

Installazione di vRealize Automation

vRealize Automation 7.0



vmware®

È possibile consultare la documentazione tecnica più aggiornata sul sito Web all'indirizzo:

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

Inoltrare eventuali commenti sulla documentazione al seguente indirizzo:

docfeedback@vmware.com

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

VMware, Inc.
P.le Biancamano 8
20121 Milano
tel: 02-6203.2075
fax: 02-6203.4000
www.vmware.com/it

Copyright © 2008–2018 VMware Inc. Tutti i diritti sono riservati. [Informazioni sul copyright e sui marchi.](#)

Contenuti

Installazione di vRealize Automation 6

Informazioni aggiornate 7

1 Cenni generali sull'installazione di vRealize Automation 8

Scelta del percorso di distribuzione 8

Panoramica della distribuzione minima 10

Panoramica della distribuzione enterprise 10

Componenti d'installazione di vRealize Automation 11

Appliance VMware vRealize Automation 12

Agenti di gestione 12

vRealize Automation Infrastructure as a Service (IaaS) 12

2 Preparazione per l'installazione 16

DNS e risoluzione dei nomi host 16

Requisiti di hardware e macchine virtuali 17

Considerazioni sui browser 17

Considerazioni sulle password 17

Requisiti di Windows Server 18

Requisiti del server di database di IaaS 18

Requisiti del servizio Web IaaS e del Model Manager Server 19

Servizio di gestione di IaaS 20

Requisiti di Distributed Execution Manager 20

Requisiti delle porte 22

Account utente e credenziali richiesti per l'installazione 25

Sicurezza 26

Certificati 26

Estrazione di certificati e chiavi private 27

Passphrase di sicurezza 28

Software di terze parti 28

Sincronizzazione di data e ora 28

3 Installazione di vRealize Automation utilizzando l'installazione guidata 29

Distribuzione di vRealize Automation appliance 29

Installazione di una distribuzione minima con l'installazione guidata 31

Esecuzione dell'installazione guidata per una distribuzione minima 31

Installazione dell'agente di gestione 32

Sincronizzazione degli orari di server 36

Esecuzione di Controllo prerequisiti	36
Selezione dei parametri di configurazione della distribuzione	37
Creazione di snapshot prima di iniziare l'installazione	37
Scenario: completamento dell'installazione	38
Risoluzione dei problemi di installazione	38
Configurazione delle credenziali per la configurazione dei contenuti iniziali	39
Installazione di una distribuzione enterprise con l'installazione guidata	40
Esecuzione dell'installazione guidata per una distribuzione enterprise	40
Installazione dell'agente di gestione	41
Sincronizzazione degli orari di server	44
Esecuzione di Controllo prerequisiti	45
Selezione dei parametri di configurazione della distribuzione	45
Creazione di snapshot prima di iniziare l'installazione	46
Completamento dell'installazione	46
Risoluzione dei problemi di installazione	47
Configurazione delle credenziali per la configurazione dei contenuti iniziali	48
4 Installazione di vRealize Automation tramite le interfacce standard	49
Distribuzione minima	49
Elenco di controllo di una distribuzione minima	49
Distribuzione e configurazione dell'appliance vRealize Automation	50
Installazione dei componenti IaaS	56
Distribuzione distribuita	62
Elenco di controllo di una distribuzione distribuita	62
Componenti di un'installazione distribuita	63
Requisiti di attendibilità dei certificati in una distribuzione distribuita	64
Fogli di lavoro per l'installazione	65
Distribuzione di vRealize Automation appliance	67
Configurazione del bilanciamento del carico	69
Configurazione di appliance per vRealize Automation	69
Installazione dei componenti di IaaS in una configurazione distribuita	77
Installazione degli agenti	104
Impostare i criteri di esecuzione di PowerShell su RemoteSigned	105
Scelta dello scenario d'installazione degli agenti	106
Posizione d'installazione dell'agente e requisiti	106
Installazione e configurazione dell'agente proxy per vSphere	106
Installazione dell'agente proxy per Hyper-V o XenServer	112
Installazione dell'agente VDI per XenDesktop	117
Installazione dell'agente EPI per Citrix	121
Installazione dell'agente EPI per Visual Basic Scripting	124
Installazione dell'agente WMI per le richieste WMI remote	128

5	Configurazione dell'accesso per il tenant predefinito	131
6	Sostituzione di certificati autofirmati con certificati forniti da un'autorità	133
7	Risoluzione dei problemi	134
	Posizioni predefinite dei registri	134
	Rollback di un'installazione non riuscita	136
	Rollback di un'installazione minima	136
	Rollback di un'installazione distribuita	136
	Creazione di un bundle di supporto per vRealize Automation	137
	Risoluzione dei problemi correlati all'installazione generale	138
	Installazione o aggiornamento non riuscito con un errore di timeout del bilanciamento del carico	138
	Gli orari dei server non sono sincronizzati	138
	Quando si utilizza Internet Explorer 9 o 10 su Windows 7 possono presentarsi pagine vuote	139
	Impossibile stabilire una relazione basata sulla fiducia per il canale sicuro SSL/TLS	140
	Connessione alla rete attraverso un server proxy	140
	Il proxy impedisce l'accesso di utenti di VMware Identity Manager	141
	Risoluzione dei problemi delle appliance vRealize Automation	142
	Download non riuscito dei programmi d'installazione	142
	Il file Encryption.key ha autorizzazioni errate	142
	Identity Manager non si avvia dopo il riavvio di Horizon Workspace	143
	Risoluzione dei problemi relativi ai componenti IaaS	144
	Convalida dei certificati del server per IaaS	144
	Errore di credenziali quando si esegue il programma d'installazione di IaaS	145
	Visualizzazione di un avviso di salvataggio impostazioni durante l'installazione di IaaS	145
	Installazione del server del sito Web e del Distributed Execution Manager non riuscita	146
	L'autenticazione di IaaS non riesce durante l'installazione dei componenti di gestione modelli e Web di IaaS	146
	Installazione di Model Manager Data e componenti Web non riuscita	147
	L'aggiunta di un endpoint XaaS causa un errore interno	148
	Disinstallazione di un agente proxy non riuscita	149
	Le richieste delle macchine non riescono quando le transazioni remote sono disabilitate	149
	Errore di comunicazione nel servizio di gestione	150
	Il comportamento della personalizzazione email è cambiato	151
	Risoluzione degli errori di accesso	152
	I tentativi di accedere come amministratore di IaaS con credenziali in formato UPN errate terminano con esito negativo senza fornire dettagli	152
	Impossibile accedere a un tenant o scomparsa degli archivi identità dei tenant	152

Installazione di vRealize Automation

Installazione di vRealize Automation contiene le istruzioni da eseguire per installare VMware vRealize™ Automation.

Nota: non tutte le funzionalità di vRealize Automation sono disponibili in tutte le edizioni. Per un confronto delle funzioni presenti in ciascuna edizione, vedere <https://www.vmware.com/products/vrealize-automation/>.

Destinatari

Le presenti informazioni sono destinate ad amministratori Windows o Linux esperti che hanno familiarità con la tecnologia delle macchine virtuali e le operazioni di data center.

Glossario delle pubblicazioni tecniche di VMware

Il sito delle pubblicazioni tecniche di VMware Technical fornisce un glossario dei termini che potrebbero risultare non familiari. Per le definizioni dei termini utilizzati nella documentazione tecnica di VMware, consultare la pagina <http://www.vmware.com/support/pubs>.

Informazioni aggiornate

Il documento *Installing vRealize Automation 7.0* viene aggiornato a ogni versione del prodotto oppure quando necessario.

La tabella riporta la cronologia degli aggiornamenti della pubblicazione *Installing vRealize Automation 7.0*.

Revisione	Descrizione
IT-001835-04	Aggiornamenti dei prerequisiti di SQL Server. Vedere Requisiti del server di database di IaaS .
IT-001835-03	Procedure di risoluzione dei problemi aggiuntive.
IT-001835-02	Rimosse le procedure obsolete relative ai failover del database, dal Capitolo 4.
IT-001835-01	<ul style="list-style-type: none">■ Aggiunta di un nuovo scenario di distribuzione per l'installazione e la configurazione di un ambiente di prototipazione e sviluppo vRealize Automation. Per una trattazione generale sullo scenario di esempio, vedere Scelta del percorso di distribuzione. Per lo scenario completo, vedere <i>Installazione e configurazione di vRealize Automation per lo scenario Rainpole</i>.■ Diversi piccoli aggiornamenti per chiarire che l'alta disponibilità non è completamente configurata finché gli amministratori tenant non impostano Gestione directory per l'alta disponibilità.■ Aggiornamenti per la versione 7.0.1 di vRealize Automation.
IT-001835-00	Release del documento iniziale.

Cenni generali sull'installazione di vRealize Automation

1

vRealize Automation può essere distribuito in svariate configurazioni. Per garantire una corretta distribuzione, è essenziale conoscere le opzioni di distribuzione e configurazione e rispettare la sequenza di attività richieste.

Se non si ha familiarità con versioni precedenti di vRealize Automation, potrebbe essere utile conoscere i cambiamenti seguenti prima di iniziare l'installazione:

- Questa versione di vRealize Automation introduce l'installazione guidata, il metodo consigliato per installazioni senza script. Con l'installazione guidata è possibile scegliere una distribuzione minima o enterprise. Le distribuzioni enterprise sono basate su architetture distribuite e possono includere bilanciamenti del carico per garantire l'alta disponibilità. È possibile installare appliance vRealize Automation autonome o con componenti IaaS.
- La gestione del supporto per SSO (Single Sign-On) e delle identità viene eseguita mediante un VMware Identity Manager incorporato amministrato dalla nuova funzionalità Gestione directory. . Essa sostituisce l'uso di VMware Identity Appliance e delle implementazioni di vSphere SSO utilizzate dalle versioni di prodotto precedenti.
- Open LDAP non è più supportato.

Dopo l'installazione, gli amministratori di sistema possono personalizzare l'ambiente d'installazione e configurare uno o più tenant, definendo in tal modo gli aspetti che permettono di eseguire in autonomia il provisioning e la gestione del ciclo di vita dei servizi cloud.

Utilizzando l'interfaccia Web del portale sicuro, amministratori, sviluppatori e utenti aziendali possono richiedere servizi IT e gestire risorse cloud e IT specifiche in base ai propri ruoli e privilegi. Gli utenti possono richiedere servizi di infrastruttura, applicazioni, desktop e IT attraverso un catalogo di servizi comune.

Questo capitolo include i seguenti argomenti:

- [Scelta del percorso di distribuzione](#)
- [Componenti d'installazione di vRealize Automation](#)

Scelta del percorso di distribuzione

In base ai requisiti della distribuzione specifica, è possibile installare e configurare i componenti di vRealize Automation utilizzando lo scenario di installazione rainpole, l'installazione guidata oppure attraverso la console di gestione.

Scegliere un'installazione minima per distribuire un ambiente di prototipazione o di sviluppo con una topologia di base. Scegliere un'installazione enterprise per distribuire un ambiente di produzione con la topologia più adatta alle proprie esigenze organizzative.

Tavola 1-1. Scelta del metodo d'installazione

Metodo d'installazione	Dettagli
Installazione guidata	<p>L'installazione guidata rappresenta il percorso più veloce per la maggior parte delle distribuzioni. Si può scegliere una distribuzione minima o enterprise per supportare componenti distribuiti con o senza bilanciamenti del carico. Prima di avviare l'installazione guidata, completare e verificare tutti i prerequisiti.</p> <p>Per ulteriori informazioni, vedere Capitolo 2 Preparazione per l'installazione.</p>
Installazione manuale	<p>Le installazioni minime, distribuite e a disponibilità elevata possono inoltre essere eseguite tramite la console di gestione. Prima di avviare l'installazione, completare e verificare tutti i prerequisiti.</p> <p>Per ulteriori informazioni, vedere Capitolo 2 Preparazione per l'installazione.</p> <p>Nota: Se si avvia o configura una qualsiasi parte dell'installazione dalla console di gestione, non è possibile avviare o continuare con l'installazione guidata.</p>
<i>Installazione e configurazione di vRealize Automation per lo scenario Rainpole</i>	<p>In qualità di amministratore di vSphere, è preferibile installare una distribuzione minima di vRealize Automation nell'ambiente vSphere esistente. Per installare vRealize Automation e creare gli elementi iniziali del catalogo si utilizza l'installazione guidata in modo da poter configurare rapidamente un ambiente in cui utilizzare una distribuzione di prova.</p> <p>Una distribuzione di prova non è utilizzabile per la produzione. Una volta completata la distribuzione di prova, configurarla come ambiente di distribuzione quando, insieme al team IT, si procede alla creazione e al test dei blueprint. È possibile esportare i blueprint e altri elementi di progettazione all'esterno dell'ambiente di sviluppo e all'interno del proprio ambiente di produzione.</p> <p>Per avviare questo scenario, vedere <i>Installazione e configurazione di vRealize Automation per lo scenario Rainpole</i>.</p>

Tavola 1-2. Scelta del tipo di distribuzione

Scopo della distribuzione	Tipo di distribuzione da scegliere
Distribuire un ambiente di prototipazione o di sviluppo con una topologia di base.	<p>Installare una distribuzione minima.</p> <p>Distribuire una singola istanza di vRealize Automation appliance e installare tutti i componenti di IaaS su un'unica macchina Windows server. È possibile installare i database sulla stessa macchina Windows o su un SQL Server dedicato.</p>
Distribuire un ambiente di produzione con la topologia più adatta alle proprie esigenze organizzative.	<p>Installare una distribuzione enterprise.</p> <p>I componenti vengono distribuiti su più server.</p> <p>Facoltativamente è possibile distribuire bilanciamenti del carico per ripartire il lavoro su più server in un ambiente a disponibilità elevata, per garantire funzionalità di failover e ridondanza.</p>

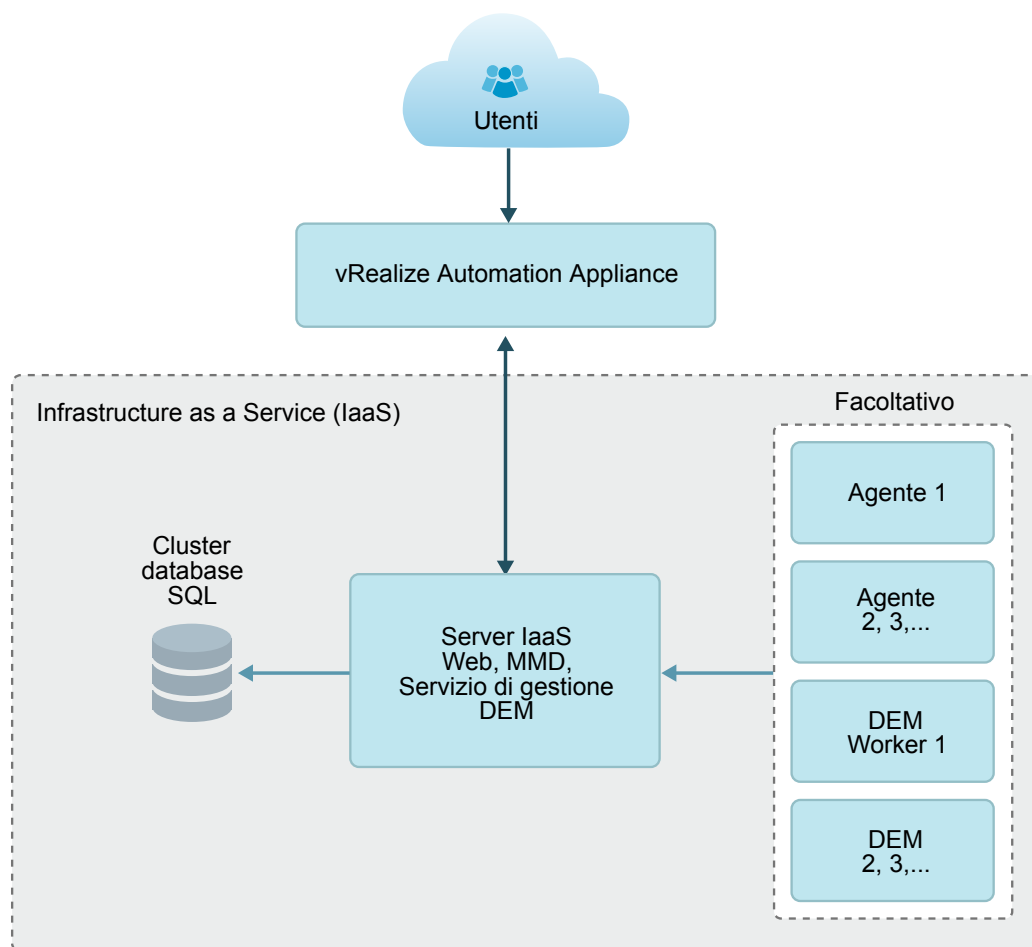
Per informazioni su scalabilità e alta disponibilità, vedere *Architettura di riferimento di VMware vRealize Automation*, disponibile come documento tecnico all'indirizzo <https://www.vmware.com/support/pubs/vcac-pubs.html>.

Panoramica della distribuzione minima

Per completare una distribuzione minima, un amministratore di sistema si occupa di installare i componenti di vRealize Automation appliance e Infrastructure as a Service (IaaS).

- vRealize Automation appliance è dotata di un'interfaccia rappresentata dalla console Web e del supporto per le funzionalità Single Sign-On. Viene installata come appliance virtuale.
- Infrastructure as a Service (IaaS) si installa su una macchina Windows Server.
- IaaS utilizza un database SQL che può essere installato sulla stessa macchina di IaaS o su un proprio server.

Nella figura seguente sono illustrati la relazione e lo scopo dei componenti di un'installazione minima.



Panoramica della distribuzione enterprise

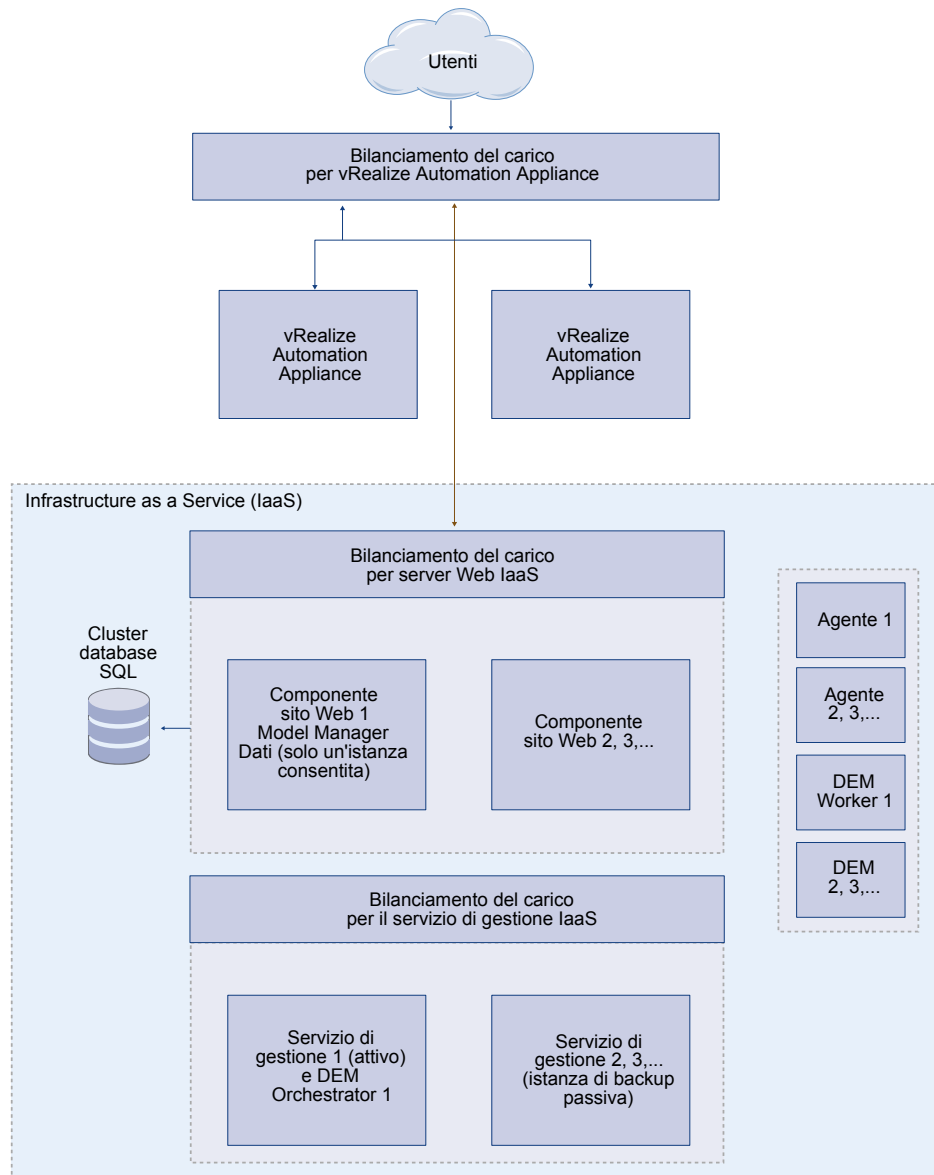
L'amministratore di sistema può distribuire e installare istanze multiple di vRealize Automation appliance e componenti IaaS per favorire scalabilità, ridondanza, alta disponibilità e disaster recovery.

