reinicialização pendente	O Centro de Controle detecta uma alteração de configuração, e o servidor do vRealize Orchestrator é reiniciado automaticamente.

Configurando o programa de aperfeiçoamento da experiência do cliente

Se você optar por participar do Programa de Aperfeiçoamento da Experiência do Cliente (CEIP), a VMware receberá informações anônimas que ajudam a melhorar a qualidade, a confiabilidade e a funcionalidade dos produtos e serviços da VMware.

Categorias de informações recebidas pela VMware

O Programa de Aperfeiçoamento da Experiência do Cliente (CEIP) fornece à VMware informações que permitem à VMware melhorar nossos produtos e serviços e corrigir problemas.

Detalhes sobre os dados coletados através do CEIP e os propósitos para os quais são usados pela VMware estão definidos no Trust & Assurance Center em <http://www.vmware.com/trustvmware/ceip.html>. Para ingressar ou sair do CEIP para este produto, consulte [Participar ou sair do Programa de Aperfeiçoamento da Experiência do Cliente](#).

Participar ou sair do Programa de Aperfeiçoamento da Experiência do Cliente

Participe do Programa de Aperfeiçoamento da Experiência do Cliente a partir da linha de comando do vRealize Orchestrator Appliance.

Procedimentos

- 1 Faça login na linha de comando do vRealize Orchestrator Appliance como **raiz**.
- 2 Para participar do Programa de Aperfeiçoamento da Experiência do Cliente, 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 Reinicie os serviços do vRealize Orchestrator.
 - a Para reiniciar o serviço do servidor, execute o comando `kubectrl -n prelude exec -it seu_vro_pod -c vco-server-app /bin/bash`.
 - b Para interromper o serviço, execute o comando `kill 1`.

- c Para reiniciar o serviço do Centro de Controle, execute o comando `kubectl -n prelude exec -it seu_vro_pod -c vco-controlcenter-app /bin/bash`.
 - d Para interromper o serviço, execute o comando `kill 1`.
- 5 Para sair do Programa de Aperfeiçoamento da Experiência do Cliente, execute o comando `vracli ceip off`.
 - 6 Repita as etapas para reiniciar os serviços.

Usando os serviços de API do vRealize Orchestrator

6

Além de configurar o vRealize Orchestrator usando o Centro de Controle, você pode modificar as definições de configuração do servidor vRealize Orchestrator usando a REST API do vRealize Orchestrator, a REST API do Centro de Controle ou o utilitário de linha de comando, armazenado no dispositivo.

O plug-in de Configuração está incluído no pacote do vRealize Orchestrator, por padrão. Você pode acessar os fluxos de trabalho do plug-in de Configuração da biblioteca de fluxo de trabalho do vRealize Orchestrator ou da REST API do vRealize Orchestrator. Com esses fluxos de trabalho, você pode alterar as configurações de certificados confiáveis e de armazenamento de chaves do servidor vRealize Orchestrator. Para obter informações sobre todas as chamadas de serviço da REST API do vRealize Orchestrator disponíveis, consulte a documentação da *API do vRealize Orchestrator Server*, localizada em https://your_orchestrator_FQDN/vco/api/docs.

■ Gerenciar certificados TLS e armazenamentos de chaves usando a REST API

Além de gerenciar certificados TLS usando o Centro de Controle, você também pode gerenciar os certificados confiáveis e os armazenamentos de chaves ao executar fluxos de trabalho a partir do plug-in de configuração ou usando a REST API.

Gerenciar certificados TLS e armazenamentos de chaves usando a REST API

Além de gerenciar certificados TLS usando o Centro de Controle, você também pode gerenciar os certificados confiáveis e os armazenamentos de chaves ao executar fluxos de trabalho a partir do plug-in de configuração ou usando a REST API.

O plug-in de Configuração contém fluxos de trabalho para importar e excluir os certificados TLS e os armazenamentos de chaves. Você pode acessar esses fluxos de trabalho navegando até **Biblioteca > Fluxos de trabalho > SSL Trust Manager** e **Biblioteca > Fluxos de trabalho > Armazenamento de chaves** no vRealize Orchestrator Client. Você também pode executar esses fluxos de trabalho usando a REST API do vRealize Orchestrator.

A REST API do Centro de Controle fornece acesso a recursos para a configuração do servidor do vRealize Orchestrator. Você pode usar a REST API do Centro de Controle com sistemas de terceiros para automatizar a configuração do vRealize Orchestrator. O endpoint raiz da REST API do Centro de Controle é `https://FQDN_seu_orquestrador/vco/api`. Para obter informações sobre todas as chamadas de serviço disponíveis que você pode fazer na REST API do Centro de Controle, consulte a *API do Centro de Controle do vRealize Orchestrator*, no `https://FQDN_seu_orquestrador/vco-controlcenter/docs`.

Excluir um certificado TLS usando a REST API

Você pode excluir um certificado TLS executando o fluxo de trabalho Excluir certificado confiável do plug-in de Configuração ou usando a REST API.

Procedimentos

- 1 Faça uma solicitação do GET no URL do serviço de Fluxo de trabalho Excluir certificado confiável.

```
GET https://{orchestrator_host}:{porta}/vco/api/workflows?conditions=name>Delete trusted certificate
```

- 2 Recupere a definição do fluxo de trabalho Excluir certificado confiável fazendo uma solicitação do GET na URL da definição.

```
GET https://{orchestrator_host}:{porta}/vco/api/workflows/8a70a326-ffd7-4fef-97e0-2002ac49f5bd
```

- 3 Faça uma solicitação do POST na URL que contém os objetos de execução do fluxo de trabalho Excluir certificado confiável.

```
POST https://{orchestrator_host}:{porta}/vco/api/workflows/8a70a326-ffd7-4fef-97e0-2002ac49f5bd/executions/
```

- 4 Forneça o nome do certificado que você deseja excluir como um parâmetro de entrada do fluxo de trabalho Excluir certificado confiável em um elemento de contexto de execução no corpo da solicitação.

Importar certificados TLS usando a REST API

Você pode importar certificados TLS executando um fluxo de trabalho a partir do plug-in de Configuração ou usando a REST API.

Você pode importar um certificado confiável de um arquivo ou de uma URL. Consulte [Importar um certificado confiável com o Centro de Controle](#)

Procedimentos

- 1 Faça uma solicitação de GET na URL do serviço de fluxo de trabalho.

Opção	Descrição
Importar certificado confiável de um arquivo	Importa um certificado confiável de um arquivo.
Importar certificado confiável da URL	Importa um certificado confiável de um endereço de URL.
Importar certificado confiável da URL usando o servidor proxy	Importa um certificado confiável de um endereço de URL usando um servidor proxy.
Importar certificado confiável da URL com alias de certificado	Importa um certificado confiável com um alias de certificado, de um endereço de URL.

Para importar um certificado confiável de um arquivo, faça a seguinte solicitação GET:

```
GET https://{orchestrator_host}:{porta}/vco/api/workflows?conditions=name=Import
trusted certificate from a file
```

- 2 Recupere a definição do fluxo de trabalho fazendo uma solicitação GET na URL da definição.

Para recuperar a definição do fluxo de trabalho Importar certificado confiável de um arquivo, faça a seguinte solicitação GET:

```
GET https://{orchestrator_host}:{porta}/vco/api/workflows/93a7bb21-0255-4750-9293-2437abe9d2e5
```

- 3 Faça uma solicitação POST na URL que contém os objetos de execução do fluxo de trabalho.

Para o fluxo de trabalho Importar certificado confiável de um arquivo, faça a seguinte solicitação POST:

```
POST https://{orchestrator_host}:{porta}/vco/api/workflows/93a7bb21-0255-4750-9293-2437abe9d2e5/
executions
```

- 4 Forneça valores para os parâmetros de entrada do fluxo de trabalho em um elemento de contexto de execução do corpo da solicitação.

Parâmetro	Descrição
cer	O arquivo CER do qual você deseja importar o certificado TLS. Esse parâmetro é aplicável para o fluxo de trabalho Importar certificado confiável de um arquivo.
url	A URL da qual você deseja importar o certificado TLS. Para serviços não HTTPS, o formato compatível é <i>endereco_IP_ou_nome_DNS:porta</i> . Esse parâmetro é aplicável para o certificado confiável Importar do fluxo de trabalho do URL.

Criar um Armazenamento de Chaves usando a REST API

Você pode criar um armazenamento de chaves executando o fluxo de trabalho Criar um armazenamento de chaves do plug-in de Configuração ou usando a REST API.

Procedimentos

- 1 Faça uma solicitação de GET na URL do serviço do Fluxo de trabalho do fluxo de trabalho Criar um armazenamento de chaves.

```
GET https://{orchestrator_host}:{porta}/vco/api/workflows?conditions=name=Create a keystore
```

- 2 Recupere a definição do fluxo de trabalho Criar um armazenamento de chaves fazendo uma solicitação de GET na URL da definição.

```
GET https://{orchestrator_host}:{porta}/vco/api/workflows/6c301bff-e8fe-4ae0-ad08-5318178594b3/
```

- 3 Faça uma solicitação de POST na URL que contém os objetos de execução do fluxo de trabalho Criar um armazenamento de chaves.

```
POST https://{orchestrator_host}:{porta}/vco/api/workflows/6c301bff-e8fe-4ae0-ad08-5318178594b3/executions/
```

- 4 Forneça o nome do armazenamento de chaves que você deseja criar como um parâmetro de entrada do fluxo de trabalho Criar um armazenamento de chaves em um elemento de contexto de execução no corpo da solicitação.

Excluir um Armazenamento de Chaves usando a REST API

Você pode excluir um armazenamento de chaves executando o fluxo de trabalho Excluir um armazenamento de chaves do plug-in de Configuração ou usando a REST API.

