

Installazione e configurazione di VMware vRealize Orchestrator

06 OTTOBRE 2020
vRealize Orchestrator 8.2

È possibile trovare la documentazione tecnica più aggiornata sul sito Web di VMware all'indirizzo:

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

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

VMware, Inc.
Centro Leoni Palazzo A
Via Spadolini 5
Ground Floor
Milan, MI 20121
tel: +39 02 30412700
fax: +39 02 30412701
www.vmware.com/it

Copyright © 2008-2020 VMware, Inc. Tutti i diritti sono riservati. [Informazioni sul copyright e sui marchi](#)

Sommario

Installazione e configurazione di VMware vRealize Orchestrator 6

1 Introduzione a VMware vRealize Orchestrator 7

Funzionalità principali della piattaforma di Orchestrator 7

Ruoli utente di vRealize Orchestrator 9

Architettura di vRealize Orchestrator 11

Plug-in di vRealize Orchestrator 11

2 Requisiti di sistema di vRealize Orchestrator 13

Requisiti hardware per vRealize Orchestrator Appliance 13

Browser supportati da vRealize Orchestrator 13

Database di vRealize Orchestrator 14

Componenti di vRealize Orchestrator Appliance 14

Livello di internazionalizzazione e supporto della localizzazione 14

Porte ed endpoint di vRealize Orchestrator 15

3 Configurazione dei componenti di vRealize Orchestrator 17

Configurazione di vCenter Server 17

Metodi di autenticazione 18

4 Installazione di vRealize Orchestrator 19

Download e distribuzione di vRealize Orchestrator Appliance 19

Accensione di vRealize Orchestrator Appliance e apertura della pagina iniziale 21

Modifica della durata della password root 21

Abilitazione o disabilitazione dell'accesso SSH a vRealize Orchestrator Appliance 21

5 Configurazione iniziale 23

Configurazione di un server vRealize Orchestrator autonomo 23

Configurazione di un server vRealize Orchestrator autonomo con l'autenticazione di vRealize Automation 23

Configurazione di un server vRealize Orchestrator autonomo con l'autenticazione di vSphere 25

Abilitazione delle funzionalità di vRealize Orchestrator con le licenze 26

Connessione al database di vRealize Orchestrator 27

Gestione dei certificati 27

Gestione dei certificati di vRealize Orchestrator 27

Configurazione dei plug-in di vRealize Orchestrator 32

Gestione dei plug-in di vRealize Orchestrator 32

Installazione o aggiornamento di un plug-in di vRealize Orchestrator	33
Eliminazione di un plug-in	33
Disponibilità e scalabilità di vRealize Orchestrator	34
Configurazione di un cluster di vRealize Orchestrator	34
Rimozione di un nodo del cluster di vRealize Orchestrator	36
Scalabilità orizzontale di una distribuzione di vRealize Orchestrator autonoma	37
Monitoraggio di un cluster di vRealize Orchestrator	38
Configurazione di Analisi utilizzo software	39
Categorie di informazioni ricevute da VMware	39
Partecipazione o uscita dal programma Analisi utilizzo software	39
6 Utilizzo dei servizi dell'API di vRealize Orchestrator	40
Gestione dei certificati SSL tramite REST API	40
Eliminazione di un certificato TLS mediante REST API	41
Importazione di certificati TLS tramite REST API	41
Creazione di un keystore mediante REST API	42
Eliminazione di un keystore mediante REST API	43
Aggiunta di una chiave tramite REST API	43
7 Opzioni di configurazione aggiuntive	45
Riconfigurazione dell'autenticazione	45
Modifica del provider di autenticazione	45
Modifica dei parametri di autenticazione	46
Configurazione delle proprietà di esecuzione dei workflow	46
File di registro di vRealize Orchestrator	47
Persistenza della registrazione	47
Configurazione dei registri di vRealize Orchestrator	48
Configurazione dell'integrazione della registrazione con vRealize Log Insight	48
Creazione o sovrascrittura di un'integrazione syslog in vRealize Orchestrator	49
Abilitazione della registrazione del debug di Kerberos	51
Abilitazione delle estensioni OpenTracing e Wavefront	52
Configurazione dell'estensione OpenTracing	52
Configurazione dell'estensione Wavefront	53
Abilitazione della sincronizzazione dell'ora per vRealize Orchestrator	54
Disabilitazione della sincronizzazione dell'ora per vRealize Orchestrator	56
8 Casi d'uso di configurazione e risoluzione dei problemi	57
Configurazione del plug-in vRealize Orchestrator per vSphere Web Client	57
Annullamento dei workflow in esecuzione	58
Abilitazione del debug del server vRealize Orchestrator	59
Ridimensionamento dei dischi di vRealize Orchestrator Appliance	61

Come scalare le dimensioni della memoria heap del server vRealize Orchestrator	61
Ripristino di emergenza di vRealize Orchestrator mediante Site Recovery Manager	63
Configurazione delle macchine virtuali per vSphere Replication	64
Creazione di gruppi di protezione	64
Creazione di un piano di ripristino	67
Organizzazione dei piani di ripristino in cartelle	68
Modifica di un piano di ripristino	68

9 Impostazione delle proprietà di sistema 70

Impostazione dell'accesso al file system del server per workflow e azioni	70
Regole del file js-io-rights.conf che consentono l'accesso in scrittura al sistema vRealize Orchestrator	70
Impostazione dell'accesso al file system del server per workflow e azioni	71
Impostazione dell'accesso ai comandi del sistema operativo per workflow e azioni	72
Impostazione dell'accesso di JavaScript alle classi Java	73
Impostazione della proprietà del timeout personalizzato	74
Aggiunta di un connettore JDBC per il plug-in SQL di vRealize Orchestrator	75

10 Operazioni successive 77

Installazione e configurazione di VMware vRealize Orchestrator

Installazione e configurazione di VMware vRealize Orchestrator include informazioni e istruzioni sull'installazione e la configurazione di VMware® vRealize Orchestrator.

Destinatari

Queste informazioni sono destinate ad amministratori di vSphere avanzati e amministratori di sistema esperti che hanno familiarità con la tecnologia delle macchine virtuali e le operazioni dei data center.

Introduzione a VMware vRealize Orchestrator

1

VMware vRealize Orchestrator è una piattaforma di automazione dello sviluppo e dei processi che offre una libreria di workflow estendibili che consentono di creare ed eseguire processi automatizzati e configurabili per gestire i prodotti VMware, nonché altre tecnologie di terze parti.

vRealize Orchestrator consente di automatizzare le attività gestionali e operative delle applicazioni di VMware e di terze parti, come i Service Desk, i sistemi di gestione delle modifiche e i sistemi di gestione degli asset IT.

Questo capitolo include i seguenti argomenti:

- [Funzionalità principali della piattaforma di Orchestrator](#)
- [Ruoli utente di vRealize Orchestrator](#)
- [Architettura di vRealize Orchestrator](#)
- [Plug-in di vRealize Orchestrator](#)

Funzionalità principali della piattaforma di Orchestrator

vRealize Orchestrator è composto da tre livelli distinti, ovvero una piattaforma di orchestrazione che fornisce le funzionalità comuni richieste per uno strumento di orchestrazione, un'architettura di plug-in per integrare il controllo dei sottosistemi e una libreria di workflow. vRealize Orchestrator è una piattaforma aperta che può essere estesa con nuovi plug-in e contenuti e può essere integrata in architetture più grandi tramite una REST API.

vRealize Orchestrator include diverse funzionalità chiave che consentono di eseguire e gestire i workflow.

Persistenza

Un database PostgreSQL a livello di produzione viene utilizzato per archiviare le informazioni pertinenti, ad esempio processi, stati dei workflow e la configurazione di vRealize Orchestrator.

Gestione centralizzata

vRealize Orchestrator fornisce uno strumento centrale per gestire i processi. La piattaforma basata su server delle applicazioni, con la cronologia delle versioni completa, può archiviare

script e primitive correlate al processo nello stesso percorso di storage. In questo modo, è possibile evitare script senza un adeguato controllo delle versioni e delle modifiche sui server.

Punti di controllo

Ogni passaggio di un workflow viene salvato nel database, che impedisce la perdita dei dati se è necessario riavviare il server. Questa funzionalità è particolarmente utile per i processi con esecuzione prolungata.

Centro di controllo

Centro di controllo è un portale basato sul Web che aumenta l'efficienza amministrativa delle istanze di vRealize Orchestrator offrendo un'interfaccia amministrativa centralizzata per le operazioni di runtime, il monitoraggio dei workflow e la correlazione tra le esecuzioni dei workflow e le risorse di sistema.

Controllo delle versioni

Tutti gli oggetti della piattaforma di vRealize Orchestrator hanno una cronologia delle versioni associata. La cronologia delle versioni è utile per la gestione delle modifiche di base durante la distribuzione dei processi nelle fasi o nelle posizioni dei progetti.

Integrazione Git

Con vRealize Orchestrator Client, è possibile integrare un repository Git per migliorare ulteriormente il controllo della versione e dell'origine dei contenuti di vRealize Orchestrator. Con Git, è possibile gestire lo sviluppo del workflow su più istanze di vRealize Orchestrator. Vedere *Utilizzo di Git con vRealize Orchestrator Client* nella guida *Utilizzo di VMware vRealize Orchestrator Client*.

Motore di script

Il motore JavaScript Mozilla Rhino offre un modo per creare blocchi predefiniti per la piattaforma di vRealize Orchestrator Client. Il motore di script è stato potenziato con il controllo delle versioni di base, il controllo del tipo di variabile, la gestione dello spazio dei nomi e la gestione delle eccezioni. Il motore può essere utilizzato nei seguenti blocchi predefiniti:

- Azioni
- Workflow
- Criteri

Motore di workflow

Il motore di workflow consente di automatizzare i processi aziendali. Utilizza gli oggetti seguenti per creare un'automazione dettagliata del processo nei workflow:

- Workflow e azioni che vRealize Orchestrator Client fornisce.
- Blocchi predefiniti personalizzati creati dal cliente.
- Oggetti che i plug-in aggiungono a vRealize Orchestrator Client.

Utenti, altri workflow, pianificazioni o criteri possono avviare i workflow.

Motore dei criteri

È possibile utilizzare il motore dei criteri per monitorare e generare eventi che reagiscono alle modifiche delle condizioni nel server di vRealize Orchestrator Client o in una tecnologia inserita. I criteri possono aggregare gli eventi dalla piattaforma o dai plug-in. Ciò consente di gestire le modifiche delle condizioni su una qualsiasi delle tecnologie integrate.

vRealize Orchestrator Client

È possibile creare, eseguire, modificare e monitorare i workflow con vRealize Orchestrator Client. È inoltre possibile utilizzare vRealize Orchestrator Client per gestire gli elementi azione, configurazione, criterio e risorsa. Vedere *Utilizzo di vRealize Orchestrator Client*.

Sviluppo e risorse

La pagina di destinazione di vRealize Orchestrator consente di accedere rapidamente alle risorse per poter sviluppare i propri plug-in, da utilizzare in vRealize Orchestrator. Sono inoltre disponibili informazioni sull'utilizzo della REST API di vRealize Orchestrator per inviare richieste al server di vRealize Orchestrator.

Sicurezza

vRealize Orchestrator offre le seguenti funzionalità di sicurezza avanzate:

- Infrastruttura a chiave pubblica (PKI) per la firma e la crittografia dei contenuti importati ed esportati tra i server.
- Digital Rights Management (DRM) per controllare il modo in cui i contenuti esportati possono essere visualizzati, modificati e ridistribuiti.
- Transport Layer Security (TLS) per fornire comunicazioni crittografate tra vRealize Orchestrator Client, il server di vRealize Orchestrator e l'accesso HTTPS al front-end Web.
- Gestione dei diritti di accesso avanzata per fornire il controllo dell'accesso ai processi e agli oggetti manipolati dai processi.

Crittografia

vRealize Orchestrator utilizza uno standard AES (Advanced Encryption Standard) compatibile con FIPS con una chiave di crittografia a 256 bit per la crittografia delle stringhe. La chiave di crittografia viene generata casualmente ed è univoca per tutte le appliance che non fanno parte di un cluster. Tutti i nodi di un cluster condividono una chiave di crittografia.

Ruoli utente di vRealize Orchestrator

vRealize Orchestrator fornisce diversi strumenti e interfacce in base alle responsabilità specifiche dei ruoli utente globali. In vRealize Orchestrator possono essere presenti utenti che dispongono di diritti completi, che fanno parte del gruppo di amministratori (**amministratori**), sviluppatori (**sviluppatori di workflow**) e utenti con accesso limitato.

Ruoli e responsabilità di vRealize Orchestrator

I ruoli utente di vRealize Orchestrator vengono gestiti nel menu **Gestione ruoli** di vRealize Orchestrator Client. Per ulteriori informazioni sulla configurazione dei ruoli utente in vRealize Orchestrator Client, vedere *Assegnazione di ruoli in vRealize Orchestrator Client* nella guida *Utilizzo di VMware vRealize Orchestrator Client*.

Nota Per le distribuzioni di vRealize Orchestrator autenticate con vRealize Automation o utilizzando una licenza di vRealize Automation, i ruoli utente vengono assegnati al servizio Gestione identità e accessi della piattaforma di vRealize Automation. Vedere *Configurazione dei ruoli di vRealize Orchestrator Client in vRealize Automation* in *Utilizzo di VMware vRealize Orchestrator Client*.

Amministratore

Questo utente dispone dell'accesso completo a tutte le funzionalità e i contenuti della piattaforma di vRealize Orchestrator, inclusi i contenuti creati da gruppi specifici. Le responsabilità principali dell'utente amministratore includono:

- Installazione e configurazione di vRealize Orchestrator.
- Aggiunta di utenti a vRealize Orchestrator Client, assegnazione di ruoli, nonché creazione ed eliminazione di gruppi. Vedere *Creazione di gruppi in vRealize Orchestrator Client* in *Utilizzo di VMware vRealize Orchestrator Client*.
- Creazione di un'integrazione con un repository Git per gli sviluppatori nel proprio ambiente di vRealize Orchestrator. Vedere *Configurazione di una connessione a un repository Git* in *Utilizzo di VMware vRealize Orchestrator Client*.
- Risoluzione dei problemi relativi all'ambiente di vRealize Orchestrator tramite funzionalità come la convalida del workflow e il debug degli script del workflow.

Sviluppatore di workflow

Questo utente può estendere la funzionalità della piattaforma di vRealize Orchestrator mediante la creazione e la modifica di oggetti. Gli sviluppatori di workflow non possono accedere alle funzionalità amministrative e di risoluzione dei problemi di vRealize Orchestrator Client. Le responsabilità principali dello sviluppatore di workflow includono:

- Creazione, modifica, esecuzione ed eliminazione di oggetti di vRealize Orchestrator come workflow, azioni, criteri ed elementi di configurazione.
- Pianificazione delle esecuzioni dei workflow. Vedere *Pianificazione di workflow in vRealize Orchestrator Client* in *Utilizzo di VMware vRealize Orchestrator Client*.
- Aggiunta di contenuti creati dallo sviluppatore del workflow ai gruppi a cui è assegnato.
- Push delle modifiche locali all'inventario dei contenuti di vRealize Orchestrator nel repository Git di connessione. Vedere *Push delle modifiche in un repository Git* in *Utilizzo di VMware vRealize Orchestrator Client*.

Utenti con diritti limitati

Gli utenti a cui non è assegnato alcun ruolo possono comunque accedere a vRealize Orchestrator Client, ma hanno accesso limitato alle funzionalità e ai contenuti del client. Se un utente con diritti limitati è assegnato a un gruppo, può visualizzare ed eseguire i contenuti inclusi in tale gruppo.

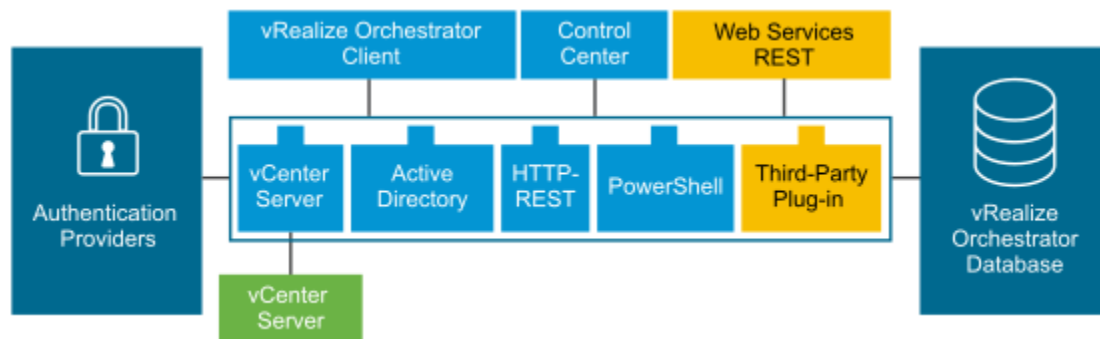
Architettura di vRealize Orchestrator

vRealize Orchestrator contiene una libreria di workflow e un motore di workflow per consentire la creazione e l'esecuzione di workflow che automatizzano i processi di orchestrazione. È possibile eseguire i workflow negli oggetti di tecnologie diverse a cui vRealize Orchestrator accede tramite una serie di plug-in.

vRealize Orchestrator fornisce un set di plug-in standard, incluso un plug-in per vCenter Server, per consentire l'orchestrazione delle attività nei vari ambienti che i plug-in espongono.

vRealize Orchestrator fornisce anche un'architettura aperta per il plug-in di applicazioni esterne di terze parti nella piattaforma di orchestrazione. È possibile eseguire workflow negli oggetti delle tecnologie collegate con plug-in definiti dall'utente. vRealize Orchestrator si connette a un provider di autenticazione per gestire gli account utente e a un database PostgreSQL preconfigurato per archiviare le informazioni dei workflow che esegue. È possibile accedere a vRealize Orchestrator, agli oggetti che espone e ai workflow di vRealize Orchestrator tramite vRealize Orchestrator Client o i servizi Web. Il monitoraggio e la configurazione dei workflow e dei servizi di vRealize Orchestrator vengono eseguiti tramite vRealize Orchestrator Client e il Centro di controllo.