In un'architettura tipica, i componenti IaaS sono distribuiti su più macchine.

Per distribuzioni ad alta disponibilità, i bilanciamenti del carico distribuiscono il carico nell'ambiente di elaborazione. Gli amministratori di sistema configurano i bilanciamento del carico al di fuori del framework di vRealize Automation.

Nella figura seguente sono illustrati i componenti di una distribuzione enterprise con componenti distribuiti, ridondanza e bilanciamenti del carico.

Figura 1-1. Configurazione della distribuzione per le installazioni enterprise



Componenti d'installazione di vRealize Automation

Un'installazione di vRealize Automation include l'installazione e la configurazione delle funzionalità Single Sign-On (SSO), il portale dell'interfaccia utente e i componenti di Infrastructure as a Service (IaaS).

Un'installazione è composta dai seguenti componenti.

- vRealize Automation appliance, che distribuisce la console di gestione, gestisce le funzionalità Single Sign-On (SSO) per l'autorizzazione e l'autenticazione, e include un'istanza di vRealize Orchestrator.
- I componenti di Infrastructure as a Service (IaaS), che vengono installati in una macchina Windows (virtuale o fisica) e per la gran parte elencati nella scheda **Infrastruttura** della console.
- Un database MS SQL Server, che viene distribuito durante l'installazione di IaaS.

Appliance VMware vRealize Automation

vRealize Automation appliance è un'appliance virtuale preconfigurata che contiene il server di vRealize Automation. vRealize Automation si presenta sotto forma di modello in formato OVF (Open Virtualization Format). L'amministratore di sistema distribuisce l'appliance virtuale in un'infrastruttura virtualizzata esistente.

Il server include la console del prodotto vRealize Automation appliance, un portale singolo che permette di eseguire in autonomia il provisioning e la gestione dei servizi cloud, nonché le attività di creazione, amministrazione e governance.

Database appliance

Durante la distribuzione delle appliance virtuali, viene creato automaticamente il database dell'appliance PostgreSQL sulla prima vRealize Automation appliance. È possibile installare un database di replica su una seconda vRealize Automation appliance per creare un ambiente a disponibilità elevata.

Agenti di gestione

Gli agenti di gestione sono componenti IaaS autonomi che registrano i nodi IaaS con le appliance vRealize Automation, automatizzano l'installazione e la gestione dei componenti IaaS e raccolgono informazioni sul supporto e la telemetria.

È necessario installare un agente di gestione su ciascuna macchina Windows che ospita componenti IaaS.

vRealize Automation Infrastructure as a Service (IaaS)

Con IaaS (Infrastructure as a Service) è possibile modellare ed eseguire il provisioning di server e desktop rapidamente su infrastrutture cloud private, pubbliche o ibride.

L'amministratore di sistema installa i componenti di IaaS su una macchina Windows. Le funzionalità di IaaS sono disponibili anche nella scheda **Infrastruttura** della console di gestione. IaaS ha diversi componenti che si possono installare in una configurazione personalizzata per soddisfare le esigenze dell'organizzazione.

Sito Web di IaaS

Il componente sito Web di IaaS fornisce le funzionalità di amministrazione dell'infrastruttura e di creazione dei servizi alla console di vRealize Automation. Il componente sito Web comunica con il servizio di gestione, da quale riceve gli aggiornamenti provenienti da Distributed Execution Manager (DEM), agenti proxy e database.

Model Manager

I modelli di vRealize Automation favoriscono l'integrazione con sistemi esterni e database. Essi si occupano di implementare la logica di business utilizzata da un Distributed Execution Manager (DEM).

Il Model Manager fornisce servizi e utilità per rendere permanenti, gestire le versioni, proteggere e distribuire elementi dei modelli. Esso comunica con il database, i DEM e il sito Web della console.

Servizio di gestione di vCloud Automation Center

Il servizio di gestione coordina la comunicazione tra i DEM, gli agenti e il database. Il servizio di gestione comunica con il sito Web della console attraverso il Model Manager. L'esecuzione di questo servizio richiede privilegi amministrativi.

Database IaaS

Il componente IaaS di vRealize Automation utilizza un database Microsoft SQL Server per conservare le informazioni sulle macchine che gestisce e sui propri elementi e criteri. In genere, il database viene creato automaticamente durante l'installazione. Tuttavia, un amministratore di sistema può anche creare il database separatamente.

Distributed Execution Manager

Un Distributed Execution Manager (DEM) esegue la logica di business di modelli personalizzati, interagendo con il database e, quando necessario, con database e sistemi esterni.

Ciascuna istanza DEM opera nel ruolo di Worker o in quello di Orchestrator. Il ruolo Worker è responsabile dell'esecuzione dei workflow. Il ruolo Orchestrator è responsabile per il monitoraggio delle istanze DEM Worker, la pre-elaborazione dei workflow da eseguire e la pianificazione dei workflow.

Il DEM Orchestrator esegue le attività seguenti.

- Monitora lo stato dei DEM Worker e garantisce l'esecuzione dei workflow di un'istanza Worker che ha smesso di funzionare o ha perso la connessione con il Model Manager, inserendoli in un coda da cui vengono prelevati da un altro DEM Worker.
- Gestisce i workflow pianificati creando nuove istanze di workflow nell'istante programmato.
- Garantisce che in un dato momento sia in esecuzione una sola istanza di un particolare workflow pianificato.

- Pre-elabora i workflow prima che vengano eseguiti, eseguendo tra le altre cose il controllo delle precondizioni per i workflow, utilizzate nell'implementazione della funzionalità RunOneOnly, e creando la cronologia di esecuzione dei workflow.

Questa attività vengono eseguite da un'istanza di DEM Orchestrator designata come attiva. Dato che il DEM Orchestrator è essenziale per l'esecuzione dei workflow, installare almeno un'istanza di Orchestrator aggiuntiva su una macchina separata per assicurare la ridondanza. Orchestrator viene installato automaticamente nella macchina in cui viene eseguito anche il Servizio di gestione. Il DEM Orchestrator aggiuntivo monitora lo stato dell'istanza Orchestrator attiva, in modo da poterne prendere il posto nel caso in cui questa vada offline.

Agenti di vRealize Automation

vRealize Automation utilizza gli agenti per assicurare l'integrazione con sistemi esterni e gestire le informazioni tra componenti vRealize Automation.

In genere l'agente vSphere viene installato come parte di una distribuzione. È possibile installare agenti aggiuntivi in base alle esigenze del proprio sito.

Agenti di integrazione

Gli agenti della PowerShell di Virtual Desktop Integration (VDI) consentono a vRealize Automation di integrarsi con i sistemi desktop virtuali esterni. Attualmente, le macchine virtuali di cui vRealize Automation effettua il provisioning possono essere registrate in XenDesktop su un Desktop Delivery Controller (DDC) Citrix e i loro proprietari possono accedere all'interfaccia Web di XenDesktop da vRealize Automation.

Gli agenti della PowerShell di External Provisioning Integration (EPI) consentono a vRealize Automation di integrare sistemi esterni nel processo di provisioning delle macchine. Ad esempio, l'integrazione con Citrix Provisioning Server consente di effettuare il provisioning di macchine tramite streaming di dischi on-demand e un agente EPI consente di eseguire script Visual Basic per eseguire operazioni aggiuntive durante il processo di provisioning.

Gli agenti di VDI ed EPI richiedono l'accesso di livello amministrativo ai sistemi esterni con cui interagiscono.

Agenti proxy di virtualizzazione

Le macchine virtuali gestite da vRealize Automation vengono create su host di virtualizzazione. vRealize Automation utilizza agenti proxy di virtualizzazione per interagire (inviando comandi e raccogliendo dati) sia con host di virtualizzazione vSphere ESX Server, XenServer e Hyper-V e sia con le macchine virtuali di cui è stato effettuato il provisioning su di essi. Un agente proxy ha le seguenti caratteristiche.

- Generalmente richiede un accesso di livello amministrativo sulla piattaforma di virtualizzazione che gestisce
- Comunica con il servizio di gestione
- Viene installato separatamente con un proprio file di configurazione

Agent di Strumentazione gestione Windows (WMI)

L'agente di Strumentazione gestione Windows (WMI) di vRealize Automation offre ancora più funzionalità di monitoraggio e controllo delle informazioni di sistema e consente di gestire server remoti da una posizione centrale. Esso consente di raccogliere dati da macchine Windows gestite da vRealize Automation.

Preparazione per l'installazione

Gli amministratori di sistema possono installare vRealize Automation all'interno del proprio ambiente di virtualizzazione esistente. Prima di avviare l'installazione, preparare l'ambiente di distribuzione in modo da soddisfare i requisiti di sistema.

Questo capitolo include i seguenti argomenti:

- [DNS e risoluzione dei nomi host](#)
- [Requisiti di hardware e macchine virtuali](#)
- [Considerazioni sui browser](#)
- [Considerazioni sulle password](#)
- [Requisiti di Windows Server](#)
- [Requisiti delle porte](#)
- [Account utente e credenziali richiesti per l'installazione](#)
- [Sicurezza](#)
- [Sincronizzazione di data e ora](#)

DNS e risoluzione dei nomi host

In vRealize Automation, l'amministratore di sistema deve identificare tutti gli host utilizzando un nome di dominio completo (FQDN).

In una distribuzione distribuita, ogni componente di vRealize Automation deve poter risolvere l'indirizzo di tutti gli altri componenti utilizzando un nome di dominio completo.

Anche il servizio Web di Model Manager, il servizio di gestione e il database Microsoft SQL Server devono poter risolvere i rispettivi indirizzi utilizzando il proprio nome WINS (Windows Internet Name Service). È necessario configurare il DNS (Domain Name System) per la risoluzione di questi nomi host nell'ambiente.

Importante: vRealize Automation non permette la navigazione verso host che contengono il carattere di sottolineatura (_) nel nome host.

Requisiti di hardware e macchine virtuali

La distribuzione richiede una serie di risorse di sistema minime per l'installazione di appliance virtuali e alcuni requisiti hardware minimi per l'installazione di componenti IaaS su Windows Server.

Per conoscere i requisiti dei sistemi operativi e degli ambienti di alto livello, incluse le informazioni sui browser e sistemi operativi supportati, vedere la *Matrice di supporto di vRealize Automation*.

La tabella Requisiti hardware mostra i requisiti di configurazione minimi necessari per poter distribuire appliance virtuali e installare componenti IaaS. Le appliance sono macchine virtuali preconfigurate che vengono aggiunte a vCenter Server o all'inventario ESXi. I componenti IaaS vengono installati su server Windows 2008 R2 SP1 o Windows 2012 R2 fisici o virtuali.

Un'Active Directory viene considerata di piccole dimensioni quando contiene fino a 25.000 utenti nell'unità organizzativa da sincronizzare nella configurazione dell'archivio identità. Un'Active Directory viene considerata di grandi dimensioni quando contiene più di 25.000 utenti nell'unità organizzativa.

Tavola 2-1. Requisiti hardware

vRealize Automation appliance per Active Directory piccole	vRealize Automation appliance per Active Directory grandi	Componenti IaaS (Windows Server).
<ul style="list-style-type: none"> 4 CPU 18 GB di memoria 60 GB di spazio su disco 	<ul style="list-style-type: none"> 4 CPU 22 GB di memoria 60 GB di spazio su disco 	<ul style="list-style-type: none"> 2 CPU 8 GB di memoria 30 GB di spazio su disco <p>Quando si include un server SQL su un host Windows, sono richieste risorse aggiuntive.</p>

Considerazioni sui browser

L'uso dei browser con vRealize Automation è soggetto ad alcune limitazioni.

- Non sono supportate le schede e le finestre multiple dei browser. vRealize Automation supporta un'unica sessione per utente.
- Le console remote di VMware Rremote Console di cui viene eseguito il provisioning su vSphere supportano un sottoinsieme dei browser supportati da vRealize Automation.

Per conoscere i requisiti dei sistemi operativi e degli ambienti di alto livello, incluse le informazioni sui browser e sistemi operativi supportati, vedere la *Matrice di supporto di vRealize Automation*.

Considerazioni sulle password

Ad alcune password si applicano restrizioni per i caratteri.

La password di amministratore di vRealize Automation definita durante l'installazione non deve contenere caratteri speciali. A partire da questa versione di vRealize Automation, è noto che i caratteri speciali seguenti causano errori:

- Virgolette doppie ("")

- Virgole (,)
- Segno di uguale (=) finale
- Spazi vuoti
- Caratteri non ASCII o ASCII estesi

Le password che contengono caratteri speciali possono essere accettate quando vengono assegnate, ma causano problemi durante l'esecuzione di operazioni quali il salvataggio di endpoint o quando la macchina tenta di unirsi al cluster di vRealize Automation.

Requisiti di Windows Server

La macchina Windows virtuale o fisica che ospita il componente IaaS, deve soddisfare requisiti di configurazione specifici per il database di IaaS, i componenti server di IaaS, il servizio di gestione di IaaS e i DEM (Distributed Execution Manager).

La procedura consigliata prevede la permanenza di tutti i server nello stesso dominio.

L'installazione guidata esegue il controllo prerequisiti di vRealize Automation su tutti i server Windows prima di iniziare il processo di installazione per assicurarsi che i server soddisfino tutte le necessarie configurazioni.

Requisiti del server di database di IaaS

Il server Windows che ospita il database SQL Server IaaS di vRealize Automation deve soddisfare determinati prerequisiti.

I requisiti sono validi quando si esegue la procedura guidata di installazione o il programma di installazione `setup_vrealize-automation-appliance-URL.exe legacy` e si seleziona il ruolo del database per l'installazione. I prerequisiti sono validi anche se si crea separatamente un database di SQL Server vuoto da utilizzare con IaaS.

- Utilizzare una versione supportata di SQL Server da *Matrice di supporto di vRealize Automation*.
- Configurare SQL Server sulla porta predefinita 1433. Non utilizzare una porta non predefinita.
- Abilitare il protocollo TCP/IP per SQL Server.
- Abilitare il servizio Distributed Transaction Coordinator (DTC) in tutti i server Windows di IaaS e nella macchina che ospita SQL Server. IaaS utilizza DTC per le transazioni e le azioni del database, come ad esempio la creazione di un workflow.

Nota: Se si clona una macchina per creare un server Windows di IaaS, installare DTC sul clone dopo la clonazione. Se si clona una macchina che dispone già di DTC, il suo identificatore univoco viene copiato nel clone, causando un errore di comunicazione. Vedere [Errore di comunicazione nel servizio di gestione](#).

Per ulteriori informazioni sull'attivazione di DTC, vedere l'[articolo 2038943 della knowledge base di VMware](#).

- Aprire le porte tra tutti i server Windows di IaaS e la macchina che ospita SQL Server. Vedere [Requisiti delle porte](#).

In alternativa, se i criteri del sito lo consentono, è possibile disabilitare i firewall tra i server Windows di IaaS e SQL Server.

Requisiti del servizio Web IaaS e del Model Manager Server

Per supportare l'installazione dei componenti del server di IaaS, l'ambiente deve soddisfare prerequisiti software e di configurazione.

Requisiti di ambiente e database per IaaS

La configurazione host e il database MS SQL devono soddisfare i requisiti descritti di seguito.

Tavola 2-2. requisiti di IaaS

Ambito di applicazione	Requisiti
Configurazione host	<p>Prima di installare IaaS è necessario che sull'host siano installati i seguenti componenti:</p> <ul style="list-style-type: none"> ■ Microsoft .NET Framework 4.5.2 o versione successiva. ■ Microsoft PowerShell 2.0 (incluso con Windows Server 2008 R2 SP1 e versioni successive) o Microsoft PowerShell 3.0 su Windows Server 2012 R2. ■ Microsoft Internet Information Services 7.5. ■ È necessario installare Java nella macchina che esegue il componente Web principale, a supporto della distribuzione del database MS SQL durante l'installazione.
Requisiti del database Microsoft SQL	<p>Il database Microsoft SQL può risiedere sull'host del server di IaaS (Windows) o su un host remoto.</p> <p>Questi requisiti relativi a Java sono applicabili ai database sull'host del server di IaaS (Windows) e non ai database esterni.</p> <ul style="list-style-type: none"> ■ Deve essere installata un'edizione a 64 bit di Java versione 1.7 o successiva. Le versioni a 32 bit non sono supportate. ■ Il valore di impostazione della variabile di ambiente JAVA_HOME deve corrispondere alla cartella d'installazione di Java. ■ Deve essere disponibile il file %JAVA_HOME%\bin\java.exe.

Requisiti di Microsoft Internet Information Services

Microsoft Internet Information Services (IIS) deve soddisfare i requisiti di configurazione descritti di seguito.

Tavola 2-3. Configurazione richiesta per Microsoft Internet Information Services

Componente IIS	Impostazione
Moduli di Internet Information Services (IIS) installati	<ul style="list-style-type: none"> ■ WindowsAuthentication ■ StaticContent ■ DefaultDocument ■ ASPNET 4.5 ■ ISAPIExtensions ■ ISAPIFilter
Impostazioni di autenticazione IIS	<ul style="list-style-type: none"> ■ Autenticazione Windows attivata ■ Autenticazione anonima disattivata ■ Provider negoziazione attivata ■ Provider NTLM attivata ■ Modalità kernel autenticazione Windows attivata ■ Protezione estesa autenticazione Windows disattivata ■ Per i certificati che utilizzano SHA512 è necessario disabilitare TLS1.2 sui server Windows 2012 e Windows 2012 R2
Ruoli del servizio Attivazione processo Windows di IIS	<ul style="list-style-type: none"> ■ ConfigurationApi ■ NetEnvironment ■ ProcessModel ■ WcfActivation (solo Windows 2008) ■ HttpActivation ■ NonHttpActivation

Servizio di gestione di IaaS

Per poter installare il servizio di gestione di IaaS, l'ambiente operativo deve soddisfare alcuni requisiti generali.

- Microsoft .NET Framework 4.5.2 sia installato.
- Microsoft PowerShell 2.0 o Microsoft PowerShell 3.0. PowerShell 2.0 sia incluso in Windows Server 2008 R2 SP1 e versioni successive. Microsoft PowerShell 3.0 sia in esecuzione su Windows Server 2012 R2.
- SecondaryLogOnService sia in esecuzione.
- Non possono esserci firewall tra l'host del DEM e il server Windows. Per informazioni sulla porta, vedere [Requisiti delle porte](#).
- IIS è installato e configurato.

Requisiti di Distributed Execution Manager

Per poter installare i Distributed Execution Manager (DEM), l'ambiente operativo deve soddisfare alcuni requisiti generali.

- Microsoft .NET Framework 4.5.2 sia installato.

- Microsoft PowerShell 2.0 o Microsoft PowerShell 3.0. PowerShell 2.0 sia incluso in Windows Server 2008 R2 SP1 e versioni successive. Microsoft PowerShell 3.0 sia in esecuzione su Windows Server 2012 R2.
- SecondaryLogOnService sia in esecuzione.
- Nessun firewall tra l'host del DEM e il server Windows, oppure porte aperte come descritto in [Requisiti delle porte](#).

I server che ospitano istanze di DEM Worker potrebbero avere requisiti aggiuntivi in base alle risorse di provisioning con cui interagiscono.

Requisiti di Amazon Web Services EC2

Windows server IaaS comunica con un account Amazon EC2 e raccoglie dati tramite esso.

Quando si utilizza Amazon Web Services per eseguire il provisioning, i server su cui si trovano i DEM Worker devono soddisfare i seguenti requisiti di configurazione.

- Gli host su cui sono installati i DEM devono avere accesso a Internet.
Se è presente un firewall, il traffico HTTPS deve essere permesso da e verso `aws.amazon.com`, nonché da e verso gli URL che rappresentano tutte le regioni di EC2 a cui hanno accesso i propri account AWS, ad esempio `ec2.us-east-1.amazonaws.com` per la regione degli Stati Uniti Orientali. Ogni URL viene risolto in una gamma di indirizzi IP, pertanto può essere necessario utilizzare uno strumento, come ad esempio quello disponibile sul sito Web di Network Solutions, che elenca e configura questi indirizzi IP.
- Se l'accesso a Internet dall'host DEM avviene attraverso un server proxy, il servizio DEM deve essere in esecuzione sotto credenziali che consentano l'autenticazione sul server proxy.