Procedimentos

- 1 Faça uma solicitação de GET na URL do serviço de Fluxo de trabalho Excluir um armazenamento de chaves.

```
GET https://{orchestrator_host}:{porta}/vco/api/workflows?conditions=name=Delete a keystore
```

- 2 Recupere a definição do fluxo de trabalho Excluir um armazenamento de chaves fazendo uma solicitação de GET na URL da definição.

```
GET https://{orchestrator_host}:{porta}/vco/api/workflows/7a3389eb-1fab-4d77-860b-81b66bb45b86/
```

- 3 Faça uma solicitação de POST na URL que contém os objetos de execução do fluxo de trabalho Excluir um armazenamento de chaves.

```
POST https://{orchestrator_host}:{porta}/vco/api/workflows/7a3389eb-1fab-4d77-860b-81b66bb45b86/executions/
```

- 4 Forneça o armazenamento de chaves que você deseja excluir como um parâmetro de entrada do fluxo de trabalho Excluir um armazenamento de chaves em um elemento de contexto de execução no corpo da solicitação.

Adicionar uma chave usando a REST API

Você pode adicionar uma chave executando o fluxo de trabalho Adicionar chave do plug-in de Configuração ou usando a REST API.

Procedimentos

- 1 Faça uma solicitação de GET no URL do serviço de Fluxo de trabalho do fluxo de trabalho Adicionar chave.

```
GET https://{orchestrator_host}:{porta}/vco/api/workflows?conditions=name=Add key
```

- 2 Recupere a definição do fluxo de trabalho Adicionar chave fazendo uma solicitação de GET na URL da definição.

```
GET https://{orchestrator_host}:{porta}/vco/api/workflows/6c301bff-e8fe-4ae0-ad08-5318178594b3/
```

- 3 Faça uma solicitação de POST na URL que contém os objetos de execução do fluxo de trabalho Adicionar chave.

```
POST https://{orchestrator_host}:{porta}/vco/api/workflows/6c301bff-e8fe-4ae0-ad08-5318178594b3/
executions/
```

- 4 Forneça o armazenamento de chaves, o alias de chave, a chave codificada por PEM, a cadeia de certificados e a senha de chave como parâmetros de entrada do fluxo de trabalho Adicionar chave em um elemento de contexto de execução no corpo da solicitação.

Opções adicionais de configuração

7

Você pode usar o Centro de Controle para alterar o comportamento padrão do vRealize Orchestrator.

Este capítulo inclui os seguintes tópicos:

- [Reconfigurar a autenticação](#)
- [Configurando as propriedades de execução do fluxo de trabalho](#)
- [Arquivos de log do vRealize Orchestrator](#)
- [Habilitar as extensões do Opentracing e do Wavefront](#)
- [Habilitar a sincronização de horário para o vRealize Orchestrator](#)
- [Desativar a sincronização de hora para o vRealize Orchestrator](#)
- [Configurar o vRealize Orchestrator Kubernetes CIDR](#)
- [Atualizar as configurações de DNS do vRealize Orchestrator](#)

Reconfigurar a autenticação

Depois de configurar o método de autenticação durante a configuração inicial do Centro de Controle, você pode alterar o provedor de autenticação ou os parâmetros configurados a qualquer momento.

Mudar o provedor de autenticação

Para alterar o modo de autenticação ou as configurações de conexão do provedor de autenticação, você deve primeiro cancelar o registro do provedor de autenticação existente.

Procedimentos

- 1 Faça login no Centro de Controle como **root**.
- 2 Na página **Configurar Provedor de Autenticação**, clique no botão **CANCELAR REGISTRO** ao lado da caixa de texto endereço do host para cancelar o registro do provedor de autenticação que está em uso.

Resultados

Você cancelou o registro do provedor de autenticação com sucesso.

Próximo passo

Reconfigure a autenticação no Centro de Controle. Consulte o [Configurando um servidor vRealize Orchestrator autônomo](#).

Alterar os parâmetros de autenticação

Ao usar o vSphere como um provedor de autenticação no Centro de Controle, você pode alterar o tenant padrão do grupo de administradores do vRealize Orchestrator.

Pré-requisitos

Configure vSphere como o provedor de autenticação para a sua implantação do vRealize Orchestrator. Consulte o [Configurar um servidor vRealize Orchestrator autônomo com autenticação do vSphere](#).

Observação A autenticação de vRealize Automation não inclui esses parâmetros.

Procedimentos

- 1 Faça login no Centro de Controle como **raiz**.
- 2 Selecionar **Configurar Provedor de Autenticação**.
- 3 Clique no botão **ALTERAR** ao lado da caixa de texto **Tenant padrão**.
- 4 Substitua o nome do tenant.
- 5 Clique no botão **ALTERAR** ao lado da caixa de texto **Grupo de administradores**.

Observação Se você não reconfigurar o grupo de administradores, ele permanecerá vazio e você não poderá mais acessar o Centro de Controle.

- 6 Insira o nome de um grupo de administradores e clique em **PESQUISAR**.
- 7 Selecione um grupo de administradores.
- 8 Altere o grupo de administradores.
- 9 Para concluir a edição dos parâmetros de autenticação, clique em **SALVAR ALTERAÇÕES**.

Configurando as propriedades de execução do fluxo de trabalho

Por padrão, você pode executar até 300 fluxos de trabalho por nó e até 10.000 os fluxos de trabalho poderão ser enfileirados se o número de fluxos de trabalho ativamente em execução for atingido.

Quando o nó do vRealize Orchestrator tem que executar mais de 300 fluxos de trabalho simultâneos, as execuções de fluxo de trabalho pendentes são enfileiradas. Quando a execução de um fluxo de trabalho ativo for concluída, o próximo fluxo de trabalho na fila começará a ser executado. Se o número máximo de fluxos de trabalho enfileirados for atingido, a próxima execução de fluxo de trabalho falhará até que um dos fluxos de trabalho pendentes comece a ser executado.

Você pode configurar as propriedades de execução do fluxo de trabalho na página **Opções Avançadas** no Centro de Controle.

Opção	Descrição
Ativar modo de segurança	Se o modo de segurança estiver ativado, todos os fluxos de trabalho em execução serão cancelados e não serão retomados no próximo início do nó do vRealize Orchestrator.
Número de fluxos de trabalho simultâneos em execução	O número de fluxos de trabalho que são executados simultaneamente. O padrão é 300 fluxos de trabalho por nó.
Quantidade máxima de fluxos de trabalho em execução na fila	O número de solicitações de execução de fluxo de trabalho aceitas pelo nó do vRealize Orchestrator antes de se tornar indisponível. O padrão é 10.000 fluxos de trabalho por nó.
Número máximo de execuções preservadas por fluxo de trabalho	O número máximo de execuções de fluxo de trabalho concluídas que são mantidas como histórico por fluxo de trabalho. Se o número for excedido, as execuções de fluxo de trabalho mais antigas serão excluídas. O padrão é 100 execuções por fluxo de trabalho.
Dias de expiração de eventos do log	O número de dias em que os eventos de log são mantidos no banco de dados antes de serem limpos. O padrão é 15 dias.

Arquivos de log do vRealize Orchestrator

O Suporte Técnico da VMware solicita informações de diagnóstico rotineiramente quando você envia uma solicitação de suporte. Essas informações de diagnóstico contêm logs específicos do produto e arquivos de configuração do host no qual o produto é executado.

Os logs do vRealize Orchestrator Appliance são armazenados no diretório `/data/vco/usr/lib/vco/app-server/logs/`. Exporte os logs da sua implantação do vRealize Orchestrator Appliance fazendo login na linha de comando do dispositivo e executando o comando `vrac li log-bundle`. O pacote de log gerado é salvo na pasta raiz do seu vRealize Orchestrator Appliance.

Log de persistência

Você pode registrar informações de qualquer tipo do script do vRealize Orchestrator, por exemplo, fluxo de trabalho, política ou ação. Essas informações têm tipos e níveis. O tipo pode ser persistente ou não persistente. O nível pode ser DEPURAÇÃO, INFORMAÇÕES, AVISO, ERRO, TRAÇO e FATAL.

Tabela 7-1. Criar logs persistentes e não persistentes

Nível de log	Tipo persistente	Tipo não persistente
DEPURAÇÃO	Server.debug("texto curto", "texto longo");	System.debug("texto")
INFORMAÇÕES	Server.log("texto curto", "texto longo");	System.log("texto");
AVISO	Server.warn("texto curto", "texto longo");	System.warn("texto");
ERRO	Server.error("texto curto", "texto longo");	System.error("texto");

Logs persistentes

Os logs persistentes (registros do servidor) rastreiam os logs de execução do fluxo de trabalho passados e são armazenados no banco de dados do vRealize Orchestrator.

Logs não persistentes

Quando você usa um log não persistente (log do sistema) para criar scripts, o servidor do vRealize Orchestrator notifica todos os aplicativos do vRealize Orchestrator em execução sobre esse log, mas essas informações não são armazenadas no banco de dados. Quando o aplicativo é reiniciado, as informações de log são perdidas. Os logs não persistentes são usados para fins de depuração e para informações dinâmicas. Para exibir os logs do sistema, você deve selecionar uma execução de fluxo de trabalho concluída no vRealize Orchestrator Client e selecionar a guia **Logs**.

Configuração de logs do vRealize Orchestrator

Na página **Configurar Logs** no Centro de Controle, você pode definir o nível de log do servidor e o log de script que você precisa. Se um dos logs for gerado várias vezes ao dia, torna-se difícil determinar a causa dos problemas.