Figura 1-1. Architettura di VMware vRealize Orchestrator



Plug-in di vRealize Orchestrator

I plug-in consentono di utilizzare vRealize Orchestrator per accedere alle tecnologie e alle applicazioni esterne, nonché controllarle. Esponendo una tecnologia esterna in un plug-in di vRealize Orchestrator è possibile incorporare oggetti e funzioni in workflow che accedono agli oggetti e alle funzioni di tale tecnologia esterna.

Le tecnologie esterne alle quali è possibile accedere mediante i plug-in includono strumenti di gestione della virtualizzazione, sistemi email, database, servizi di directory, e interfacce di controllo remoto.

vRealize Orchestrator fornisce un set di plug-in standard che è possibile utilizzare per incorporare in workflow tali tecnologie come l'API di VMware vCenter Server e le funzionalità email. Utilizzando i plug-in, è possibile automatizzare la consegna di nuovi servizi IT o adattare le funzionalità dei servizi dell'infrastruttura e dell'applicazione esistenti. È inoltre possibile utilizzare l'architettura aperta dei plug-in di vRealize Orchestrator per sviluppare plug-in per accedere ad altre applicazioni.

I plug-in di vRealize Orchestrator sviluppati da VMware vengono distribuiti come file .vmoapp. Per ulteriori informazioni sui plug-in di vRealize Orchestrator sviluppati e distribuiti da VMware, vedere [Plug-in esterni di vRealize Orchestrator](#). Per ulteriori informazioni sui plug-in di vRealize Orchestrator di terze parti, vedere [VMware Solution Exchange](#).

Requisiti di sistema di vRealize Orchestrator

2

Il sistema deve soddisfare i requisiti tecnici necessari affinché vRealize Orchestrator funzioni correttamente.

Per un elenco delle versioni supportate di vCenter Server, vSphere Web Client, vRealize Automation e altre soluzioni VMware, vedere [Matrice di interoperabilità dei prodotti VMware](#).

Questo capitolo include i seguenti argomenti:

- [Requisiti hardware per vRealize Orchestrator Appliance](#)
- [Browser supportati da vRealize Orchestrator](#)
- [Database di vRealize Orchestrator](#)
- [Componenti di vRealize Orchestrator Appliance](#)
- [Livello di internazionalizzazione e supporto della localizzazione](#)
- [Porte ed endpoint di vRealize Orchestrator](#)

Requisiti hardware per vRealize Orchestrator Appliance

vRealize Orchestrator Appliance è una macchina virtuale basata su Photon preconfigurata che viene eseguita in contenitori. Prima di distribuire l'appliance, verificare che il sistema soddisfi i requisiti hardware minimi.

vRealize Orchestrator Appliance ha i seguenti requisiti hardware:

- 4 CPU
- 12 GB di memoria
- Disco rigido di 200 GB

Non ridurre le dimensioni predefinite della memoria, perché il server vRealize Orchestrator richiede almeno 8 GB di memoria libera.

Browser supportati da vRealize Orchestrator

Verificare che i browser supportino vRealize Orchestrator.

Per accedere a vRealize Orchestrator Client e al Centro di controllo, è necessario utilizzare uno dei seguenti browser:

- Microsoft Edge
- Mozilla Firefox
- Google Chrome

Database di vRealize Orchestrator

Il server di vRealize Orchestrator include un database PostgreSQL preconfigurato che è pronto per la produzione.

Componenti di vRealize Orchestrator Appliance

vRealize Orchestrator Appliance è un'appliance virtuale basata su Photon che viene eseguita in contenitori.

vRealize Orchestrator Appliance include i seguenti componenti:

- Livello Kubernetes di un'infrastruttura.
- Database PostgreSQL preconfigurato.
- Servizi di vRealize Orchestrator di base, ovvero il servizio del server, il servizio del Centro di controllo e il servizio dell'interfaccia utente di orchestrazione.

La configurazione predefinita del database di vRealize Orchestrator Appliance è pronta per la produzione.

Nota Per utilizzare vRealize Orchestrator Appliance in un ambiente di produzione, è necessario configurare il server di vRealize Orchestrator per l'autenticazione tramite vRealize Automation o vSphere. Vedere [Configurazione di un server vRealize Orchestrator autonomo](#).

Livello di internazionalizzazione e supporto della localizzazione

Il Centro di controllo di vRealize Orchestrator e vRealize Orchestrator Client includono il supporto per i sistemi operativi non in lingua inglese, la formattazione dei dati non in lingua inglese e il supporto multilingue per l'interfaccia utente del Centro di controllo e del client.

Il Centro di controllo di vRealize Orchestrator e vRealize Orchestrator Client supportano l'utilizzo di sistemi operativi non in lingua inglese, di input e output non in lingua inglese, nonché della formattazione non in lingua inglese di dati come date, orari e numeri.

Le interfacce utente di vRealize Orchestrator e vRealize Orchestrator Client sono localizzate nelle lingue seguenti:

- Spagnolo

- Francese
- Tedesco
- Cinese tradizionale
- Cinese semplificato
- Coreano
- Giapponese
- Italiano
- Olandese
- Portoghese (Brasile)
- Russo

Porte ed endpoint di vRealize Orchestrator

Il servizio Kubernetes di vRealize Orchestrator include due endpoint e diverse porte di rete principali.

Porte ed endpoint di rete di vRealize Orchestrator

È possibile accedere a vRealize Orchestrator tramite la porta 443. La porta 443 è protetta con un certificato autofirmato che viene generato durante l'installazione e non può essere sostituito dall'utente. Quando si utilizza un bilanciamento del carico esterno, deve essere configurato per eseguire il bilanciamento nella porta 443.

Protocollo	Numero di porta	Descrizione
TCP	22	Porta utilizzata per accedere a vRealize Orchestrator Appliance tramite SSH.
TCP	443	Porta utilizzata per accedere a vRealize Orchestrator.
TCP	2379	Porta interna utilizzata dall'archivio chiave-valore etcd.
TCP	2380	Porta interna utilizzata dall'archivio chiave-valore etcd.
TCP	6443	Porta interna utilizzata dal server API kube-apiserver.
TCP	8008	Porta interna utilizzata dal proxy di rete kube-proxy.
TCP	10250	Porta utilizzata dall'agente kubelet.
TCP	16000	Porta interna.
TCP	20849	Porta interna.

Protocollo	Numero di porta	Descrizione
TCP	30333	Porta interna utilizzata dal servizio mitm proxy.
TCP	30821	Porta interna.
TCP	31090	Porta interna.
UDP	500	Porta interna utilizzata dal servizio del traffico IKE (Internal Key Exchange).
UDP	4500	Porta interna utilizzata dal servizio NAT (Network Address Transition).
UDP	8285	Porta interna utilizzata dal proxy di rete kube-proxy.

È possibile accedere ai servizi di vRealize Orchestrator Client e al Centro di controllo negli endpoint seguenti:

`https://your_orchestrator_FQDN/orchestration-ui`

`https://your_orchestrator_FQDN/vco-controlcenter`

Configurazione dei componenti di vRealize Orchestrator

3

Quando si scarica e distribuisce vRealize Orchestrator Appliance, il server di vRealize Orchestrator è preconfigurato. Dopo la distribuzione, i servizi vengono avviati automaticamente.

Per migliorare la disponibilità e la scalabilità della configurazione di vRealize Orchestrator, attenersi alle seguenti linee guida:

- Installare e configurare un provider di autenticazione e configurare vRealize Orchestrator in modo che funzioni con il provider. Vedere [Configurazione di un server vRealize Orchestrator autonomo](#).
- Per gli ambienti di vRealize Orchestrator in cluster, installare e configurare un server di bilanciamento del carico e configurarlo per distribuire il carico di lavoro tra i server di vRealize Orchestrator.

Questo capitolo include i seguenti argomenti:

- [Configurazione di vCenter Server](#)
- [Metodi di autenticazione](#)

Configurazione di vCenter Server

Se si aumenta il numero di istanze di vCenter Server nella configurazione di vRealize Orchestrator, vRealize Orchestrator deve gestire più sessioni. Troppe sessioni attive possono causare il timeout di vRealize Orchestrator quando si verificano più di 10 connessioni di vCenter Server.

Per un elenco delle versioni supportate di vCenter Server, vedere [Matrice di interoperabilità dei prodotti VMware](#).

Nota Se la rete dispone di larghezza di banda e latenza sufficienti, è possibile eseguire più istanze di vCenter Server su macchine virtuali diverse nella configurazione di vRealize Orchestrator. Se si utilizza la LAN per migliorare la comunicazione tra vRealize Orchestrator e vCenter Server, una riga di 100 MB è obbligatoria.

Metodi di autenticazione

Per autenticare e gestire le autorizzazioni utente, vRealize Orchestrator richiede una connessione a vRealize Automation oppure a un'istanza del server vSphere.

Quando si scarica e si distribuisce vRealize Orchestrator Appliance, è necessario configurare il server con un'autenticazione di vRealize Automation o vSphere. Vedere [Configurazione di un server vRealize Orchestrator autonomo](#).

Nota L'autenticazione di vRealize Orchestrator 8.x con vRealize Automation è supportata solo con vRealize Automation 8.x.

Installazione di vRealize Orchestrator

4

vRealize Orchestrator è costituito da un componente server e da un componente client.

Per utilizzare vRealize Orchestrator, è necessario distribuire vRealize Orchestrator Appliance e configurare il server di vRealize Orchestrator.

È possibile modificare le impostazioni di configurazione predefinite di vRealize Orchestrator utilizzando il Centro di controllo di vRealize Orchestrator.

Questo capitolo include i seguenti argomenti:

- [Download e distribuzione di vRealize Orchestrator Appliance](#)

Download e distribuzione di vRealize Orchestrator Appliance

Prima di poter accedere ai contenuti e ai servizi di vRealize Orchestrator, è necessario scaricare e distribuire vRealize Orchestrator Appliance.

Prerequisiti

- Verificare di disporre di un'istanza di vCenter Server in esecuzione. La versione di vCenter Server deve essere 6.0 o successiva.
- Verificare che l'host in cui si sta distribuendo vRealize Orchestrator Appliance soddisfi i requisiti hardware minimi. Vedere [Requisiti hardware per vRealize Orchestrator Appliance](#).
- Se il sistema è isolato e senza accesso a Internet, è necessario scaricare il file .ova per l'appliance dal sito Web VMware.

Procedura

- 1 Accedere a vSphere Web Client come **amministratore**.
- 2 Selezionare un oggetto di inventario che sia un oggetto principale valido di una macchina virtuale, ad esempio un data center, una cartella, un cluster, un pool di risorse o un host.
- 3 Selezionare **Azioni > Distribuisci modello OVF**.
- 4 Immettere il percorso del file o l'URL del file .ova e fare clic su **Avanti**.

- 5 Immettere un nome e una posizione per l'vRealize Orchestrator Appliance, quindi fare clic su **Avanti**.
- 6 Selezionare un host, un cluster, un pool di risorse o una vApp come destinazione in cui si desidera eseguire l'appliance, quindi fare clic su **Avanti**.
- 7 Rivedere i dettagli della distribuzione e fare clic su **Avanti**.
- 8 Accettare i termini dell'accordo di licenza e scegliere **Avanti**.
- 9 Selezionare il formato di storage che si desidera utilizzare per vRealize Orchestrator Appliance.

Formato	Descrizione
Azzeramento lazy con thick provisioning	Crea un disco virtuale in un formato thick predefinito. Lo spazio richiesto per il disco virtuale viene allocato al momento della creazione del disco virtuale. Se rimangono dati sul dispositivo fisico, non vengono cancellati durante la creazione, ma vengono azzerati su richiesta in un secondo momento alla prima scrittura dalla macchina virtuale.
Azzeramento eager con thick provisioning	Supporta funzionalità di clustering come la tolleranza di errore. Lo spazio richiesto per il disco virtuale viene allocato al momento della creazione del disco virtuale. Se rimangono dati sul dispositivo fisico, vengono azzerati quando viene creato il disco virtuale. La creazione di dischi in questo formato potrebbe richiedere molto più tempo rispetto alla creazione di dischi con altri formati.
Formato thin provisioning	Consente di risparmiare spazio sul disco rigido. Per il disco thin, si esegue il provisioning della quantità di spazio del datastore richiesta dal disco in base al valore selezionato per le dimensioni del disco. All'inizio il disco thin è piccolo e utilizza solo la quantità di spazio del datastore di cui necessita per le operazioni iniziali.

- 10 Fare clic su **Avanti**.
- 11 Configurare le impostazioni di rete e immettere la password **root**.

Quando si configurano le impostazioni di rete di vRealize Orchestrator Appliance, è necessario utilizzare il protocollo IPv4. Per le configurazioni di rete DHCP e statica, è necessario aggiungere un nome di dominio completo per vRealize Orchestrator Appliance.

Se il nome host visualizzato nella shell dell'istanza di vRealize Orchestrator Appliance distribuita è *photon-machine*, i requisiti della configurazione di rete precedente non vengono soddisfatti.
- 12 (Facoltativo) Configurare impostazioni di rete aggiuntive per vRealize Orchestrator Appliance, ad esempio l'abilitazione dell'accesso SSH.
- 13 Fare clic su **Avanti**.
- 14 Rivedere la pagina **Pronto per il completamento** e fare clic su **Fine**.

Risultati

L'istanza di vRealize Orchestrator Appliance è stata distribuita correttamente.

Operazioni successive

Accedere alla riga di comando di vRealize Orchestrator Appliance come **root** e verificare che sia possibile eseguire una ricerca DNS diretta o inversa.

- Per eseguire una ricerca DNS diretta, eseguire il comando `nslookup your_orchestrator_FQDN`. Il comando deve restituire l'indirizzo IP di vRealize Orchestrator Appliance.
- Per eseguire una ricerca DNS inversa, eseguire il comando `nslookup your_orchestrator_IP`. Il comando deve restituire il nome di dominio completo di vRealize Orchestrator Appliance.

Accensione di vRealize Orchestrator Appliance e apertura della pagina iniziale

Per utilizzare l'istanza autonoma di vRealize Orchestrator Appliance, è innanzitutto necessario accenderla.

Procedura

- 1 Accedere a vSphere Web Client come **amministratore**.
- 2 Fare clic con il pulsante destro del mouse su vRealize Orchestrator Appliance e scegliere **Alimentazione > Accendi**.
- 3 In un browser Web, passare all'indirizzo host della macchina virtuale di vRealize Orchestrator Appliance configurata durante la distribuzione di OVA.

`https://your_orchestrator_FQDN/vco.`

Modifica della durata della password root

Per impostazione predefinita, la password root di vRealize Orchestrator Appliance scade dopo 365 giorni.

Prerequisiti

- Scaricare e distribuire vRealize Orchestrator Appliance.
- Verificare che vRealize Orchestrator Appliance sia attiva e in esecuzione.

Procedura

- 1 Accedere a vRealize Orchestrator Appliance tramite SSH come **root**.
- 2 Eseguire il comando `passwd -x number_of_daysnumber_of_days root`.
- 3 Per aumentare indefinitamente la durata della password root, eseguire il comando `passwd -x 99999 root`.

Abilitazione o disabilitazione dell'accesso SSH a vRealize Orchestrator Appliance

È possibile abilitare o disabilitare l'accesso SSH a vRealize Orchestrator Appliance.

Prerequisiti

- Scaricare e distribuire vRealize Orchestrator Appliance.
- Verificare che vRealize Orchestrator Appliance sia attiva e in esecuzione.

Procedura

- 1** Accedere alla riga di comando di vRealize Orchestrator Appliance come **root**.
- 2** Per abilitare l'accesso SSH, eseguire il comando `/usr/bin/toggle-ssh enable`.
- 3** Per disabilitare l'accesso SSH, eseguire il comando `/usr/bin/toggle-ssh disable`.