Requisiti di KVM per Red Hat Enterprise Virtualization (RHEV)

Quando si utilizza Red Hat Enterprise Virtualization per il provisioning il server Windows di IaaS comunica con e raccoglie dati da tale account.

L'ambiente deve soddisfare i requisiti Red Hat Enterprise indicati di seguito.

- Ogni ambiente di KVM (RHEV) deve essere unito al dominio che contiene il server IaaS.
- Le credenziali utilizzate per gestire l'endpoint che rappresenta un ambiente KVM (RHEV) devono godere di privilegi di amministratore sull'ambiente RHEV. Queste credenziali devono anche avere privilegi sufficienti per creare oggetti sugli host contenuti all'interno dell'ambiente.

Requisiti di SCVMM

Tutti i DEM Worker utilizzati per gestire macchine virtuali attraverso SCVMM devono essere installati su un host su cui è già installata la console di SCVMM.

Inoltre devono essere soddisfatti i seguenti requisiti:

- Il DEM deve avere accesso al modulo SCVMM PowerShell installato con la console.

- I criteri di esecuzione di MS PowerShell devono essere impostati su RemoteSigned o Unrestricted.

Per informazioni sui criteri di esecuzione di PowerShell, eseguire uno dei seguenti comandi al prompt dei comandi della PowerShell:

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

- Se non tutti i DEM Worker all'interno dell'istanza si trovano su risorse di elaborazione che rispettano questi requisiti, è necessario utilizzare Competenze per indirizzare tutti i workflow correlati a SCVMM verso quelle che li rispettano.

Di seguito sono elencati i requisiti aggiuntivi che si applicano a SCVMM.

- È necessario installare la console di SCVMM prima di installare i DEM Worker che utilizzano elementi di lavoro di SCVMM.

Se si installano i DEM Worker prima della console di SCVMM, verranno generati errori di registro simili al seguente:

```
Workflow 'ScvmmEndpointDataCollection' failed with the following exception: The term 'Get-
VMMServer' is not recognized as the name of a cmdlet, function, script file, or operable program.
Check the spelling of the name, or if a path was included, verify that the path is correct and try
again.
```

Per affrontare questo problema, verificare che la console di SCVMM sia installata e riavviare il servizio del DEM Worker.

- Ogni istanza di SCVMM deve essere unita al dominio che contiene il server.
- Le credenziali utilizzate per gestire l'endpoint che rappresenta un'istanza di SCVMM devono essere dotate di privilegi amministrativi sul server di SCVMM. Queste credenziali devono anche avere privilegi amministrativi sui server Hyper-V all'interno dell'istanza.
- I server Hyper-V all'interno di un'istanza SCVMM da gestire devono essere server Windows 2008 R2 SP1 con Hyper-V installato. Il processore deve essere equipaggiato con le necessarie estensioni di virtualizzazione. La libreria .NET Framework 4.5.1 o successiva deve essere installata e Windows Management Instrumentation (WMI) deve essere abilitato.
- Per eseguire il provisioning di macchine su una risorsa di elaborazione SCVMM, un utente deve essere aggiunto in almeno un ruolo di sicurezza all'interno dell'istanza di SCVMM.

Requisiti delle porte

vRealize Automation utilizza porte designate per la comunicazione e l'accesso ai dati.

Sebbene vRealize Automation utilizzi solo la porta 443 per la comunicazione, potrebbero esserci altre porte aperte nel sistema. Le porte aperte sono poco sicure e possono essere all'origine di vulnerabilità di sicurezza, pertanto è consigliabile rivedere tutte le porte aperte nel sistema e assicurarsi che restino aperte solo quelle necessarie alle applicazioni dell'azienda.

Appliance vRealize Automation

vRealize Automation appliance utilizza le porte seguenti.

Tavola 2-4. Porte in ingresso per la vRealize Automation appliance

Porta	Protocollo	Commenti
22	TCP	Facoltativi. SSH.
80	TCP	Facoltativi. Reindirizza alla 443.
111	TCP, UDP	RPC
443	TCP	Consente di accedere alla console di vRealize Automation e alle chiamate API.
5480	TCP	Consente di accedere all'interfaccia di gestione Web dell'appliance virtuale.
5480	TCP	Utilizzata dall'agente di gestione.
5488, 5489	TCP	Interne. Utilizzate dalla vRealize Automation appliance per gli aggiornamenti.
4369, 25672,5671,5672	TCP	Messaggistica RabbitMQ.
8230, 8280, 8281	TCP	Istanza di vRealize Orchestrator interna.
8444	TCP	Comunicazione proxy della console per connessioni a VMware Remote Console di vSphere.

Tavola 2-5. Porte in uscita per l'appliance vRealize Automation

Porta	Protocollo	Commenti
25, 587	TCP, UDP	SMTP per l'invio di notifiche via email in uscita.
53	TCP, UDP	DNS.
67, 68, 546, 547	TCP, UDP	DHCP
80	TCP	Facoltativi. Per il recupero degli aggiornamenti software. Gli aggiornamenti possono essere scaricati separatamente e applicati.
110, 995	TCP, UDP	POP per la ricezione delle notifiche via email in entrata.
143, 993	TCP, UDP	IMAP per la ricezione delle notifiche via email in entrata.
123	TCP, UDP	Facoltativi. Per la connessione diretta a NTP evitando di utilizzare l'orario dell'host.
443	TCP	Servizio di gestione di IaaS su HTTPS. Comunicazione con host di virtualizzazione su protocollo HTTPS.
902	TCP	Operazioni di copia file di rete ESXi e connessioni VMware Remote Console (VMRC).
5432	TCP, UDP	Facoltativi. Per la comunicazione con un database dell'appliance.
7444	TCP	Comunicazione con il servizio SSO su protocollo HTTPS.
8281	TCP	Facoltativi. Per la comunicazione con un'istanza di vRealize Orchestrator esterna.

Specifici plug-in di vRealize Orchestrator che comunicano con sistemi esterni potrebbero richiedere altre porte. Consultare la documentazione relativa al plug-in di vRealize Orchestrator.

Infrastructure as a Service (IaaS)

Le porte elencate nelle tabelle Porte in entrata per i componenti di Infrastructure as a Service e le porte in uscita per Infrastructure as a Service devono poter essere utilizzate dal server Windows di IaaS.

Tavola 2-6. Porte in entrata per i componenti di Infrastructure as a Service

Componente	Porta	Protocollo	Commenti
Istanza di SQL Server	1433	TCP	MSSQL.
Servizio di gestione	443*	TCP	Comunicazione con i componenti di IaaS e con la vRealize Automation appliance su protocollo HTTPS.
vRealize Automation appliance	443	TCP	Comunicazione con i componenti di IaaS e con la vRealize Automation appliance su protocollo HTTPS.

* In tutti gli host di virtualizzazione gestiti da agenti proxy deve essere aperta anche la porta TCP 443 per il traffico in ingresso.

Tavola 2-7. Porte in uscita per i componenti di Infrastructure as a Service

Componente	Porta	Protocollo	Commenti
Tutto	53	TCP, UDP	DNS.
Tutto	67, 68, 546, 547	TCP, UDP	DHCP
Tutto	123	TCP, UDP	Facoltativi. NTP.
Servizio di gestione	443	TCP	Comunicazione con vRealize Automation appliancesu protocollo HTTPS.
Sito Web	443	TCP	Comunicazione con il servizio di gestione su protocollo HTTPS.
Distributed Execution Manager	443	TCP	Comunicazione con il servizio di gestione su protocollo HTTPS.
Agenti proxy	443	TCP	Comunicazione con il servizio di gestione e gli host di virtualizzazione su protocollo HTTPS.
Agente guest	443	TCP	Comunicazione con il servizio di gestione su protocollo HTTPS.
Servizio di gestione, sito Web.	1433	TCP	MSSQL.

Servizio Microsoft Distributed Transaction Coordinator

Oltre a verificare che le porte elencate nelle precedenti tabelle siano libere l'uso, è necessario abilitare la comunicazione del servizio Microsoft Distributed Transaction Coordinator Service (MS DTC) tra tutti i server nella distribuzione. MS DTC richiede l'uso della porta 135 su TCP e di una porta casuale compresa tra 1024 e 65535.

Il Controllo prerequisiti convalida l'ambiente se MS DTC è in esecuzione e le porte richieste sono aperte.

Account utente e credenziali richiesti per l'installazione

Per poter installare i componenti di vRealize Automation è necessario disporre dei ruoli e delle credenziali necessarie.

Account del servizio di vCenter

Se si intende utilizzare un endpoint vSphere, è necessario un account di dominio o locale che disponga del livello di accesso appropriato configurato in vCenter.

Installazione dell'appliance virtuale

Per distribuire l'vRealize Automation appliance, è necessario disporre di privilegi appropriati sulla piattaforma di distribuzione (ad esempio le credenziali di amministratore di vSphere).

Durante il processo di distribuzione viene specificata la password relativa all'account di amministratore dell'appliance virtuale. Questo account consente di accedere alla console di gestione dell'vRealize Automation appliance dalla quale è possibile configurare e amministrare le appliance virtuali.

installazione di IaaS

Prima di installare i componenti di IaaS, aggiungere l'utente che si intende utilizzare per eseguire i programmi di installazione di IaaS al gruppo Administrators dell'host d'installazione.

Credenziali del database di IaaS

È possibile creare il database durante l'installazione del prodotto oppure crearlo manualmente nel server SQL.

Quando si crea o si popola un database MS SQL tramite vRealize Automation, utilizzando l'installazione guidata o la console di gestione, si applicano i seguenti requisiti:

- Se si utilizza l'opzione **Usa autenticazione di Windows**, è necessario assegnare il ruolo **sysadmin** in SQL Server all'utente che esegue l'agente di gestione sul server Web IaaS primario per poter creare e modificare la dimensione del database.
- Se non si seleziona **Usa autenticazione di Windows**, è necessario concedere il ruolo **sysadmin** in SQL Server anche all'utente che esegue l'agente di gestione sul server Web IaaS primario. Le credenziali sono utilizzate in fase di runtime.
- Se si popola un database creato in precedenza tramite vRealize Automation, le credenziali utente fornite (utente Windows corrente o utente SQL specificato) richiedono solo privilegi di **dbo** per il database di IaaS.

Nota: Gli utenti di vRealize Automation richiedono anche il livello di autenticazione Windows appropriato per accedere e utilizzare vRealize Automation.

Credenziali utente del servizio di IaaS

IaaS installa diversi servizi di Windows che condividono un singolo utente di servizio.

L'utente utilizzato per i servizi di IaaS deve avere i seguenti requisiti:

- Deve essere un utente di dominio.
- Deve avere privilegi amministrativi locali su tutti gli host su cui è installato il servizio di gestione o il componente sito Web. Non eseguire un'installazione gruppo di lavoro.
- Dev'essere configurato con privilegi **Accedi come servizio**. Questo privilegio garantisce al servizio di gestione la possibilità di avviarsi e di generare file di registro.
- Deve avere privilegi di **dbo** per il database di IaaS. Se si utilizza il programma d'installazione per creare il database, assicurarsi che l'accesso utente del servizio venga aggiunto a SQL Server prima di eseguire il programma d'installazione. Il programma d'installazione assegna all'utente del servizio i privilegi di **dbo** dopo la creazione del database.
- Il programma di installazione viene eseguito con l'account che esegue l'agente di gestione sul server Web primario. Se si desidera utilizzare il programma di installazione per creare un database MS SQL durante l'installazione, è necessario che il ruolo **sysadmin** sia abilitato in MS SQL. Questo non è un requisito se si sceglie di utilizzare un database vuoto creato in precedenza.
- L'account utente del dominio che si intende utilizzare come identità del pool di applicazioni di IIS per il servizio Web di Model Manager deve essere configurato con privilegi **Accesso come processo batch**.

Specifiche del server di Model Manager

Specificare il nome del server di Model Manager utilizzando il formato del nome di dominio completo. Non utilizzare un indirizzo IP per specificare il server.

Sicurezza

vRealize Automation utilizza SSL per garantire la sicurezza delle comunicazioni tra componenti. La protezione dello storage dei database è garantita dall'impiego di passphrase.

Per ulteriori informazioni, vedere [Requisiti di attendibilità dei certificati in una distribuzione distribuita](#).

Certificati

vRealize Automation utilizza certificati SSL per garantire la sicurezza delle comunicazioni tra componenti IaaS e istanze della vRealize Automation appliance. Le appliance e le macchine d'installazione Windows si scambiano questi certificati per stabilire connessioni attendibili. È possibile ottenere certificati da un'autorità di certificazione interna o esterna, oppure generare certificati autofirmati durante il processo di distribuzione per ciascun componente.

Per informazioni importanti su risoluzione dei problemi, supporto e requisiti di attendibilità, vedere l'articolo della knowledgebase di VMware all'indirizzo <http://kb.vmware.com/kb/2106583>.

È possibile aggiornare o sostituire i certificati dopo la distribuzione. Ad esempio, un certificato può scadere o si può scegliere di utilizzare certificati autofirmati durante la distribuzione iniziale, ma poi ottenere certificati da un'autorità attendibile prima di rendere operativa l'implementazione di vRealize Automation.

Tavola 2-8. Implementazioni dei certificati

Componente	Distribuzione minima (non di produzione)	Distribuzione distribuita (pronta per la produzione)
Appliance vRealize Automation	Generare un certificato autofirmato durante la configurazione dell'appliance.	Per ciascun cluster di appliance, è possibile utilizzare un certificato proveniente da un'autorità di certificazione interna o esterna. Vengono supportati certificati multiuso e certificati wildcard.
Componenti IaaS	Durante l'installazione, accettare i certificati autofirmati generati o selezionare la soppressione dei certificati.	Ottenere un certificato multiuso, come ad esempio un certificato SAN (Subject Alternative Name, nome alternativo del soggetto), da un'autorità di certificazione interna o esterna ritenuta attendibile dal client Web.

Catene di certificati

Se si utilizzano catene di certificati, specificare i certificati nel seguente ordine:

- Certificato client/server firmato mediante il certificato di un'autorità di certificazione intermedia
- Uno o più certificati intermedi
- Certificato di un'autorità di certificazione radice

Includere l'intestazione BEGIN CERTIFICATE e il piè di pagina END CERTIFICATE per ciascun certificato quando si importano certificati.

Estrazione di certificati e chiavi private

I certificati utilizzati con le appliance virtuali devono essere nel formato file PEM.

Gli esempi della seguente tabella utilizzano i comandi Gnu openssl per estrarre le informazioni del certificato necessarie a configurare le appliance virtuali.

Tavola 2-9. Esempi di comandi e valori dei certificati (openssl)

Elementi forniti dall'autorità di certificazione	Comando	Voci delle appliance virtuali
Chiave privata RSA	<code>openssl pkcs12 -in <i>path_to_.pfx_certificate_file</i> -nocerts -out key.pem</code>	Chiave privata RSA
File PEM	<code>openssl pkcs12 -in <i>path_to_.pfx_certificate_file</i> -clcerts -nokeys -out cert.pem</code>	Catena di certificati
(Facoltativa) Passphrase	n/a	Passphrase

Passphrase di sicurezza

vRealize Automation utilizza passphrase di sicurezza per la protezione dei database. Una passphrase è costituita da una serie di parole che compongono una frase, da cui viene generata una chiave utilizzata per proteggere i dati conservati nel database.

Attenersi alle linee guida quando si crea una passphrase di sicurezza per la prima volta.

- Utilizzare la stessa passphrase per l'intera installazione per assicurarsi che tutti i componenti abbiano la stessa chiave di crittografia.
- Utilizzare una frase composta da più di otto caratteri.
- Includere lettere maiuscole, minuscole, numeri e simboli.
- Memorizzare la passphrase o conservarla in un luogo sicuro. La passphrase è richiesta per ripristinare le informazioni del database in caso di errore di sistema o per aggiungere componenti dopo l'installazione iniziale. Senza la passphrase non è possibile eseguire correttamente il ripristino.

Software di terze parti

Alcuni componenti di vRealize Automation sono basati su software di terze parti, inclusi Microsoft Windows e SQL Server. Per salvaguardare il sistema contro vulnerabilità alla sicurezza che possono interessare i prodotti di terze parti, mantenere il software costantemente aggiornato con le patch più recenti rilasciate dai vendor.

Sincronizzazione di data e ora

L'amministratore di sistema deve configurare un accurato sistema di sincronizzazione di data e ora come parte dell'installazione di vRealize Automation.

L'installazione non riesce se la sincronizzazione di data e ora non è configurata correttamente.

La sincronizzazione di data e ora deve essere coerente e aggiornata in tutte le vRealize Automation appliance e i server Windows. Per ottenere questa coerenza, utilizzare lo stesso metodo di sincronizzazione per tutti i componenti.

Per le macchine virtuali è possibile utilizzare i seguenti metodi:

- Configurazione mediante il protocollo Network Time Protocol (direttamente)
- Configurazione mediante il protocollo Network Time Protocol attraverso ESXi con VMware Tools. È necessario avere NTP configurato su ESXi.

Per i server Windows, consultare l'articolo [Timekeeping best practices for Windows, including NTP](#).

Installazione di vRealize Automation utilizzando l'installazione guidata

3

L'installazione guidata di vRealize Automation è un sistema semplice e rapido per installare distribuzioni minime o enterprise.

Prima di avviare la procedura guidata, è necessario distribuire una vRealize Automation appliance, configurare i server Windows per soddisfare i prerequisiti d'installazione e verificare che ogni appliance e server utilizzi lo stesso metodo di sincronizzazione di data e ora.

Navigazione nell'installazione guidata

L'installazione guidata viene visualizzata la prima volta che si accede a vRealize Automation appliance. Se si desidera arrestare l'installazione guidata e riprenderla successivamente, uscire utilizzando il pulsante **Disconnetti** presente in ciascuno schermo. Utilizzare il pulsante **Annulla** per uscire dall'installazione guidata ed effettuare l'installazione tramite la console di gestione. L'installazione guidata viene disattivata facendo clic su **Annulla** oppure quando si esce dall'installazione guidata e si inizia un'installazione attraverso la console di gestione.

Utilizzare i pulsanti **Indietro** e **Avanti** per navigare attraverso le schermate dell'installazione guidata.

Questo capitolo include i seguenti argomenti:

- [Distribuzione di vRealize Automation appliance](#)
- [Installazione di una distribuzione minima con l'installazione guidata](#)
- [Installazione di una distribuzione enterprise con l'installazione guidata](#)

Distribuzione di vRealize Automation appliance

Per distribuire vRealize Automation appliance, è necessario che un amministratore di sistema acceda al client vSphere e selezioni le impostazioni di distribuzione.

La password radice creata per l'amministratore di vRealize Automation è soggetta ad alcune restrizioni. Vedere [Considerazioni sulle password](#).

Prerequisiti

- Scaricare vRealize Automation appliance dal sito Web di VMware.
- Accedere al client vSphere come utente con privilegi di amministratore di sistema.

Procedura

- 1 Selezionare **File > Distribuisci modello OVF** dal client di vSphere.
- 2 Selezionare il file di vRealize Automation appliance scaricato e fare clic su **Apri**.
- 3 Fare clic su **Avanti**.
- 4 Fare clic su **Avanti** nella pagina Dettagli modello OVF.
- 5 Accettare il contratto di licenza e fare clic su **Avanti**.
- 6 Immettere un nome univoco per l'appliance virtuale nella casella di controllo **Nome** rispettando la convenzione di denominazione IT dell'organizzazione, selezionare il data center e la posizione in cui si desidera distribuire l'appliance virtuale e fare clic su **Avanti**.
- 7 Seguire le istruzioni presentate fino alla visualizzazione della pagina Formato disco.
- 8 Nella pagina Formato disco, verificare che vi sia spazio sufficiente per distribuire l'appliance virtuale e fare clic su **Avanti**.
- 9 Seguire le istruzioni presentate fino alla pagina Proprietà.
Le opzioni visualizzate dipendono dalla configurazione di vSphere.
- 10 Configurare i valori nella pagina Proprietà.
 - a Immettere la password radice da utilizzare quando si accede alla console dell'appliance virtuale nelle caselle di testo **Immetti password** e **Conferma password**.
 - b Selezionare o deselezionare la casella di testo **Servizio SSH** per attivare o disattivare il servizio SSH per l'appliance.