O nível de log padrão do log do servidor e do log de script é **INFORMAÇÕES**. A alteração do nível de log afeta todas as novas mensagens que o servidor insere nos logs e o número de conexões ativas com o banco de dados. A verbosidade do log diminui em ordem decrescente.

Cuidado Defina apenas o nível de log como **DEPURAÇÃO** ou **TODOS** para depurar um problema. Não use essas configurações em um ambiente de produção, pois isso pode prejudicar seriamente o desempenho.

Gerar Logs do vRealize Orchestrator

Você pode exportar os logs da sua implantação fazendo login na linha de comando do vRealize Orchestrator Appliance como **raiz** e executando o comando `vraccli log-bundle`. O pacote de log gerado é armazenado na pasta raiz do dispositivo.

Observação Quando você tem mais de uma instância de vRealize Orchestrator em um cluster, o pacote de log inclui os logs de todas as instâncias do vRealize Orchestrator no cluster.

Configurar a integração de log com o vRealize Log Insight

Você pode configurar o vRealize Orchestrator para enviar suas informações de log para um servidor vRealize Log Insight.

Você pode configurar uma integração de log para um servidor vRealize Log Insight por meio da linha de comando vRealize Orchestrator Appliance.

Observação Para obter informações sobre como configurar uma integração de log com um servidor de syslog remoto, consulte [Criar ou substituir uma integração de syslog no vRealize Orchestrator](#).

Pré-requisitos

- Configure o servidor vRealize Log Insight. Consulte a *Documentação do vRealize Log Insight*.
- Verifique se a sua versão do vRealize Log Insight é 4.7.1 ou posterior.

Procedimentos

- 1 Faça login na linha de comando do vRealize Orchestrator Appliance como **raiz**.
- 2 Para configurar a integração de log com o vRealize Log Insight, execute o comando `vrcli vrli set vRLI_FQDN`.

Observação Se a sua instância do vRealize Orchestrator usar um certificado autoassinado, você poderá desativar a autenticação SSL, incluindo o argumento opcional `-k` ou `--insecure`.

Próximo passo

Para obter mais informações sobre as opções de configuração do vRealize Log Insight, execute o comando `vrcli vrli -h`.

Criar ou substituir uma integração de syslog no vRealize Orchestrator

Você pode configurar o vRealize Orchestrator para enviar suas informações de log para um ou mais servidores de syslog remotos.

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

A integração do syslog remoto do vRealize Orchestrator oferece suporte a três tipos de conexão:

- Sobre UDP.

- Sobre TCP sem TLS.

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

- Sobre TCP com TLS.

Para obter informações sobre como configurar uma integração de log com o vRealize Log Insight, consulte [Configurar a integração de log com o vRealize Log Insight](#).

Pré-requisitos

Configure um ou mais servidores de syslog remotos.

Procedimentos

- 1 Faça login na linha de comando do vRealize Orchestrator Appliance como **raiz**.
- 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 da porta será padronizado como 514.

Observação Você pode adicionar um certificado à configuração do syslog. Para adicionar um arquivo de certificado, use o sinalizador `--ca-file`. Para adicionar um certificado como texto sem formatação, use o sinalizador `--ca-cert`.

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

Observação Por padrão, o vRealize Orchestrator Appliance solicita que você confirme se deseja substituir a integração de syslog. Para ignorar 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`.

Excluir uma integração de syslog no vRealize Orchestrator

Você pode excluir as integrações de syslog do seu vRealize Orchestrator Appliance executando o comando `vracli remote-syslog unset`.

Pré-requisitos

Crie uma ou mais integrações de syslog no vRealize Orchestrator Appliance. Consulte o [Criar ou substituir uma integração de syslog no vRealize Orchestrator](#).

Procedimentos

- 1 Faça login na linha de comando do vRealize Orchestrator Appliance como **raiz**.
- 2 Exclua as integrações de syslog do vRealize Orchestrator Appliance.
 - a Para excluir uma integração de syslog específica, execute o comando `vraccli remote-syslog unset -id Integration_name`.
 - b Para excluir todas as integrações de syslog no vRealize Orchestrator Appliance, execute o comando `vraccli remote-syslog unset` sem o sinalizador `-id`.

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

Ativar logs de depuração do Kerberos

Você pode solucionar problemas de plug-in do vRealize Orchestrator modificando o arquivo de configuração Kerberos usado pelo plug-in.

O arquivo de configuração Kerberos está localizado no diretório `/data/vco/usr/lib/vco/app-server/conf/` do vRealize Orchestrator Appliance.

Procedimentos

- 1 Faça login na linha de comando do vRealize Orchestrator Appliance como **raiz**.
- 2 Execute o comando `kubectl -n prelude edit deployment vco-app`.
- 3 No arquivo de implantação, localize e edite a cadeia de caracteres do `-Djava.security.krb5.conf=/usr/lib/vco/app-server/conf/krb5.conf`.

```
-Djava.security.krb5.conf=/usr/lib/vco/app-server/conf/krb5.conf -Dsun.security.krb5.debug=true'
```

- 4 Salve as alterações e feche o editor do arquivo.
- 5 Execute o comando `kubectl -n prelude get pods`.
Aguarde até que todos os pods estejam em execução.
- 6 Verifique se o log de depuração Kerberos está ativado.

```
kubectl -n prelude log {vco_app_name} -c vco-server-app | grep krb5
```

Verifique se os logs contêm uma mensagem semelhante.

```
kubectl -n prelude log vco-app-5c965f9b9d-v8srd -c vco-server-app | grep krb5
12:23:05,417 INFO 011N:75 - Sysprop: java.security.krb5.conf = /usr/lib/vco/app-server/conf/krb5.conf
12:23:05,421 INFO 011N:75 - Sysprop: sun.security.krb5.debug = true
2019-10-22 12:23:38.521+0000 [Thread-19] INFO {} [011N] Sysprop: java.security.krb5.conf = /usr/lib/vco/app-server/conf/krb5.conf
2019-10-22 12:23:38.525+0000 [Thread-19] INFO {} [011N] Sysprop: sun.security.krb5.debug = true
Java config name: /usr/lib/vco/app-server/conf/krb5.conf
EType: sun.security.krb5.internal.crypto.Aes256CtsHmacSha1EType
```

Habilitar as extensões do Opentracing e do Wavefront

As extensões Opentracing e Wavefront para o vRealize Orchestrator fornecem ferramentas para a coleta de dados sobre o ambiente do vRealize Orchestrator. Você pode usar esses dados para solucionar problemas com o sistema e os fluxos de trabalho do vRealize Orchestrator.

Para configurar o vRealize Orchestrator para usar as extensões do Opentracing e do Wavefront, você deve habilitá-las no vRealize Orchestrator Appliance.

Pré-requisitos

- Verifique se o serviço SSH do vRealize Orchestrator Appliance está ativado. Consulte o [Ativar ou desativar acesso SSH ao vRealize Orchestrator Appliance](#).
- Se você tiver ativado as versões anteriores das extensões do Opentracing ou do Wavefront, deverá removê-las antes de ativar a versão atual. Por exemplo, se você tiver ativado anteriormente a versão 8.1.0 da extensão Wavefront, deverá executar o comando `rm /data/vco/usr/lib/vco/app-server/extensions/wavefront-8.1.0.jar`.

Procedimentos

- 1 Faça login para o vRealize Orchestrator Appliance pelo SSH como **raiz**.
- 2 Para listar todas as extensões disponíveis, execute o comando `ls /data/vco/usr/lib/vco/app-server/extensions/`.
- 3 Execute o seguinte comando para ativar a extensão Opentracing:

```
mv /data/vco/usr/lib/vco/app-server/extensions/opentracing-8.5.0.jar.inactive /
data/vco/usr/lib/vco/app-server/extensions/opentracing-8.5.0.jar
```

- 4 Execute o seguinte comando para ativar a extensão Wavefront:

```
mv /data/vco/usr/lib/vco/app-server/extensions/wavefront-8.5.0.jar.inactive /data/vco/usr/lib/vco/
app-server/extensions/wavefront-8.5.0.jar
```

- 5 Faça login no Centro de Controle e confirme que as extensões aparecem na página **Propriedades da Extensão**.

Próximo passo

Configure a integração do Opentracing e Wavefront com o vRealize Orchestrator na página **Propriedades da Extensão**. Consulte [Configurar a extensão do Opentracing](#) e [Configurar a extensão do Wavefront](#).

Configurar a extensão do Opentracing

A extensão do Opentracing envia dados sobre execuções de fluxo de trabalho para um servidor Jaeger. Os dados incluem o status do fluxo de trabalho, parâmetros de entrada e saída, o usuário que iniciou a execução do fluxo de trabalho e os dados do ID do fluxo de trabalho.

Pré-requisitos

- Certifique-se de que o Opentracing esteja ativado no vRealize Orchestrator Appliance. Consulte o [Habilitar as extensões do Opentracing e do Wavefront](#).
- Implante um servidor Jaeger para uso na extensão do Opentracing. Para obter mais informações, consulte a [documentação Introdução ao Jaeger](#).

Procedimentos

- 1 Faça login no Centro de Controle como **raiz**.
- 2 Selecione a página **Propriedades da Extensão**.
- 3 Selecione a extensão do Opentracing.
- 4 Insira o endereço e a porta do host do servidor Jaeger.

Observação Insira duas barras ("/") antes de inserir o endereço do servidor.

- 5 Clique em **Salvar**.

Resultados

Você configurou a extensão do Opentracing para vRealize Orchestrator.

Próximo passo

- Para acessar a Jaeger UI que contém os dados coletados pela extensão do Opentracing, visite o endereço do host inserido durante a configuração.
- Na opção **Serviço**, selecione **Fluxos de Trabalho**.
- Para especificar quais dados exibir, use a opção **Tags**. Por exemplo, para visualizar dados sobre fluxos de trabalho com falha, insira **status=failed**.