Configurazione iniziale

5

Prima di iniziare ad automatizzare le attività e gestire i sistemi e le applicazioni con vRealize Orchestrator, è necessario utilizzare il Centro di controllo di vRealize Orchestrator per configurare un provider di autenticazione esterno. È inoltre possibile utilizzare il Centro di controllo di vRealize Orchestrator per ulteriori attività di configurazione, come la gestione delle informazioni sulla licenza e il certificato, l'installazione dei plug-in e il monitoraggio dello stato del cluster di vRealize Orchestrator.

Questo capitolo include i seguenti argomenti:

- [Configurazione di un server vRealize Orchestrator autonomo](#)
- [Abilitazione delle funzionalità di vRealize Orchestrator con le licenze](#)
- [Connessione al database di vRealize Orchestrator](#)
- [Gestione dei certificati](#)
- [Configurazione dei plug-in di vRealize Orchestrator](#)
- [Disponibilità e scalabilità di vRealize Orchestrator](#)
- [Configurazione di Analisi utilizzo software](#)

Configurazione di un server vRealize Orchestrator autonomo

Anche se vRealize Orchestrator Appliance è una macchina virtuale basata su Photon preconfigurata, è necessario configurare un provider di autenticazione prima di accedere alle funzionalità complete del Centro di controllo di vRealize Orchestrator e vRealize Orchestrator Client.

Configurazione di un server vRealize Orchestrator autonomo con l'autenticazione di vRealize Automation

Per preparare vRealize Orchestrator Appliance per l'utilizzo, è necessario configurare le impostazioni dell'host e il provider di autenticazione. È possibile configurare vRealize Orchestrator per l'autenticazione con vRealize Automation. Utilizzare l'autenticazione vRealize Automation con vRealize Automation 8.x.

Prerequisiti

- Scaricare e distribuire la versione più recente di vRealize Orchestrator Appliance. Vedere [Download e distribuzione di vRealize Orchestrator Appliance](#).
- Installare e configurare vRealize Automation 8.x e verificare che il server vRealize Automation sia in esecuzione. Vedere la documentazione di vRealize Automation.

Se si intende creare un cluster:

- Configurare un bilanciamento del carico per distribuire il traffico tra più istanze di vRealize Orchestrator. Vedere [Guida al bilanciamento del carico di VMware vRealize Orchestrator](#).

Procedura

- 1 Accedere al Centro di controllo per avviare la configurazione guidata.
 - a Passare a `https://your_orchestrator_FQDN/vco-controlcenter`.
 - b Accedere come **root** utilizzando la password immessa durante la distribuzione di OVA.
- 2 Configurare il provider di autenticazione.
 - a Nella pagina **Configura provider di autenticazione**, selezionare **vRealize Automation** dal menu a discesa **Modalità di autenticazione**.
 - b Nella casella di testo **Indirizzo host**, immettere l'indirizzo host di vRealize Automation e fare clic su **Connetti**.

Il formato dell'indirizzo host di vRealize Automation deve essere `https://your_vra_hostname`.
 - c Fare clic su **Accetta certificato**.
 - d Immettere le credenziali del proprietario dell'organizzazione vRealize Automation in cui vRealize Orchestrator verrà configurato. Fare clic su **Registra**.
 - e Fare clic su **Salva modifiche**.

Un messaggio indica che la configurazione è stata salvata correttamente.

Risultati

La configurazione del server vRealize Orchestrator è stata completata correttamente.

Operazioni successive

- Verificare che **CSP** sia il provider di licenze configurato nella pagina **Gestione licenze**.
- Verificare che il nodo sia configurato correttamente nella pagina **Convalida configurazione**.

Nota In seguito alla configurazione del provider di autenticazione, il server vRealize Orchestrator viene riavviato automaticamente dopo 2 minuti. Se si verifica la configurazione immediatamente dopo l'autenticazione, è possibile che venga restituito uno stato di configurazione non valido.

Configurazione di un server vRealize Orchestrator autonomo con l'autenticazione di vSphere

È possibile registrare il server vRealize Orchestrator in un server vCenter Single Sign-On utilizzando la modalità di autenticazione di vSphere. Utilizzare l'autenticazione di vCenter Single Sign-On con vCenter Server 6.0 e versioni successive.

Prerequisiti

- Scaricare e distribuire la versione più recente di vRealize Orchestrator Appliance. Vedere [Download e distribuzione di vRealize Orchestrator Appliance](#).
- Installare e configurare un vCenter Server con vCenter Single Sign-On in esecuzione. Vedere la documentazione di vSphere.

Se si intende creare un cluster:

- Configurare un bilanciamento del carico per distribuire il traffico tra più istanze di vRealize Orchestrator. Vedere [Guida al bilanciamento del carico di VMware vRealize Orchestrator](#).

Procedura

- 1 Accedere al Centro di controllo per avviare la configurazione guidata.
 - a Passare a `https://your_orchestrator_FQDN/vco-controlcenter`.
 - b Accedere come **root** utilizzando la password immessa durante la distribuzione di OVA.
- 2 Configurare il provider di autenticazione.
 - a Nella pagina **Configura provider di autenticazione**, selezionare **vSphere** dal menu a discesa **Modalità di autenticazione**.
 - b Nella casella di testo **Indirizzo host**, immettere il nome di dominio completo o l'indirizzo IP dell'istanza di Platform Services Controller che contiene vCenter Single Sign-On e fare clic su **Connetti**.

Nota Se si utilizza un Platform Services Controller esterno o più istanze di Platform Services Controller dietro un bilanciamento del carico, è necessario importare manualmente i certificati di tutti i Platform Services Controller che condividono un dominio di vCenter Single Sign-On.

Nota Per integrare un vSphere Client diverso con l'ambiente di vRealize Orchestrator configurato, è necessario configurare vSphere in modo che utilizzi lo stesso Platform Services Controller registrato in vRealize Orchestrator. Per gli ambienti di vRealize Orchestrator ad alta disponibilità, è necessario replicare le istanze di PCS dietro il server di bilanciamento del carico vRealize Orchestrator.

- c Rivedere le informazioni del certificato del provider di autenticazione e fare clic su **Accetta certificato**.

- d Immettere le credenziali dell'account dell'amministratore locale per il dominio di vCenter Single Sign-On. Fare clic su **Registra**.

Per impostazione predefinita, questo account è **administrator@vsphere.local** e il nome del tenant predefinito è **vsphere.local**.

- e Nella casella di testo **Gruppo di amministratori**, immettere il nome di un gruppo di amministratori e fare clic su **Cerca**.

Ad esempio, **vsphere.local\vcoadmins**.

- f Selezionare il gruppo di amministrazione che si desidera utilizzare.

- g Fare clic su **Salva modifiche**.

Un messaggio indica che la configurazione è stata salvata correttamente.

Risultati

La configurazione del server vRealize Orchestrator è stata completata correttamente.

Operazioni successive

- Verificare che **CIS** sia il provider di licenze configurato nella pagina **Gestione licenze**.
- Verificare che il nodo sia configurato correttamente nella pagina **Convalida configurazione**.

Nota In seguito alla configurazione del provider di autenticazione, il server vRealize Orchestrator viene riavviato automaticamente dopo 2 minuti. Se si verifica la configurazione immediatamente dopo l'autenticazione, è possibile che venga restituito uno stato di configurazione non valido.

Abilitazione delle funzionalità di vRealize Orchestrator con le licenze

L'accesso a determinate funzionalità di vRealize Orchestrator si basa sulla licenza applicata alla distribuzione di vRealize Orchestrator.

Dopo l'autenticazione, all'istanza di vRealize Orchestrator viene assegnata una licenza in base al provider di tale autenticazione. Le licenze controllano l'accesso alle seguenti funzionalità di vRealize Orchestrator:

- Integrazione Git
- Gestione ruoli
- Supporto multilingue (Python, Node.js e PowerShell)

È possibile modificare manualmente la licenza del server di vRealize Orchestrator dalla pagina **Licenze** del Centro di controllo.

Autenticazione	Licenza	Integrazione Git	Gestione ruoli	Supporto multilingue
vSphere	vSphere	No	No	No
vSphere	vRealize Automation/vRealize Suite	Sì	Sì	Sì
vRealize Automation	vRealize Automation/vRealize Suite	Sì	I ruoli vengono gestiti dall'istanza di vRealize Automation utilizzata per autenticare vRealize Orchestrator.	Sì

Connessione al database di vRealize Orchestrator

Il server vRealize Orchestrator richiede un database per l'archiviazione dei dati.

L'istanza di vRealize Orchestrator Appliance distribuita include un database PostgreSQL preconfigurato utilizzato dal server vRealize Orchestrator per archiviare i dati.

Il database PostgreSQL non è accessibile agli utenti.

Gestione dei certificati

Emesso per un determinato server e contenente informazioni sulla chiave pubblica del server, il certificato consente di firmare tutti gli elementi creati in vRealize Orchestrator e di garantire l'autenticità. Quando riceve un elemento dal server, in genere un pacchetto, il client verifica l'identità dell'utente e decide se considerare attendibile la firma.

■ [Gestione dei certificati di vRealize Orchestrator](#)

È possibile gestire i certificati di vRealize Orchestrator dalla pagina **Certificati** nel Centro di controllo di vRealize Orchestrator o con vRealize Orchestrator Client, utilizzando i workflow con tag *SSL_Trust_Manager*.

Gestione dei certificati di vRealize Orchestrator

È possibile gestire i certificati di vRealize Orchestrator dalla pagina **Certificati** nel Centro di controllo di vRealize Orchestrator o con vRealize Orchestrator Client, utilizzando i workflow con tag *SSL_Trust_Manager*.

Importazione di un certificato nell'archivio di attendibilità di Orchestrator

Il Centro di controllo di vRealize Orchestrator utilizza una connessione sicura per comunicare con vCenter Server, il sistema di gestione dei database relazionali (RDBMS), LDAP, Single Sign-On e altri server. È possibile importare il certificato TLS richiesto da un URL o da un file con codifica PEM. Ogni volta che si desidera utilizzare una connessione TLS a un'istanza del server, è necessario importare il certificato corrispondente dalla scheda **Certificati attendibili** nella pagina **Certificati** e importare il certificato TLS corrispondente.

È possibile caricare il certificato TLS in vRealize Orchestrator da un indirizzo URL o da un file con codifica PEM.

Opzione	Descrizione
Importa da URL o URL proxy	URL del server remoto: <code>https://your_server_IP_address</code> o <code>your_server_IP_address:port</code>
Importa da file	Percorso del file del certificato con codifica PEM. Nota È inoltre possibile importare un certificato attendibile eseguendo il workflow Importa certificato attendibile da file in vRealize Orchestrator Client. Il file importato tramite questo workflow deve essere codificato con DER.

Per ulteriori informazioni sull'importazione di un certificato, vedere [Importazione di un certificato attendibile con il Centro di controllo](#).

Certificato di firma pacchetto

I pacchetti esportati da un server di vRealize Orchestrator sono firmati digitalmente. Importare, esportare o generare un nuovo certificato da utilizzare per la firma dei pacchetti. I certificati di firma del pacchetto sono una forma di identificazione digitale utilizzata per garantire la comunicazione crittografata e una firma per i pacchetti di Orchestrator.

vRealize Orchestrator Appliance include un certificato di firma del pacchetto generato automaticamente, in base alle impostazioni di rete dell'appliance. Se le impostazioni di rete dell'appliance cambiano, è necessario generare manualmente un nuovo certificato di firma del pacchetto. Dopo aver generato un nuovo certificato di firma del pacchetto, tutti i futuri pacchetti esportati vengono firmati con il nuovo certificato.

Generazione di un certificato TLS personalizzato per vRealize Orchestrator

È possibile utilizzare vRealize Orchestrator Appliance per generare un nuovo certificato TLS per l'ambiente o impostare un certificato personalizzato esistente.

vRealize Orchestrator Appliance include un certificato TLS (Trusted Layer Security) generato automaticamente in base alle impostazioni di rete dell'appliance. Se le impostazioni di rete dell'appliance vengono modificate, è necessario generare un nuovo certificato manualmente. È possibile creare una catena di certificati per garantire la comunicazione crittografata e fornire una firma per i pacchetti. Il destinatario non può tuttavia essere sicuro che il pacchetto autofirmato sia in effetti un pacchetto emesso dal server dell'utente e non da una terza parte che afferma di essere l'utente. Per dimostrare l'identità del server, l'utente deve utilizzare un certificato firmato da un'autorità di certificazione (CA).

vRealize Orchestrator genera un certificato del server che è univoco per l'ambiente dell'utente. La chiave privata viene archiviata nella tabella `vmo_keystore` del database di vRealize Orchestrator.

Nota Per configurare vRealize Orchestrator Appliance per l'utilizzo di un certificato TLS personalizzato esistente, vedere [Impostazione di un certificato TLS personalizzato per vRealize Orchestrator](#).

Prerequisiti

Verificare che l'accesso SSH per vRealize Orchestrator Appliance sia abilitato. Vedere [Abilitazione o disabilitazione dell'accesso SSH a vRealize Orchestrator Appliance](#).

Procedura

- 1 Accedere alla riga di comando di vRealize Orchestrator Appliance tramite SSH come **root**.
- 2 Eseguire il comando `vracli certificate ingress --generate auto --set stdin`.
- 3 Per applicare il certificato personalizzato a vRealize Orchestrator Appliance, eseguire lo script di distribuzione.
 - a Passare alla directory `/opt/scripts/`.

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

- b Eseguire lo script `./deploy.sh`.

Importante Non interrompere lo script di distribuzione. Quando l'esecuzione dello script viene completata, viene visualizzato il seguente messaggio:

```
Prelude è stato distribuito correttamente. Per accedere, passare a your_orchestrator_address
```

Operazioni successive

Per verificare che la nuova catena di certificati sia stata applicata, eseguire il comando `vracli certificate ingress --list`.

Impostazione di un certificato TLS personalizzato per vRealize Orchestrator

Impostare un certificato TLS personalizzato per vRealize Orchestrator Appliance.

vRealize Orchestrator Appliance include un certificato TLS (Trusted Layer Security) generato automaticamente in base alle impostazioni di rete dell'appliance.

È possibile configurare vRealize Orchestrator Appliance in modo che utilizzi un certificato TLS personalizzato esistente. È possibile impostare il certificato importando il file PEM pertinente dalla macchina locale a vRealize Orchestrator Appliance. È inoltre possibile impostare il certificato TLS personalizzato copiando la catena di certificati direttamente in vRealize Orchestrator Appliance. Entrambe le procedure richiedono l'esecuzione dello script `./deploy.sh` prima che il nuovo certificato TLS possa essere utilizzato nella distribuzione di vRealize Orchestrator.

Per informazioni sulla creazione di un nuovo certificato TLS personalizzato, vedere [Generazione di un certificato TLS personalizzato per vRealize Orchestrator](#).

Prerequisiti

- Verificare che l'accesso SSH per vRealize Orchestrator Appliance sia abilitato. Vedere [Abilitazione o disabilitazione dell'accesso SSH a vRealize Orchestrator Appliance](#).

- Verificare che il file PEM contenente il certificato TLS includa i seguenti componenti nell'ordine impostato:
 - a La chiave privata per il certificato.
 - b Il certificato primario.
 - c Se applicabile, il certificato o i certificati intermedi dell'autorità di certificazione (CA).
 - d Il certificato CA root.

Ad esempio, il certificato TLS può avere la seguente struttura:

```
-----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-----
```

Procedura

- 1 Impostare il certificato importando il file PEM in vRealize Orchestrator Appliance.
 - a Importare il file PEM del certificato dalla macchina locale eseguendo un comando Secure Copy (SCP) da una shell SSH.

Per Linux, è possibile utilizzare un comando SCP del terminale:

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

Per Windows, è possibile utilizzare un comando PSCP del client PuTTY:

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

- b Accedere alla riga di comando di vRealize Orchestrator Appliance tramite SSH come **root**.
 - c Eseguire il comando `vracli certificate ingress --set your_cert_file.PEM`.
- 2 (Facoltativo) Impostare il certificato copiando la catena di certificati direttamente nell'appliance.
 - a Accedere alla riga di comando di vRealize Orchestrator Appliance tramite SSH come **root**.
 - b Eseguire il comando `vracli certificate ingress --set stdin`.
 - c Copiare e incollare la catena di certificati e premere CTRL+D.

3 Per applicare il nuovo certificato TLS, eseguire lo script di distribuzione.

a Passare alla directory `/opt/scripts/`.

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

b Eseguire lo script `./deploy.sh`.

Importante Non interrompere lo script di distribuzione. Quando l'esecuzione dello script viene completata, viene visualizzato il seguente messaggio:

```
Prelude è stato distribuito correttamente. Per accedere, passare a https://your_orchestrator_FQDN
```

Risultati

È stato impostato un certificato TLS personalizzato per vRealize Orchestrator Appliance.

Operazioni successive

Per verificare che la nuova catena di certificati sia stata applicata, eseguire il comando `vrac li certificate ingress --list`.

Importazione di un certificato attendibile con il Centro di controllo

Per comunicare con altri server in modo sicuro, il server di vRealize Orchestrator deve essere in grado di verificarne l'identità. A tale scopo, potrebbe essere necessario importare il certificato TLS dell'entità remota nell'archivio di attendibilità di vRealize Orchestrator. Per considerare attendibile un certificato, è possibile importarlo nell'archivio di attendibilità stabilendo una connessione a un URL specifico o direttamente come file con codifica PEM.