Questo valore è utilizzato per impostare lo stato iniziale del servizio SSH nell'appliance. Se si sta eseguendo l'installazione guidata, attivare questa opzione prima di avviare la procedura guidata. Dopo l'installazione sarà possibile modificare questa impostazione dalla console di gestione dell'appliance.
 - c Immettere il nome di dominio completo della macchina virtuale nella casella di testo **Nome host**, anche se si utilizza il DHCP.
 - d Configurare le proprietà di networking.
- 11 Fare clic su **Avanti**.
- 12 In base alle configurazioni di vCenter e DNS utilizzate, la risoluzione DNS potrebbe impiegare del tempo. Per accelerare il processo, eseguire i seguenti passaggi.
 - Se nella pagina Completamento è disponibile **Accendi dopo la distribuzione**.
 - a Selezionare **Accendi dopo la distribuzione** e fare clic su **Fine**.
 - b Scegliere **Chiudi** al completamento della distribuzione del file in vCenter.

- c Attendere l'avvio della macchina.

Questa fase potrebbe richiedere fino a 5 minuti.

- Se nella pagina Completamento non è disponibile **Accendi dopo la distribuzione**.
 - a Scegliere **Chiudi** al completamento della distribuzione del file in vCenter.
 - b Accendere la VM e attendere il tempo necessario alla VM per avviarsi.
 - c Assicurarsi che sia possibile eseguire un ping al DNS della macchina virtuale. Se non è possibile eseguire un ping al DNS, riavviare la macchina virtuale.
 - d Attendere l'avvio della macchina. Questa fase potrebbe richiedere fino a 5 minuti.

- 13 Aprire un prompt dei comandi ed eseguire un ping sul nome di dominio completo per verificare che questo venga correttamente risolto nell'indirizzo IP vRealize Automation appliance.

Installazione di una distribuzione minima con l'installazione guidata

Esecuzione dell'installazione guidata per una distribuzione minima

Installare una distribuzione minima come modello di prova. Nella procedura guidata per l'installazione minima si presuppone che l'utente stia installando tutti i componenti IaaS su una singola macchina Windows.

Le distribuzioni minime in genere supportano una singola vRealize Automation appliance, un server IaaS e utilizzano un agente vSphere per supportare endpoint.

Prerequisiti

- Assicurarsi che siano soddisfatti i prerequisiti descritti in [Capitolo 2 Preparazione per l'installazione](#)
- [Distribuzione di vRealize Automation appliance](#)
-

Procedura

- 1 Aprire un browser.
- 2 Accedere alla console di gestione della vRealize Automation appliance utilizzando il suo nome di dominio completo, `https://vra-va-hostname.domain.name:5480/`.
- 3 Accedere utilizzando il nome utente **root** e la password specificati al momento della distribuzione dell'appliance.
- 4 Quando compare l'installazione guidata, fare clic su **Avanti**.
- 5 Accettare l'accordo di licenza con l'utente finale e fare clic su **Avanti**.

- 6 Nella schermata Tipo di distribuzione selezionare **Distribuzione minima e Installa infrastruttura come servizio**, quindi fare clic su **Avanti**.
- 7 Verificare che siano soddisfatti i prerequisiti elencati nella pagina Prerequisiti d'installazione e che siano elencati i server Windows su cui è stato installato un agente di gestione.
- 8 Se necessario, è possibile modificare il metodo di registrazione dell'ora per l'appliance vRealize Automation. Fare clic su **Modifica impostazioni ora** se si desidera apportare modifiche.
- 9 Fare clic su **Avanti**.
- 10 Fare clic su **Esegui** nella schermata Esegui controllo prerequisiti per verificare che i server Windows della distribuzione siano correttamente configurati per l'uso con vRealize Automation.

Questo passaggio potrebbe richiedere diversi minuti perché viene eseguito in remoto.

- a Se una macchina restituisce un esito negativo del controllo, fare clic su **Correggi** per avviare le correzioni automatiche o scegliere **Mostra dettagli** e seguire le istruzioni. Verranno riavviate anche le correzioni automatiche.
 - b Fare clic su **Esegui** per eseguire nuovamente il controllo.
 - c Quando tutti gli stati indicano un esito positivo, fare clic su **Avanti**.
- 11 Procedere alle schermate successive, fornendo le informazioni richieste per la configurazione dei componenti della distribuzione, incluso il server Web, il servizio di gestione, Distributed Execution Manager, l'agente proxy vSphere e le informazioni sui certificati.

Ulteriori informazioni sono disponibili anche tramite i pulsanti della Guida.

Passi successivi

[Creazione di snapshot prima di iniziare l'installazione](#)

Installazione dell'agente di gestione

È necessario installare un agente di gestione su ciascuna macchina Windows che ospita componenti IaaS.

Per le installazioni enterprise, non è richiesto un agente di gestione per l'host MS SQL.

Se si verifica un guasto nell'appliance vRealize Automation principale, sarà necessario reinstallare gli agenti di gestione.

Gli agenti di gestione non vengono eliminati automaticamente quando si disinstalla un componente IaaS. Disinstallare l'agente di gestione esattamente come si disinstalla qualsiasi programma Windows mediante lo strumento di aggiunta o rimozione programma.

Procedura

- 1 [Individuazione dell'impronta digitale del certificato SSL per il servizio del sito di gestione](#)

Quando si installa un agente di gestione, è necessario convalidare l'impronta digitale del certificato SSL per il servizio del sito di gestione.

2 Download e installazione di un agente di gestione

Un amministratore può scaricare e installare un agente di gestione su macchine IaaS nella distribuzione. L'agente di gestione deve essere installato su tutti i server IaaS, ad eccezione di quelli utilizzati esclusivamente per il database MS SQL.

Individuazione dell'impronta digitale del certificato SSL per il servizio del sito di gestione

Quando si installa un agente di gestione, è necessario convalidare l'impronta digitale del certificato SSL per il servizio del sito di gestione.

È possibile ottenere l'impronta digitale nel prompt dei comandi in vRealize Automation appliance.

Procedura

- 1 Accedere alla console della vRealize Automation appliance come utente root.
- 2 Immettere il seguente comando:

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

Viene visualizzata l'impronta digitale SHA1. Ad esempio:

```
SHA1 Fingerprint=E4:F0:37:9A:32:52:FA:7D:2E:91:BD:12:7A:2F:A3:75:F8:A1:7B:C4
```

- 3 Copiare l'UID dell'impronta digitale. Per la convalida potrebbe essere necessario rimuovere i due punti.

Passi successivi

Conservare l'impronta digitale copiata per utilizzarla con il programma d'installazione dell'agente di gestione.

Download e installazione di un agente di gestione

Un amministratore può scaricare e installare un agente di gestione su macchine IaaS nella distribuzione. L'agente di gestione deve essere installato su tutti i server IaaS, ad eccezione di quelli utilizzati esclusivamente per il database MS SQL.

L'agente di gestione registra i nodi IaaS con vRealize Automation appliance, automatizza l'installazione e la gestione dei componenti IaaS e raccoglie le informazioni di supporto e telemetria. L'agente di gestione viene eseguito come servizio di Windows sulla macchina IaaS ed è necessario disporre dei diritti di amministratore locale per installare l'agente.

Prerequisiti

- [Individuazione dell'impronta digitale del certificato SSL per il servizio del sito di gestione](#)
- Verificare che l'utente dell'account del servizio, o l'utente del dominio, faccia parte del gruppo di amministratori locale di ciascuna macchina IaaS.

Procedura

- 1 Aprire vRealize Automation appliance specificando un indirizzo nel seguente formato in un browser Web, dove *vra-va-hostname.domain.name* è il nome di dominio completo di vRealize Automation appliance. Non utilizzare l'indirizzo di un bilanciamento del carico.

`https://vra-va-hostname.domain.name:5480/installer`

- 2 Fare clic sul **programma di installazione dell'agente di gestione** per scaricarlo.
- 3 Eseguire il programma d'installazione dell'agente di gestione, vCAC-IaaSManagementAgent-Setup.msi.
Il percorso di installazione predefinito è *%Programmi (x86)%\VMware\vCAC\Management Agent*
- 4 Fare clic su **Avanti** nella pagina iniziale.
- 5 Accettare il contratto EULA e fare clic su **Avanti**.
- 6 Fornire un percorso di installazione alternativo o accettare il valore predefinito.
- 7 Fare clic su **Avanti**.
- 8 Specificare i dettagli del servizio del sito di gestione per i seguenti campi e fare clic su **Avanti**.

Casella di testo	Input
Indirizzo appliance vRA	<code>https://vra-va-hostname.domain.name:5480</code> È necessario specificare il numero di porta.
Nome utente radice	Utente radice di vRealize Automation appliance.
Password	Password dell'utente radice di vRealize Automation appliance.

Casella di testo	Input
Certificato server del sito di gestione	Impronta digitale SHA1 per il certificato del servizio del sito di gestione. Il servizio del sito di gestione è ospitato su vRealize Automation appliance. Esempio di impronta digitale SHA1: DFF5FA0886DA2920D227ADF8BC9CDE4EF13EEF78.
Carica	Fare clic su Carica per caricare l'impronta digitale predefinita.

VMware vRealize Automation Management Agent Setup

Management Site Service

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

vRA appliance address:

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

Root username: Password:

Provide vRealize Automation appliance root user credentials

Management Site Service certificate SHA1 fingerprint:

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

- 9 Selezionare la casella di controllo di **conferma della corrispondenza delle impronte digitali** dopo aver verificato che l'impronta digitale visualizzata corrisponda a quella del certificato SSL del sito di gestione.

Se le impronte digitali non coincidono, controllare la correttezza dell'indirizzo inserito nella casella di testo **Indirizzo appliance vRA**.

- 10 Fare clic su **Avanti**.
- 11 Inserire il nome utente e la password dell'account del servizio.
- 12 Fare clic su **Avanti**.
- 13 Fare clic su **Installa**.
- 14 Fare clic su **Fine**.
- 15 Ripetere la procedura per ciascun host IaaS Windows.

Dopo aver installato l'agente di gestione, il server Windows viene elencato nella pagina Prerequisiti di installazione dell'installazione guidata.

Sincronizzazione degli orari di server

Gli orologi dei server vRealize Automation e Windows devono essere sincronizzati per garantire l'esito positivo dell'installazione.

Le opzioni disponibili nella pagina Prerequisiti dell'installazione guidata consentono di selezionare un metodo di sincronizzazione dell'orario per le appliance virtuali. La tabella degli host IaaS mostra gli scostamenti degli orari.

Procedura

- 1 Selezionare un'opzione dal menu **Modalità sincronizzazione ora**.

Opzione	Azione
Usa server di riferimento ora	Selezionare Usa server di riferimento ora dal menu Modalità sincronizzazione ora per utilizzare il protocollo NTP (Network Time Protocol). Immettere l'indirizzo IP o il nome host di ogni server orario utilizzato nella casella di testo Server di riferimento ora .
Usa ora dell'host	Selezionare Usa ora dell'host dal menu Modalità sincronizzazione ora per utilizzare la sincronizzazione di data e ora di VMware Tools. È necessario configurare le connessioni ai server NTP prima di poter utilizzare la sincronizzazione di data e ora di VMware Tools.

- 2 Fare clic su **Modifica impostazioni ora**.

- 3 Fare clic su **Avanti**.

Passi successivi

Verificare che i server IaaS siano configurati correttamente.

Esecuzione di Controllo prerequisiti

Eseguire il controllo prerequisiti per verificare che i componenti del server Windows per IaaS siano configurati correttamente.

Procedura

- 1 Fare clic su **Esegui** sulla schermata del controllo prerequisiti.

Durante l'esecuzione dei controlli, viene elencato ciascun server Windows per componenti IaaS assieme allo stato relativo.

- 2 Se viene visualizzato un avviso, è possibile ottenere ulteriori informazioni sull'errore oppure scegliere di correggere l'errore automaticamente.
 - ◆ Fare clic su **Mostra dettagli** per ulteriori informazioni sull'errore e sull'azione da eseguire per risolverlo.
 - ◆ Fare clic su **Correggi** per correggere automaticamente l'errore. In questo modo la macchina Windows verrà inoltre riavviata in base alle esigenze.
- 3 Fare clic su **Esegui** per verificare le correzioni.

- 4 Fare clic su **Avanti** una volta risolti tutti gli errori.

I server Windows saranno quindi configurati correttamente per l'installazione dei componenti IaaS.

Passi successivi

Continuare alla schermata host di vRealize Automation.

Selezione dei parametri di configurazione della distribuzione

Specificare i parametri di configurazione per i componenti della distribuzione.

Prerequisiti

Procedura

- 1 Nella schermata Host di vRealize Automation, specificare l'host.
 - Fare clic su Risolvi automaticamente per lasciare a vRealize Automation il compito di fornire l'indirizzo predefinito.
 - Fare clic su Inserire host e specificare l'alias DNS o il nome di dominio completo di un host differente.
- 2 Fare clic su Avanti.
- 3 Nella schermata Single Sign-On, immettere la password dell'amministratore di sistema per l'account del tenant predefinito e confermare la password reimmettendola.
- 4 Fare clic su Avanti.
- 5 Continuare nelle schermate successive, utilizzando la guida contestuale nel caso occorressero informazioni aggiuntive.
- 6 Fare clic su Avanti dopo aver completato la schermata di convalida.

Passi successivi

Creare uno snapshot delle macchine prima di iniziare l'installazione del prodotto.

Creazione di snapshot prima di iniziare l'installazione

Creare snapshot di tutte le appliance e dei server Windows. In caso di problemi di installazione, è possibile tornare a questi snapshot e provare a effettuare una nuova installazione.

Gli snapshot preservano il lavoro di configurazione. Assicurarsi di includere uno snapshot di vRealize Automation appliance su cui viene eseguita l'installazione guidata.

Le istruzioni fornite sono per utenti di vSphere.

Nota: Non uscire dall'installazione guidata né annullare l'installazione.

Procedura

- 1 Aprire un altro browser e accedere a vSphere Client.

- 2 Individuare il server o l'appliance nell'inventario di vSphere Client.
- 3 Fare clic con il pulsante destro del mouse sul server nell'inventario e selezionare **Crea snapshot**.
- 4 Immettere il nome dello snapshot.
- 5 Selezionare la casella di controllo **Includere la memoria?** per catturare la memoria del server e fare clic su **OK**.

Lo snapshot viene creato.

Ripetere questi passaggi per creare snapshot per ogni server o appliance.

Passi successivi

[Completamento dell'installazione](#)

Scenario: completamento dell'installazione

In qualità di amministratore di vSphere, si è giunti all'ultima parte del processo di installazione. Si avvia l'installazione di vRealize Automation e se ne attende il completamento.

Procedura

- 1 Tornare all'installazione guidata.
- 2 Esaminare il riepilogo dell'installazione e fare clic su **Avanti**.
- 3 Immettere la chiave di licenza del prodotto e fare clic su **Avanti**.
- 4 Accettare o modificare le impostazioni di telemetria predefinite e fare clic su **Avanti**.
- 5 Fare clic su **Avanti**.
- 6 Fare clic su **Fine**.

L'installazione ha inizio. La procedura d'installazione può richiedere da quindici minuti a un'ora, in base alla configurazione della rete.

Al termine dell'installazione viene visualizzato un messaggio di conferma.

Passi successivi

A questo punto è possibile procedere con la configurazione della distribuzione.

Risoluzione dei problemi di installazione

Quando si esegue l'installazione dalla pagina Dettagli installazione, vengono visualizzate informazioni sugli eventuali problemi che impediscono il completamento dell'installazione.

Quando vengono rilevati problemi, il componente viene contrassegnato e vengono visualizzate informazioni dettagliate sull'errore, oltre alle operazioni da eseguire per trovare una soluzione. Dopo aver risolto il problema, provare a eseguire di nuovo il passaggio di installazione. I passaggi di correzione da eseguire variano a seconda del tipo di errore rilevato.

Procedura

- 1 Se il pulsante **Nuovo tentativo non riuscito** è abilitato, procedere come indicato di seguito.
 - a Esaminare l'errore.
 - b Stabilire quali elementi devono essere modificati e apportare le modifiche necessarie.
 - c Tornare alla schermata d'installazione e fare clic su **Nuovo tentativo non riuscito**.
Il programma d'installazione prova a installare tutti i componenti non riusciti.
- 2 Se il pulsante **Nuovo tentativo per tutti i server IaaS** è abilitato, procedere come indicato di seguito.
 - a Esaminare l'errore.
 - b Stabilire quali elementi devono essere modificati.
 - c Ripristinare gli snapshot di tutti i server IaaS creati in precedenza.
 - d Eliminare il database MS SQL, se si utilizza un database esterno.
 - e Apportare le modifiche necessarie.
 - f Fare clic su **Nuovo tentativo per tutti i server IaaS**.
- 3 Se l'errore si verifica nei componenti dell'appliance virtuale, procedere come indicato di seguito.
 - a Esaminare l'errore.
 - b Stabilire quali elementi devono essere modificati.
 - c Ripristinare gli snapshot di tutti i server, incluso quello dal quale si sta eseguendo la procedura guidata.
 - d Apportare le modifiche necessarie.
 - e Aggiornare la pagina della procedura guidata.
 - f Accedere ed eseguire di nuovo la procedura guidata.
La procedura guidata si apre al passaggio della pre-installazione.

Configurazione delle credenziali per la configurazione dei contenuti iniziali

Facoltativamente, è possibile iniziare un workflow dei contenuti iniziali per un endpoint vSphere.

Il processo utilizza un utente locale chiamato configurationadmin a cui sono concessi diritti amministrativi.

Procedura

- 1 Creare e immettere una password per l'account configurationadmin nella casella di testo **Password**.
- 2 Reimmettere la password nella casella di testo **Conferma password**. Prendere nota della password per l'utilizzo futuro.
- 3 Fare clic su **Crea contenuto iniziale**.
- 4 Fare clic su **Avanti**.

Vengono creati l'utente di amministrazione della configurazione e una voce di catalogo di configurazione nel tenant predefinito. All'amministratore di configurazione vengono concessi i diritti seguenti:

- Amministratore approvazioni
- Amministratore del catalogo
- Amministratore di IaaS
- Architetto dell'infrastruttura
- Amministratore tenant
- Architetto XaaS

Passi successivi

- Quando si completa la procedura guidata, accedere al tenant predefinito come utente configurationadmin e richiedere gli elementi di catalogo Contenuto iniziale. Per un esempio di come richiedere l'elemento e completare l'azione utente manuale, vedere *Installazione e configurazione di vRealize Automation per lo scenario Rainpole*.
- Configurare l'accesso al tenant predefinito per altri utenti. Vedere [Capitolo 5 Configurazione dell'accesso per il tenant predefinito](#).

Installazione di una distribuzione enterprise con l'installazione guidata

È possibile personalizzare la distribuzione enterprise alle esigenze specifiche dell'organizzazione. Una distribuzione enterprise può essere composta da componenti distribuiti o distribuzioni ad alta disponibilità configurate con bilanciamenti del carico.

Le distribuzioni enterprise sono pensate per strutture d'installazione più complesse con componenti distribuiti e ridondanti e generalmente includono bilanciamenti del carico. L'installazione di componenti di IaaS è facoltativa in entrambi i tipi di distribuzione.

Per le distribuzioni con bilanciamento del carico, istanze server Web attive e appliance vRealize Automation appliance multiple possono causare la non riuscita dell'installazione. Durante l'installazione è consigliabile che siano attive una singola istanza server Web e una singola vRealize Automation appliance.

Esecuzione dell'installazione guidata per una distribuzione enterprise

Le distribuzioni enterprise sono utilizzate per gli ambienti di produzione. È possibile utilizzare l'installazione guidata per distribuire un'installazione distribuita regolare o con bilanciamenti del carico per garantire alta disponibilità e failover.

Se si installare un'installazione distribuita con bilanciamento del carico per alta disponibilità e failover, avvertire il team responsabile della configurazione dell'ambiente vRealize Automation. Gli amministratori tenant devono configurare Gestione directory per l'alta disponibilità quando configurano il collegamento ad Active Directory.

Prerequisiti

- Assicurarsi che siano soddisfatti i prerequisiti descritti in [Capitolo 2 Preparazione per l'installazione](#)
- [Distribuzione di vRealize Automation appliance](#).