Configurar a extensão do Wavefront

Use a extensão do Wavefront para coletar dados de métrica sobre o sistema do vRealize Orchestrator e os fluxos de trabalho.

Pré-requisitos

- 1 Verifique se o Wavefront está ativado no vRealize Orchestrator Appliance. Consulte o [Habilitar as extensões do Opentracing e do Wavefront](#).
- 2 Importe o certificado Wavefront:
 - a Faça login no Centro de Controle do vRealize Orchestrator como **raiz**.
 - b Selecione a página **Certificados**.
 - c Clique no menu suspenso **Importar** e selecione **Importar da URL**.
 - d Insira a URL do Wavefront e clique em **Importar**.
- 3 Configure um proxy do Wavefront. Para obter mais informações, consulte [Instalando e gerenciando proxies do Wavefront](#).

Procedimentos

- 1 Faça login no Centro de Controle do vRealize Orchestrator como **raiz**.
- 2 Selecione a página **Propriedades da Extensão**.
- 3 Selecione a extensão do Wavefront.
- 4 Configure as propriedades do Wavefront.

Opção	Descrição
Proxy	O endereço de proxy do Wavefront.
Host	Opcional. O endereço do host do Wavefront.
Token	Opcional. O token de API do Wavefront. Para obter mais informações sobre como gerar um token de API do Wavefront, consulte Gerando um token de API .
Prefixo	Adicione rótulos de prefixo para cada métrica enviada ao Wavefront. Os rótulos de prefixo são separados por um símbolo de ponto.

- 5 (Opcional) Selecione **Enviar painel padrão na próxima inicialização**.
- 6 Clique em **Salvar**.

Resultados

Você configurou a extensão do Wavefront para vRealize Orchestrator.

Próximo passo

- Para acessar as métricas coletadas pelo Wavefront, acesse o painel no endereço inserido durante a configuração.
- Para obter notificações sobre eventos específicos em seu ambiente do vRealize Orchestrator, você pode usar Alertas do Wavefront. Para obter mais informações, consulte a [documentação de Alertas do Wavefront](#).

Habilitar a sincronização de horário para o vRealize Orchestrator

Você pode habilitar a sincronização de hora em sua implantação do vRealize Orchestrator com a linha de comando do vRealize Orchestrator Appliance.

Você pode configurar a sincronização de hora para a implantação autônoma ou agrupada em cluster do vRealize Orchestrator usando o protocolo de comunicação do Network Time Protocol (NTP). O vRealize Orchestrator é compatível com duas configurações de NTP mutuamente exclusivas:

Configuração de NTP	Descrição
ESXi	<p>Essa configuração pode ser usada quando o servidor ESXi que hospeda o vRealize Orchestrator Appliance está sincronizado com um servidor NTP. Se você estiver usando uma implantação agrupada em cluster, todos os hosts ESXi deverão ser sincronizados com um servidor NTP. Para obter mais informações sobre como configurar o NTP para ESXi, consulte Configurar o Network Time Protocol (NTP) em um host ESXi usando o vSphere Web Client.</p> <hr/> <p>Observação Se a sua implantação do vRealize Orchestrator for migrada para um host ESXi que não está sincronizado com um servidor NTP, você poderá experimentar o descompasso do relógio.</p>
systemd	<p>Essa configuração usa o daemon de systemd-timesyncd para sincronizar os relógios da sua implantação do vRealize Orchestrator.</p> <hr/> <p>Observação Por padrão, o daemon de systemd-timesyncd está ativado, mas configurado sem servidores NTP. Se o vRealize Orchestrator Appliance usar uma configuração de IP dinâmico, o dispositivo poderá usar todos os servidores NTP recebidos pelo protocolo DHCP.</p>

Procedimentos

- 1 Faça login na linha de comando do vRealize Orchestrator Appliance como **raiz**.
- 2 Habilite o NTP com ESXi.
 - a Execute o comando `vracli ntp esxi`.
 - b (Opcional) Para confirmar o status da configuração de NTP, execute o comando `vracli ntp status`.

3 Habilite o NTP com systemd.

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

Observação Você pode adicionar vários servidores NTP systemd separando seus endereços de rede com uma vírgula. Cada endereço de rede deve ser colocado entre aspas simples. Por exemplo, `vracli ntp systemd --set 'ntp_address_1','ntp_address_2'`

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

Resultados

Você ativou a sincronização de hora para sua implantação do vRealize Orchestrator.

Próximo passo

A configuração de NTP poderá falhar se houver uma diferença de tempo de acima 10 minutos entre o servidor NTP e a implantação do vRealize Orchestrator. Para resolver esse problema, reinicie o vRealize Orchestrator Appliance.

Desativar a sincronização de hora para o vRealize Orchestrator

Você pode desativar a sincronização de hora do Network Time Protocol (NTP) na sua implantação do vRealize Orchestrator com a linha de comando do vRealize Orchestrator Appliance.

Você também pode redefinir a configuração de NTP do seu vRealize Orchestrator Appliance para o estado padrão executando o comando `vracli ntp reset`.

Pré-requisitos

Verifique se você configurou a sincronização de hora com o ESXi ou systemd. Consulte o [Habilitar a sincronização de horário para o vRealize Orchestrator](#).

Procedimentos

- 1 Faça login na linha de comando do vRealize Orchestrator Appliance como **raiz**.
- 2 Para desativar a sincronização de hora com o ESXi ou systemd, execute o comando `vracli ntp disable`.
- 3 (Opcional) Para confirmar o status da configuração de NTP, execute o comando `vracli ntp status`.

Configurar o vRealize Orchestrator Kubernetes CIDR

Você pode alterar as máscaras de sub-rede de roteamento entre domínios sem classe (CIDR) do Kubernetes após a implantação.

O vRealize Orchestrator Appliance configura e executa um cluster do Kubernetes. Os pods e os serviços nesse cluster são implantados em sub-redes IPv4 separadas, representadas pelo CIDR do cluster interno e pelo CIDR de serviço interno, respectivamente. Os valores padrão das máscaras de sub-rede definidas durante a implantação do OVF são os seguintes:

Kubernetes network property	Default value	Property description
cluster-cidr	10.244.0.0/22	O CIDR usado para pods em execução no cluster do Kubernetes.
service-cidr	10.244.4.0/22	O CIDR usado para serviços do Kubernetes no cluster do Kubernetes.

Os endereços de rede CIDR padrão podem criar um conflito com redes privadas externas que você possa estar usando. Nesses cenários, você pode alterar a configuração desses valores de CIDR durante ou após a implantação do vRealize Orchestrator Appliance.

Observação Para obter informações sobre como alterar a configuração do CIDR durante a implantação do dispositivo, consulte [Baixar e implantar o vRealize Orchestrator Appliance](#).

Pré-requisitos

- Verifique se os valores de endereço CIDR dão suporte a pelo menos 1024 hosts.
- O CIDR do cluster interno e o CIDR de serviço interno não devem compartilhar o mesmo valor de sub-rede.
- O valor de CIDR de uma das sub-redes não pode incluir o valor que você deseja adicionar à outra sub-rede.

Observação Por exemplo, o valor de `cluster-cidr` não pode ser **10.244.4.0/22** **10.244.4.0/24**, pois isso também incluiria o valor de sub-rede da propriedade `service-cidr`. Cada valor de sub-rede deve ser adicionado separadamente.

Procedimentos

- 1 Faça login no vRealize Orchestrator Appliance como **root**.
- 2 Execute o comando `vracli upgrade exec -y --prepare --profile k8s-subnets`.
- 3 Faça backup da implantação do vRealize Orchestrator tirando um snapshot da máquina virtual (VM). Consulte [Fazer snapshot de uma máquina virtual](#).

Cuidado O vRealize Orchestrator 8.x não é compatível atualmente com instantâneos da memória. Antes de criar o snapshot de sua implantação do vRealize Orchestrator, verifique se a opção **Fazer snapshot da memória de uma máquina virtual** está desativada.

- 4 Altere os valores das sub-redes de CIDR de cluster e CIDR de serviço executando o comando `vracli network k8s-subnets`.

```
vracli network k8s-subnets --cluster-cidr <CIDR_value> --service-cidr <CIDR_value>
```

- 5 Para concluir o processo de configuração do CIDR, execute o comando `vracli upgrade exec`.

Atualizar as configurações de DNS do vRealize Orchestrator

Um administrador pode atualizar as configurações de DNS da implantação do vRealize Orchestrator usando o comando `vracli network dns`.

Pré-requisitos

Verifique se o serviço SSH do vRealize Orchestrator Appliance está ativado. Consulte o [Ativar ou desativar acesso SSH ao vRealize Orchestrator Appliance](#).

Procedimentos

- 1 Faça login na linha de comando do vRealize Orchestrator Appliance pelo SSH como **raiz**.

Observação Para implantações em cluster, faça login no dispositivo de qualquer nó do cluster.

- 2 Para definir novos servidores DNS para sua implantação do vRealize Orchestrator, execute o comando `vracli network dns set`.

```
vracli network dns set --servers DNS1,DNS2
```

- 3 Verifique se os novos servidores DNS estão corretamente aplicados a todos os nós do vRealize Orchestrator executando o comando `vracli network dns status`.
- 4 Para interromper os serviços do vRealize Orchestrator em sua implantação, execute o seguinte conjunto de comandos:

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

- 5 Reinicie os nós do vRealize Orchestrator e aguarde até que eles sejam iniciados completamente.
- 6 Faça login na linha de comando para cada nó do vRealize Orchestrator sobre SSH e verifique se os novos servidores DNS estão listados no arquivo `/etc/resolve.conf`.
- 7 Para iniciar os serviços do vRealize Orchestrator, execute o script `/opt/scripts/deploy.sh` em um dos nós na sua implantação.