Procedura

- 1** Accedere al Centro di controllo come **root**.
- 2** Passare alla pagina **Certificati**.
- 3** Selezionare **Certificati attendibili** e fare clic su **Importa**.
- 4** Per importare il certificato da un file, selezionare **Importa da file con codifica PEM**.
- 5** Passare al file del certificato e fare clic su **Importa**.
- 6** Per importare il certificato da un indirizzo URL, selezionare **Importa da URL**.
- 7** Immettere l'indirizzo URL in cui archiviare il certificato e fare clic su **Importa**.

Risultati

È stato importato un certificato del server remoto nell'archivio di attendibilità di vRealize Orchestrator.

Configurazione dei plug-in di vRealize Orchestrator

I plug-in di vRealize Orchestrator predefiniti vengono configurati con esecuzioni dei workflow specifici dei plug-in in vRealize Orchestrator Client.

vRealize Orchestrator Appliance consente di accedere a una libreria preinstallata di plug-in predefiniti. È possibile configurare questi plug-in predefiniti eseguendo workflow specifici per tali plug-in da vRealize Orchestrator Client.

Ad esempio, se si immettono i tag *AMQP* e *Configuration* nella casella di testo di ricerca della libreria dei workflow, vengono recuperati i workflow utilizzati per gestire i gestori e le sottoscrizioni AMQP.

Gestione dei plug-in di vRealize Orchestrator

Nella pagina **Gestisci plug-in** del Centro di controllo di vRealize Orchestrator, è possibile visualizzare l'elenco di tutti i plug-in installati in vRealize Orchestrator ed eseguire operazioni di gestione di base.

Installazione o aggiornamento di un plug-in

Con i plug-in di vRealize Orchestrator, il server di vRealize Orchestrator può integrarsi con altri prodotti software. vRealize Orchestrator Appliance include un set di plug-in preinstallati. È possibile espandere ulteriormente le funzionalità della piattaforma di vRealize Orchestrator installando plug-in personalizzati.

È possibile installare o aggiornare i plug-in dalla pagina **Gestisci plug-in** di vRealize Orchestrator. Le estensioni di file che è possibile utilizzare sono `.vmoapp` e `.dar`. Un file `.vmoapp` può contenere una raccolta di diversi file `.dar` e può essere installato come applicazione. Un file `.dar` contiene tutte le risorse associate a un plug-in.

Nota Il formato di file preferito per i plug-in di vRealize Orchestrator è `.vmoapp`.

Per ulteriori informazioni sull'installazione o l'aggiornamento dei plug-in di vRealize Orchestrator, vedere [Installazione o aggiornamento di un plug-in di vRealize Orchestrator](#).

Modifica del livello di registrazione del plug-in

Anziché modificare il livello di registrazione di vRealize Orchestrator, è possibile modificare il livello di registrazione solo per plug-in specifici.

Disabilitazione di un plug-in

È possibile disabilitare un plug-in deselezionando l'opzione **Abilita plug-in** accanto al nome del plug-in.

Questa azione non rimuove il file del plug-in. Per ulteriori informazioni sulla disinstallazione di un plug-in in vRealize Orchestrator, vedere [Eliminazione di un plug-in](#).

Installazione o aggiornamento di un plug-in di vRealize Orchestrator

È possibile installare o aggiornare plug-in di terze parti nel Centro di controllo di vRealize Orchestrator.

Prerequisiti

Scaricare il file *.dar* o *.vmoapp* del plug-in.

Nota Il formato di file preferito per i plug-in di vRealize Orchestrator è *.vmoapp*.

Procedura

- 1 Accedere al Centro di controllo come **root**.
- 2 Selezionare la pagina **Gestisci plug-in**.
- 3 Fare clic su **Sfoglia** e selezionare il file di *.dar* o *.vmoapp* del plug-in che si desidera installare o aggiornare.
- 4 Fare clic su **Carica**.
- 5 Rivedere le informazioni del plug-in. Se applicabile, accettare il contratto di licenza con l'utente finale e fare clic su **Installa**.

Il plug-in viene installato o aggiornato e il servizio del server di vRealize Orchestrator viene riavviato.

Operazioni successive


Verificare che le informazioni del plug-in corrette siano disponibili nella pagina **Gestisci plug-in**.

Eliminazione di un plug-in

È possibile eliminare i plug-in di terze parti da vRealize Orchestrator Appliance tramite il Centro di controllo.

Nota A partire da vRealize Orchestrator 8.0, non è più necessario eliminare manualmente il pacchetto del plug-in da vRealize Orchestrator Client.

Procedura

- 1 Accedere al Centro di controllo come **root**.
- 2 Selezionare **Gestisci plug-in**.
- 3 Individuare il plug-in che si desidera eliminare e fare clic sull'icona di eliminazione ().
- 4 Confermare che si desidera eliminare il plug-in e fare clic su **Elimina**.

Risultati

Il plug-in è stato eliminato da vRealize Orchestrator Appliance.

Disponibilità e scalabilità di vRealize Orchestrator

Per aumentare la disponibilità dei servizi di vRealize Orchestrator, avviare più istanze del server di vRealize Orchestrator in un cluster con un database condiviso. vRealize Orchestrator funziona come una singola istanza finché non viene configurato per funzionare come parte di un cluster.

Cluster di vRealize Orchestrator

Più istanze del server di vRealize Orchestrator con configurazioni di server e plug-in identiche funzionano insieme in un cluster e condividono un database.

Tutte le istanze del server di vRealize Orchestrator comunicano tra loro scambiando heartbeat. Ogni heartbeat è un timestamp che il nodo scrive nel database condiviso del cluster in un determinato intervallo di tempo. I problemi di rete, un server di database che non risponde o un overload potrebbero causare il blocco di un nodo del cluster di vRealize Orchestrator. Se un'istanza del server di vRealize Orchestrator attiva non riesce a inviare heartbeat entro il periodo di timeout del failover, viene considerata bloccata. Il timeout del failover è uguale al valore dell'intervallo di heartbeat moltiplicato per il numero di heartbeat del failover. Serve come definizione per un nodo non affidabile e può essere personalizzato in base alle risorse disponibili e al carico di produzione.

Un nodo di vRealize Orchestrator passa alla modalità standby quando perde la connessione al database e rimane in questa modalità finché la connessione al database non viene ripristinata. Gli altri nodi del cluster assumono il controllo del lavoro attivo, ripristinando tutti i workflow interrotti dai loro ultimi elementi non completati, come le attività di script o le chiamate dei workflow.

È possibile monitorare lo stato del cluster di vRealize Orchestrator dalla pagina **Gestione cluster di Orchestrator** del Centro di controllo di vRealize Orchestrator. È inoltre possibile utilizzare questa pagina per configurare l'heartbeat del cluster, il numero di heartbeat di failover e il numero di nodi attivi di vRealize Orchestrator.

Configurazione di un cluster di vRealize Orchestrator

È possibile configurare la distribuzione di una nuova istanza di vRealize Orchestrator in modo che venga eseguita con alta disponibilità distribuendo tre nodi e connettendoli come un cluster.

Un cluster di vRealize Orchestrator è costituito da tre istanze di vRealize Orchestrator che condividono un database PostgreSQL comune. Il database del cluster di vRealize Orchestrator configurato può essere eseguito solo in modalità asincrona.

Per creare un cluster di vRealize Orchestrator, è necessario selezionare un'istanza di vRealize Orchestrator come nodo primario del cluster. Dopo aver configurato il nodo primario, unire i nodi secondari a tale nodo.

Il cluster di vRealize Orchestrator creato è preconfigurato con il failover automatico.

Nota Un errore del failover automatico può causare la perdita di dati del database.

Prerequisiti

- Scaricare e distribuire tre istanze di vRealize Orchestrator autonome. Vedere [Download e distribuzione di vRealize Orchestrator Appliance](#).

Nota Il numero di nodi consigliato per creare un ambiente di vRealize Orchestrator in cluster è tre.

- Verificare che l'accesso SSH sia abilitato per tutti i nodi di vRealize Orchestrator. Vedere [Abilitazione o disabilitazione dell'accesso SSH a vRealize Orchestrator Appliance](#).
- Configurare un server di bilanciamento del carico. Vedere [Guida al bilanciamento del carico di VMware vRealize Orchestrator](#).

Procedura

1 Configurare il nodo primario.

- a Accedere a vRealize Orchestrator Appliance del nodo primario tramite SSH come **root**.
- b Per configurare il server di bilanciamento del carico del cluster, eseguire il comando `vracli load-balancer set load_balancer_FQDN`.
- c Accedere al Centro di controllo del nodo primario e selezionare **Impostazioni host**.
- d Fare clic su **Modifica** e impostare l'indirizzo host del server di bilanciamento del carico connesso.
- e Configurare il provider di autenticazione. Vedere [Configurazione di un server vRealize Orchestrator autonomo](#).

2 Unire i nodi secondari al nodo primario.

- a Accedere a vRealize Orchestrator Appliance del nodo secondario tramite SSH come **root**.
- b Per unire il nodo secondario al nodo primario, eseguire il comando `vracli cluster join primary_node_hostname_or_IP`.
- c Immettere la password root del nodo primario.
- d Ripetere la procedura per l'altro nodo secondario.

3 (Facoltativo) Se il nodo primario utilizza un certificato personalizzato, è necessario impostare il certificato nell'appliance o generare un nuovo certificato. Vedere [Generazione di un certificato TLS personalizzato per vRealize Orchestrator](#).

Nota Il file contenente la catena di certificati deve essere codificato con PEM.

4 Completare la distribuzione del cluster.

- a Accedere a vRealize Orchestrator Appliance del nodo primario tramite SSH come **root**.
- b Per verificare che tutti i nodi siano pronti, eseguire il comando `kubectl -n prelude get nodes`.
- c Eseguire lo script `/opt/scripts/deploy.sh` e attendere il completamento della distribuzione.

Risultati

È stato creato un cluster vRealize Orchestrator. Dopo aver creato il cluster, è possibile accedere all'ambiente di vRealize Orchestrator solo dall'indirizzo del nome di dominio completo del server di bilanciamento del carico.

Nota Poiché è possibile accedere al Centro di controllo del cluster solo con la password root del bilanciamento del carico, non è possibile modificare la configurazione di un nodo del cluster se ha una password root diversa. Per modificare la configurazione di questo nodo, rimuoverlo dal bilanciamento del carico, modificare la configurazione nel Centro di controllo e aggiungere nuovamente il nodo al bilanciamento del carico.

Operazioni successive

Per monitorare lo stato del cluster di vRealize Orchestrator, accedere al Centro di controllo e selezionare la pagina **Gestione cluster di Orchestrator**. Vedere [Monitoraggio di un cluster di vRealize Orchestrator](#).

Rimozione di un nodo del cluster di vRealize Orchestrator

È possibile eliminare un'istanza di vRealize Orchestrator in modo da ridurre la capacità del cluster.

Un nodo rimosso dal cluster di vRealize Orchestrator non funziona più. Se si desidera utilizzarlo di nuovo, è necessario eliminare l'istanza di vRealize Orchestrator Appliance del nodo da vCenter Server e distribuirlo di nuovo. Vedere [Download e distribuzione di vRealize Orchestrator Appliance](#).

Prerequisiti

Creare un cluster di vRealize Orchestrator. Vedere [Configurazione di un cluster di vRealize Orchestrator](#).

Procedura

- 1 Accedere alla riga di comando di vRealize Orchestrator Appliance del nodo che si desidera rimuovere come **root**.
- 2 Per rimuovere il nodo da vRealize Orchestrator, eseguire il comando `vracli cluster leave`.
- 3 Accedere alla riga di comando di vRealize Orchestrator Appliance di uno dei nodi rimanenti come **root**.

- 4 Eseguire il comando `kubectl -n prelude get nodes` e verificare che il nodo rimosso non faccia più parte del cluster.

Scalabilità orizzontale di una distribuzione di vRealize Orchestrator autonoma

È possibile aumentare la disponibilità e la scalabilità della distribuzione di vRealize Orchestrator configurata scalandola orizzontalmente.

Prerequisiti

- Scaricare, distribuire e configurare un'istanza di vRealize Orchestrator. Vedere [Download e distribuzione di vRealize Orchestrator Appliance](#) e [Configurazione di un server vRealize Orchestrator autonomo](#).
- Scaricare e distribuire due istanze di vRealize Orchestrator aggiuntive. Vedere [Download e distribuzione di vRealize Orchestrator Appliance](#).
- Configurare un server di bilanciamento del carico. Vedere [Guida al bilanciamento del carico di VMware vRealize Orchestrator 8.x](#).

Procedura

- 1 Configurare il nodo primario.
 - a Accedere al Centro di controllo della distribuzione di vRealize Orchestrator configurata come **root**.
 - b Selezionare **Configura provider di autenticazione** e annullare la registrazione del provider di autenticazione.
 - c Selezionare **Impostazioni host** e immettere il nome host del server del bilanciamento del carico.
 - d Selezionare **Configura provider di autenticazione** e registrare di nuovo il provider di autenticazione.
 - e Accedere alla riga di comando di vRealize Orchestrator Appliance dell'istanza configurata come **root**.
 - f Per arrestare tutti i servizi dell'istanza di vRealize Orchestrator, eseguire il comando `/opt/scripts/deploy.sh --onlyClean`.
 - g Per impostare il bilanciamento del carico, eseguire `vracli load-balancer set load_balancer_FQDN`.
 - h (Facoltativo) Se l'istanza di vRealize Orchestrator utilizza un certificato personalizzato, eseguire il comando `vracli certificate ingress --set your_cert_file.pem`.

Nota Il file contenente la catena di certificati deve essere codificato con PEM.

2 Unire i nodi secondari all'istanza di configurata.

- a Accedere alla riga di comando di vRealize Orchestrator Appliance del nodo secondario come **root**.
- b Per unire il nodo secondario all'istanza configurata, eseguire il comando `vracli cluster join primary_node_hostname_or_IP`.
- c Ripetere l'operazione per l'altro nodo secondario.

3 Completare il processo per la scalabilità orizzontale.

- a Accedere alla riga di comando di vRealize Orchestrator Appliance dell'istanza configurata come **root**.
- b Eseguire `/opt/scripts/deploy.sh` e attendere il completamento dello script.

Risultati

La distribuzione di vRealize Orchestrator è stata scalata orizzontalmente.

Monitoraggio di un cluster di vRealize Orchestrator

È possibile monitorare il cluster di vRealize Orchestrator esistente tramite il Centro di controllo di vRealize Orchestrator.

È possibile monitorare gli stati di sincronizzazione della configurazione delle istanze di vRealize Orchestrator che vengono unite in un cluster dalla pagina **Gestione cluster di Orchestrator** nel Centro di controllo.

Stato di sincronizzazione della configurazione	Descrizione
IN ESECUZIONE	Il servizio vRealize Orchestrator è disponibile e può accettare richieste.
STANDBY	<p>Il servizio vRealize Orchestrator non può elaborare le richieste perché:</p> <ul style="list-style-type: none"> ■ Il nodo fa parte di un cluster ad alta disponibilità e rimane in modalità standby finché non si verifica un errore nel nodo primario. ■ Il servizio non può verificare i prerequisiti della configurazione, come una connessione valida al database, il provider di autenticazione e la licenza dell'istanza di vRealize Orchestrator.
Recupero stato di integrità del servizio non riuscito	Il servizio del server di vRealize Orchestrator non può essere contattato perché è stato interrotto o si è verificato un problema della rete.
Riavvio in sospeso	Il Centro di controllo rileva una modifica della configurazione e il server di vRealize Orchestrator viene riavviato automaticamente.

Configurazione di Analisi utilizzo software

Se si sceglie di partecipare al programma Analisi utilizzo software, VMware riceve informazioni anonime che consentono di migliorare la qualità, l'affidabilità e la funzionalità dei prodotti e dei servizi VMware.

Categorie di informazioni ricevute da VMware

Il programma Analisi utilizzo software fornisce a VMware una serie di informazioni utili per migliorare i propri prodotti e servizi, nonché per risolvere i problemi.

I dettagli relativi ai dati raccolti tramite il programma Analisi utilizzo software e gli scopi per cui vengono utilizzati da VMware sono disponibili sul sito Trust & Assurance Center all'indirizzo <http://www.vmware.com/trustvmware/ceip.html>. Per partecipare o abbandonare il programma Analisi utilizzo software per questo prodotto, vedere [Partecipazione o uscita dal programma Analisi utilizzo software](#).

Partecipazione o uscita dal programma Analisi utilizzo software

È possibile partecipare al programma Analisi utilizzo software dalla riga di comando di vRealize Orchestrator Appliance.