Procedura

- 1 Aprire un browser.
- 2 Accedere alla console di gestione della vRealize Automation appliance utilizzando il suo nome di dominio completo, `https://vra-va-hostname.domain.name:5480/`.
- 3 Accedere utilizzando il nome utente **root** e la password specificati al momento della distribuzione dell'appliance.
- 4 L'installazione guidata viene visualizzata la prima volta che si accede all'appliance.
- 5 Accettare l'accordo di licenza con l'utente finale e fare clic su **Avanti**.
- 6 Selezionare **Distribuzione enterprise e Installa Infrastructure as a Service (IaaS)** nella schermata Tipo di distribuzione, quindi scegliere **Avanti**.
- 7 Verificare che siano soddisfatti i prerequisiti elencati nella pagina Prerequisiti d'installazione e che siano elencati i server Windows su cui è stato installato un agente di gestione.
- 8 Se necessario, è possibile modificare il metodo di registrazione dell'ora per l'appliance vRealize Automation. Fare clic su **Modifica impostazioni ora** se si desidera apportare modifiche.
- 9 Fare clic su **Avanti**.

Installazione dell'agente di gestione

È necessario installare un agente di gestione su ciascuna macchina Windows che ospita componenti IaaS.

Se si verifica un guasto nell'appliance vRealize Automation principale, sarà necessario reinstallare gli agenti di gestione.

Gli agenti di gestione non vengono eliminati automaticamente quando si disinstalla un componente IaaS. Disinstallare l'agente di gestione esattamente come si disinstalla qualsiasi programma Windows mediante lo strumento di aggiunta o rimozione programma.

Individuazione dell'impronta digitale del certificato SSL per il servizio del sito di gestione

Quando si installa un agente di gestione, è necessario convalidare l'impronta digitale del certificato SSL per il servizio del sito di gestione.

È possibile ottenere l'impronta digitale nel prompt dei comandi in vRealize Automation appliance.

Procedura

1 Accedere alla console della vRealize Automation appliance come utente root.

2 Immettere il seguente comando:

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

Viene visualizzata l'impronta digitale SHA1. Ad esempio:

```
SHA1 Fingerprint=E4:F0:37:9A:32:52:FA:7D:2E:91:BD:12:7A:2F:A3:75:F8:A1:7B:C4
```

3 Copiare l'UID dell'impronta digitale. Per la convalida potrebbe essere necessario rimuovere i due punti.

Passi successivi

Conservare l'impronta digitale copiata per utilizzarla con il programma d'installazione dell'agente di gestione.

Download e installazione di un agente di gestione

Un amministratore può scaricare e installare un agente di gestione su macchine IaaS nella distribuzione. L'agente di gestione deve essere installato su tutti i server IaaS, ad eccezione di quelli utilizzati esclusivamente per il database MS SQL.

L'agente di gestione registra i nodi IaaS con vRealize Automation appliance, automatizza l'installazione e la gestione dei componenti IaaS e raccoglie le informazioni di supporto e telemetria. L'agente di gestione viene eseguito come servizio di Windows sulla macchina IaaS ed è necessario disporre dei diritti di amministratore locale per installare l'agente.

Prerequisiti

- [Individuazione dell'impronta digitale del certificato SSL per il servizio del sito di gestione](#)
- Verificare che l'utente dell'account del servizio, o l'utente del dominio, faccia parte del gruppo di amministratori locale di ciascuna macchina IaaS.

Procedura

1 Aprire vRealize Automation appliance specificando un indirizzo nel seguente formato in un browser Web, dove *vra-virtual-hostname.domain.name* è il nome di dominio completo di vRealize Automation appliance. Non utilizzare l'indirizzo di un bilanciamento del carico.

```
https://vra-virtual-hostname.domain.name:5480/installer
```

2 Fare clic sul **programma di installazione dell'agente di gestione** per scaricarlo.

- 3 Eseguire il programma d'installazione dell'agente di gestione, vCAC-laaSManagementAgent-Setup.msi.

Il percorso di installazione predefinito è `%Programmi (x86)%\VMware\vCAC\Management Agent\`

- 4 Fare clic su **Avanti** nella pagina iniziale.
- 5 Accettare il contratto EULA e fare clic su **Avanti**.
- 6 Fornire un percorso di installazione alternativo o accettare il valore predefinito.
- 7 Fare clic su **Avanti**.
- 8 Specificare i dettagli del servizio del sito di gestione per i seguenti campi e fare clic su **Avanti**.

Casella di testo	Input
Indirizzo appliance vRA	<code>https://vra-va-hostname.domain.name:5480</code> È necessario specificare il numero di porta.
Nome utente radice	Utente radice di vRealize Automation appliance.
Password	Password dell'utente radice di vRealize Automation appliance.
Certificato server del sito di gestione	Impronta digitale SHA1 per il certificato del servizio del sito di gestione. Il servizio del sito di gestione è ospitato su vRealize Automation appliance. Esempio di impronta digitale SHA1: <code>DFF5FA0886DA2920D227ADF8BC9CDE4EF13EEF78</code> .
Carica	Fare clic su Carica per caricare l'impronta digitale predefinita.

The screenshot shows the 'Management Site Service' configuration window. It includes fields for 'vRA appliance address' (pre-filled with 'https://vra-address:5480/'), 'Root username' (pre-filled with 'root'), and 'Password'. Below these is a 'Management Site Service certificate SHA1 fingerprint' field with a 'Load' button. A checkbox is checked, indicating confirmation of the fingerprint. At the bottom are 'Back', 'Next', and 'Cancel' buttons.

VMware vRealize Automation Management Agent Setup

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

vRA appliance address:

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

Root username: Password:

Provide vRealize Automation appliance root user credentials

Management Site Service certificate SHA1 fingerprint:

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

- 9 Selezionare la casella di controllo di **conferma della corrispondenza delle impronte digitali** dopo aver verificato che l'impronta digitale visualizzata corrisponda a quella del certificato SSL del sito di gestione.

Se le impronte digitali non coincidono, controllare la correttezza dell'indirizzo inserito nella casella di testo **Indirizzo appliance vRA**.

- 10 Fare clic su **Avanti**.
- 11 Inserire il nome utente e la password dell'account del servizio.
- 12 Fare clic su **Avanti**.
- 13 Fare clic su **Installa**.
- 14 Fare clic su **Fine**.
- 15 Ripetere la procedura per ciascun host IaaS Windows.

Dopo aver installato l'agente di gestione, il server Windows viene elencato nella pagina Prerequisiti di installazione dell'installazione guidata.

Sincronizzazione degli orari di server

Gli orologi dei server vRealize Automation e Windows devono essere sincronizzati per garantire l'esito positivo dell'installazione.

Le opzioni disponibili nella pagina Prerequisiti dell'installazione guidata consentono di selezionare un metodo di sincronizzazione dell'orario per le appliance virtuali. La tabella degli host IaaS mostra gli scostamenti degli orari.

Procedura

- 1 Selezionare un'opzione dal menu **Modalità sincronizzazione ora**.

Opzione	Azione
Usa server di riferimento ora	Selezionare Usa server di riferimento ora dal menu Modalità sincronizzazione ora per utilizzare il protocollo NTP (Network Time Protocol). Immettere l'indirizzo IP o il nome host di ogni server orario utilizzato nella casella di testo Server di riferimento ora .
Usa ora dell'host	Selezionare Usa ora dell'host dal menu Modalità sincronizzazione ora per utilizzare la sincronizzazione di data e ora di VMware Tools. È necessario configurare le connessioni ai server NTP prima di poter utilizzare la sincronizzazione di data e ora di VMware Tools.

- 2 Fare clic su **Modifica impostazioni ora**.
- 3 Fare clic su **Avanti**.

Passi successivi

Verificare che i server IaaS siano configurati correttamente.

Esecuzione di Controllo prerequisiti

Eseguire Controllo prerequisiti per verificare che i server Windows per i componenti IaaS siano correttamente configurati.

Procedura

- 1 Fare clic su **Esegui** sulla schermata del controllo prerequisiti.
Durante l'esecuzione dei controlli, viene elencato ciascun server Windows per componenti IaaS assieme allo stato relativo.
- 2 Se viene visualizzato un avviso, è possibile ottenere ulteriori informazioni sull'errore oppure scegliere di correggere l'errore automaticamente.
 - ◆ Fare clic su **Mostra dettagli** per ulteriori informazioni sull'errore e sull'azione da eseguire per risolverlo.
 - ◆ Fare clic su **Correggi** per correggere automaticamente l'errore. In questo modo la macchina Windows verrà inoltre riavviata in base alle esigenze.
- 3 Fare clic su **Esegui** per verificare le correzioni.
- 4 Fare clic su **Avanti** una volta risolti tutti gli errori.

I server Windows saranno quindi configurati correttamente per l'installazione dei componenti IaaS.

Passi successivi

Continuare alla schermata host di vRealize Automation.

Selezione dei parametri di configurazione della distribuzione

Specificare i parametri di configurazione per i componenti della distribuzione.

Prerequisiti

Procedura

- 1 Nella schermata Host di vRealize Automation, specificare l'host.
 - Fare clic su Risolvi automaticamente per lasciare a vRealize Automation il compito di fornire l'indirizzo predefinito.
 - Fare clic su Inserire host e specificare l'alias DNS o il nome di dominio completo di un host differente.
- 2 Fare clic su Avanti.
- 3 Nella schermata Single Sign-On, immettere la password dell'amministratore di sistema per l'account del tenant predefinito e confermare la password reimmettendola.
- 4 Fare clic su Avanti.

- 5 Continuare nelle schermate successive, utilizzando la guida contestuale nel caso occorressero informazioni aggiuntive.
- 6 Fare clic su **Avanti** dopo aver completato la schermata di convalida.

Passi successivi

Creare uno snapshot delle macchine prima di iniziare l'installazione del prodotto.

Creazione di snapshot prima di iniziare l'installazione

Creare snapshot di tutte le appliance e dei server Windows. In caso di problemi di installazione, è possibile tornare a questi snapshot e provare a effettuare una nuova installazione.

Gli snapshot preservano il lavoro di configurazione. Assicurarsi di includere uno snapshot di vRealize Automation appliance su cui viene eseguita l'installazione guidata.

Le istruzioni fornite sono per utenti di vSphere.

Nota: Non uscire dall'installazione guidata né annullare l'installazione.

Procedura

- 1 Aprire un altro browser e accedere a vSphere Client.
- 2 Individuare il server o l'appliance nell'inventario di vSphere Client.
- 3 Fare clic con il pulsante destro del mouse sul server nell'inventario e selezionare **Crea snapshot**.
- 4 Immettere il nome dello snapshot.
- 5 Selezionare la casella di controllo **Includere la memoria?** per catturare la memoria del server e fare clic su **OK**.

Lo snapshot viene creato.

Ripetere questi passaggi per creare snapshot per ogni server o appliance.

Passi successivi

Completamento dell'installazione

Completamento dell'installazione

Una volta arrestati gli snapshot, verrà avviata l'installazione di vRealize Automation, pertanto sarà necessario attenderne il completamento.

Procedura

- 1 Tornare all'installazione guidata.
- 2 Esaminare il riepilogo dell'installazione e fare clic su **Avanti**.
- 3 Fare clic su **Avanti**.
- 4 Fare clic su **Fine**.

L'installazione ha inizio. La procedura d'installazione può richiedere da quindici minuti a un'ora, in base alla configurazione della rete.

Al termine dell'installazione viene visualizzato un messaggio di conferma.

Passi successivi

A questo punto è possibile procedere con la configurazione della distribuzione.

Risoluzione dei problemi di installazione

Quando si esegue l'installazione dalla pagina Dettagli installazione, vengono visualizzate informazioni sugli eventuali problemi che impediscono il completamento dell'installazione.

Quando vengono rilevati problemi, il componente viene contrassegnato e vengono visualizzate informazioni dettagliate sull'errore, oltre alle operazioni da eseguire per trovare una soluzione. Dopo aver risolto il problema, provare a eseguire di nuovo il passaggio di installazione. I passaggi di correzione da eseguire variano a seconda del tipo di errore rilevato.

Procedura

- 1 Se il pulsante **Nuovo tentativo non riuscito** è abilitato, procedere come indicato di seguito.
 - a Esaminare l'errore.
 - b Stabilire quali elementi devono essere modificati e apportare le modifiche necessarie.
 - c Tornare alla schermata d'installazione e fare clic su **Nuovo tentativo non riuscito**.
Il programma d'installazione prova a installare tutti i componenti non riusciti.
- 2 Se il pulsante **Nuovo tentativo per tutti i server IaaS** è abilitato, procedere come indicato di seguito.
 - a Esaminare l'errore.
 - b Stabilire quali elementi devono essere modificati.
 - c Ripristinare gli snapshot di tutti i server IaaS creati in precedenza.
 - d Eliminare il database MS SQL, se si utilizza un database esterno.
 - e Apportare le modifiche necessarie.
 - f Fare clic su **Nuovo tentativo per tutti i server IaaS**.
- 3 Se l'errore si verifica nei componenti dell'appliance virtuale, procedere come indicato di seguito.
 - a Esaminare l'errore.
 - b Stabilire quali elementi devono essere modificati.
 - c Ripristinare gli snapshot di tutti i server, incluso quello dal quale si sta eseguendo la procedura guidata.
 - d Apportare le modifiche necessarie.

- e Aggiornare la pagina della procedura guidata.
- f Accedere ed eseguire di nuovo la procedura guidata.

La procedura guidata si apre al passaggio della pre-installazione.

Configurazione delle credenziali per la configurazione dei contenuti iniziali

Facoltativamente, è possibile iniziare un workflow dei contenuti iniziali per un endpoint vSphere.

Il processo utilizza un utente locale chiamato configurationadmin a cui sono concessi diritti amministrativi.

Procedura

- 1 Creare e immettere una password per l'account configurationadmin nella casella di testo **Password**.
- 2 Reimmettere la password nella casella di testo **Conferma password**. Prendere nota della password per l'utilizzo futuro.
- 3 Fare clic su **Crea contenuto iniziale**.
- 4 Fare clic su **Avanti**.

Vengono creati l'utente di amministrazione della configurazione e una voce di catalogo di configurazione nel tenant predefinito. All'amministratore di configurazione vengono concessi i diritti seguenti:

- Amministratore approvazioni
- Amministratore del catalogo
- Amministratore di IaaS
- Architetto dell'infrastruttura
- Amministratore tenant
- Architetto XaaS

Passi successivi

- Quando si completa la procedura guidata, accedere al tenant predefinito come utente configurationadmin e richiedere gli elementi di catalogo Contenuto iniziale. Per un esempio di come richiedere l'elemento e completare l'azione utente manuale, vedere *Installazione e configurazione di vRealize Automation per lo scenario Rainpole*.
- Configurare l'accesso al tenant predefinito per altri utenti. Vedere [Capitolo 5 Configurazione dell'accesso per il tenant predefinito](#).

Installazione di vRealize Automation tramite le interfacce standard

4

In alternativa all'installazione guidata, è possibile installare vRealize Automation tramite la console di gestione di vRealize Automation Appliance e il programma di installazione manuale di IaaS.

L'installazione tramite l'interfaccia standard è richiesta principalmente per

Questo capitolo include i seguenti argomenti:

- [Distribuzione minima](#)
- [Distribuzione distribuita](#)
- [Installazione degli agenti](#)

Distribuzione minima

È possibile installare una distribuzione minima autonoma da utilizzare in un ambiente di sviluppo o di prototipazione. Le distribuzioni minime non sono adatte all'uso in ambienti di produzione.

Elenco di controllo di una distribuzione minima

Un amministratore di sistema può distribuire un vRealize Automation completo in una configurazione minima. Le distribuzioni minime vengono di solito utilizzate in ambienti di sviluppo o di prototipazione e la loro installazione richiede meno passaggi.

L'elenco di controllo di una distribuzione minima è una panoramica ad alto livello della sequenza di passaggi necessari per completare un'installazione minima.

Stampare una copia dell'elenco di controllo e utilizzarla per tenere traccia del lavoro durante l'installazione. Completare le attività nell'ordine in cui sono riportate.

Tavola 4-1. Elenco di controllo di una distribuzione minima

Attività	Dettagli
<input type="checkbox"/> Pianificare e preparare l'ambiente d'installazione e verificare che tutti i prerequisiti d'installazione siano soddisfatti.	Capitolo 2 Preparazione per l'installazione
<input type="checkbox"/> Configurare vRealize Automation appliance	Distribuzione e configurazione dell'appliance vRealize Automation
<input type="checkbox"/> Installare i componenti IaaS su un singolo server Windows.	Installazione dei componenti IaaS

Tavola 4-1. Elenco di controllo di una distribuzione minima (Continua)

Attività	Dettagli
<input type="checkbox"/> Installare agenti aggiuntivi, se necessario.	Installazione degli agenti
<input type="checkbox"/> Eseguire le attività post-installazione, come la configurazione del tenant predefinito.	

Distribuzione e configurazione dell'appliance vRealize Automation

vRealize Automation appliance è una appliance virtuale preconfigurata che distribuisce il server e la console Web (portale dell'utente) di vRealize Automation appliance. Essa viene fornita come modello in formato di virtualizzazione aperto (OVF, Open Virtualization Format). L'amministratore di sistema scarica l'appliance e la distribuisce in vCenter Server o nell'inventario ESX/ESXi.

1 [Distribuzione di vRealize Automation appliance](#)

Per distribuire vRealize Automation appliance, è necessario che un amministratore di sistema acceda al client vSphere e selezioni le impostazioni di distribuzione.

2 [Attivazione della sincronizzazione di data e ora su vRealize Automation Appliance](#)

Gli orologi dei server vRealize Automation e Windows devono essere sincronizzati per garantire l'esito positivo dell'installazione.

3 [Configurazione dell'appliance di vRealize Automation](#)

Per preparare la vRealize Automation appliance all'uso, un amministratore di sistema deve configurare le impostazioni dell'host, generare un certificato SSL e specificare le informazioni di connessione SSO.

Distribuzione di vRealize Automation appliance

Per distribuire vRealize Automation appliance, è necessario che un amministratore di sistema acceda al client vSphere e selezioni le impostazioni di distribuzione.

La password radice creata per l'amministratore di vRealize Automation è soggetta ad alcune restrizioni. Vedere [Considerazioni sulle password](#).

Prerequisiti

- Scaricare vRealize Automation appliance dal sito Web di VMware.
- Accedere al client vSphere come utente con privilegi di amministratore di sistema.

Procedura

- 1 Selezionare **File > Distribuisci modello OVF** dal client di vSphere.
- 2 Selezionare il file di vRealize Automation appliance scaricato e fare clic su **Apri**.
- 3 Fare clic su **Avanti**.
- 4 Fare clic su **Avanti** nella pagina Dettagli modello OVF.
- 5 Accettare il contratto di licenza e fare clic su **Avanti**.

- 6 Immettere un nome univoco per l'appliance virtuale nella casella di controllo **Nome** rispettando la convenzione di denominazione IT dell'organizzazione, selezionare il data center e la posizione in cui si desidera distribuire l'appliance virtuale e fare clic su **Avanti**.
- 7 Seguire le istruzioni presentate fino alla visualizzazione della pagina Formato disco.
- 8 Nella pagina Formato disco, verificare che vi sia spazio sufficiente per distribuire l'appliance virtuale e fare clic su **Avanti**.
- 9 Seguire le istruzioni presentate fino alla pagina Proprietà.
Le opzioni visualizzate dipendono dalla configurazione di vSphere.
- 10 Configurare i valori nella pagina Proprietà.
 - a Immettere la password radice da utilizzare quando si accede alla console dell'appliance virtuale nelle caselle di testo **Immetti password** e **Conferma password**.
 - b Selezionare o deselezionare la casella di testo **Servizio SSH** per attivare o disattivare il servizio SSH per l'appliance.

Questo valore è utilizzato per impostare lo stato iniziale del servizio SSH nell'appliance. Se si sta eseguendo l'installazione guidata, attivare questa opzione prima di avviare la procedura guidata. Dopo l'installazione sarà possibile modificare questa impostazione dalla console di gestione dell'appliance.
 - c Immettere il nome di dominio completo della macchina virtuale nella casella di testo **Nome host**, anche se si utilizza il DHCP.
 - d Configurare le proprietà di networking.
- 11 Fare clic su **Avanti**.
- 12 In base alle configurazioni di vCenter e DNS utilizzate, la risoluzione DNS potrebbe impiegare del tempo. Per accelerare il processo, eseguire i seguenti passaggi.
 - Se nella pagina Completamento è disponibile **Accendi dopo la distribuzione**.
 - a Selezionare **Accendi dopo la distribuzione** e fare clic su **Fine**.
 - b Scegliere **Chiudi** al completamento della distribuzione del file in vCenter.
 - c Attendere l'avvio della macchina.