Resultados

As configurações de DNS do vRealize Orchestrator são alteradas conforme especificado.

Casos de uso de configuração e solução de problemas

8

Os casos de uso de configuração fornecem fluxos de tarefas que você pode executar para atender aos requisitos de configuração específicos do seu servidor vRealize Orchestrator e aos tópicos de resolução de problemas para entender e resolver um problema.

Este capítulo inclui os seguintes tópicos:

- [Verifique o número da compilação do servidor do vRealize Orchestrator](#)
- [Configurar o plug-in do vRealize Orchestrator para o vSphere Web Client](#)
- [Cancelar fluxos de trabalho em execução](#)
- [Ativar a depuração do servidor do vRealize Orchestrator](#)
- [Redimensionar os discos do vRealize Orchestrator Appliance](#)
- [Como dimensionar o tamanho de memória do heap do servidor do vRealize Orchestrator](#)
- [Recuperação de desastres do vRealize Orchestrator usando o Site Recovery Manager](#)

Verifique o número da compilação do servidor do vRealize Orchestrator

Em determinados cenários, pode ser necessário verificar o número da compilação do servidor de sua implantação do vRealize Orchestrator.

Você pode verificar o número da compilação do servidor do vRealize Orchestrator navegando até https://your_orchestrator_FQDN/vco/api/about. O número da compilação do servidor é exibido nas tags `<ns2:build-number>`.

A verificação do número da compilação do servidor pode ser útil em casos de uso, como o fornecimento de informações adicionais para uma solicitação de suporte (SR) que você registrou no Suporte da VMware. Você também pode verificar o número da compilação do servidor para poder confirmar se o upgrade para a versão mais recente do vRealize Orchestrator foi bem-sucedido.

Configurar o plug-in do vRealize Orchestrator para o vSphere Web Client

Para usar o plug-in do vRealize Orchestrator para o vSphere Web Client, você deve registrar vRealize Orchestrator como uma extensão do vCenter Server.

Depois de registrar o seu servidor vRealize Orchestrator com vCenter Single Sign-On e configurá-lo para funcionar com o vCenter Server, você deve registrar vRealize Orchestrator como uma extensão do vCenter Server.

Pré-requisitos

- Verifique se o acesso SSH está habilitado para o vRealize Orchestrator Appliance. Consulte o [Ativar ou desativar acesso SSH ao vRealize Orchestrator Appliance](#).
- Você deve registrar vRealize Orchestrator com a autenticação vSphere no mesmo Platform Services Controller com o qual o vCenter Server gerenciado se autentica.
- Copie o vco-plugin.zip para o vRealize Orchestrator Appliance:
 - a Faça o download do arquivo vco-plugin.zip do [VMware Technology Network](#).
 - b Abra um cliente SSH.

Observação Para ambientes Linux ou MacOS, você pode usar a interface da linha de comandos do Terminal. Para ambientes do Windows, você pode usar o cliente PuTTY.

- c Para copiar o arquivo vco-plugin.zip, execute o comando de cópia segura.

```
For Linux/MacOS: scp ~/<zip_download_dir>/vco-plugin.zip root@<orchestrator_FQDN_or_IP>:/data/vco/usr/lib/vco/downloads/vco-plugin.zip
```

```
For Windows: pscp C:\<zip_download_dir>\vco-plugin.zip root@<orchestrator_FQDN_or_IP>:/data/vco/usr/lib/vco/downloads/vco-plugin.zip
```

Procedimentos

- 1 Faça login no vRealize Orchestrator Client.
- 2 Vá para **Biblioteca > Fluxos de trabalho**.
- 3 Pesquise por **Registrar o vCenter Orchestrator como um fluxo de trabalho de extensão do vCenter Server** e clique em **Executar**.
- 4 Selecione a instância vCenter Server a ser registrada com o vRealize Orchestrator.
- 5 Insira `https://your_orchestrator_FQDN` ou a URL do serviço do balanceador de carga que redireciona as solicitações para os nós do servidor vRealize Orchestrator.
- 6 Clique em **Executar**.

Cancelar fluxos de trabalho em execução

Você pode usar o Centro de Controle de vRealize Orchestrator para cancelar fluxos de trabalho que não são concluídos corretamente.

Procedimentos

- 1 Faça login no Centro de Controle como **root**.
- 2 Clique em **Solução de Problemas**.
- 3 Cancele os fluxos de trabalho em execução.

Opção	Descrição
Cancelar todas as execuções de fluxo de trabalho	Insira um ID de fluxo de trabalho para cancelar todos os tokens para esse fluxo de trabalho.
Cancelar execuções de fluxo de trabalho por ID	Insira todos os IDs de token que você deseja cancelar. Separe os IDs com uma vírgula.
Cancelar todos os fluxos de trabalho em execução	Cancele todos os fluxos de trabalho em execução no servidor.

Observação As operações nas quais você cancela fluxos de trabalho por ID podem não ter êxito, pois não há maneira confiável de cancelar o segmento de execução imediatamente.

Resultados

Na próxima inicialização do servidor, os fluxos de trabalho são definidos em um estado cancelado.

Ativar a depuração do servidor do vRealize Orchestrator

Você pode iniciar o servidor do vRealize Orchestrator no modo de depuração para depurar problemas ao desenvolver um plug-in.

Pré-requisitos

Instale e configure a ferramenta de linha de comando Kubernetes em sua máquina local. Consulte [Instalar e configurar kubectl](#).

Procedimentos

- 1 Faça login na linha de comando do vRealize Orchestrator Appliance como **raiz**.
- 2 Execute o comando `kubectl -n prelude edit deployment vco-app`.

- 3 Edite o arquivo YAML de implantação adicionando uma variável de ambiente de depuração ao contêiner `vco-server-app`. A variável deve ser adicionada na seção `env` do contêiner `vco-server-app`.

```
containers:
  - command:
    ...
    env:
      - name: DEBUG_PORT
        value: "your_desired_debug_port"
    ...
  name: vco-server-app
  ...
```

Observação Ao adicionar a variável de ambiente de depuração à seção `env`, você deve seguir a formatação de recuo YAML conforme apresentado no exemplo anterior.

- 4 Salve as alterações no arquivo de implantação.
Se a edição para o arquivo de implantação for bem-sucedida, você receberá a mensagem `deployment.extensions/vco-app edited`.
- 5 Gere o arquivo de configuração Kubernetes executando o comando `vracli dev kubeconfig`.
Como o `kubeconfig` é um ambiente de desenvolvedor, você será solicitado a confirmar que deseja continuar. Insira **yes** para continuar ou **no** para parar.
- 6 Copie o conteúdo do arquivo de configuração gerado do `apiVersion: v1` até e incluindo o conteúdo `client-key-data`.
- 7 Salve o arquivo de configuração Kubernetes gerado na sua máquina local.
- 8 Faça logoff do vRealize Orchestrator Appliance.
- 9 Conclua a configuração do modo de depuração na sua máquina local.
 - a Abra um shell de linha de comando.
 - b Vincule a variável de ambiente `KUBECONFIG` ao arquivo de configuração salvo.

Observação Este exemplo se baseia em um ambiente Linux.

```
export KUBECONFIG=/file/path/fileName
```


- c Para validar que os serviços estão em execução, execute o comando `kubectl cluster-info`.
- d Para concluir a configuração do modo de depuração, execute a seguinte solicitação de API do Kubernetes.

Observação O valor da variável `localhost_debug_port` é o conjunto de portas na sua configuração de depuração remota do seu Ambiente de Desenvolvimento Integrado (IDE). O valor da variável `vro_debug_port` é gerado durante a etapa 3 deste procedimento.

```
kubectl port-forward pod/vco_app_pod_ID localhost_debug_port:vro_debug_port
```

Importante Ao configurar sua ferramenta de depuração, forneça as configurações de DNS e IP da máquina local na qual você executou o comando de encaminhamento de porta.

Resultados

Você configurou a depuração de servidor para a sua vRealize Orchestrator Appliance.

Redimensionar os discos do vRealize Orchestrator Appliance

Você pode modificar o tamanho do disco do vRealize Orchestrator Appliance editando as configurações de tamanho do disco da máquina virtual do vRealize Orchestrator Appliance no vSphere.

Pré-requisitos

Verifique se o serviço SSH do vRealize Orchestrator Appliance está ativado. Consulte o [Ativar ou desativar acesso SSH ao vRealize Orchestrator Appliance](#).

Procedimentos

- 1 Verifique o espaço em disco disponível no momento no vRealize Orchestrator Appliance.

Observação Os discos do vRealize Orchestrator Appliance precisam de pelo menos 20% de espaço livre em disco.

- a Faça login na linha de comando do vRealize Orchestrator Appliance pelo SSH como **raiz**.
- b Execute o comando `vracli disk-mgr`.

2 Redimensione o disco da máquina virtual do vRealize Orchestrator Appliance no vSphere.

- Efetue login no vSphere Client como um **administrador**.
- Clique com o botão direito da máquina virtual e selecione **Editar Configurações**.
- Na guia **Hardware Virtual**, expanda o **Disco rígido** para exibir e alterar as configurações do disco, e clique em **OK**.

Para obter mais informações sobre como alterar o tamanho do disco de máquinas virtuais do vSphere, consulte *Alterar configuração do disco virtual na Administração da Máquina Virtual do vSphere*.

3 Acione o redimensionamento automático no Photon OS.

- Faça login na linha de comando do vRealize Orchestrator Appliance pelo SSH como **raiz**.
- Execute o comando `vracli disk-mgr resize`.