Procedura

- 1 Accedere alla riga di comando di vRealize Orchestrator Appliance come **root**.
- 2 Per partecipare al programma Analisi utilizzo software, eseguire il comando `vracli ceip on`.
- 3 Rivedere le informazioni del programma Analisi utilizzo software ed eseguire il comando `vracli ceip on --acknowledge-ceip`.
- 4 Riavviare i servizi di vRealize Orchestrator.
 - a Per riavviare il servizio del server, eseguire il comando `kubectl -n prelude exec -it your_vro_pod -c vco-server-app /bin/bash`.
 - b Per arrestare il servizio, eseguire il comando `kill 1`.
 - c Per riavviare il servizio del Centro di controllo, eseguire il comando `kubectl -n prelude exec -it your_vro_pod -c vco-controlcenter-app /bin/bash`.
 - d Per arrestare il servizio, eseguire il comando `kill 1`.
- 5 Per uscire dal programma Analisi utilizzo software, eseguire il comando `vracli ceip off`.
- 6 Ripetere i passaggi per riavviare i servizi.

Utilizzo dei servizi dell'API di vRealize Orchestrator

6

Oltre a configurare vRealize Orchestrator utilizzando il Centro di controllo, è possibile modificare le impostazioni di configurazione del server vRealize Orchestrator utilizzando la REST API di vRealize Orchestrator, la REST API del Centro di controllo o l'utilità della riga di comando, archiviata nell'appliance.

Per impostazione predefinita, il plug-in di configurazione è incluso nel pacchetto di vRealize Orchestrator. È possibile accedere ai workflow del plug-in di configurazione dalla libreria dei workflow di vRealize Orchestrator o dalla REST API di vRealize Orchestrator. Con questi workflow, è possibile modificare le impostazioni del certificato attendibile e del keystore del server vRealize Orchestrator. Per informazioni su tutte le chiamate dei servizi della REST API di vRealize Orchestrator disponibili, vedere la documentazione relativa all'*API di vRealize Orchestrator Server*, disponibile all'indirizzo https://your_orchestrator_FQDN/vco/api/docs.

■ Gestione dei certificati TLS e dei keystore tramite REST API

Oltre a gestire i certificati TLS utilizzando il Centro di controllo, è possibile gestire certificati attendibili e keystore quando si eseguono workflow dal plug-in di configurazione o utilizzando la REST API.

Gestione dei certificati TLS e dei keystore tramite REST API

Oltre a gestire i certificati TLS utilizzando il Centro di controllo, è possibile gestire certificati attendibili e keystore quando si eseguono workflow dal plug-in di configurazione o utilizzando la REST API.

Il plug-in di configurazione contiene workflow per l'importazione e l'eliminazione di keystore e certificati TLS. È possibile accedere a questi workflow passando a **Libreria > Workflow > Gestore di attendibilità SSL** e **Libreria > Workflow > Keystore** in vRealize Orchestrator Client. È inoltre possibile eseguire questi workflow utilizzando la REST API di vRealize Orchestrator.

La REST API del Centro di controllo consente di accedere alle risorse per la configurazione del server di vRealize Orchestrator. È possibile utilizzare la REST API del Centro di controllo con sistemi di terze parti per automatizzare la configurazione di vRealize Orchestrator. L'endpoint root della REST API del Centro di controllo è `https://your_orchestrator_FQDN/vco/api`. Per informazioni su tutte le chiamate ai servizi disponibili che è possibile eseguire alla REST API del Centro di controllo, consultare la documentazione dell'*API del Centro di controllo di vRealize Orchestrator*, all'indirizzo `https://your_orchestrator_FQDN/vco-controlcenter/docs`.

Eliminazione di un certificato TLS mediante REST API

È possibile eliminare un certificato TLS eseguendo il workflow per l'eliminazione del certificato attendibile del plug-in di configurazione o utilizzando la REST API.

Procedura

- 1 Eseguire una richiesta GET all'URL del servizio del workflow per l'eliminazione del certificato attendibile.

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

- 2 Recuperare la definizione del workflow per l'eliminazione del certificato attendibile eseguendo una richiesta GET all'URL della definizione.

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

- 3 Eseguire una richiesta POST all'URL che contiene gli oggetti di esecuzione del workflow per l'eliminazione del certificato attendibile.

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

- 4 Specificare il nome del certificato che si desidera eliminare come parametro di input del workflow per l'eliminazione del certificato attendibile in un elemento del contesto di esecuzione nel corpo della richiesta.

Importazione di certificati TLS tramite REST API

È possibile importare certificati TLS eseguendo un workflow dal plug-in di configurazione o utilizzando la REST API.

È possibile importare un certificato attendibile da un file o un URL. Vedere [Importazione di un certificato attendibile con il Centro di controllo](#)

Procedura

- 1 Eseguire una richiesta GET all'URL del servizio del workflow.

Opzione	Descrizione
Importa certificato attendibile da file	Importa un certificato attendibile da un file.
Importa certificato attendibile da URL	Importa un certificato attendibile da un indirizzo URL.
Importa certificato attendibile da URL utilizzando un server proxy	Importa un certificato attendibile da un indirizzo URL utilizzando un server proxy.
Importa certificato attendibile da URL con alias del certificato	Importa un certificato attendibile da un indirizzo URL con un alias del certificato.

Per importare un certificato attendibile da un file, eseguire la richiesta GET seguente:

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

- 2 Recuperare la definizione del workflow eseguendo una richiesta GET all'URL della definizione.

Per recuperare la definizione del workflow Importa certificato attendibile da file, eseguire la richiesta GET seguente:

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

- 3 Eseguire una richiesta POST all'URL che contiene gli oggetti di esecuzione del workflow.

Per il workflow Importa certificato attendibile da file, eseguire la richiesta POST seguente:

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

- 4 Specificare i valori per i parametri di input del workflow in un elemento del contesto di esecuzione del corpo della richiesta.

Parametro	Descrizione
cer	File CER da cui si desidera importare il certificato TLS. Questo parametro è applicabile per il workflow Importa certificato attendibile da file.
url	URL da cui si desidera importare il certificato TLS. Per i servizi non HTTPS, il formato supportato è <i>IP_address_or_DNS_name:port</i> . Questo parametro è applicabile per il workflow Importa certificato attendibile da URL.

Creazione di un keystore mediante REST API

È possibile creare un keystore eseguendo il workflow di creazione di un keystore del plug-in di configurazione o utilizzando la REST API.

Procedura

- 1 Eseguire una richiesta GET all'URL del servizio del workflow di creazione di un keystore.

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

- 2 Recuperare la definizione del workflow di creazione di un keystore eseguendo una richiesta GET all'URL della definizione.

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

- 3 Eseguire una richiesta POST all'URL che contiene gli oggetti di esecuzione del workflow di creazione di un keystore.

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

- 4 Specificare il nome del keystore che si desidera creare come parametro di input del workflow di creazione di un keystore in un elemento del contesto di esecuzione nel corpo della richiesta.

Eliminazione di un keystore mediante REST API

È possibile eliminare un keystore eseguendo il workflow per l'eliminazione di un keystore del plug-in di configurazione o utilizzando la REST API.

Procedura

- 1 Eseguire una richiesta GET all'URL del servizio del workflow per l'eliminazione di un keystore.

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

- 2 Recuperare la definizione del workflow per l'eliminazione di un keystore eseguendo una richiesta GET all'URL della definizione.

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

- 3 Eseguire una richiesta POST all'URL che contiene gli oggetti di esecuzione del workflow per l'eliminazione di un keystore.

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

- 4 Specificare il keystore che si desidera eliminare come parametro di input del workflow per l'eliminazione di un keystore in un elemento del contesto di esecuzione nel corpo della richiesta.

Aggiunta di una chiave tramite REST API

È possibile aggiungere una chiave eseguendo il workflow per l'aggiunta della chiave del plug-in Configurazione o utilizzando la REST API.

Procedura

- 1 Eseguire una richiesta GET all'URL del servizio del workflow per l'aggiunta della chiave.

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

- 2 Recuperare la definizione del workflow per l'aggiunta della chiave eseguendo una richiesta GET all'URL della definizione.

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

- 3 Eseguire una richiesta POST all'URL che contiene gli oggetti di esecuzione del workflow per l'aggiunta della chiave.

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

- 4 Specificare il keystore, l'alias della chiave, la chiave con codifica PEM, la catena di certificati e la password della chiave come parametri di input del workflow per l'aggiunta della chiave in un elemento del contesto di esecuzione nel corpo della richiesta.

Opzioni di configurazione aggiuntive

7

È possibile utilizzare il Centro di controllo per modificare il comportamento predefinito di vRealize Orchestrator.

Questo capitolo include i seguenti argomenti:

- [Riconfigurazione dell'autenticazione](#)
- [Configurazione delle proprietà di esecuzione dei workflow](#)
- [File di registro di vRealize Orchestrator](#)
- [Abilitazione delle estensioni OpenTracing e Wavefront](#)
- [Abilitazione della sincronizzazione dell'ora per vRealize Orchestrator](#)
- [Disabilitazione della sincronizzazione dell'ora per vRealize Orchestrator](#)

Riconfigurazione dell'autenticazione

Dopo aver configurato il metodo di autenticazione durante la configurazione iniziale del Centro di controllo, è possibile modificare il provider di autenticazione o i parametri configurati in qualsiasi momento.

Modifica del provider di autenticazione

Per modificare la modalità di autenticazione o le impostazioni di connessione del provider di autenticazione, è innanzitutto necessario annullare la registrazione del provider di autenticazione esistente.

Procedura

- 1 Accedere al Centro di controllo come **root**.
- 2 Nella pagina **Configura provider di autenticazione**, fare clic sul pulsante **Annulla registrazione** accanto alla casella di testo dell'indirizzo host per annullare la registrazione del provider di autenticazione in uso.

Risultati

La registrazione del provider di autenticazione è stata annullata correttamente.

Operazioni successive

Riconfigurare l'autenticazione nel Centro di controllo. Vedere [Configurazione di un server vRealize Orchestrator autonomo](#).

Modifica dei parametri di autenticazione

Quando si utilizza vSphere come provider di autenticazione nel Centro di controllo, è possibile modificare il tenant predefinito del gruppo di amministratori di vRealize Orchestrator.

Prerequisiti

Configurare vSphere come provider di autenticazione per la distribuzione di vRealize Orchestrator. Vedere [Configurazione di un server vRealize Orchestrator autonomo con l'autenticazione di vSphere](#).

Nota L'autenticazione di vRealize Automation non include questi parametri.

Procedura

- 1 Accedere al Centro di controllo come **root**.
- 2 Selezionare **Configura provider di autenticazione**.
- 3 Fare clic sul pulsante **Modifica** accanto alla casella di testo **Tenant predefinito**.
- 4 Sostituire il nome del tenant.
- 5 Fare clic sul pulsante **Modifica** accanto alla casella di testo **Gruppo di amministratori**.

Nota Se non si riconfigura il gruppo di amministratori, rimane vuoto e non è più possibile accedere al Centro di controllo.

- 6 Immettere il nome di un gruppo di amministratori e fare clic su **Cerca**.
- 7 Selezionare un gruppo di amministratori.
- 8 Modificare il gruppo di amministratori.
- 9 Per completare la modifica dei parametri di autenticazione, fare clic su **Salva modifiche**.

Configurazione delle proprietà di esecuzione dei workflow

Per impostazione predefinita, è possibile eseguire fino a 300 workflow per nodo e possono essere messi in coda fino a 10.000 workflow se viene raggiunto il numero massimo di workflow in esecuzione attivamente.

Quando il nodo vRealize Orchestrator deve eseguire più di 300 workflow simultanei, le esecuzioni dei workflow in sospeso vengono messe in coda. Quando viene completata l'esecuzione di un workflow attivo, inizia l'esecuzione del workflow successivo nella coda. Se viene raggiunto il numero massimo di workflow in coda, l'esecuzione del workflow successivo non riesce finché non viene avviata l'esecuzione di uno dei workflow in sospeso.

Nella pagina **Opzioni avanzate** nel Centro di controllo, è possibile configurare le proprietà delle esecuzioni dei workflow.

Opzione	Descrizione
Abilita modalità sicura	Se la modalità sicura è abilitata, tutti i workflow in esecuzione vengono annullati e non verranno ripresi al successivo avvio del nodo di Orchestrator.
Numero di workflow in esecuzione simultanei	Numero massimo di workflow del nodo di Orchestrator simultanei che vengono eseguiti contemporaneamente.
Quantità massima di workflow in esecuzione nella coda	Numero di richieste di esecuzione del workflow che il nodo di Orchestrator accetta prima di diventare non disponibile.
Numero massimo di esecuzioni preservate per workflow	Numero massimo di esecuzioni di workflow terminate conservate come cronologia per workflow in un cluster. Al superamento della soglia vengono eliminate le più vecchie.
Giorni scadenza eventi registro	Numero di giorni per cui gli eventi del registro per il cluster vengono conservati nel database prima di essere eliminati.

File di registro di vRealize Orchestrator

Il supporto tecnico di VMware richiede regolarmente informazioni diagnostiche quando si invia una richiesta di supporto. Queste informazioni diagnostiche contengono registri specifici del prodotto e file di configurazione dell'host in cui il prodotto viene eseguito.

I registri di vRealize Orchestrator Appliance vengono archiviati nella directory `/data/vco/usr/lib/vco/app-server/logs/`. È possibile esportare i registri della distribuzione di vRealize Orchestrator Appliance accedendo alla riga di comando dell'appliance ed eseguendo il comando `vrac li log-bundle`. Il bundle dei registri generato viene salvato nella cartella root di vRealize Orchestrator Appliance.

Persistenza della registrazione

È possibile registrare informazioni in qualsiasi tipo di script di vRealize Orchestrator, ad esempio workflow, criteri o azioni. Queste informazioni hanno tipi e livelli. Il tipo può essere persistente o non persistente. Il livello può essere DEBUG, INFO, WARN, ERROR, TRACE e FATAL.

Tabella 7-1. Creazione di registri persistenti e non persistenti

Livello di registrazione	Tipo persistente	Tipo non persistente
DEBUG	<code>Server.debug("short text", "long text");</code>	<code>System.debug("text")</code>
INFO	<code>Server.log("short text", "long text");</code>	<code>System.log("text");</code>
WARN	<code>Server.warn("short text", "long text");</code>	<code>System.warn("text");</code>
ERROR	<code>Server.error("short text", "long text");</code>	<code>System.error("text");</code>

Registri persistenti

I registri persistenti (registri del server) tengono traccia delle esecuzioni dei workflow precedenti e vengono archiviati nel database di vRealize Orchestrator.

Registri non persistenti

Quando si utilizza un registro non persistente (registro di sistema) per creare script, il server di vRealize Orchestrator notifica tale registro a tutte le applicazioni di vRealize Orchestrator in esecuzione, ma queste informazioni non vengono archiviate nel database. Quando l'applicazione viene riavviata, le informazioni del registro vengono perse. I registri non persistenti vengono utilizzati a scopo di debug e per le informazioni in tempo reale. Per visualizzare i registri di sistema, è necessario selezionare un'esecuzione di workflow completa in vRealize Orchestrator Client e selezionare la scheda **Registri**.

Configurazione dei registri di vRealize Orchestrator

Nella pagina **Configura registri** nel Centro di controllo, è possibile impostare il livello di registrazione desiderato per il registro del server e il registro di scripting. Se uno dei registri viene generato più volte al giorno, risulta difficile determinare ciò che causa problemi.

Il livello di registrazione predefinito del registro del server e del registro di scripting è Info. La modifica del livello di registrazione influisce su tutti i nuovi messaggi che il server inserisce nei registri e sul numero di connessioni attive al database. La verbosità della registrazione diminuisce in ordine decrescente.

Attenzione Impostare il livello di registrazione su Debug o su Tutto per eseguire il debug di un problema. Non utilizzare queste impostazioni in un ambiente di produzione perché possono compromettere gravemente le prestazioni.

Generare registri di vRealize Orchestrator

È possibile esportare i registri della distribuzione accedendo alla riga di comando di vRealize Orchestrator Appliance come **root** ed eseguendo il comando `vraccli log-bundle`. Il bundle del registro generato viene archiviato nella cartella root dell'appliance.

Nota Quando in un cluster sono presenti più istanze di vRealize Orchestrator, il bundle del registro include i registri di tutte le istanze di vRealize Orchestrator nel cluster.

Configurazione dell'integrazione della registrazione con vRealize Log Insight

È possibile configurare vRealize Orchestrator per l'invio delle informazioni di registrazione a un server vRealize Log Insight.

È possibile configurare un'integrazione della registrazione in un server vRealize Log Insight tramite la riga di comando di vRealize Orchestrator Appliance.

Nota Per informazioni sulla configurazione di un'integrazione della registrazione con un server syslog remoto, vedere [Creazione o sovrascrittura di un'integrazione syslog in vRealize Orchestrator](#).

Prerequisiti

- Configurare il server vRealize Log Insight. Consultare la *documentazione di vRealize Log Insight*.
- Verificare che la versione di vRealize Log Insight sia 4.7.1 o successiva.

Procedura

- 1 Accedere alla riga di comando di vRealize Orchestrator Appliance come **root**.
- 2 Per configurare l'integrazione della registrazione con vRealize Log Insight, eseguire il comando `vraccli vrli setvRLI_FQDN`.

Nota Se l'istanza di vRealize Orchestrator utilizza un certificato autofirmato, è possibile disabilitare l'autenticazione SSL includendo l'argomento facoltativo `-k` o `--insecure`.