Questa fase potrebbe richiedere fino a 5 minuti.
 - Se nella pagina Completamento non è disponibile **Accendi dopo la distribuzione**.
 - a Scegliere **Chiudi** al completamento della distribuzione del file in vCenter.
 - b Accendere la VM e attendere il tempo necessario alla VM per avviarsi.
 - c Assicurarsi che sia possibile eseguire un ping al DNS della macchina virtuale. Se non è possibile eseguire un ping al DNS, riavviare la macchina virtuale.
 - d Attendere l'avvio della macchina. Questa fase potrebbe richiedere fino a 5 minuti.
- 13 Aprire un prompt dei comandi ed eseguire un ping sul nome di dominio completo per verificare che questo venga correttamente risolto nell'indirizzo IP vRealize Automation appliance.

Attivazione della sincronizzazione di data e ora su vRealize Automation Appliance

Gli orologi dei server vRealize Automation e Windows devono essere sincronizzati per garantire l'esito positivo dell'installazione.

Se durante questo processo vengono visualizzati avvisi relativi ai certificati, è possibile ignorarli e continuare per completare l'installazione.

Prerequisiti

[Distribuzione di vRealize Automation appliance.](#)

Procedura

- 1 Accedere alla console di gestione della vRealize Automation appliance utilizzando il suo nome di dominio completo, `https://vra-va-hostname.domain.name:5480/`.
- 2 Accedere utilizzando il nome utente **root** e la password specificati al momento della distribuzione dell'appliance.
- 3 Selezionare **Amministrazione > Impostazioni ora**.
- 4 Selezionare un'opzione dal menu **Modalità sincronizzazione ora**.

Opzione	Azione
Usa server di riferimento ora	Selezionare Usa server di riferimento ora dal menu Modalità sincronizzazione ora per utilizzare il protocollo NTP (Network Time Protocol). Immettere l'indirizzo IP o il nome host di ogni server orario utilizzato nella casella di testo Server di riferimento ora .
Usa ora dell'host	Selezionare Usa ora dell'host dal menu Modalità sincronizzazione ora per utilizzare la sincronizzazione di data e ora di VMware Tools. È necessario configurare le connessioni ai server NTP prima di poter utilizzare la sincronizzazione di data e ora di VMware Tools.

- 5 Fare clic su **Salva impostazioni**.
- 6 Fare clic su **Aggiorna**.
- 7 Verificare che il valore in **Ora corrente** sia corretto.
Dalla scheda **Sistema** della pagina Impostazioni fuso orario è possibile cambiare il fuso orario.
- 8 (Facoltativo) Fare clic su **Fuso orario** dalla scheda **Sistema** e selezionare un fuso orario per il sistema dalle opzioni disponibili nel menu.
L'impostazione predefinita è ETC/UTC.
- 9 Fare clic su **Salva impostazioni**.

Configurazione dell'appliance di vRealize Automation

Per preparare la vRealize Automation appliance all'uso, un amministratore di sistema deve configurare le impostazioni dell'host, generare un certificato SSL e specificare le informazioni di connessione SSO.

Prerequisiti

Attivazione della sincronizzazione di data e ora su vRealize Automation Appliance.

Procedura

- 1 Accedere alla console di gestione della vRealize Automation appliance utilizzando il suo nome di dominio completo, `https://vra-va-hostname.domain.name:5480/`.
- 2 Continuare ignorando l'avviso sul certificato.
- 3 Accedere con il nome utente root e la password specificati quando è stata distribuita vRealize Automation appliance.
- 4 Selezionare **Impostazioni vRA > Impostazioni host**.

Opzione	Azione
Risolvi automaticamente	Selezionare Risolvi automaticamente per specificare il nome dell'host corrente per vRealize Automation appliance.
Aggiorna host	<p>Per i nuovi host, selezionare Aggiorna host. Immettere il nome di dominio completo di vRealize Automation appliance, <code>vra-hostname.domain.name</code>, nella casella di testo Nome host.</p> <p>Per le distribuzioni distribuite che utilizzano bilanciamenti del carico, selezionare Aggiorna host. Immettere il nome di dominio completo del server del bilanciamento del carico, <code>vra-loadbalancename.domain.name</code>, nella casella di testo Nome host.</p>

Nota: configurare le impostazioni SSO come descritto più avanti in questa procedura ogni volta che si utilizza **Aggiorna host** per cambiare un nome host.

6 Selezionare il tipo di certificato dal menu **Azione certificato**.

Se si utilizza un certificato con codifica PEM, ad esempio per un ambiente distribuito, selezionare **Importa**.

I certificati importati devono essere attendibili nonché applicabili a tutte le istanze di vRealize Automation appliance e a qualsiasi bilanciamento del carico attraverso l'uso di certificati SAN (Subject Alternative Name).

Nota: se si utilizzano catene di certificati, specificare i certificati nel seguente ordine:

- a Certificato client/server firmato mediante il certificato di un'autorità di certificazione intermedia
- b Uno o più certificati intermedi
- c Certificato di un'autorità di certificazione radice

Opzione	Azione
Mantieni esistente	Lasciare invariata la configurazione SSL corrente. Selezionare questa opzione per annullare le modifiche.
Genera certificato	<ol style="list-style-type: none"> a Il valore visualizzato nella casella di testo Nome comune è il nome host visualizzato nella parte superiore della pagina. Se sono disponibili istanze aggiuntive di vRealize Automation appliance, i rispettivi nomi di dominio completi (FQDN) sono inclusi nell'attributo SAN del certificato. b Immettere il nome dell'organizzazione, come ad esempio quello della propria azienda, nella casella di testo Organizzazione. c Immettere l'unità organizzativa, ad esempio il nome o la posizione del proprio reparto, nella casella di testo Unità organizzativa. d Immettere il codice di paese ISO 3166 a due lettere, ad esempio IT, nella casella di testo Paese.
Importazione	<ol style="list-style-type: none"> a Copiare i valori del certificato dalla stringa BEGIN PRIVATE KEY alla stringa END PRIVATE KEY, inclusi intestazione e piè di pagina, quindi incollarli nella casella di testo Chiave privata RSA. b Copiare i valori del certificato dalla stringa BEGIN CERTIFICATE alla stringa END CERTIFICATE, inclusi intestazione e piè di pagina, quindi incollarli nella casella di testo Catena di certificati. Per valori di certificati multipli, includere un'intestazione BEGIN CERTIFICATE e un piè di pagina END CERTIFICATE per ciascun certificato. <p>Nota: In caso di certificati concatenati, possono essere disponibili attributi aggiuntivi.</p> <ol style="list-style-type: none"> c (Facoltativo) Se il certificato utilizza una passphrase per crittografare la chiave del certificato, copiare la passphrase e incollarla nella casella di testo Passphrase.

7 Fare clic su **Salva impostazioni** per salvare le informazioni sull'host e la configurazione SSL.

8 Configurare le impostazioni SSO.

9 Fare clic su **Messaggistica**. Vengono visualizzate le impostazioni di configurazione e lo stato della messaggistica per l'appliance. Non cambiare queste impostazioni.

- 10** Fare clic sulla scheda **Telemetria** per scegliere se partecipare al programma CEIP (Customer Experience Improvement Program) di VMware.

I dettagli relativi ai dati raccolti con il programma CEIP e gli scopi per cui è utilizzato da VMware sono disponibili nel Trust & Assurance Center all'indirizzo <http://www.vmware.com/trustvmware/ceip.html>.

- Selezionare **Partecipa al programma CEIP (Customer Experience Improvement Program) di VMware** per entrare a far parte del programma.
- Deselezionare **Partecipa al programma CEIP (Customer Experience Improvement Program) di VMware** per non entrare a far parte del programma.

- 11** Fare clic su **Servizi** e verificare che i servizi siano registrati.

L'operazione può richiedere circa 10 minuti, in base alla configurazione del sito.

Nota: è possibile accedere all'appliance ed eseguire `tail -f /var/log/vcac/catalina.out` per monitorare l'avvio dei servizi.

- 12** Immettere le informazioni della licenza.

- a Fare clic su **Impostazioni vRA > Gestione licenze**.
- b Fare clic su **Gestione licenze**.
- c Inserire una chiave di licenza di vRealize Automation valida scaricata all'atto del download dei file d'installazione e fare clic su **Invia chiave**.

Nota: se si verifica un errore di connessione, è possibile che ci sia un problema con il bilanciamento del carico. Controllare la connettività della rete al bilanciamento del carico.

- 13** Assicurarsi che sia possibile accedere alla console di vRealize Automation.

- a Aprire un browser e accedere alla pagina `https://vcac-hostname.domain.name/vcac`.
- b Accettare il certificato di vRealize Automation.
- c Accettare il certificato SSO.
- d Accedere con il nome utente `administrator@vsphere.local` e la password specificati quando è stato configurato SSO.

La console si apre alla scheda **Amministrazione** della pagina Tenant. Nell'elenco viene visualizzato un unico tenant chiamato `vsphere.local`.

Distribuzione e configurazione di vRealize Automation appliance sono completati. Se l'appliance non funziona correttamente dopo la configurazione, distribuire e configurare nuovamente l'appliance. Non apportare modifiche all'appliance esistente.

Passi successivi

[Installare i componenti dell'infrastruttura](#)

Installazione dei componenti IaaS

L'amministratore installa un set completo di componenti di infrastruttura (IaaS) su una macchina Windows (fisica o virtuale). Per eseguire queste attività sono necessari diritti di amministratore.

In un'installazione minima vengono installati tutti i componenti sullo stesso server Windows, eccetto il database SQL, che è possibile installare su un server separato.

Attivazione della sincronizzazione di data e ora su Windows Server

Gli orologi dei server vRealize Automation e Windows devono essere sincronizzati per garantire l'esito positivo dell'installazione.

La procedura seguente descrive come attivare la sincronizzazione di data e ora con l'host ESX/ESXi utilizzando VMware Tools. Se si stanno installando i componenti IaaS su un host fisico o se non si desidera utilizzare VMware Tools per la sincronizzazione di data e ora, assicurarsi in altro modo che l'orario dei server sia preciso.

Procedura

- 1 Aprire un prompt dei comandi sulla macchina d'installazione di Windows.
- 2 Immettere il comando seguente per passare alla directory di VMware Tools.

```
cd C:\Programmi\VMware\VMware Tools
```

- 3 Digitare il comando per visualizzare lo stato di timesync.

```
VMwareToolboxCmd.exe timesync status
```

- 4 Se timesync è disattivato, digitare il seguente comando per attivarlo.

```
VMwareToolboxCmd.exe timesync enable
```

Certificati IaaS

I componenti IaaS di vRealize Automation utilizzano i certificati e il protocollo SSL per rendere sicure le comunicazioni tra componenti. In un'installazione minima con finalità di prova, è possibile utilizzare certificati autofirmati.

In un ambiente di produzione, ottenere un certificato di dominio da un'autorità di certificazione attendibile. Per informazioni sull'installazione di certificati di dominio per i componenti IaaS, vedere [Installazione dei certificati IaaS](#) nel capitolo della distribuzione distribuita.

Installare i componenti dell'infrastruttura

Per installare i componenti dell'infrastruttura (IaaS) sulla macchina virtuale o fisica Windows, l'amministratore di sistema accede alla macchina Windows e segue la procedura d'installazione guidata.

Prerequisiti

- Verificare che la macchina dell'installazione soddisfi i requisiti descritti in [Requisiti del servizio Web IaaS e del Model Manager Server](#).
- [Attivazione della sincronizzazione di data e ora su Windows Server](#).
- Assicurarsi di aver distribuito e configurato completamente la vRealize Automation appliance e che i servizi necessari siano in esecuzione (plugin-service, catalog-service, iaas-proxy-provider).

Procedura

1 [Download del programma d'installazione di IaaS](#)

Un amministratore di sistema scarica il programma d'installazione su una macchina fisica o virtuale Windows 2008 o Windows 2012.

2 [Selezione del tipo di installazione](#)

L'amministratore di sistema esegue l'installazione guidata dalla macchina d'installazione di Windows 2008 o 2012.

3 [Controllo dei prerequisiti](#)

Il Controllo prerequisiti verifica che la macchina soddisfi i requisiti d'installazione di IaaS.

4 [Specificare le impostazioni di server e account](#)

L'amministratore di sistema di vRealize Automation definisce le impostazioni di server e account per il server d'installazione di Windows e seleziona un'istanza server del database SQL e il metodo di autenticazione.

5 [Specificare manager e agenti](#)

L'installazione minima installa i Distributed Execution Manager richiesti e l'agente proxy di vSphere predefinito. L'amministratore di sistema può installare agenti proxy aggiuntivi (XenServer o Hyper-V, ad esempio) dopo l'installazione utilizzando il programma d'installazione personalizzato.

6 [Registrare i componenti di IaaS](#)

L'amministratore di sistema installa il certificato IaaS e registra i componenti di IaaS con SSO.

7 [Completamento dell'installazione](#)

L'amministratore di sistema completa l'installazione di IaaS.

Download del programma d'installazione di IaaS

Un amministratore di sistema scarica il programma d'installazione su una macchina fisica o virtuale Windows 2008 o Windows 2012.

Se durante questo processo vengono visualizzati avvisi relativi ai certificati, è possibile ignorarli e continuare per completare l'installazione.

Prerequisiti

- Sulla macchina di installazione di IaaS deve essere installato Microsoft .NET Framework 4.5.1 o versione successiva. È possibile scaricare il programma d'installazione di .NET dalla pagina Web del programma d'installazione.

- Se si utilizza Internet Explorer per il download, verificare che non sia abilitata la configurazione di sicurezza avanzata. Vedere `res://iesetup.dll/SoftAdmin.htm`.
- Accedere al server Windows come amministratore locale.

Procedura

- 1 Accedere alla macchina Windows su cui occorre eseguire l'installazione.
- 2 Aprire un browser.
- 3 Immettere l'URL della pagina di download VMware vRealize Automation IaaS Installation.
Ad esempio `https://vra-va-hostname.domain.name:5480/installer`, dove `vra-va-hostname.domain.name` è il nome dell'host di vRealize Automation appliance.
- 4 Scaricare il programma d'installazione facendo clic sul collegamento **Programma di installazione IaaS**.
- 5 Quando richiesto, salvare sul desktop il file del programma d'installazione, `setup__vra-va-hostname.domain.name@5480`.

Non modificare il nome del file poiché esso è utilizzato per collegare l'installazione alla vRealize Automation appliance.

Selezione del tipo di installazione

L'amministratore di sistema esegue l'installazione guidata dalla macchina d'installazione di Windows 2008 o 2012.

Prerequisiti

[Download del programma d'installazione di IaaS](#).

Procedura

- 1 Fare clic con il pulsante destro del mouse sul file d'installazione `setup__vra-va-hostname.domain.name@5480.exe` e scegliere **Esegui come amministratore**.
- 2 Fare clic su **Avanti**.
- 3 Accettare il contratto di licenza e fare clic su **Avanti**.

- 4 Nella pagina di accesso, inserire le credenziali di amministratore per vRealize Automation appliance e verificare il certificato SSL.
 - a Specificare il nome utente, ovvero **root**, e la password.
Questa è la password che è stata immessa quando è stata distribuita la vRealize Automation appliance.
 - b Selezionare **Accetta certificato**.
 - c Fare clic su **Visualizza certificato**.
Confrontare l'identificazione digitale del certificato con quella impostata per la vRealize Automation appliance. È possibile visualizzare il certificato della vRealize Automation appliance nel browser client quando si accede alla console di gestione sulla porta 5480.
- 5 Selezionare **Accetta certificato**.
- 6 Fare clic su **Avanti**.
- 7 Selezionare **Installazione completa** nella pagina **Tipo di installazione** se si sta creando una distribuzione minima e fare clic su **Avanti**.

Controllo dei prerequisiti

Il Controllo prerequisiti verifica che la macchina soddisfi i requisiti d'installazione di IaaS.

Prerequisiti

[Selezione del tipo di installazione.](#)

Procedura

- 1 Completare il Controllo prerequisiti.

Opzione	Descrizione
Nessun errore	Fare clic su Avanti .
Errori non critici	Fare clic su Bypass .
Errori critici	Se si ignorano gli errori critici, l'installazione non riuscirà. Se vengono visualizzati avvisi, selezionare l'avviso nel riquadro di sinistra e seguire le istruzioni visualizzate a destra. Risolvere tutti gli errori critici e fare clic su Controlla di nuovo per verificare.

- 2 Fare clic su **Avanti**.

La macchina soddisfa i requisiti d'installazione.

Specificare le impostazioni di server e account

L'amministratore di sistema di vRealize Automation definisce le impostazioni di server e account per il server d'installazione di Windows e seleziona un'istanza server del database SQL e il metodo di autenticazione.

Prerequisiti

[Controllo dei prerequisiti.](#)

Procedura

- 1 Nella pagina **Impostazioni server e account** della pagina **Impostazioni rilevate**, specificare il nome utente e la password di un utente dotato di privilegi di amministrazione SQL o di un amministratore locale.

- 2 Immettere una frase nella casella di testo **Passphrase**.

La passphrase è costituita da una serie di parole da cui viene generata una chiave di crittografia utilizzata per proteggere i dati del database.

Nota: salvare la passphrase in modo da poterla riutilizzare in installazioni future o in un eventuale ripristino del sistema.

- 3 Nella casella di testo **Server** della sezione Informazioni installazione SQL Server Database, accettare il server predefinito per installare l'istanza del database sullo stesso server con i componenti IaaS, oppure immettere un nome server differente se il database si trova su un'altra macchina.

Se si specifica un server differente, è necessario indicare il nome del server e il numero della porta nella forma *nomeserver,numeroporta*.

- 4 Accettare il valore predefinito della casella di testo **Database name** o immettere un nome appropriato, se applicabile.

- 5 Selezionare il metodo di autenticazione.

- ◆ Selezionare **Use Windows authentication** se si desidera creare il database utilizzando le credenziali Windows dell'utente corrente. L'utente deve avere privilegi di sys_admin SQL.
- ◆ Deselezionare **Use Windows authentication** se si desidera creare il database utilizzando l'autenticazione SQL. Immettere **User name** e **Password** dell'utente di SQL Server dotato di privilegi di sys_admin SQL sull'istanza del server SQL.

- 6 (Facoltativo) Selezionare la casella di controllo **Use SSL for database connection**.

La casella di controllo è selezionata per impostazione predefinita. SSL offre una connessione più sicura tra il server IaaS e il database SQL. Tuttavia è necessario prima configurare il protocollo SSL sul server SQL per supportare l'opzione. Per informazioni correlate alla configurazione di SSL su SQL Server, vedere l'articolo KB 316898 *How to enable SSL encryption for an instance of SQL Server by using Microsoft Management Console* sul sito del supporto di Microsoft.

- 7 Fare clic su **Avanti**.

Specificare manager e agenti

L'installazione minima installa i Distributed Execution Manager richiesti e l'agente proxy di vSphere predefinito. L'amministratore di sistema può installare agenti proxy aggiuntivi (XenServer o Hyper-V, ad esempio) dopo l'installazione utilizzando il programma d'installazione personalizzato.

Prerequisiti

[Specificare le impostazioni di server e account.](#)

Procedura

- 1 Nella pagina **Distributed Execution Manager e agente proxy vSphere**, accettare i valori predefiniti o cambiare i nomi, se necessario.
- 2 Accettare l'impostazione predefinita per l'installazione di un agente vSphere e abilitare così il provisioning con vSphere, oppure deselezionarla se applicabile.
 - a Selezionare **Installa e configura agente vSphere**.
 - b Accettare l'agente e l'endpoint predefiniti o specificare un nome.

Annotare il valore relativo al nome dell'endpoint. È necessario immettere correttamente questa informazione quando si configura l'endpoint vSphere nella console di vRealize Automation, altrimenti la configurazione potrebbe non riuscire.
- 3 Fare clic su **Avanti**.

Registrare i componenti di IaaS

L'amministratore di sistema installa il certificato IaaS e registra i componenti di IaaS con SSO.

Prerequisiti

[Download del programma d'installazione di IaaS.](#)

Procedura

- 1 Accettare il valore predefinito del campo **Server**, in cui è inserito il nome di dominio completo del server della vRealize Automation appliance da cui è stato scaricato il programma d'installazione. Verificare che per identificare il server sia utilizzato un nome di dominio completo e non un indirizzo IP.

Se si hanno più appliance virtuali e si utilizza un bilanciamento del carico, immettere il percorso dell'appliance virtuale del bilanciamento del carico.
- 2 Fare clic su **Carica** per popolare il valore di **Tenant predefinito SSO** (vsphere.local).
- 3 Fare clic su **Scarica** per ottenere il certificato dalla vRealize Automation appliance.

È possibile fare clic su **Visualizza certificato** per visualizzare i dettagli del certificato.
- 4 Selezionare **Accetta certificato** per installare il certificato SSO.
- 5 Nel pannello dell'amministratore SSO, immettere **administrator** nella casella di testo **Nome utente** e la password definita per questo utente quando è stato configurato SSO in **Password** e **Conferma password**.
- 6 Fare clic sul collegamento di prova alla destra del campo **Nome utente** per convalidare la password immessa.