Observação Você pode rastrear o progresso do procedimento de redimensionamento de disco em `/var/log/vmware/prelude/disk_resize.log`.

Você redimensionou os discos do vRealize Orchestrator Appliance.

4 Verifique se o procedimento de redimensionamento do disco foi bem-sucedido executando o comando `disk-mgr`.

```
vracli disk-mgr
```

Próximo passo

Para solucionar problemas com o procedimento de redimensionamento do tamanho do disco, consulte [KB 79925](#).

Como dimensionar o tamanho de memória do heap do servidor do vRealize Orchestrator

Você pode dimensionar o tamanho da memória de heap do servidor do vRealize Orchestrator editando o arquivo `values.yaml`.

Você pode ajustar o tamanho da memória de heap do servidor do vRealize Orchestrator, para que seu ambiente de orquestração possa gerenciar as cargas de trabalho alteradas. Por exemplo, você poderá aumentar a memória de heap de sua implantação do vRealize Orchestrator se estiver planejando gerenciar vários servidores vCenter.

Pré-requisitos

- Habilite o acesso SSH para o vRealize Orchestrator Appliance. Consulte o [Ativar ou desativar acesso SSH ao vRealize Orchestrator Appliance](#).

- Aumente a RAM da máquina virtual na qual o vRealize Orchestrator é implantado até o próximo incremento adequado. Para obter informações sobre como aumentar a RAM de uma máquina virtual no vSphere, consulte *Alterar a configuração de memória em Administração da máquina virtual do vSphere*.

Procedimentos

- 1 Faça login na linha de comando do vRealize Orchestrator Appliance pelo SSH como **raiz**.
- 2 Navegue até o diretório `/opt/charts/vco/`.
- 3 Usando o editor preferido, edite o arquivo `values.yaml`.

```
vi values.yaml
```

- 4 Modifique os parâmetros `serverMemoryLimit`, `serverMemoryRequest` e `serverJvmHeapMax` padrão.
 - a Defina o valor de memória do heap editando o parâmetro `serverJvmHeapMax`.
 - b Atualize os valores dos parâmetros `serverMemoryLimit` e `serverMemoryRequest`.

Cuidado O valor do parâmetro `serverMemoryLimit` deve ser 2 Gigabytes maior do que o valor definido no parâmetro `serverJvmHeapMax`. O valor do parâmetro `serverMemoryRequest` deve ser 1 Gigabyte maior do que o valor definido no parâmetro `serverJvmHeapMax`. Veja um exemplo de configuração de memória:

```
serverMemoryLimit: 8G
serverMemoryRequest: 7G
serverJvmHeapMax: 6G
```

Observação Para ambientes agrupados em cluster, execute as etapas anteriores em todos os nós do cluster.

- 5 Salve as alterações no arquivo `values.yaml` e navegue até o diretório `/opt/scripts`.
- 6 Execute o comando `deploy.sh`.

Resultados

Você alterou o tamanho da memória de heap do seu servidor vRealize Orchestrator.

Recuperação de desastres do vRealize Orchestrator usando o Site Recovery Manager

Você deve configurar o Site Recovery Manager para proteger o vRealize Orchestrator. Proteja essa proteção concluindo as tarefas comuns de configuração para o Site Recovery Manager.

Preparar o ambiente

Você deve garantir que atende aos seguintes pré-requisitos antes de começar a configurar o Site Recovery Manager.

- Verifique se o vSphere 6.0 ou posterior está instalado nos sites protegidos e de recuperação.
- Verifique se você está usando o Site Recovery Manager 8.1 ou posterior.
- Verifique se o vRealize Orchestrator foi configurado.

Configurar máquinas virtuais para o vSphere Replication

Você deve configurar as máquinas virtuais para o vSphere Replication ou para replicação baseada em matriz para usar o Site Recovery Manager.

Para ativar o vSphere Replication nas máquinas virtuais necessárias, execute as seguintes etapas.

Procedimentos

- 1 No vSphere Web Client, selecione uma máquina virtual na qual o vSphere Replication deve ser ativado e clique em **Ações > Todas as Ações do vSphere Replication > Configurar a Replicação**.
- 2 Na janela **Tipo de replicação**, selecione **Replicar para um vCenter Server** e clique em **Avançar**.
- 3 Na janela **Site de destino**, selecione o vCenter para o site de recuperação e clique em **Avançar**.
- 4 Na janela **Servidor de Replicação**, selecione um servidor vSphere Replication e clique em **Avançar**.
- 5 Na janela **Local de destino**, clique em **Editar** e selecione o repositório de dados de destino, onde os arquivos replicados serão armazenados e clique em **Avançar**.
- 6 Na janela **Opções de replicação**, mantenha a configuração padrão e clique em **Avançar**.
- 7 Na janela **Configurações de recuperação**, insira a hora para **Objetivo de Ponto de Recuperação (RPO)** e o **Instância de point-in-time** e clique em **Avançar**.
- 8 Na janela **Pronto para ser concluído**, verifique as configurações e clique em **Concluir**.
- 9 Repita essas etapas para todas as máquinas virtuais nas quais o vSphere Replication deve ser ativado.

Criar grupos de proteção

Você cria grupos de proteção para permitir que o Site Recovery Manager proteja suas máquinas virtuais.

Você pode organizar grupos de proteção em pastas. A guia **Grupos de Proteção** exibe os nomes dos grupos de proteção, mas não exibe em qual pasta eles são colocados. Se você tiver dois grupos de proteção com o mesmo nome em pastas diferentes, poderá ser difícil informá-los. Portanto, certifique-se de que os nomes dos grupos de proteção sejam exclusivos em todas as pastas. Em ambientes nos quais nem todos os usuários têm privilégios de exibição para todas as pastas, certifique-se de garantir a exclusividade dos nomes de grupos de proteção. Não coloque grupos de proteção em pastas.

Quando você cria grupos de proteção, aguarde para garantir que as operações sejam concluídas conforme o esperado. Certifique-se de que o Site Recovery Manager crie o grupo de proteção e que a proteção das máquinas virtuais no grupo seja bem-sucedida.

Pré-requisitos

Verifique se você executou uma das seguintes tarefas:

- Incluiu máquinas virtuais em repositórios de dados para os quais você configurou a replicação baseada em matriz.
- Atendeu aos requisitos em *Pré-requisitos para Grupos de Proteção da Política de Armazenamento* e revisou as *Limitações dos Grupos de Proteção da Política de Armazenamento* no guia *Administração do Site Recovery Manager*.
- Configurou o vSphere Replication em suas máquinas virtuais.
- Realizou uma combinação de alguns ou todos os itens acima.

Procedimentos

- 1 No vSphere Client ou vSphere Web Client, clique em **Site Recovery > Abrir Site Recovery**.
- 2 Na guia inicial do Site Recovery, selecione um par de sites e clique em **Exibir Detalhes**.
- 3 Selecione a guia **Grupos de Proteção** e clique em **Novo** para criar um grupo de proteção.
- 4 Na página Nome e direção, insira um nome e uma descrição para o grupo de proteção, selecione uma direção e clique em **Avançar**.
- 5 Na página Tipo de grupo de proteção, selecione o tipo de grupo de proteção e clique em **Avançar**.

Opção	Ação
Criar um grupo de proteção de replicação baseada em matriz	Selecione Grupos de repositório de dados (replicação baseada em matriz) e selecione um par de matrizes.
Criar um grupo de proteção do vSphere Replication	Selecione VMs Individuais (vSphere Replication) .
Criar um grupo de proteção de política de armazenamento	Selecione Políticas de Armazenamento (replicação baseada em matriz) .

- 6 Selecione grupos de repositórios de dados, máquinas virtuais ou políticas de armazenamento para adicionar ao grupo de proteção.

Opção	Ação
Grupos de proteção de replicação baseada em matriz	Selecione grupos de repositório de dados e clique em Avançar . Quando você seleciona um grupo de repositório de dados, as máquinas virtuais que o grupo contém aparecem na tabela Máquinas virtuais.
Grupos de proteção do vSphere Replication	Selecione máquinas virtuais na lista e clique em Avançar . Apenas as máquinas virtuais que você configurou para vSphere Replication e que ainda não estão em um grupo de proteção aparecem na lista.
Grupos de proteção da política de armazenamento	Selecione as políticas de armazenamento na lista e clique em Avançar .

- 7 Na página Plano de recuperação, você pode, opcionalmente, adicionar o grupo de proteção a um plano de recuperação.

Opção	Ação
Adicionar a um plano de recuperação existente	Adiciona o grupo de proteção a um plano de recuperação existente.
Adicionar a um novo plano de recuperação	Adiciona o grupo de proteção a um novo plano de recuperação. Se você selecionar essa opção, deverá inserir um nome de plano de recuperação.
Não adicione ao plano de recuperação agora.	.Selecione essa opção se você não quiser adicionar o grupo de proteção a um plano de recuperação.

- 8 Revise as configurações e clique em **Concluir**.

Você pode monitorar o progresso da criação do grupo de proteção na guia **Grupo de Proteção**.

- Para os grupos de proteção do vSphere Replication e de replicação baseada em matriz, se o Site Recovery Manager aplicou com êxito os mapeamentos de inventário às máquinas virtuais protegidas, o status de proteção do grupo de proteção será *OK*.
- Para grupos de proteção de política de armazenamento, se o Site Recovery Manager protegeu com êxito todas as máquinas virtuais associadas à política de armazenamento, o status de proteção do grupo de proteção será *OK*.
- Para os grupos de proteção do vSphere Replication e de replicação baseada em matriz, se você não tiver configurado os mapeamentos de inventário ou se o Site Recovery Manager não puder aplicá-los, o status de proteção do grupo de proteção será *Não Configurado*.
- Para grupos de proteção de política de armazenamento, se o Site Recovery Manager não puder proteger todas as máquinas virtuais associadas à política de armazenamento, o status de proteção do grupo de proteção será *Não Configurado*.