Operazioni successive

Per ulteriori informazioni sulle opzioni di configurazione di vRealize Log Insight, eseguire il comando `vraccli vrli -h`.

Creazione o sovrascrittura di un'integrazione syslog in vRealize Orchestrator

È possibile configurare vRealize Orchestrator per l'invio delle informazioni di registrazione a uno o più server syslog remoti.

Il comando `vraccli remote-syslog set` viene utilizzato per creare un'integrazione syslog o sovrascrivere le integrazioni esistenti.

L'integrazione syslog remota di vRealize Orchestrator supporta tre tipi di connessione:

- Tramite UDP.
- Tramite TCP senza TLS.

Nota Per creare un'integrazione syslog senza utilizzare TLS, aggiungere il flag `--disable-ssl` al comando `vraccli remote-syslog set`.

- Tramite TCP con TLS.

Per informazioni sulla configurazione di un'integrazione di registrazione con vRealize Log Insight, vedere [Configurazione dell'integrazione della registrazione con vRealize Log Insight](#).

Prerequisiti

Configurare uno o più server syslog remoti.

Procedura

- 1 Accedere alla riga di comando di vRealize Orchestrator Appliance come **root**.
- 2 Per creare un'integrazione in un server syslog, eseguire il comando `vraccli remote-syslog set`.

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

Nota Se non si immette una porta nel comando `vraccli remote-syslog set`, viene utilizzato il valore di porta predefinito, ovvero 514.

Nota È possibile aggiungere un certificato alla configurazione syslog. Per aggiungere un file di certificato, utilizzare il flag `--ca-file`. Per aggiungere un certificato come testo normale, utilizzare il flag `--ca-cert`.

- 3 (Facoltativo) Per sovrascrivere un'integrazione syslog esistente, eseguire `vraccli remote-syslog set` e impostare il valore del flag `-id` sul nome dell'integrazione che si desidera sovrascrivere.

Nota Per impostazione predefinita, vRealize Orchestrator Appliance chiede di confermare se si desidera sovrascrivere l'integrazione syslog. Per ignorare la richiesta di conferma, aggiungere il flag `-f` o `--force` al comando `vraccli remote-syslog set`.

Operazioni successive

Per rivedere le integrazioni syslog correnti nell'appliance, eseguire il comando `vraccli remote-syslog`.

Eliminazione di un'integrazione syslog in vRealize Orchestrator

È possibile eliminare integrazioni syslog da vRealize Orchestrator Appliance eseguendo il comando `vraccli remote-syslog unset`.

Prerequisiti

Creare una o più integrazioni syslog in vRealize Orchestrator Appliance. Vedere [Creazione o sovrascrittura di un'integrazione syslog in vRealize Orchestrator](#).

Procedura

- 1 Accedere alla riga di comando di vRealize Orchestrator Appliance come **root**.

2 Eliminare le integrazioni syslog da vRealize Orchestrator Appliance.

- a Per eliminare un'integrazione syslog specifica, eseguire il comando `vracli remote-syslog unset -id Integration_name`.
- b Per eliminare tutte le integrazioni syslog in vRealize Orchestrator Appliance, eseguire il comando `vracli remote-syslog unset` senza il flag `-id`.

Nota Per impostazione predefinita, vRealize Orchestrator Appliance chiede di confermare che si desidera eliminare tutte le integrazioni syslog. Per ignorare la richiesta di conferma, aggiungere il flag `-f` o `--force` al comando `vracli remote-syslog unset`.

Abilitazione della registrazione del debug di Kerberos

È possibile risolvere i problemi del plug-in vRealize Orchestrator modificando il file di configurazione di Kerberos utilizzato dal plug-in.

Il file di configurazione di Kerberos si trova nella directory `/data/vco/usr/lib/vco/app-server/conf/` di vRealize Orchestrator Appliance.

Procedura

- 1 Accedere alla riga di comando di vRealize Orchestrator Appliance come **root**.
- 2 Eseguire il comando `kubect1 -n prelude edit deployment vco-app`.
- 3 Nel file di distribuzione, individuare e modificare la stringa `-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 Salvare le modifiche e uscire dall'editor di file.
- 5 Eseguire il comando `kubect1 -n prelude get pods`.
Attendere che tutti i pod siano in esecuzione.
- 6 Verificare che la registrazione del debug di Kerberos sia abilitata.

```
kubect1 -n prelude log {vco_app_name} -c vco-server-app | grep krb5
```

Verificare che i registri contengano un messaggio simile.

```
kubect1 -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
```

Abilitazione delle estensioni OpenTracing e Wavefront

Le estensioni OpenTracing e Wavefront per vRealize Orchestrator forniscono strumenti per la raccolta dei dati relativi all'ambiente di vRealize Orchestrator. È possibile utilizzare questi dati per la risoluzione dei problemi relativi al sistema e ai workflow di vRealize Orchestrator.

Prima di poter configurare vRealize Orchestrator per l'utilizzo delle estensioni OpenTracing e Wavefront, è necessario abilitarle in vRealize Orchestrator Appliance.

Prerequisiti

Verificare che il servizio SSH di vRealize Orchestrator Appliance sia abilitato. Vedere [Abilitazione o disabilitazione dell'accesso SSH a vRealize Orchestrator Appliance](#).

Procedura

- 1 Accedere a vRealize Orchestrator Appliance tramite SSH come **root**.
- 2 Eseguire il comando `kubectl -n prelude get pod`.
- 3 Per visualizzare un elenco di tutte le estensioni disponibili, eseguire il comando `kubectl -n prelude exec -it vco-app-your_pod_ID -c vco-server-app -- ls /var/lib/vco/app-server/extensions`.
- 4 Eseguire il comando seguente per abilitare l'estensione OpenTracing.

```
kubectl -n prelude exec -it vco-app-your_pod_ID -c vco-server-app --
mv /var/lib/vco/app-server/extensions/
opentracing-8.1.0.jar.inactive /var/lib/vco/app-server/extensions/
opentracing-8.1.0.jar
```
- 5 Eseguire il comando seguente per abilitare l'estensione Wavefront.

```
kubectl -n prelude exec -it vco-app-your_pod_ID -c vco-server-app --
mv /var/lib/vco/app-server/extensions/wavefront-8.1.0.jar.inactive /var/lib/vco/
app-server/extensions/wavefront-8.1.0.jar
```
- 6 Accedere al Centro di controllo e verificare che le estensioni vengano visualizzate nella pagina **Proprietà estensione**.

Operazioni successive

Configurare l'integrazione di OpenTracing e Wavefront con vRealize Orchestrator nella pagina **Proprietà estensione**. Vedere [Configurazione dell'estensione OpenTracing](#) e [Configurazione dell'estensione Wavefront](#).

Configurazione dell'estensione OpenTracing

L'estensione OpenTracing invia i dati relativi alle esecuzioni dei workflow a un server Jaeger. I dati includono lo stato del workflow, i parametri di input e output, l'utente che ha avviato l'esecuzione del workflow e i dati dell'ID del workflow.

Prerequisiti

- Verificare che OpenTracing sia abilitato in vRealize Orchestrator Appliance. Vedere [Abilitazione delle estensioni OpenTracing e Wavefront](#).
- Distribuire un server Jaeger per l'utilizzo nell'estensione OpenTracing. Per ulteriori informazioni, vedere la [documentazione introduttiva di Jaeger](#).

Procedura

- 1 Accedere al Centro di controllo come **root**.
- 2 Selezionare la pagina **Proprietà estensione**.
- 3 Selezionare l'estensione OpenTracing.
- 4 Immettere l'indirizzo host e la porta del server Jaeger.

Nota Inserire due barre ("/") prima di immettere l'indirizzo del server.

- 5 Fare clic su **Salva**.

Risultati

È stata configurata l'estensione OpenTracing per vRealize Orchestrator.

Operazioni successive

- Per accedere all'interfaccia utente di Jaeger contenente i dati raccolti dall'estensione OpenTracing, visitare l'indirizzo host immesso durante la configurazione.
- Nell'opzione **Servizio**, selezionare **Workflow**.
- Per specificare i dati da visualizzare, utilizzare l'opzione **Tag**. Ad esempio, per visualizzare i dati relativi ai workflow non riusciti, immettere **status=failed**.

Configurazione dell'estensione Wavefront

Utilizzare l'estensione Wavefront per raccogliere i dati delle metriche relativi al sistema e ai workflow di vRealize Orchestrator.

Prerequisiti

- 1 Verificare che Wavefront sia abilitato in vRealize Orchestrator Appliance. Vedere [Abilitazione delle estensioni OpenTracing e Wavefront](#).
- 2 Importare il certificato di Wavefront:
 - a Accedere al Centro di controllo di vRealize Orchestrator come **root**.
 - b Selezionare la pagina **Certificati**.
 - c Fare clic sul menu a discesa **Importa** e selezionare **Importa da URL**.
 - d Immettere l'URL di Wavefront e fare clic su **Importa**.

- 3 Configurare un proxy Wavefront. Per ulteriori informazioni, vedere [Installazione e gestione dei proxy Wavefront](#).

Procedura

- 1 Accedere al Centro di controllo di vRealize Orchestrator come **root**.
- 2 Selezionare la pagina **Proprietà estensione**.
- 3 Selezionare l'estensione Wavefront.
- 4 Configurare le proprietà di Wavefront.

Opzione	Descrizione
Proxy	Indirizzo del proxy Wavefront.
Host	Facoltativo. Indirizzo host di Wavefront.
Token	Facoltativo. Token dell'API di Wavefront. Per ulteriori informazioni sulla generazione di un token dell'API di Wavefront, vedere Generazione di un token dell'API .
Prefisso	Aggiungere etichette del prefisso per ogni metrica inviata a Wavefront. Le etichette del prefisso sono separate da un simbolo di punto.

- 5 (Facoltativo) Selezionare **Invia al dashboard predefinito al prossimo avvio**.
- 6 Fare clic su **Salva**.

Risultati

È stata configurata l'estensione Wavefront per vRealize Orchestrator.

Operazioni successive

- Per accedere alle metriche raccolte da Wavefront, accedere al dashboard all'indirizzo immesso durante la configurazione.
- Per ricevere notifiche su eventi specifici dell'ambiente di vRealize Orchestrator, è possibile utilizzare gli avvisi di Wavefront. Per ulteriori informazioni, vedere la [documentazione degli avvisi di Wavefront](#).

Abilitazione della sincronizzazione dell'ora per vRealize Orchestrator

È possibile abilitare la sincronizzazione dell'ora nella distribuzione di vRealize Orchestrator con la riga di comando di vRealize Orchestrator Appliance.

È possibile configurare la sincronizzazione dell'ora per la distribuzione di vRealize Orchestrator autonoma o in cluster utilizzando il protocollo di comunicazione NTP (Network Time Protocol). vRealize Orchestrator supporta due configurazioni NTP reciprocamente esclusive:

Configurazione NTP	Descrizione
ESXi	<p>Questa configurazione può essere utilizzata quando il server ESXi che ospita vRealize Orchestrator Appliance è sincronizzato con un server NTP. Se si utilizza una distribuzione in cluster, tutti gli host ESXi devono essere sincronizzati con un server NTP. Per ulteriori informazioni sulla configurazione di NTP per ESXi, vedere Configurazione di NTP (Network Time Protocol) in un host ESXi mediante vSphere Web Client.</p> <p>Nota Se la distribuzione di vRealize Orchestrator viene migrata in un host ESXi che non è sincronizzato con un server NTP, è possibile che si verifichi la deviazione dell'orologio.</p>
systemd	<p>Questa configurazione utilizza il daemon systemd-timesyncd per sincronizzare gli orologi della distribuzione di vRealize Orchestrator.</p> <p>Nota Per impostazione predefinita, il daemon systemd-timesyncd è abilitato, ma è configurato senza server NTP. Se vRealize Orchestrator Appliance utilizza una configurazione IP dinamica, l'appliance può utilizzare tutti i server NTP ricevuti dal protocollo DHCP.</p>

Procedura

- 1 Accedere alla riga di comando di vRealize Orchestrator Appliance come **root**.
- 2 Abilitazione di NTP con ESXi.
 - a Eseguire il comando `vracli ntp esxi`.
 - b Eseguire il comando `vracli ntp apply`.

La configurazione di NTP per ESXi viene applicata alla distribuzione di vRealize Orchestrator.
- 3 Abilitazione di NTP con systemd.
 - a Eseguire il comando `vracli ntp systemd --set FQDN_or_IP_of_systemd_server`.

Nota È possibile aggiungere più server NTP systemd separando gli indirizzi di rete con una virgola.
 - b Eseguire il comando `vracli ntp apply`.

La configurazione di NTP per systemd viene applicata alla distribuzione di vRealize Orchestrator.
- 4 (Facoltativo) Per verificare lo stato della configurazione NTP, eseguire il comando `vracli ntp status`.

Operazioni successive

È possibile che la configurazione di NTP non riesca se la differenza temporale tra il server NTP e la distribuzione di vRealize Orchestrator è superiore a 10 minuti. Per risolvere questo problema, riavviare vRealize Orchestrator Appliance.

Disabilitazione della sincronizzazione dell'ora per vRealize Orchestrator

È possibile disabilitare la sincronizzazione dell'ora del protocollo NTP (Network Time Protocol) nella distribuzione di vRealize Orchestrator con la riga di comando di vRealize Orchestrator Appliance.

È inoltre possibile ripristinare lo stato predefinito della configurazione NTP di vRealize Orchestrator Appliance eseguendo il comando `vraccli ntp reset`. Dopo aver ripristinato la configurazione, è necessario applicare le modifiche eseguendo il comando `vraccli ntp apply`.

Prerequisiti

Verificare di aver configurato la sincronizzazione dell'ora con ESXi o systemd. Vedere [Abilitazione della sincronizzazione dell'ora per vRealize Orchestrator](#).

Procedura

- 1 Accedere alla riga di comando di vRealize Orchestrator Appliance come **root**.
- 2 Per disabilitare la sincronizzazione dell'ora con ESXi o systemd, eseguire il comando `vraccli ntp disable`.
- 3 Eseguire il comando `vraccli ntp apply`.
- 4 (Facoltativo) Per verificare lo stato della configurazione NTP, eseguire il comando `vraccli ntp status`.

Casi d'uso di configurazione e risoluzione dei problemi

8

I casi d'uso di configurazione forniscono flussi di attività che è possibile eseguire per soddisfare i requisiti di configurazione specifici del server vRealize Orchestrator, nonché argomenti relativi alla risoluzione dei problemi per comprendere e risolvere un problema.

Questo capitolo include i seguenti argomenti:

- [Configurazione del plug-in vRealize Orchestrator per vSphere Web Client](#)
- [Annullamento dei workflow in esecuzione](#)
- [Abilitazione del debug del server vRealize Orchestrator](#)
- [Ridimensionamento dei dischi di vRealize Orchestrator Appliance](#)
- [Come scalare le dimensioni della memoria heap del server vRealize Orchestrator](#)
- [Ripristino di emergenza di vRealize Orchestrator mediante Site Recovery Manager](#)

Configurazione del plug-in vRealize Orchestrator per vSphere Web Client

Per utilizzare il plug-in vRealize Orchestrator per vSphere Web Client, è necessario registrare vRealize Orchestrator come estensione di vCenter Server.

Dopo aver registrato il server vRealize Orchestrator in vCenter Single Sign-On e averlo configurato in modo che funzioni con vCenter Server, è necessario registrare vRealize Orchestrator come estensione di vCenter Server.

Prerequisiti

- Verificare che l'accesso SSH sia abilitato per vRealize Orchestrator Appliance. Vedere [Abilitazione o disabilitazione dell'accesso SSH a vRealize Orchestrator Appliance](#).
- È necessario registrare vRealize Orchestrator con l'autenticazione vSphere nello stesso Platform Services Controller in cui vCenter Server gestito esegue l'autenticazione.
- Copiare `vco-plugin.zip` in vRealize Orchestrator Appliance:
 - a Scaricare il file `vco-plugin.zip` da [VMware Technology Network](#).

- b Aprire un client SSH.

Nota Per gli ambienti Linux o MacOS, è possibile utilizzare l'interfaccia della riga di comando del terminale. Per gli ambienti Windows, è possibile utilizzare il client PuTTY.

- c Per copiare il file `vco-plugin.zip`, eseguire il comando Secure Copy.

```
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
```

Procedura

- 1 Accedere a vRealize Orchestrator Client.
- 2 Passare a **Libreria > Workflow**.
- 3 Cercare il workflow **Registra vCenter Orchestrator come estensione di vCenter Server** e fare clic su **Esegui**.
- 4 Selezionare l'istanza di vCenter Server in cui registrare vRealize Orchestrator.
- 5 Immettere `https://your_orchestrator_FQDN` o l'URL del servizio del bilanciamento del carico che reindirizza le richieste ai nodi del server vRealize Orchestrator.
- 6 Fare clic su **Esegui**.

Annullamento dei workflow in esecuzione

È possibile utilizzare il Centro di controllo di vRealize Orchestrator per annullare i workflow che non vengono completati correttamente.

Procedura

- 1 Accedere al Centro di controllo come **root**.
- 2 Fare clic su **Risoluzione dei problemi**.