- 7 Accettare il valore predefinito del campo **Server IaaS**, contenente il nome host della macchina Windows in cui si sta eseguendo l'installazione.
- 8 Far clic sul collegamento di prova alla destra del campo **Server IaaS** per convalidare la connettività.
- 9 Fare clic su **Avanti**.

Se dopo aver fatto clic su **Avanti** vengono visualizzati errori, risolverli prima di procedere.

Completamento dell'installazione

L'amministratore di sistema completa l'installazione di IaaS.

Prerequisiti

- [Registrare i componenti di IaaS](#).
- Verificare che la macchina su cui si sta eseguendo l'installazione sia connessa alla rete e che sia in grado di connettersi alla vRealize Automation appliance da cui è possibile scaricare il programma d'installazione di IaaS.

Procedura

- 1 Riesaminare le informazioni contenute nella pagina **Procedere con l'installazione** e fare clic su **Installa**.

L'installazione ha inizio. La procedura d'installazione può richiedere da cinque minuti a un'ora, in base alla configurazione della rete.

- 2 Alla visualizzazione del messaggio di operazione eseguita, lasciare selezionata la casella di controllo **Esegui configurazione iniziale guidata** e fare clic su **Avanti** e poi su **Fine**.
- 3 Chiudere la finestra di messaggio **Configura il sistema**.

L'installazione a questo punto è terminata.

Passi successivi

[Verifica dei servizi di IaaS](#).

Distribuzione distribuita

In una distribuzione distribuita, l'amministratore di sistema installa i componenti su più macchine nell'ambiente di distribuzione.

Elenco di controllo di una distribuzione distribuita

Un amministratore di sistema può distribuire vRealize Automation in una configurazione distribuita, che offre protezione in caso di failover e alta disponibilità grazie alla ridondanza.

L'elenco di controllo di una distribuzione distribuita è una panoramica ad alto livello dei passaggi necessari per implementare una distribuzione distribuita.

Tavola 4-2. Elenco di controllo di una distribuzione distribuita

Attività	Dettagli
<input type="checkbox"/> Pianificare e preparare l'ambiente d'installazione e verificare che tutti i prerequisiti d'installazione siano soddisfatti.	Capitolo 2 Preparazione per l'installazione
<input type="checkbox"/> Pianificare e ottenere i certificati SSL.	Requisiti di attendibilità dei certificati in una distribuzione distribuita
<input type="checkbox"/> Distribuire il server vRealize Automation appliance principale e tutte le appliance aggiuntive a scopo di ridondanza e alta disponibilità.	Distribuzione di vRealize Automation appliance
<input type="checkbox"/> Configurare il bilanciamento del carico per gestire il traffico dell'appliance vRealize Automation.	
<input type="checkbox"/> Configurare il server vRealize Automation appliance principale e tutte le appliance aggiuntive distribuite a scopo di ridondanza e alta disponibilità.	Configurazione di appliance per vRealize Automation
<input type="checkbox"/> Configurare il bilanciamento del carico per gestire il traffico del componente IaaS vRealize Automation e installare i componenti IaaS vRealize Automation.	Installazione dei componenti di IaaS in una configurazione distribuita
<input type="checkbox"/> Se richiesto, installare gli agenti per l'integrazione con i sistemi esterni.	Installazione degli agenti
<input type="checkbox"/> Configurare il tenant predefinito e fornire la licenza di IaaS.	

vRealize Orchestrator

Utilizzare implementazioni esterne di vRealize Orchestrator in distribuzioni ad alta disponibilità. Se si utilizza un server vRealize Orchestrator su una vRealize Automation appliance, configurarlo in modo che sia esterno. È sempre sconsigliabile utilizzare versioni embedded.

Gestione directory

Se si esegue un'installazione distribuita con bilanciamenti del carico per l'alta disponibilità e il failover, informare il responsabile del team in modo che configuri l'ambiente di vRealize Automation. Gli amministratori tenant devono configurare Gestione directory per l'alta disponibilità durante la configurazione del collegamento ad Active Directory.

Per ulteriori informazioni sulla configurazione di Gestione directory per l'alta disponibilità, vedere *Configurazione di vRealize Automation*.

Componenti di un'installazione distribuita

In un'installazione distribuita, l'amministratore di sistema distribuisce appliance virtuali e i componenti correlati per supportare l'ambiente di distribuzione.

Tavola 4-3. Appliance virtuali e database appliance

Componente	Descrizione
vRealize Automation appliance	Appliance virtuale preconfigurata che distribuisce il server vRealize Automation. Il server include la console di vRealize Automation, un portale singolo che permette di eseguire in autonomia il provisioning e la gestione dei servizi cloud, nonché le attività di creazione e amministrazione.
Database appliance	Memorizza le informazioni richieste dalle appliance virtuali. Il database è incorporato in una o due istanze di vRealize Automation appliance.

È possibile selezionare i singoli componenti di IaaS da installare e specificarne la posizione d'installazione.

Tavola 4-4. Componenti IaaS

Componente	Descrizione
Sito Web	Fornisce alla console di vRealize Automation le funzionalità di amministrazione dell'infrastruttura e di creazione dei servizi. Il componente sito Web comunica con il Model Manager, da quale riceve gli aggiornamenti provenienti da Distributed Execution Manager (DEM), agenti proxy e database.
Servizio di gestione	Il servizio di gestione coordina la comunicazione tra gli agenti, il database, Active Directory e SMTP. Il servizio di gestione comunica con il sito Web della console attraverso il Model Manager. L'esecuzione di questo servizio richiede privilegi amministrativi.
Model Manager	Il Model Manager comunica con il database, i DEM e il sito Web del portale. Il Model Manager è suddiviso in due componenti installabili separatamente, il servizio Web del Model Manager e il componente Model Manager Data.
Distributed Execution Manager (Orchestrator e Worker)	Un Distributed Execution Manager (DEM) esegue la logica di business di modelli personalizzati, interagendo con il database di IaaS e i database esterni. I DEM inoltre gestiscono le macchine cloud e fisiche.
Agenti	Agenti di virtualizzazione, integrazione e WMI che comunicano con le risorse dell'infrastruttura.

Requisiti di attendibilità dei certificati in una distribuzione distribuita

Per garantire la sicurezza delle comunicazioni, vRealize Automation utilizza i certificati per creare le relazioni basate sulla fiducia tra componenti.

L'implementazione specifica dei certificati necessari a ottenere questa fiducia dipende dall'ambiente esistente.

Per offrire alta disponibilità e supporto per il failover, è possibile distribuire cluster di componenti con bilanciamento del carico. In questo caso si ottiene un certificato multiuso che comprende il componente Web IaaS contenuti nel cluster, il quale può quindi essere copiato in ciascun componente del cluster. È possibile utilizzare certificati SAN (Subject Alternative Name, nome alternativo del soggetto), certificati con caratteri jolly o qualsiasi altro metodo di certificazione multiuso appropriato per l'ambiente esistente, purché soddisfi i requisiti di attendibilità. In base alla configurazione del bilanciamento del carico, potrebbe essere necessario certificare il sistema di bilanciamento del carico come parte del certificato multiuso per il cluster.

Ad esempio, se la configurazione del bilanciamento del carico richiede un certificato sul sistema di bilanciamento e sui suoi componenti, è possibile ottenere un certificato SAN che certifichi @@web-load-balancer.eng.mycompany.com, web-component-1.eng.mycompany.com e web-component-2.eng.mycompany.com. Sarà sufficiente copiare quel singolo certificato multiuso sul sistema di bilanciamento del carico e su ognuna delle appliance, quindi registrare il certificato sulle macchine dei componenti Web.

Nella tabella Importazione e registrazione dei certificati sono riepilogati i requisiti di registrazione per i diversi certificati importati.

Tavola 4-5. Importazione e registrazione dei certificati

Importazione	Registrazione
Cluster vRealize Automation appliance	Cluster componenti Web
Cluster componenti Web	<ul style="list-style-type: none"> Cluster vRealize Automation appliance Cluster componenti del servizio di gestione Componenti di DEM Orchestrator e DEM Worker
Cluster componenti del servizio di gestione	<ul style="list-style-type: none"> Componenti di DEM Orchestrator e DEM Worker Agenti e agenti proxy

Fogli di lavoro per l'installazione

È possibile utilizzare questi fogli di lavoro per registrare informazioni importati da consultare durante il processo d'installazione.

Qui viene fornita una copia di ciascun foglio di lavoro. Creare copie aggiuntive quando occorrono. Per le impostazioni viene fatta distinzione tra lettere maiuscole e minuscole.

Tavola 4-6. Informazioni sulla vRealize Automation appliance del cluster iniziale

Variabile	Valore	Esempio
Nome host (nome di dominio completo)		vcac-va.mycompany.com
Porta di uscita servizio SSO su HTTPS (predefinita)	7444 (non cambiare)	7444
IP		192.168.1.105
Nome utente	administrator@vsphere.local (predefinito)	administrator@vsphere.local
Password		vmware

Tavola 4-7. Informazioni aggiuntive sulla vRealize Automation appliance

Variabile	Valore	Esempio
Nome host (nome di dominio completo)		vcac-va2.mycompany.com
Porta di uscita servizio SSO su HTTPS (predefinita)	7444 (non cambiare)	7444
IP		192.168.1.110
Nome utente	administrator@vsphere.local (predefinito)	administrator@vsphere.local
Password		vmware

Tavola 4-8. Passphrase del database di IaaS

Variabile	Valore	Esempio
Passphrase (riutilizzata in installazione, aggiornamento e migrazione di IaaS)		myPassphrase

Tavola 4-9. Sito Web di IaaS

Variabile	Valore	Esempio
Nome host (nome di dominio completo)		iaas-web.mycompany.com
Porta di uscita servizio SSO su HTTPS (predefinita)		
IP		192.168.1.106
Nome utente		
Password		

Tavola 4-10. IaaS Model Manager Data

Variabile	Valore	Esempio
Nome host (nome di dominio completo)		iaas-model-man.mycompany.com
Porta di uscita servizio SSO su HTTPS (predefinita)		
IP		192.168.1.107
Nome utente		
Password		

Tavola 4-11. IaaS Model Service

Variabile	Valore	Esempio
Nome host (nome di dominio completo)		iaas-model-service.mycompany.com
Porta di uscita servizio SSO su HTTPS (predefinita)		
IP		192.168.1.108

Tavola 4-11. IaaS Model Service (Continua)

Variabile	Valore	Esempio
Nome utente		
Password		

Tavola 4-12. Distributed Execution Manager

Nome univoco	Orchestrator/Worker
es. myuniqueorchestratorname	Orchestrator: Worker:
	Orchestrator: Worker:
	Orchestrator: Worker:
	Orchestrator: Worker:

Distribuzione di vRealize Automation appliance

Per distribuire vRealize Automation appliance, è necessario che un amministratore di sistema acceda al client vSphere e selezioni le impostazioni di distribuzione.

La password radice creata per l'amministratore di vRealize Automation è soggetta ad alcune restrizioni. Vedere [Considerazioni sulle password](#).

Prerequisiti

- Scaricare vRealize Automation appliance dal sito Web di VMware.
- Accedere al client vSphere come utente con privilegi di amministratore di sistema.

Procedura

- 1 Selezionare **File > Distribuisci modello OVF** dal client di vSphere.
- 2 Selezionare il file di vRealize Automation appliance scaricato e fare clic su **Apri**.
- 3 Fare clic su **Avanti**.
- 4 Fare clic su **Avanti** nella pagina Dettagli modello OVF.
- 5 Accettare il contratto di licenza e fare clic su **Avanti**.
- 6 Immettere un nome univoco per l'appliance virtuale nella casella di controllo **Nome** rispettando la convenzione di denominazione IT dell'organizzazione, selezionare il data center e la posizione in cui si desidera distribuire l'appliance virtuale e fare clic su **Avanti**.
- 7 Seguire le istruzioni presentate fino alla visualizzazione della pagina Formato disco.
- 8 Nella pagina Formato disco, verificare che vi sia spazio sufficiente per distribuire l'appliance virtuale e fare clic su **Avanti**.

9 Seguire le istruzioni presentate fino alla pagina Proprietà.

Le opzioni visualizzate dipendono dalla configurazione di vSphere.

10 Configurare i valori nella pagina Proprietà.

- a Immettere la password radice da utilizzare quando si accede alla console dell'appliance virtuale nelle caselle di testo **Immetti password** e **Conferma password**.
- b Selezionare o deselezionare la casella di testo **Servizio SSH** per attivare o disattivare il servizio SSH per l'appliance.

Questo valore è utilizzato per impostare lo stato iniziale del servizio SSH nell'appliance. Se si sta eseguendo l'installazione guidata, attivare questa opzione prima di avviare la procedura guidata. Dopo l'installazione sarà possibile modificare questa impostazione dalla console di gestione dell'appliance.
- c Immettere il nome di dominio completo della macchina virtuale nella casella di testo **Nome host**, anche se si utilizza il DHCP.
- d Configurare le proprietà di networking.

11 Fare clic su **Avanti**.

12 In base alle configurazioni di vCenter e DNS utilizzate, la risoluzione DNS potrebbe impiegare del tempo. Per accelerare il processo, eseguire i seguenti passaggi.

- Se nella pagina Completamento è disponibile **Accendi dopo la distribuzione**.
 - a Selezionare **Accendi dopo la distribuzione** e fare clic su **Fine**.
 - b Scegliere **Chiudi** al completamento della distribuzione del file in vCenter.
 - c Attendere l'avvio della macchina.

Questa fase potrebbe richiedere fino a 5 minuti.
- Se nella pagina Completamento non è disponibile **Accendi dopo la distribuzione**.
 - a Scegliere **Chiudi** al completamento della distribuzione del file in vCenter.
 - b Accendere la VM e attendere il tempo necessario alla VM per avviarsi.
 - c Assicurarsi che sia possibile eseguire un ping al DNS della macchina virtuale. Se non è possibile eseguire un ping al DNS, riavviare la macchina virtuale.
 - d Attendere l'avvio della macchina. Questa fase potrebbe richiedere fino a 5 minuti.

Per verificare l'avvenuta distribuzione dell'appliance, aprire un prompt dei comandi ed eseguire un ping al nome di dominio completo della vRealize Automation appliance.

Passi successivi

Ripetere questa procedura per distribuire altre istanze della vRealize Automation appliance per garantire la ridondanza in un ambiente ad alta disponibilità.

Configurazione del bilanciamento del carico

Dopo aver distribuito le appliance per vRealize Automation, è possibile configurare un bilanciamento del carico per distribuire il traffico tra più istanze di vRealize Automation appliance.

Nell'elenco seguente viene riportata la procedura di massima da eseguire per configurare un bilanciamento del carico per il traffico di vRealize Automation:

- 1 Installare il bilanciamento del carico.
- 2 Attivare l'affinità di sessione.
- 3 Assicurarsi che il timeout sul bilanciamento del carico sia di almeno 100 secondi.
- 4 Se la rete o il bilanciamento del carico lo richiedono, importare un certificato nel bilanciamento del carico. Per informazioni sulle relazioni basate sulla fiducia e sui certificati, vedere [Requisiti di attendibilità dei certificati in una distribuzione distribuita](#). Per informazioni sull'estrazione dei certificati, vedere [Estrazione di certificati e chiavi private](#)
- 5 Configurare il bilanciamento del carico per il traffico delle vRealize Automation appliance.
- 6 Configurare le appliance per vRealize Automation. Vedere [Configurazione di appliance per vRealize Automation](#).

Nota: se si desidera includere appliance virtuali nella configurazione del bilanciamento del carico, considerare solo quelle che sono state configurate per l'uso con vRealize Automation. Se si includono appliance non configurate si otterranno risposte di errore.

Per informazioni su scalabilità e alta disponibilità, vedere *Architettura di riferimento di VMware vRealize Automation*, disponibile come documento tecnico all'indirizzo <https://www.vmware.com/support/pubs/vcac-pubs.html>.

Configurazione di appliance per vRealize Automation

Dopo aver distribuito le appliance e configurato il bilanciamento del carico, si procede configurando le appliance per vRealize Automation.

Configurazione di vRealize Automation Appliance primario

vRealize Automation appliance è una appliance virtuale preconfigurata che distribuisce il server e la console Web (portale dell'utente) di vRealize Automation. Essa viene fornita come modello in formato di virtualizzazione aperto (OVF, Open Virtualization Format). L'amministratore di sistema scarica l'appliance e la distribuisce in vCenter Server o nell'inventario ESX/ESXi.

Se la rete o il bilanciamento del carico lo richiede, il certificato configurato per l'istanza primaria dell'appliance viene copiato nel bilanciamento del carico e nelle istanze dell'appliance aggiuntive in procedure successive.

Prerequisiti

- [Distribuzione di vRealize Automation appliance](#).

- Ottenere un certificato di dominio per vRealize Automation appliance.

Procedura

1 Attivazione della sincronizzazione di data e ora sulla vRealize Automation appliance

Gli orologi dei server vRealize Automation appliance e Windows devono essere sincronizzati per garantire l'esito positivo dell'installazione.

2 Configurazione dell'appliance di vRealize Automation

Per preparare la vRealize Automation appliance all'uso, un amministratore di sistema deve configurare le impostazioni dell'host, generare un certificato SSL e specificare le informazioni di connessione SSO.

Attivazione della sincronizzazione di data e ora sulla vRealize Automation appliance

Gli orologi dei server vRealize Automation appliance e Windows devono essere sincronizzati per garantire l'esito positivo dell'installazione.

Se durante questo processo vengono visualizzati avvisi relativi ai certificati, è possibile ignorarli e continuare per completare l'installazione.

Procedura

- 1 Accedere alla console di gestione della vRealize Automation appliance utilizzando il suo nome di dominio completo, <https://vra-vr-hostname.domain.name:5480/>.
- 2 Accedere utilizzando il nome utente **root** e la password specificati al momento della distribuzione dell'appliance.
- 3 Selezionare **Amministrazione > Impostazioni ora**.
- 4 Selezionare un'opzione dal menu **Modalità sincronizzazione ora**.

Opzione	Azione
Usa server di riferimento ora	Selezionare Usa server di riferimento ora dal menu Modalità sincronizzazione ora per utilizzare il protocollo NTP (Network Time Protocol). Immettere l'indirizzo IP o il nome host di ogni server orario utilizzato nella casella di testo Server di riferimento ora .
Usa ora dell'host	Selezionare Usa ora dell'host dal menu Modalità sincronizzazione ora per utilizzare la sincronizzazione di data e ora di VMware Tools. È necessario configurare le connessioni ai server NTP prima di poter utilizzare la sincronizzazione di data e ora di VMware Tools.

- 5 Fare clic su **Salva impostazioni**.
- 6 Verificare che il valore in **Ora corrente** sia corretto.

Dalla scheda **Sistema** della pagina Impostazioni fuso orario è possibile cambiare il fuso orario.

Configurazione dell'appliance di vRealize Automation

Per preparare la vRealize Automation appliance all'uso, un amministratore di sistema deve configurare le impostazioni dell'host, generare un certificato SSL e specificare le informazioni di connessione SSO.

Procedura

- 1 Accedere alla console di gestione della vRealize Automation appliance utilizzando il suo nome di dominio completo, `https://vra-va-hostname.domain.name:5480/`.
- 2 Continuare ignorando l'avviso sul certificato.
- 3 Accedere con il nome utente root e la password specificati quando è stata distribuita vRealize Automation appliance.
- 4 Selezionare **Impostazioni vRA > Impostazioni host**.

Opzione	Azione
Risolvi automaticamente	Selezionare Risolvi automaticamente per specificare il nome dell'host corrente per vRealize Automation appliance.
Aggiorna host	<p>Per i nuovi host, selezionare Aggiorna host. Immettere il nome di dominio completo di vRealize Automation appliance, <code>vra-hostname.domain.name</code>, nella casella di testo Nome host.</p> <p>Per le distribuzioni distribuite che utilizzano bilanciamenti del carico, selezionare Aggiorna host. Immettere il nome di dominio completo del server del bilanciamento del carico, <code>vra-loadbalancename.domain.name</code>, nella casella di testo Nome host.</p>

Nota: configurare le impostazioni SSO come descritto più avanti in questa procedura ogni volta che si utilizza **Aggiorna host** per cambiare un nome host.

5 Selezionare il tipo di certificato dal menu **Azione certificato**.

Se si utilizza un certificato con codifica PEM, ad esempio per un ambiente distribuito, selezionare **Importa**.