Próximo passo

Para os grupos de proteção do vSphere Replication e de replicação baseada em matriz, se o status de proteção dos grupos de proteção for *Não Configurado*, aplique os mapeamentos de inventário às máquinas virtuais:

- Para aplicar mapeamentos de inventário em todo o site ou para verificar se os mapeamentos de inventário que você já definiu são válidos, consulte *Configurar Mapeamentos de Inventário* no guia *Administração do Site Recovery Manager*. Para aplicar esses mapeamentos a todas as máquinas virtuais, consulte *Aplicar Mapeamentos de Inventário a Todos os Membros de um Grupo de Proteção* no guia *Administração do Site Recovery Manager*.
- Para aplicar os mapeamentos de inventário a cada máquina virtual no grupo de proteção individualmente, consulte *Configurar Mapeamentos de Inventário para uma Máquina Virtual Individual em um Grupo de Proteção* no guia *Administração do Site Recovery Manager*.

Para grupos de proteção de política de armazenamento, se o status de proteção do grupo de proteção for *Não Configurado*, verifique se você atendeu aos requisitos em *Pré-requisitos para Grupos de Proteção de Política de Armazenamento* e revisou as *Limitações dos Grupos de Proteção de Política de Armazenamento* no guia *Administração do Site Recovery Manager*.

Criar um plano de recuperação

Você cria um plano de recuperação para estabelecer como o Site Recovery Manager recupera as máquinas virtuais.

Procedimentos

- 1 No vSphere Client ou no vSphere Web Client, clique em **Site Recovery > Abrir Site Recovery**.
- 2 Na guia inicial do Site Recovery, selecione um par de sites e clique em **Exibir Detalhes**.
- 3 Selecione a guia **Planos de Recuperação** e clique em **Novo** para criar um plano de recuperação.
- 4 Insira um nome, uma descrição e uma direção para o plano, selecione uma pasta e clique em **Avançar**.
- 5 Selecione o tipo de grupo no menu.

Opção	Descrição
Grupos de proteção para VMs individuais ou grupos de repositórios de dados	Selecione essa opção para criar um plano de recuperação que contenha replicação baseada em matriz e grupos de proteção do vSphere Replication.
Grupos de proteção da política de armazenamento	Selecione essa opção para criar um plano de recuperação que contenha grupos de proteção da política de armazenamento. Se você estiver usando o armazenamento estendido, selecione essa opção.

- 6 Selecione um ou mais grupos de proteção para o plano a ser recuperado e clique em **Avançar**.

- 7 No menu suspenso **Rede de Teste**, selecione uma rede a ser usada durante a recuperação de teste e clique em **Avançar**.

Se não houver mapeamentos em nível de site, a opção padrão **Usar o mapeamento de nível de site** criará uma rede de teste isolada.

- 8 Revise as informações de resumo e clique em **Concluir** para criar o plano de recuperação.

Organizar planos de recuperação em pastas

Para controlar o acesso de diferentes usuários ou grupos aos planos de recuperação, você pode organizar seus planos de recuperação em pastas.

Organizar planos de recuperação em pastas é algo útil se você tiver muitos planos de recuperação. Você pode limitar o acesso aos planos de recuperação colocando-os em pastas e atribuindo permissões diferentes às pastas para diferentes usuários ou grupos. Para obter informações sobre como atribuir permissões a pastas, consulte *Atribuir funções e permissões do Site Recovery Manager* no guia *Administração do Site Recovery Manager*.

Procedimentos

- 1 Na guia inicial do **Site Recovery**, selecione um par de sites e clique em **Exibir Detalhes**.
- 2 Clique na guia **Planos de Recuperação** e, no painel esquerdo, clique com o botão direito do mouse em **Planos de Recuperação** e clique em **Nova Pasta**.
- 3 Insira um nome para a pasta a ser criada e clique em **Adicionar**.
- 4 Adicione planos de recuperação novos ou existentes à pasta.

Opção	Descrição
Criar um novo plano de recuperação	Clique com o botão direito do mouse na pasta e selecione Novo Plano de Recuperação .
Adicionar um plano de recuperação existente	Clique com o botão direito do mouse em um plano de recuperação na árvore de inventário e clique em Mover . Selecione uma pasta de destino e clique em Mover .

Editar um plano de recuperação

Você pode editar um plano de recuperação para alterar as propriedades que você especificou quando o criou. Você pode editar planos de recuperação do site protegido ou do site de recuperação.

Procedimentos

- 1 No vSphere Client ou no vSphere Web Client, clique em **Site Recovery > Abrir Site Recovery**.
- 2 Na guia inicial do **Site Recovery**, selecione um par de sites e clique em **Exibir Detalhes**.
- 3 Clique na guia **Planos de Recuperação**, clique com o botão direito do mouse em um plano de recuperação e clique em **Editar**.

- 4 (Opcional) Altere o nome ou a descrição do plano e clique em **Avançar**.

Não é possível alterar a direção e a localização do plano de recuperação.

- 5 (Opcional) Marque ou desmarque um ou mais grupos de proteção para adicioná-los ou removê-los do plano, e clique em **Avançar**.

- 6 (Opcional) No menu suspenso, selecione uma rede de teste diferente no site de recuperação e clique em **Avançar**.

- 7 Revise as informações de resumo e clique em **Concluir** para fazer as alterações especificadas no plano de recuperação.

Você pode monitorar a atualização do plano no modo de exibição **Tarefas Recentes**.

Configurar propriedades do sistema

9

Você pode definir as propriedades do sistema para alterar o comportamento padrão do Orchestrator.

Este capítulo inclui os seguintes tópicos:

- [Configurar acesso ao sistema de arquivos do servidor para fluxos de trabalho e ações](#)
- [Definir acesso a comandos do sistema operacional para fluxos de trabalho e ações](#)
- [Definir acesso de JavaScript a classes Java](#)
- [Definir propriedade de tempo limite personalizada](#)
- [Adicionando um conector JDBC para o plug-in SQL do vRealize Orchestrator.](#)

Configurar acesso ao sistema de arquivos do servidor para fluxos de trabalho e ações

No vRealize Orchestrator, os fluxos de trabalho e as ações têm acesso limitado a diretórios de sistema de arquivos específicos. Você pode estender o acesso a outras partes do sistema de arquivos do servidor modificando o arquivo de configuração `js-io-rights.conf`.

Regras no arquivo `js-io-rights.conf` que autorizam acesso de gravação ao sistema vRealize Orchestrator

O arquivo `js-io-rights.conf` contém regras que permitem o acesso de gravação a diretórios definidos no sistema de arquivos do servidor.

Conteúdo obrigatório do arquivo `js-io-rights.conf`

Cada linha do arquivo `js-io-rights.conf` deve conter as seguintes informações.

- O sinal de mais (+) ou menos (-) para indicar se os direitos são permitidos ou negados
- Os níveis de direitos de leitura (r), gravação (w) e execução (x)

- O caminho no qual os direitos devem ser aplicados.

Observação A pasta raiz para o arquivo `js-io-rights.conf` é sempre `/var/run/vco`. No sistema de arquivos do vRealize Orchestrator Appliance, essa pasta está localizada em `/data/vco/var/run/vco`. Todo o conteúdo com acesso ao sistema de arquivos do vRealize Orchestrator deve ser mapeado nesta pasta raiz.

Conteúdo padrão do arquivo `js-io-rights.conf`

O conteúdo padrão do arquivo de configuração `js-io-rights.conf` no Orchestrator Appliance é o seguinte:

```
-rwx /
+rwX /var/run/vco
+rx /etc/vco
-rwx /etc/vco/app-server/security/
+rx /var/log/vco/
```

As duas primeiras linhas no arquivo de configuração padrão `js-io-rights.conf` permitem os seguintes direitos de acesso:

-rwx /

Todo o acesso ao sistema de arquivos foi negado.

+rwX /var/run/vco

Ler, gravar e executar o acesso é permitido no diretório `/var/run/vco`.

Regras no arquivo `js-io-rights.conf`

O vRealize Orchestrator resolve os direitos de acesso na ordem em que aparecem no arquivo `js-io-rights.conf`. Cada linha pode substituir as linhas anteriores.

Importante Você pode permitir o acesso a todas as partes do sistema de arquivos, configurando `+rwx /` no arquivo `js-io-rights.conf`. No entanto, isso representa um risco de alta segurança.

Definir acesso do sistema de arquivos do servidor para fluxos de trabalho e ações

Para alterar as partes do sistema de arquivos do servidor que os fluxos de trabalho e a API do vRealize Orchestrator podem acessar, modifique o arquivo de configuração `js-io-rights.conf`. O arquivo `js-io-rights.conf` é criado quando um fluxo de trabalho tenta acessar o sistema de arquivos do servidor do vRealize Orchestrator.

Procedimentos

- 1 Faça login na linha de comando do vRealize Orchestrator Appliance como **raiz**.
- 2 Acesse o diretório `/data/vco/var/run/vco/`.

- 3 Abra o arquivo de configuração `js-io-rights.conf` em um editor de texto.
- 4 Adicione as linhas necessárias ao arquivo `js-io-rights.conf` para permitir ou negar o acesso a áreas do sistema de arquivos.

Por exemplo, a linha a seguir nega os direitos de execução no diretório `/data/vco/var/run/vco/noexec`:

```
-x /data/vco/var/run/vco/noexec
```

`/data/vco/var/run/vco/noexec` retém os direitos de execução, mas `/data/vco/var/run/vco/noexec/bar` não retém. Ambos os diretórios permanecem legíveis e graváveis.