3 Annullare i workflow in esecuzione.

Opzione	Descrizione
Annulla tutte le esecuzioni dei workflow	Immettere un ID workflow per annullare tutti i token per tale workflow.
Annulla esecuzioni workflow in base all'ID	Immettere tutti gli ID token che si desidera annullare. Separare gli ID con una virgola.
Annulla tutti i workflow in esecuzione	Annulla tutti i workflow in esecuzione sul server.

Nota È possibile che le operazioni in cui si annullano i workflow in base all'ID non vengano eseguite correttamente perché non esiste un modo affidabile per annullare immediatamente il thread di esecuzione.

Risultati

Al successivo avvio del server, i workflow vengono impostati sullo stato Annullato.

Abilitazione del debug del server vRealize Orchestrator

È possibile avviare il server vRealize Orchestrator in modalità di debug per eseguire il debug dei problemi durante lo sviluppo di un plug-in.

Prerequisiti

Installare e configurare lo strumento della riga di comando di Kubernetes nella macchina locale. Vedere [Installazione e configurazione di kubectl](#).

Procedura

- 1 Accedere alla riga di comando di vRealize Orchestrator Appliance come **root**.
- 2 Eseguire il comando `kubectl -n prelude edit deployment vco-app`.
- 3 Modificare il file YAML di distribuzione aggiungendo una variabile di ambiente di debug al contenitore `vco-server-app`. La variabile deve essere aggiunta nella sezione `env` del contenitore `vco-server-app`.

```
containers:
  - command:
    ...
    env:
      - name: DEBUG_PORT
```

```

        value: "your_desired_debug_port"
    ...
name: vco-server-app
    ...

```

Nota Quando si aggiunge la variabile di ambiente di debug alla sezione `env`, è necessario seguire la formattazione di indentazione di YAML come illustrato nell'esempio precedente.

4 Salvare le modifiche apportate al file di distribuzione.

Se la modifica del file di distribuzione viene eseguita correttamente, viene visualizzato il messaggio `deployment.extensions/vco-app edited`.

5 Generare il file di configurazione di Kubernetes eseguendo il comando `vracli dev kubeconfig`.

Poiché `kubeconfig` è un ambiente di sviluppo, viene richiesto di confermare se si desidera continuare. Immettere **yes** per continuare o **no** per interrompere l'operazione.

6 Copiare il contenuto del file di configurazione generato da `apiVersion: v1` fino al contenuto di `client-key-data` incluso.

7 Salvare il file di configurazione di Kubernetes generato nella macchina locale.

8 Disconnettersi da vRealize Orchestrator Appliance.

9 Completare la configurazione della modalità di debug nella macchina locale.

- a Aprire una shell della riga di comando.
- b Associare la variabile di ambiente `KUBECONFIG` al file di configurazione salvato.

Nota Questo esempio si basa su un ambiente Linux.

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

- c Per verificare che i servizi siano in esecuzione, eseguire il comando `kubectl cluster-info`.
- d Per completare la configurazione della modalità di debug, eseguire la seguente richiesta dell'API di Kubernetes.

Nota Il valore della variabile `localhost_debug_port` indica la porta impostata nella configurazione di debug remoto di IDE (Integrated Development Environment). Il valore della variabile `vro_debug_port` viene generato durante il passaggio 3 di questa procedura.

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

Importante Quando si configura lo strumento di debug, specificare le impostazioni DNS e IP della macchina locale in cui è stato eseguito il comando di port forwarding.

Risultati

È stato configurato il debug del server per vRealize Orchestrator Appliance.

Ridimensionamento dei dischi di vRealize Orchestrator Appliance

È possibile modificare le dimensioni del disco di vRealize Orchestrator Appliance modificando le impostazioni delle dimensioni del disco della macchina virtuale di vRealize Orchestrator Appliance in vSphere.

Prerequisiti

Verificare che il servizio SSH di vRealize Orchestrator Appliance sia abilitato. Vedere [Abilitazione o disabilitazione dell'accesso SSH a vRealize Orchestrator Appliance](#).

Procedura

- 1 Verificare lo spazio su disco attualmente disponibile in vRealize Orchestrator Appliance.

Nota I dischi di vRealize Orchestrator Appliance richiedono almeno il 20% di spazio libero su disco.

- a Accedere alla riga di comando di vRealize Orchestrator Appliance tramite SSH come **root**.
 - b Eseguire il comando `vracli disk-mgr`.
- 2 Ridimensionare il disco della macchina virtuale di vRealize Orchestrator Appliance in vSphere.
 - a Accedere a vSphere Client come **amministratore**.
 - b Spegnerla la macchina virtuale di vRealize Orchestrator Appliance.
 - c Fare clic con il pulsante destro del mouse sulla macchina virtuale e scegliere **Modifica impostazioni**.
 - d Nella scheda **Hardware virtuale** espandere **Disco rigido** per visualizzare e modificare le impostazioni del disco, quindi fare clic su **OK**.

Per ulteriori informazioni sulla modifica delle dimensioni del disco delle macchine virtuali di vSphere, vedere *Modifica configurazione disco virtuale in Amministrazione della macchina virtuale vSphere*.

Come scalare le dimensioni della memoria heap del server vRealize Orchestrator

È possibile scalare le dimensioni della memoria heap del server vRealize Orchestrator modificando il file di distribuzione.

È possibile modificare le dimensioni della memoria heap del server vRealize Orchestrator, in modo che l'ambiente di orchestrazione possa gestire i carichi di lavoro che cambiano. È ad esempio possibile aumentare la memoria heap della distribuzione di vRealize Orchestrator se si intende gestire più server vCenter.

Prerequisiti

- Abilitare l'accesso SSH a vRealize Orchestrator Appliance. Vedere [Abilitazione o disabilitazione dell'accesso SSH a vRealize Orchestrator Appliance](#).
- Aumentare la RAM della macchina virtuale in cui è distribuito vRealize Orchestrator fino all'incremento successivo appropriato. Per informazioni su come aumentare la RAM di una macchina virtuale in vSphere, vedere *Modifica della configurazione della memoria in Amministrazione della macchina virtuale vSphere*.

Procedura

- 1 Accedere alla riga di comando di vRealize Orchestrator Appliance tramite SSH come **root**.
- 2 Passare alla directory `/opt/charts/vco/templates/`.
- 3 Eseguire il backup del file `deployment.yaml`.

```
cp deployment.yaml /tmp/
```

- 4 Utilizzando l'editor preferito, modificare il file `deployment.yaml`.

```
vi deployment.yaml
```

- 5 Cercare le righe contenenti la stringa `env` finché non si trova il contenitore `vco-server-app`.

```
- name: vco-server-app
  image: {{ .Values.image.repository }}:{{ .Values.image.tag }}
  env:
    - name: JAVA_PROXY_SCHEMEE
```

- 6 Nella sezione `env`, aggiungere una variabile di ambiente `JVM_HEAP` con un valore, dove `{DESIRED_HEAP_SIZE}` corrisponde alle nuove dimensioni della memoria heap desiderate, ad esempio 4G.

```
- name: vco-server-app
  image: {{ .Values.image.repository }}:{{ .Values.image.tag }}
  env:
    - name: JVM_HEAP
      value: {DESIRED_HEAP_SIZE}
    - name: JAVA_PROXY_SCHEME
```

- 7 Cercare le righe contenenti la stringa `memory: 5G` nel file di distribuzione.

Nota Il file di distribuzione può includere una sola stringa `memory: 5G`.

```
resources:
  limits:
    memory: 5G
  requests:
    memory: 4G
```

- 8 Aumentare i limiti e le richieste dei contenitori.

Attenzione Il valore `memory:` di `limits` deve essere 2 Gigabyte superiore al valore della memoria `JVM_HEAP` nel passaggio 6. Ad esempio, se il valore nel passaggio 6 è `value: 4G`, è necessario impostare il valore della memoria di `limits` su `memory: 6G`. Il valore di `requests: memory` deve essere 1 Gigabyte superiore al valore della memoria `JVM_HEAP` nel passaggio 6. Ad esempio, se il valore dell'heap nel passaggio 6 è `value: 4G`, è necessario impostare il valore di `requests: memory` su `memory: 5G`.

```
resources:
  limits:
    memory: {Desired heap size + 2G}
  requests:
    memory: {Desired heap size + 1G}
```

- 9 Salvare le modifiche apportate al file di distribuzione e passare alla directory `/opt/scripts`.

Nota Per gli ambienti in cluster, eseguire i passaggi precedenti in tutti i nodi del cluster.

- 10 Eseguire il comando `deploy.sh`.

Nota Per gli ambienti in cluster, eseguire lo script di distribuzione nel nodo primario.

Risultati

Sono state modificate le dimensioni della memoria heap del server vRealize Orchestrator.

Ripristino di emergenza di vRealize Orchestrator mediante Site Recovery Manager

È necessario configurare Site Recovery Manager per proteggere vRealize Orchestrator. Applicare questa protezione completando le attività di configurazione comuni per Site Recovery Manager.

Preparare l'ambiente

Prima di iniziare a configurare Site Recovery Manager, è necessario assicurarsi che siano soddisfatti i prerequisiti seguenti.

- Verificare che vSphere 6.0 o versione successiva sia installato nel sito protetto e nel sito di ripristino.
- Assicurarsi di utilizzare Site Recovery Manager 8.1 o versione successiva.
- Verificare che vRealize Orchestrator sia configurato.

Configurazione delle macchine virtuali per vSphere Replication

Per poter utilizzare Site Recovery Manager, è necessario configurare le macchine virtuali per vSphere Replication o la replica basata su array.

Per abilitare vSphere Replication nelle macchine virtuali necessarie, eseguire i passaggi seguenti.

Procedura

- 1 In vSphere Web Client, selezionare una macchina virtuale in cui abilitare vSphere Replication e fare clic su **Azioni > Tutte le azioni di vSphere Replication > Configura replica**.
- 2 Nella finestra **Tipo di replica**, selezionare **Esegui replica in un vCenter Server** e fare clic su **Avanti**.
- 3 Nella finestra **Sito target**, selezionare vCenter per il sito di ripristino e fare clic su **Avanti**.
- 4 Nella finestra **Server di replica**, selezionare un server vSphere Replication e fare clic su **Avanti**.
- 5 Nella finestra **Posizione target**, fare clic su **Modifica** e selezionare l'archivio dati target in cui verranno archiviati i file replicati, quindi fare clic su **Avanti**.
- 6 Nella finestra **Opzioni replica**, mantenere le impostazioni predefinite e fare clic su **Avanti**.
- 7 Nella finestra **Impostazioni ripristino**, immettere l'ora per **Recovery Point Objective (RPO)** e **Istanze punti temporali**, quindi fare clic su **Avanti**.
- 8 Nella finestra **Pronto per il completamento**, verificare le impostazioni e fare clic su **Fine**.
- 9 Ripetere questi passaggi per tutte le macchine virtuali in cui è necessario abilitare vSphere Replication.

Creazione di gruppi di protezione

È possibile creare gruppi di protezione per consentire a Site Recovery Manager di proteggere le macchine virtuali.

È possibile organizzare i gruppi di protezione in cartelle. Nella scheda **Gruppi di protezione** sono visualizzati i nomi dei gruppi di protezione, ma non sono specificate le cartelle in cui si trovano. Se sono presenti due gruppi di protezione con lo stesso nome in cartelle diverse, potrebbe essere difficile distinguerli. È quindi consigliabile assicurarsi che i nomi dei gruppi di protezione siano univoci in tutte le cartelle. Negli ambienti in cui non tutti gli utenti dispongono di privilegi di visualizzazione per tutte le cartelle, non posizionare i gruppi di protezione in cartelle per essere sicuri dell'univocità dei nomi dei gruppi di protezione.

Quando si creano gruppi di protezione, attendere che le operazioni vengano completate nel modo previsto. Assicurarsi che Site Recovery Manager crei il gruppo di protezione e che la protezione delle macchine virtuali nel gruppo funzioni correttamente.

Prerequisiti

Verificare di aver eseguito una delle seguenti attività:

- Aver incluso macchine virtuali in datastore per cui è stata configurata la replica basata su array.
- Aver soddisfatto i *prerequisiti per i gruppi di protezione del criterio di storage* e aver rivisto i *limiti dei gruppi di protezione del criterio di storage* nella guida *Amministrazione di Site Recovery Manager*.
- Aver configurato vSphere Replication nelle macchine virtuali.
- Aver eseguito una combinazione di alcune o tutte le attività precedenti.

Procedura

- 1 In vSphere Client o vSphere Web Client, fare clic su **Site Recovery > Apri Site Recovery**.
- 2 Nella scheda Home di Site Recovery, selezionare una coppia di siti e fare clic su **Visualizza dettagli**.
- 3 Selezionare la scheda **Gruppi di protezione** e fare clic su **Nuovo** per creare un gruppo di protezione.
- 4 Nella pagina Nome e direzione immettere un nome e una descrizione per il gruppo di protezione, selezionare una direzione e fare clic su **Avanti**.
- 5 Nella pagina Tipo di gruppo di protezione, selezionare il tipo del gruppo di protezione e fare clic su **Avanti**.

Opzione	Azione
Crea gruppo di protezione con replica basata su array	Selezionare Gruppi di datastore (replica basata su array) e selezionare una coppia di array.
Crea gruppo di protezione di vSphere Replication	Selezionare Singole macchine virtuali (vSphere Replication) .
Crea gruppo di protezione criterio di storage	Selezionare Criteri di storage (replica basata su array) .

- 6 Selezionare i gruppi di datastore, le macchine virtuali o i criteri di storage da aggiungere al gruppo di protezione.

Opzione	Azione
Gruppi di protezione con replica basata su array	Selezionare i gruppi di datastore e fare clic su Avanti . Quando si seleziona un gruppo di datastore, le macchine virtuali contenute nel gruppo vengono visualizzate nella tabella Macchine virtuali.
Gruppi di protezione di vSphere Replication	Selezionare le macchine virtuali nell'elenco e fare clic su Avanti . Nell'elenco vengono visualizzate solo le macchine virtuali configurate per vSphere Replication e che non sono già presenti in un gruppo di protezione.
Gruppi di protezione dei criteri di storage	Selezionare i criteri di storage nell'elenco e fare clic su Avanti .

- 7 Nella pagina Piano di ripristino, è possibile aggiungere facoltativamente il gruppo di protezione a un piano di ripristino.

Opzione	Azione
Aggiungi a un piano di ripristino esistente	Aggiunge il gruppo di protezione a un piano di ripristino esistente.
Aggiungi a un nuovo piano di ripristino	Aggiunge il gruppo di protezione a un nuovo piano di ripristino. Se si seleziona questa opzione, è necessario immettere un nome per il piano di ripristino.
Non aggiungere al piano di ripristino adesso	Selezionare questa opzione se non si desidera aggiungere il gruppo di protezione a un piano di ripristino.

- 8 Rivedere le impostazioni e fare clic su **Fine**.

È possibile monitorare lo stato di avanzamento della creazione del gruppo di protezione nella scheda **Gruppo di protezione**.

- Per i gruppi di protezione con replica basata su array e vSphere Replication, se Site Recovery Manager ha applicato correttamente le mappature dell'inventario alle macchine virtuali protette, lo stato di protezione del gruppo di protezione è *OK*.
- Per i gruppi di protezione del criterio di storage, se Site Recovery Manager ha protetto correttamente tutte le macchine virtuali associate al criterio di storage, lo stato di protezione del gruppo di protezione è *OK*.
- Per i gruppi di protezione con replica basata su array e vSphere Replication, se non sono state configurate le mappature dell'inventario oppure se Site Recovery Manager non è stato in grado di applicarle, lo stato di protezione del gruppo di protezione è *Not Configured*.
- Per i gruppi di protezione dei criteri di storage, se Site Recovery Manager non è in grado di proteggere tutte le macchine virtuali associate al criterio di storage, lo stato di protezione del gruppo di protezione è *Not Configured*.

Operazioni successive

Per i gruppi di protezione con replica basata su array e vSphere Replication, se lo stato di protezione dei gruppi di protezione è *Not Configured*, applicare le mappature dell'inventario alle macchine virtuali:

- Per applicare le mappature dell'inventario a livello di sito o per verificare che le mappature dell'inventario già impostate siano valide, consultare *Configurazione delle mappature dell'inventario* nella guida *Amministrazione di Site Recovery Manager*. Per applicare queste mappature a tutte le macchine virtuali, vedere *Applicazione delle mappature dell'inventario a tutti i membri di un gruppo di protezione* nella guida *Amministrazione di Site Recovery Manager*.
- Per applicare le mappature dell'inventario a ciascuna macchina virtuale nel gruppo di protezione singolarmente, vedere *Configurazione delle mappature dell'inventario per una singola macchina virtuale in un gruppo di protezione* nella guida *Amministrazione di Site Recovery Manager*.

Per i gruppi di protezione del criterio di storage, se lo stato di protezione del gruppo di protezione è *Not Configured*, verificare di aver soddisfatto i *prerequisiti per i gruppi di protezione del criterio di storage* e di aver rivisto i *limiti dei gruppi di protezione del criterio di storage* nella guida *Amministrazione di Site Recovery Manager*.

Creazione di un piano di ripristino

È possibile creare un piano di ripristino per stabilire in che modo Site Recovery Manager ripristina le macchine virtuali.

Procedura

- 1 In vSphere Client o vSphere Web Client, fare clic su **Site Recovery > Apri Site Recovery**.
- 2 Nella scheda Home di Site Recovery, selezionare una coppia di siti e fare clic su **Visualizza dettagli**.
- 3 Selezionare la scheda **Piani di ripristino** e fare clic su **Nuovo** per creare un piano di ripristino.
- 4 Immettere un nome, una descrizione e una direzione per il piano, selezionare una cartella e fare clic su **Avanti**.
- 5 Selezionare il tipo di gruppo nel menu.

Opzione	Descrizione
Gruppi di protezione per singole macchine virtuali o gruppi di datastore	Selezionare questa opzione per creare un piano di ripristino che contenga la replica basata su array e gruppi di protezione di vSphere Replication.
Gruppi di protezione dei criteri di storage	Selezionare questa opzione per creare un piano di ripristino che contenga gruppi di protezione dei criteri di storage. Se si utilizza lo storage esteso, selezionare questa opzione.

- 6 Selezionare uno o più gruppi di protezione per il piano di ripristino e fare clic su **Avanti**.

- 7 Nel menu a discesa **Rete test**, selezionare una rete da utilizzare durante il test di ripristino e fare clic su **Avanti**.

Se non sono presenti mappature a livello di sito, l'opzione predefinita **Utilizza mappatura a livello di sito** crea una rete di test isolata.

- 8 Rivedere le informazioni di riepilogo e fare clic su **Fine** per creare il piano di ripristino.

Organizzazione dei piani di ripristino in cartelle

Per controllare l'accesso di diversi utenti o gruppi ai piani di ripristino, è possibile organizzare i piani di ripristino in cartelle.

L'organizzazione dei piani di ripristino in cartelle è utile se si dispone di molti piani di ripristino. È possibile limitare l'accesso ai piani di ripristino posizionandoli in cartelle e assegnando autorizzazioni diverse per le cartelle a utenti o gruppi diversi. Per informazioni su come assegnare autorizzazioni per le cartelle, vedere *Assegnazione di ruoli e autorizzazioni di Site Recovery Manager* nella guida *Amministrazione di Site Recovery Manager*.

Procedura

- 1 Nella scheda Home di **Site Recovery**, selezionare una coppia di siti e fare clic su **Visualizza dettagli**.
- 2 Fare clic sulla scheda **Piani di ripristino** e nel riquadro a sinistra fare clic con il pulsante destro del mouse su **Piani di ripristino** e scegliere **Nuova cartella**.
- 3 Immettere un nome per la cartella da creare e fare clic su **Aggiungi**.
- 4 Aggiungere piani di ripristino nuovi o esistenti alla cartella.

Opzione	Descrizione
Crea nuovo piano di ripristino	Fare clic con il pulsante destro del mouse sulla cartella e scegliere Nuovo piano di ripristino .
Aggiungi piano di ripristino esistente	Fare clic con il pulsante destro del mouse su un piano di ripristino nell'albero dell'inventario e scegliere Sposta . Selezionare una cartella di destinazione e fare clic su Sposta .

Modifica di un piano di ripristino

È possibile modificare un piano di ripristino per modificare le proprietà specificate al momento della creazione. È possibile modificare i piani di ripristino dal sito protetto o dal sito di ripristino.

Procedura

- 1 In vSphere Client o vSphere Web Client, fare clic su **Site Recovery > Apri Site Recovery**.
- 2 Nella scheda Home di **Site Recovery**, selezionare una coppia di siti e fare clic su **Visualizza dettagli**.
- 3 Fare clic sulla scheda **Piani di ripristino**, fare clic con il pulsante destro del mouse su un piano di ripristino e scegliere **Modifica**.

- 4 (Facoltativo) Modificare il nome o la descrizione del piano, quindi fare clic su **Avanti**.

Non è possibile modificare la direzione e la posizione del piano di ripristino.

- 5 (Facoltativo) Selezionare o deselezionare uno o più gruppi di protezione per aggiungerli o rimuoverli dal piano e fare clic su **Avanti**.

- 6 (Facoltativo) Nel menu a discesa, selezionare una rete di test diversa nel sito di ripristino e fare clic su **Avanti**.

- 7 Rivedere le informazioni di riepilogo e fare clic su **Fine** per apportare le modifiche specificate al piano di ripristino.

È possibile monitorare l'aggiornamento del piano nella visualizzazione **Attività recenti**.

Impostazione delle proprietà di sistema

9

È possibile impostare proprietà di sistema per modificare il comportamento predefinito di Orchestrator.

Questo capitolo include i seguenti argomenti:

- [Impostazione dell'accesso al file system del server per workflow e azioni](#)
- [Impostazione dell'accesso ai comandi del sistema operativo per workflow e azioni](#)
- [Impostazione dell'accesso di JavaScript alle classi Java](#)
- [Impostazione della proprietà del timeout personalizzato](#)
- [Aggiunta di un connettore JDBC per il plug-in SQL di vRealize Orchestrator](#)

Impostazione dell'accesso al file system del server per workflow e azioni

In vRealize Orchestrator, i workflow e le azioni hanno accesso limitato a determinate directory del file system. È possibile estendere l'accesso ad altre parti del file system del server modificando il file di configurazione `js-io-rights.conf`.

Regole del file `js-io-rights.conf` che consentono l'accesso in scrittura al sistema vRealize Orchestrator

Il file `js-io-rights.conf` contiene regole che consentono l'accesso in scrittura alle directory definite nel file system del server.

Contenuto obbligatorio del file `js-io-rights.conf`

Ciascuna riga del file `js-io-rights.conf` deve includere le informazioni seguenti.

- Un segno più (+) o meno (-) per indicare se i diritti sono consentiti o negati
- I livelli dei diritti lettura (r), scrittura (w) ed esecuzione (x)

- Il percorso in cui applicare i diritti.

Nota La cartella root del file `js-io-rights.conf` è sempre `/var/run/vco`. Nel file system di vRealize Orchestrator Appliance, questa cartella si trova in `/data/vco/var/run/vco`. Tutti i contenuti con accesso al file system di vRealize Orchestrator devono essere mappati sotto questa cartella root.

Contenuto predefinito del file `js-io-rights.conf`

Il contenuto predefinito del file `js-io-rights.conf` in Orchestrator Appliance è il seguente:

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

Le prime due righe del file di configurazione predefinito `js-io-rights.conf` consentono i seguenti diritti di accesso:

-rwx /

Tutto l'accesso al file system è negato.

+rwX /var/run/vco

L'accesso lettura, scrittura ed esecuzione è consentito nella directory `/var/run/vco`.

Regole nel file `js-io-rights.conf`

vRealize Orchestrator risolve i diritti di accesso nell'ordine in cui vengono visualizzati nel file `js-io-rights.conf`. Ogni riga può sostituire le righe precedenti.

Importante È possibile consentire l'accesso a tutte le parti del file system impostando `+rwX /` nel file `js-io-rights.conf`. Ciò rappresenta tuttavia un rischio elevato per la sicurezza.

Impostazione dell'accesso al file system del server per workflow e azioni

Per modificare le parti del file system del server a cui i workflow e l'API di vRealize Orchestrator possono accedere, modificare il file di configurazione `js-io-rights.conf`. Il file `js-io-rights.conf` viene creato quando un workflow tenta di accedere al file system del server di vRealize Orchestrator.

Procedura

- 1 Accedere alla riga di comando di vRealize Orchestrator Appliance come **root**.
- 2 Passare alla directory `/data/vco/var/run/vco/`.
- 3 Aprire il file di configurazione `js-io-rights.conf` in un editor di testo.

- 4 Aggiungere le righe necessarie al file `js-io-rights.conf` per consentire o negare l'accesso alle aree del file system.

Ad esempio, la riga seguente nega i diritti di esecuzione nella directory `/data/vco/var/run/vco/noexec`:

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

`/data/vco/var/run/vco/noexec` conserva i diritti di esecuzione, mentre `/data/vco/var/run/vco/noexec/bar` non li conserva. Entrambe le directory restano leggibili e scrivibili.

Risultati

Sono stati modificati i diritti di accesso al file system per i workflow e l'API di vRealize Orchestrator.

Impostazione dell'accesso ai comandi del sistema operativo per workflow e azioni

L'API di vRealize Orchestrator fornisce una classe di scripting, `Command`, che esegue i comandi nel sistema operativo host del server di vRealize Orchestrator. Per impedire l'accesso non autorizzato all'host del server, per impostazione predefinita, le applicazioni di vRealize Orchestrator non dispongono dell'autorizzazione per eseguire la classe `Command`. Se le applicazioni di vRealize Orchestrator richiedono l'autorizzazione per l'esecuzione dei comandi nel sistema operativo host, è possibile attivare la classe di scripting `Command`.

È possibile concedere l'autorizzazione a utilizzare la classe `Command` impostando una proprietà di sistema della configurazione di vRealize Orchestrator.

Procedura

- 1 Accedere al Centro di controllo come **root**.
- 2 Fare clic su **Proprietà di sistema**.
- 3 Fare clic su **Nuovo**.
- 4 Nella casella di testo **Chiave**, immettere **com.vmware.js.allow-local-process**.
- 5 Nella casella di testo **Valore**, immettere **true**.
- 6 Nella casella di testo **Descrizione**, immettere una descrizione per la proprietà di sistema.
- 7 Fare clic su **Aggiungi**.
- 8 Fare clic su **Salva modifiche** nel menu a comparsa.
Un messaggio indica che il salvataggio è stato eseguito correttamente.
- 9 Attendere il riavvio del server di vRealize Orchestrator.

Risultati

Ora le applicazioni di vRealize Orchestrator dispongono delle autorizzazioni per eseguire comandi locali nel sistema operativo host del server di vRealize Orchestrator.

Nota Impostando la proprietà di sistema `com.vmware.js.allow-local-process` su `true`, è possibile consentire alla classe di scripting `Command` di scrivere in qualsiasi punto del file system. Questa proprietà sostituisce qualsiasi autorizzazione di accesso al file system impostata nel file `js-io-rights.conf` solo per la classe di scripting `Command`. Le autorizzazioni di accesso al file system impostate nel file `js-io-rights.conf` si applicano comunque a tutte le classi di scripting diverse da `Command`.

Impostazione dell'accesso di JavaScript alle classi Java

Per impostazione predefinita, vRealize Orchestrator limita l'accesso di JavaScript a un set limitato di classi Java. Per consentire l'accesso di JavaScript a un intervallo più ampio di classi Java, è necessario impostare una proprietà di sistema di vRealize Orchestrator.

Se si consente al motore JavaScript l'accesso completo alla macchina virtuale Java (JVM), è possibile che si verifichino problemi di sicurezza. Gli script non validi o dannosi potrebbero accedere a tutti i componenti del sistema a cui l'utente che esegue il server di vRealize Orchestrator ha accesso. Per impostazione predefinita, il motore JavaScript di vRealize Orchestrator può pertanto accedere solo alle classi del pacchetto `java.util.*`.

Se si desidera che JavaScript acceda a classi che non si trovano nel pacchetto `java.util.*`, è possibile elencare in un file di configurazione i pacchetti Java a cui JavaScript deve poter accedere. È quindi necessario impostare la proprietà di sistema `com.vmware.scripting.rhino-class-shutter-file` in modo che punti a tale file.

Procedura

- 1 Creare un file di configurazione di testo per archiviare l'elenco dei pacchetti Java a cui JavaScript deve poter accedere.

Ad esempio, per consentire a JavaScript di accedere a tutte le classi del pacchetto `java.net` e alla classe `java.lang.Object`, aggiungere i seguenti contenuti al file.

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

- 2 Immettere un nome per il file di configurazione.
- 3 Salvare il file di configurazione in una sottodirectory di `/data/vco/usr/lib/vco`.

Nota Il file di configurazione non può essere salvato in un'altra directory.

- 4 Accedere al Centro di controllo come **root**.
- 5 Fare clic su **Proprietà di sistema**.

- 6 Fare clic su **Nuovo**.
- 7 Nella casella di testo **Chiave**, immettere `com.vmware.scripting.rhino-class-shutter-file`.
- 8 Nella casella di testo **Valore**, immettere `vco/usr/lib/vco/
your_configuration_file_subdirectory`.
- 9 Nella casella di testo **Descrizione**, immettere una descrizione per la proprietà di sistema.
- 10 Fare clic su **Aggiungi**.
- 11 Fare clic su **Salva modifiche** nel menu a comparsa.
Un messaggio indica che il salvataggio è stato eseguito correttamente.
- 12 Attendere il riavvio del server di vRealize Orchestrator.

Risultati

Il motore JavaScript può accedere alle classi Java specificate.

Impostazione della proprietà del timeout personalizzato

Quando si verifica l'overload di vCenter Server, per restituire la risposta al server di vRealize Orchestrator serve più tempo dei 20000 millisecondi predefiniti impostati. Per evitare questa situazione, è necessario modificare il file di configurazione di vRealize Orchestrator per aumentare il periodo di timeout predefinito.

Se il periodo di timeout predefinito scade prima del completamento di determinate operazioni, il registro del server di vRealize Orchestrator contiene errori.

```
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
```

Procedura

- 1 Accedere al Centro di controllo come **root**.
- 2 Fare clic su **Proprietà di sistema**.
- 3 Fare clic su **Nuovo**.
- 4 Nella casella di testo **Chiave** immettere `com.vmware.vmo.plugin.vi4.waitUpdatesTimeout`.
- 5 Nella casella di testo **Valore** immettere il nuovo periodo di timeout in millisecondi.
- 6 (Facoltativo) Nella casella di testo **Descrizione**, immettere una descrizione per la proprietà di sistema.
- 7 Fare clic su **Aggiungi**.
- 8 Fare clic su **Salva modifiche** nel menu a comparsa.
Un messaggio indica che il salvataggio è stato eseguito correttamente.

9 Riavviare il server di Orchestrator.

Risultati

Il valore impostato sostituisce il valore del timeout predefinito di 20000 millisecondi.

Aggiunta di un connettore JDBC per il plug-in SQL di vRealize Orchestrator

Questo esempio illustra come è possibile aggiungere un connettore MySQL per il plug-in SQL di vRealize Orchestrator.

Procedura

- 1 Aggiungere il file connector.jar di MySQL in vRealize Orchestrator Appliance.
 - a Accedere alla riga di comando di vRealize Orchestrator Appliance tramite SSH come **root**.
 - b Passare alla directory `/data/vco/var/run/vco`.

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

- c Creare una directory `plugins/SQL/lib/`.

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

- d Copiare il file connector.jar di MySQL dalla macchina locale alla directory `/data/vco/var/run/vco/plugins/SQL/lib/` eseguendo un comando Secure Copy (SCP).

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

Nota Per copiare il file connector.jar in vRealize Orchestrator Appliance, è inoltre possibile utilizzare metodi alternativi, ad esempio PSCP.

- 2 Aggiungere la nuova proprietà MySQL al Centro di controllo.
 - a Accedere al Centro di controllo come **root**.
 - b Selezionare **Proprietà di sistema**.
 - c Fare clic su **Nuovo**.
 - d In **Chiave**, immettere `o11n.plugin.SQL.classpath`.
 - e In **Valore**, immettere `/var/run/vco/plugins/SQL/lib/your_mysql_connector.jar`.

Nota La casella di testo del valore può includere più connettori JDBC. Ogni connettore JDBC è separato da un punto e virgola (;). Ad esempio:

```
/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 (Facoltativo) Immettere una descrizione per la proprietà di sistema MySQL.
- g Fare clic su **Aggiungi** e attendere il riavvio del server vRealize Orchestrator.

Nota Non salvare il file connector.jar di JDBC in un'altra directory e non impostare un valore diverso per la proprietà `o11n.plugin.SQL.classpath`. In caso contrario, il connettore JDBC non sarà disponibile per la distribuzione di vRealize Orchestrator.

Operazioni successive

10

Dopo aver installato e configurato vRealize Orchestrator, è possibile utilizzare vRealize Orchestrator per automatizzare i processi ripetuti di frequente correlati alla gestione dell'ambiente virtuale.

- Accedere a vRealize Orchestrator Client, eseguire e pianificare i workflow per gli oggetti dell'inventario di vCenter Server o altri oggetti a cui vRealize Orchestrator accede tramite i relativi plug-in. Vedere *Utilizzo di VMware vRealize Orchestrator Client*.
- Duplicare e modificare i workflow di vRealize Orchestrator standard e scrivere azioni e workflow personalizzati per automatizzare le operazioni in vCenter Server.
- Per estendere la funzionalità della piattaforma di vRealize Orchestrator, sviluppare plug-in.
- Gestire l'inventario di vRealize Orchestrator in più istanze di vRealize Orchestrator con l'integrazione di un repository Git remoto. Vedere *Utilizzo di VMware vRealize Orchestrator Client*.
- Eseguire i workflow per gli oggetti dell'inventario di vSphere utilizzando vSphere Web Client.