Resultados

Você modificou os direitos de acesso ao sistema de arquivos para fluxos de trabalho e para a API do vRealize Orchestrator.

Definir acesso a comandos do sistema operacional para fluxos de trabalho e ações

A API do vRealize Orchestrator fornece uma classe de script, `Command`, que executa comandos no sistema operacional do host do servidor do vRealize Orchestrator. Para impedir o acesso não autorizado ao host do servidor, por padrão, os aplicativos do vRealize Orchestrator não têm permissão para executar a classe `Command`. Se os aplicativos do vRealize Orchestrator exigirem permissão para executar comandos no sistema operacional do host, você poderá ativar a classe de script `Command`.

Você concede permissão para usar a classe `Command` ao configurar uma propriedade do sistema de configuração do vRealize Orchestrator.

Procedimentos

- 1 Faça login no Centro de Controle como **root**.
- 2 Clique em **Propriedades do Sistema**.
- 3 Clique em **Novo**.
- 4 Na caixa de texto **Chave**, insira **com.vmware.js.allow-local-process**.
- 5 Na caixa de texto **Valor**, insira **true**.
- 6 Na caixa de texto **Descrição**, insira uma descrição para a propriedade do sistema.
- 7 Clique em **Adicionar**.
- 8 Clique em **Salvar alterações** no menu pop-up.
Uma mensagem indica que você salvou com sucesso.
- 9 Aguarde até que o servidor do vRealize Orchestrator seja reiniciado.

Resultados

Você concedeu permissões para os aplicativos do vRealize Orchestrator executarem comandos locais no sistema operacional do host do servidor do vRealize Orchestrator.

Observação Ao definir a propriedade do sistema `com.vmware.js.allow-local-process` como `true`, você permite que a classe de script `Command` grave em qualquer lugar no sistema de arquivos. Essa propriedade substitui quaisquer permissões de acesso do sistema de arquivos que você define no arquivo `js-io-rights.conf` apenas para a classe de script `Command`. As permissões de acesso do sistema de arquivos que você define no arquivo `js-io-rights.conf` ainda se aplicam a todas as classes de script diferentes de `Command`.

Definir acesso de JavaScript a classes Java

Por padrão, o vRealize Orchestrator restringe o acesso de JavaScript a um conjunto limitado de classes Java. Se você precisar de acesso de JavaScript a um intervalo maior de classes Java, deverá definir uma propriedade de sistema do vRealize Orchestrator.

Permitir o acesso completo do mecanismo de JavaScript à máquina virtual Java (JVM) apresenta problemas de segurança em potencial. Scripts malformados ou maliciosos podem ter acesso a todos os componentes do sistema aos quais o usuário que executa o servidor do vRealize Orchestrator tem acesso. Portanto, por padrão, o mecanismo de JavaScript do vRealize Orchestrator pode acessar apenas as classes no pacote `java.util.*`.

Se você precisar de acesso de JavaScript a classes fora do pacote `java.util.*`, poderá listar em um arquivo de configuração os pacotes Java aos quais deve permitir o acesso de JavaScript. Em seguida, defina a propriedade do sistema `com.vmware.scripting.rhino-class-shutter-file` para apontar para este arquivo.

Procedimentos

- 1 Crie um arquivo de configuração de texto para armazenar a lista de pacotes Java aos quais deve permitir o acesso de JavaScript.

Por exemplo, para permitir o acesso de JavaScript a todas as classes no pacote `java.net` e à classe `java.lang.Object`, adicione o seguinte conteúdo ao arquivo.

```
java.net.*
java.lang.Object
```

- 2 Insira um nome para o arquivo de configuração.
- 3 Salve o arquivo de configuração em um subdiretório de `/data/vco/usr/lib/vco`.

Observação O arquivo de configuração não pode ser salvo em outro diretório.

- 4 Faça login no Centro de Controle como **root**.
- 5 Clique em **Propriedades do Sistema**.

- 6 Clique em **Novo**.
- 7 Na caixa de texto **Chave**, insira **com.vmware.scripting.rhino-class-shutter-file**.
- 8 Na caixa de texto **Valor**, insira `vco/usr/lib/vco/subdiretorio_seu_arquivo_configuracao`.
- 9 Na caixa de texto **Descrição**, insira uma descrição para a propriedade do sistema.
- 10 Clique em **Adicionar**.
- 11 Clique em **Salvar alterações** no menu pop-up.
Uma mensagem indica que você salvou com sucesso.
- 12 Aguarde até que o servidor do vRealize Orchestrator seja reiniciado.

Resultados

O mecanismo de JavaScript tem acesso às classes Java que você especificou.

Definir propriedade de tempo limite personalizada

Quando o vCenter Server está sobrecarregado, demora mais tempo para retornar a resposta ao servidor do vRealize Orchestrator do que os 20.000 milissegundos definidos por padrão. Para evitar essa situação, você deve modificar o arquivo de configuração do vRealize Orchestrator para aumentar o período de tempo limite padrão.

Se o período de tempo limite padrão expirar antes da conclusão de determinadas operações, o log do servidor do vRealize Orchestrator conterá erros.

```
Operation 'getPropertyContent' total time : '5742228' for 1823 calls, mean time :
'3149.0', min time : '0', max time : '32313' Timeout, unable to get property 'info'
com.vmware.vmo.plugin.vi4.model.TimeoutException
```

Procedimentos

- 1 Faça login no Centro de Controle como **root**.
- 2 Clique em **Propriedades do Sistema**.
- 3 Clique em **Novo**.
- 4 Na caixa de texto **Chave**, insira **com.vmware.vmo.plugin.vi4.waitUpdatesTimeout**.
- 5 Na caixa de texto **Valor**, insira o novo período de tempo limite em milissegundos.
- 6 (Opcional) Na caixa de texto **Descrição**, insira uma descrição para a propriedade do sistema.
- 7 Clique em **Adicionar**.
- 8 Clique em **Salvar alterações** no menu pop-up.
Uma mensagem indica que você salvou com sucesso.
- 9 Reinicie o servidor do Orchestrator.

Resultados

O valor que você define substitui a configuração padrão de tempo limite de 20.000 milissegundos.

Adicionando um conector JDBC para o plug-in SQL do vRealize Orchestrator.

Este exemplo demonstra como você pode adicionar um conector MySQL para o plug-in SQL do vRealize Orchestrator.

Procedimentos

- 1 Adicione o arquivo connector.jar do MySQL ao vRealize Orchestrator Appliance.
 - a Faça login na linha de comando do vRealize Orchestrator Appliance pelo SSH como **raiz**.
 - b Vá para o diretório `/data/vco/var/run/vco`.

```
cd /data/vco/var/run/vco
```

- c Crie um diretório `plugins/SQL/lib/`.

```
mkdir -p plugins/SQL/lib/
```

- d Copie o seu arquivo connector.jar do MySQL da sua máquina local para o diretório `/data/vco/var/run/vco/plugins/SQL/lib/` executando um comando de cópia segura (SCP).

```
scp ~/local_machine_dir/your_mysql_connector.jar root@orchestrator_FQDN_or_IP:/data/vco/var/run/vco/plugins/SQL/lib/
```

Observação Você também pode usar métodos alternativos para copiar o arquivo connector.jar para o vRealize Orchestrator Appliance, como PSCP.

- 2 Adicione a nova propriedade MySQL ao Centro de Controle.
 - a Faça login no Centro de Controle como **raiz**.
 - b Selecione **Propriedades do Sistema**.
 - c Clique em **Novo**.
 - d Em **Chave**, insira `o11n.plugin.SQL.classpath`.

- e Em **Valor**, insira `/var/run/vco/plugins/SQL/lib/your_mysql_connector.jar`.

Observação A caixa de texto do valor pode incluir vários conectores JDBC. Cada conector JDBC é separado por um ponto-e-vírgula (;). Por exemplo:

```
/var/run/vco/plugins/SQL/lib/your_mysql_connector.jar;/var/run/vco/plugins/SQL/lib/your_mssql_connector.jar;/var/run/vco/plugins/SQL/lib/your_other_connector.jar
```

- f (Opcional) Insira uma descrição para a propriedade do sistema MySQL.
- g Clique em **Adicionar** e aguarde o servidor vRealize Orchestrator ser reiniciado.

Observação Não salve o seu arquivo connector.jar do JDBC em outro diretório e não configure um valor diferente para a propriedade `o11n.plugin.SQL.classpath`. Fazer isso torna o conector JDBC indisponível para a sua implantação do vRealize Orchestrator.

Aonde ir a partir daqui

10

Quando você tem o vRealize Orchestrator instalado e configurado, pode usar o vRealize Orchestrator para automatizar os processos repetidos com frequência relacionados ao gerenciamento do ambiente virtual.

- Faça login no vRealize Orchestrator Client, execute e agende fluxos de trabalho nos objetos de inventário do vCenter Server ou em outros objetos que o vRealize Orchestrator acessa por meio dos plug-ins. Consulte *Usar o Cliente VMware vRealize Orchestrator*.
- Duplique e modifique os fluxos de trabalho padrão do vRealize Orchestrator e escreva suas próprias ações e fluxos de trabalho para automatizar operações no vCenter Server.
- Para estender a funcionalidade da plataforma do vRealize Orchestrator, desenvolva os plug-ins.
- Gerencie seu inventário do vRealize Orchestrator em várias instâncias do vRealize Orchestrator com a integração de um repositório remoto do Git. Consulte *Usar Cliente VMware vRealize Orchestrator*.
- Execute fluxos de trabalho em seus objetos de inventário do vSphere usando o vSphere Web Client.