I certificati importati devono essere attendibili nonché applicabili a tutte le istanze di vRealize Automation appliance e a qualsiasi bilanciamento del carico attraverso l'uso di certificati SAN (Subject Alternative Name).

Nota: se si utilizzano catene di certificati, specificare i certificati nel seguente ordine:

- a Certificato client/server firmato mediante il certificato di un'autorità di certificazione intermedia
- b Uno o più certificati intermedi
- c Certificato di un'autorità di certificazione radice

Opzione	Azione
Mantieni esistente	Lasciare invariata la configurazione SSL corrente. Selezionare questa opzione per annullare le modifiche.
Genera certificato	<ol style="list-style-type: none"> a Il valore visualizzato nella casella di testo Nome comune è il nome host visualizzato nella parte superiore della pagina. Se sono disponibili istanze aggiuntive di vRealize Automation appliance, i rispettivi nomi di dominio completi (FQDN) sono inclusi nell'attributo SAN del certificato. b Immettere il nome dell'organizzazione, come ad esempio quello della propria azienda, nella casella di testo Organizzazione. c Immettere l'unità organizzativa, ad esempio il nome o la posizione del proprio reparto, nella casella di testo Unità organizzativa. d Immettere il codice di paese ISO 3166 a due lettere, ad esempio IT, nella casella di testo Paese.
Importazione	<ol style="list-style-type: none"> a Copiare i valori del certificato dalla stringa BEGIN PRIVATE KEY alla stringa END PRIVATE KEY, inclusi intestazione e piè di pagina, quindi incollarli nella casella di testo Chiave privata RSA. b Copiare i valori del certificato dalla stringa BEGIN CERTIFICATE alla stringa END CERTIFICATE, inclusi intestazione e piè di pagina, quindi incollarli nella casella di testo Catena di certificati. Per valori di certificati multipli, includere un'intestazione BEGIN CERTIFICATE e un piè di pagina END CERTIFICATE per ciascun certificato. <p>Nota: In caso di certificati concatenati, possono essere disponibili attributi aggiuntivi.</p> <ol style="list-style-type: none"> c (Facoltativo) Se il certificato utilizza una passphrase per crittografare la chiave del certificato, copiare la passphrase e incollarla nella casella di testo Passphrase.

6 Fare clic su **Salva impostazioni** per salvare le informazioni sull'host e la configurazione SSL.

- 7 Se la rete o il bilanciamento del carico lo richiedono, copiare il certificato importato o appena creato nel bilanciamento del carico dell'appliance virtuale.

L'esportazione del certificato potrebbe richiedere l'abilitazione dell'accesso SSH root.

- a Se non già fatto, accedere alla console di gestione dell'appliance vRealize Automation in qualità di root.
- b Fare clic sulla scheda **Amministrazione**.
- c Scegliere il sottomenu **Amministrazione**.
- d Selezionare la casella di controllo **Servizio SSH abilitato**.

Completata l'operazione, deselezionare la casella di controllo per disabilitare SSL.

- e Selezionare la casella di controllo **Accesso SSH amministratore**.

Completata l'operazione, deselezionare la casella di controllo per disabilitare SSL.

- f Fare clic su **Salva impostazioni**.

- 8 Configurare le impostazioni SSO.

- 9 Fare clic su **Servizi**.

Prima di poter installare una licenza o accedere alla console, tutti i servizi devono essere in esecuzione. Per avviarsi, i servizi di solito impiegano una decina di minuti.

Nota: è possibile anche accedere all'appliance ed eseguire `tail -f /var/log/vcac/catalina.out` per monitorare l'avvio dei servizi.

- 10 Immettere le informazioni della licenza.

- a Fare clic su **Impostazioni vRA > Gestione licenze**.
- b Fare clic su **Gestione licenze**.
- c Inserire una chiave di licenza di vRealize Automation valida scaricata all'atto del download dei file d'installazione e fare clic su **Invia chiave**.

Nota: se si verifica un errore di connessione, è possibile che ci sia un problema con il bilanciamento del carico. Controllare la connettività della rete al bilanciamento del carico.

- 11 Fare clic su **Messaggistica**. Vengono visualizzate le impostazioni di configurazione e lo stato della messaggistica per l'appliance. Non cambiare queste impostazioni.

- 12 Fare clic sulla scheda **Telemetria** per scegliere se partecipare al programma CEIP (Customer Experience Improvement Program) di VMware.

I dettagli relativi ai dati raccolti con il programma CEIP e gli scopi per cui è utilizzato da VMware sono disponibili nel Trust & Assurance Center all'indirizzo <http://www.vmware.com/trustvmware/ceip.html>.

- Selezionare **Partecipa al programma CEIP (Customer Experience Improvement Program) di VMware** per entrare a far parte del programma.
- Deselezionare **Partecipa al programma CEIP (Customer Experience Improvement Program) di VMware** per non entrare a far parte del programma.

- 13 Fare clic su **Salva impostazioni**.

- 14 Assicurarsi che sia possibile accedere alla console di vRealize Automation.

- a Aprire un browser e accedere alla pagina `https://vcac-hostname.domain.name/vcac/`.

Se si utilizza un bilanciamento del carico, il nome host deve essere il nome di dominio completo del bilanciamento del carico.

- b Se richiesto, continuare ignorando gli avvisi sul certificato.
- c Accedere con il nome utente **administrator@vsphere.local** e la password specificati quando è stato configurato SSO.

La console si apre alla scheda **Amministrazione** della pagina **Tenant**. Nell'elenco viene visualizzato un unico tenant chiamato `vsphere.local`.

- 15 Se non si utilizza un bilanciamento del carico e tutti i nodi sotto il bilanciamento del carico sono stati configurati, configurare e abilitare tutti i controlli di integrità applicabili.

Configurazione di istanze aggiuntive di vRealize Automation Appliance

L'amministratore di sistema può distribuire istanze multiple della vRealize Automation appliance per garantire la ridondanza in un ambiente ad alta disponibilità.

Per ogni vRealize Automation appliance, è necessario attivare la sincronizzazione dell'orario e aggiungere l'appliance a un cluster. Quando si aggiunge l'appliance al cluster, le informazioni di configurazione basate sulle impostazioni della vRealize Automation appliance iniziale (primaria) vengono aggiunte automaticamente.

Se si esegue un'installazione distribuita con bilanciamenti del carico per l'alta disponibilità e il failover, informare il responsabile del team in modo che configuri l'ambiente di vRealize Automation. Gli amministratori tenant devono configurare Gestione directory per l'alta disponibilità durante la configurazione del collegamento ad Active Directory.

Attivazione della sincronizzazione di data e ora sulla vRealize Automation Appliance

Gli orologi dei server vRealize Automation appliance e Windows devono essere sincronizzati per garantire l'esito positivo dell'installazione.

Se durante questo processo vengono visualizzati avvisi relativi ai certificati, è possibile ignorarli e continuare per completare l'installazione.

Prerequisiti

Configurazione di vRealize Automation Appliance primario.

Procedura

- 1 Accedere alla console di gestione della vRealize Automation appliance utilizzando il suo nome di dominio completo, `https://vra-va-hostname.domain.name:5480/`.
- 2 Accedere utilizzando il nome utente **root** e la password specificati al momento della distribuzione dell'appliance.
- 3 Selezionare **Amministrazione > Impostazioni ora**.
- 4 Selezionare un'opzione dal menu **Modalità sincronizzazione ora**.

Opzione	Azione
Usa server di riferimento ora	Selezionare Usa server di riferimento ora dal menu Modalità sincronizzazione ora per utilizzare il protocollo NTP (Network Time Protocol). Immettere l'indirizzo IP o il nome host di ogni server orario utilizzato nella casella di testo Server di riferimento ora .
Usa ora dell'host	Selezionare Usa ora dell'host dal menu Modalità sincronizzazione ora per utilizzare la sincronizzazione di data e ora di VMware Tools. È necessario configurare le connessioni ai server NTP prima di poter utilizzare la sincronizzazione di data e ora di VMware Tools.

- 5 Fare clic su **Salva impostazioni**.
- 6 Verificare che il valore in **Ora corrente** sia corretto.

Dalla scheda **Sistema** della pagina Impostazioni fuso orario è possibile cambiare il fuso orario.

Unione di una vRealize Automation appliance a un cluster

Le installazioni distribuite che utilizzano bilanciamenti del carico supportano l'uso di più di una vRealize Automation appliance in una distribuzione. Ogni appliance della distribuzione deve appartenere a un cluster.

L'unione di una vRealize Automation appliance a un cluster viene eseguita dalla console di gestione. L'operazione di unione copia le informazioni della configurazione dell'appliance per il cluster nell'appliance che si sta aggiungendo al cluster, incluse le informazioni relative a certificati, SSO, licenze, database e messaggistica.

Eseguire questa operazione dalla console di gestione di ciascun server da unire al cluster, a eccezione del nodo di cluster iniziale.

L'operazione di unione non è necessaria per il nodo di cluster iniziale, perché l'operazione di unione collega il nodo di cluster iniziale al nodo sulla cui console di gestione si sta operando, il che rende entrambi i nodi parte dello stesso cluster. Dopo che un'appliance è divenuta parte del cluster, è possibile specificare il suo nome di dominio completo come nodo di cluster iniziale.

Nota: Quando si aggiunge il primo nodo a un cluster, può essere necessario reimportare o ricreare il certificato. Inoltre, è consigliabile aggiungere i nodi a un cluster uno alla volta e non in parallelo.

Prerequisiti

- [Configurazione di vRealize Automation Appliance primario.](#)
- Se il sito utilizza un bilanciamento del carico, verificare che sia configurato per l'uso con la propria istanza di vRealize Automation appliance.
- [Attivazione della sincronizzazione di data e ora sulla vRealize Automation Appliance.](#) Per ogni appliance deve essere attivata la sincronizzazione di data e ora.
- Verificare che il traffico possa attraversare il bilanciamento del carico e raggiungere i nodi installati e il nodo che si sta configurando. Deve essere disponibile anche il nodo primario.

Procedura

- 1 Accedere alla console di gestione della vRealize Automation appliance utilizzando il suo nome di dominio completo, `https://vra-va-hostname.domain.name:5480/`.
- 2 Continuare indipendentemente dall'eventuale visualizzazione di avvisi sui certificati.
- 3 Accedere con il nome utente root e la password specificata per la distribuzione della vRealize Automation appliance.
- 4 Selezionare **Impostazioni vRA > Cluster**.
- 5 Immettere il nome di dominio completo di una vRealize Automation appliance precedentemente configurata nella casella di testo **Nodo di cluster iniziale**.
È possibile utilizzare il nome di dominio completo della vRealize Automation appliance primaria o di qualunque vRealize Automation appliance già unita al cluster.
- 6 Immettere la password di root nella casella di testo **Password**.
- 7 Fare clic su **Unisci cluster**.
- 8 Continuare indipendentemente dall'eventuale visualizzazione di avvisi sui certificati.
I servizi relativi al cluster vengono riavviati.
- 9 Verificare che i servizi siano in esecuzione.
 - a Fare clic sulla scheda **Servizi**.
 - b Fare clic sulla scheda **Aggiorna** per monitorare l'avanzamento dell'avvio dei servizi.

Disattivazione dei servizi inutilizzati

Un amministratore di sistema può disattivare i servizi di vRealize Orchestrator incorporati. Questi servizi non vengono utilizzati in una distribuzione distribuita, pertanto è consigliabile disattivarli in modo che non consumino inutilmente risorse.

Prerequisiti

[Unione di una vRealize Automation appliance a un cluster](#)

Procedura

- 1 Accedere a vRealize Automation appliance utilizzando SSH.

- 2 Arrestare il servizio vRealize Orchestrator incorporato.

```
service vco-server stop
chkconfig vco-server off
```

- 3 Disconnettersi dalla vRealize Automation appliance.

Convalida della distribuzione distribuita

Dopo aver distribuito istanze aggiuntive della vRealize Automation appliance, è consigliabile verificare che sia possibile accedere alle appliance in cluster.

Procedura

- 1 Nell'interfaccia di gestione del bilanciamento del carico o nel file di configurazione disabilitare temporaneamente tutti i nodi, eccetto il nodo che si vuole testare.
- 2 Verificare che sia possibile accedere alla console di vRealize Automation accedendo a `https://vcac-hostname.domain.name/vcac`, dove `vcac-hostname.domain.name` è l'indirizzo del bilanciamento del carico.
- 3 Dopo aver verificato che la nuova vRealize Automation appliance è accessibile utilizzando il bilanciamento del carico, abilitare nuovamente gli altri nodi.

Installazione dei componenti di IaaS in una configurazione distribuita

L'amministratore di sistema installa i componenti di IaaS dopo aver distribuito e configurato completamente le appliance. I componenti di IaaS danno accesso alle funzionalità dell'infrastruttura di vRealize Automation.

Tutti i componenti devono essere eseguiti con lo stesso account di servizio.

Prerequisiti

- [Configurazione di vRealize Automation Appliance primario.](#)
- Se il sito include istanze multiple di vRealize Automation appliance, [Unione di una vRealize Automation appliance a un cluster.](#)
- Verificare che i server dell'installazione soddisfino i requisiti descritti in [Requisiti del servizio Web IaaS e del Model Manager Server.](#)
- Ottenere un certificato da un'autorità di certificazione attendibile per importarlo nell'archivio dei certificati radice attendibili delle macchine su cui si intende installare il componente sito Web e Model Manager Data.
- Se nell'ambiente si utilizzano bilanciamenti del carico, verificare che questi soddisfino i requisiti di configurazione.

Procedura

1 Installazione dei certificati IaaS

Per ambienti di produzione, ottenere un certificato di dominio da un'autorità di certificazione attendibile. Importare il certificato nell'archivio dei certificati radice attendibili di tutte le macchine su cui si intende installare il componente sito Web e il servizio di gestione (le macchine IIS) durante l'installazione di IaaS.

2 Download del programma d'installazione di IaaS

Un amministratore di sistema scarica il programma d'installazione di IaaS da vRealize Automation appliance a una macchina fisica o virtuale Windows 2008 o Windows 2012.

3 Scelta di uno scenario di database IaaS

vRealize Automation IaaS utilizza un database Microsoft SQL Server per conservare le informazioni sulle macchine che gestisce e sui propri elementi e criteri.

4 Installazione di un componente sito Web di IaaS e di Model Manager Data

L'amministratore di sistema installa il componente sito Web per permettere di accedere alle funzionalità dell'infrastruttura nella console Web di vRealize Automation. È possibile installare una o più istanze del componente sito Web, ma è necessario configurare Model Manager Data sulla stessa macchina che ospita il primo componente sito Web. Model Manager Data viene installato una sola volta.

5 Installazione di componenti sito Web di IaaS aggiuntivi

Il componente sito Web fornisce accesso alle funzionalità dell'infrastruttura nella console Web di vRealize Automation. L'amministratore di sistema può installare una sola o molte istanze del componente sito Web.

6 Installazione del servizio di gestione attivo

Il componente servizio di gestione coordina la comunicazione tra agenti e agenti proxy, database, e SMTP. Deve essere installata almeno un'istanza del componente servizio di gestione. È possibile installare un'istanza attiva e un'istanza di backup del componente servizio di gestione per fornire ridondanza in una distribuzione ad alta disponibilità.

7 Installazione di un componente servizio di gestione di backup

È possibile installare un'istanza di backup passiva del componente servizio di gestione che è possibile avviare manualmente per fornire ridondanza in una distribuzione ad alta disponibilità.

8 Installazione dei Distributed Execution Manager

Distributed Execution Manager può essere installato con due ruoli: DEM Orchestrator e DEM Worker. È necessario installare almeno un'istanza di DEM per ogni ruolo, quindi è possibile installare istanze aggiuntive di DEM per motivi di failover e alta disponibilità.

9 Configurazione di un servizio Windows per l'accesso al database IaaS

Gli amministratori di sistema possono cambiare il metodo di autenticazione utilizzato per accedere al database SQL durante il runtime (dopo il completamento dell'installazione). Per impostazione predefinita, la connessione al database dopo la sua installazione viene eseguita utilizzando l'identità Windows dell'account correntemente connesso al sistema.

10 Verifica dei servizi di IaaS

Dopo l'installazione, l'amministratore di sistema verifica che i servizi di IaaS siano in esecuzione. Se i servizi sono in esecuzione, l'installazione ha esito positivo.

Passi successivi

Installare un DEM Orchestrator e almeno un'istanza DEM Worker. Vedere [Installazione dei Distributed Execution Manager](#).

Installazione dei certificati IaaS

Per ambienti di produzione, ottenere un certificato di dominio da un'autorità di certificazione attendibile. Importare il certificato nell'archivio dei certificati radice attendibili di tutte le macchine su cui si intende installare il componente sito Web e il servizio di gestione (le macchine IIS) durante l'installazione di IaaS.

Prerequisiti

È necessario disabilitare TLS1.2 per i certificati che utilizzano SHA512 su macchine Windows 2012. Per ulteriori informazioni sulla disabilitazione di TLS1.2, vedere l'articolo della Knowledge Base di Microsoft all'indirizzo <http://support.microsoft.com/kb/245030>.

Procedura

- 1 Ottenere un certificato da un'autorità di certificazione attendibile.
- 2 Aprire Gestione Internet Information Services (IIS).
- 3 Fare doppio clic su **Certificati del server** dalla visualizzazione funzionalità.
- 4 Fare clic su **Importa** nel riquadro Azioni.
 - a Specificare un nome file nella casella di testo **File di certificato** o fare clic sul pulsante Sfoglia (...) per specificare il nome del file nella posizione in cui verrà memorizzato il certificato.
 - b Immettere una password nella casella di testo **Password** se il certificato è stato esposto con una password.
 - c Selezionare **Contrassegna la chiave come esportabile**.
- 5 Fare clic su **OK**.
- 6 Fare clic sul certificato importato e scegliere **Visualizza**.
- 7 Verificare che il certificato e la sua catena siano attendibili.

Se il certificato non è attendibile, verrà visualizzato il messaggio Questo certificato principale CA non è considerato attendibile.

Nota: è necessario risolvere il problema di attendibilità per poter continuare l'installazione, altrimenti la distribuzione avrà esito negativo.

- 8 Riavviare IIS o aprire la finestra del prompt dei comandi con autorizzazioni amministrative e digitare `iisreset`.

Passi successivi

[Download del programma d'installazione di IaaS.](#)

Download del programma d'installazione di IaaS

Un amministratore di sistema scarica il programma d'installazione di IaaS da vRealize Automation appliance a una macchina fisica o virtuale Windows 2008 o Windows 2012.

Se durante questo processo vengono visualizzati avvisi relativi ai certificati, è possibile ignorarli e continuare per completare l'installazione.

Prerequisiti

- [Configurazione di vRealize Automation Appliance primario](#) e facoltativamente [Unione di una vRealize Automation appliance a un cluster](#).
- Verificare che i server dell'installazione soddisfino i requisiti descritti in [Requisiti del servizio Web IaaS e del Model Manager Server](#).
- Verificare di aver importato un certificato in IIS e che la radice del certificato o l'autorità di certificazione sia nella radice attendibile sulla macchina d'installazione.
- Se nell'ambiente si utilizzano bilanciamenti del carico, verificare che questi soddisfino i requisiti di configurazione.

Procedura

- 1 (Facoltativo) Attivare HTTP se si sta installando su una macchina Windows 2012.
 - a Selezionare **Funzionalità > Aggiungi funzionalità** da Server Manager.
 - b Espandere **Servizi WCF** in Funzionalità .NET Framework.
 - c Selezionare **Attivazione HTTP**.
- 2 Accedere alla macchina Windows su cui occorre eseguire l'installazione.
- 3 Aprire un browser.
- 4 Immettere l'URL della pagina di download VMware vRealize Automation IaaS Installation.
Ad esempio **`https://vra-va-hostname.domain.name:5480/installer`**, dove *vra-va-hostname.domain.name* è il nome dell'host vRealize Automation appliance.
- 5 Scaricare il programma d'installazione facendo clic sul collegamento **IaaS Installer**.
- 6 Quando richiesto, salvare sul desktop il file del programma d'installazione `setup__vra-va-hostname.domain.name@5480.exe`.

Non modificare il nome del file poiché esso è utilizzato per collegare l'installazione alla vRealize Automation appliance.
- 7 Scaricare il file del programma d'installazione per ogni macchina su cui si stanno installando componenti.

Passi successivi

Installare un database di IaaS, vedere [Scelta di uno scenario di database IaaS](#).

Scelta di uno scenario di database IaaS

vRealize Automation IaaS utilizza un database Microsoft SQL Server per conservare le informazioni sulle macchine che gestisce e sui propri elementi e criteri.

In base alle preferenze e ai privilegi dell'utente, è possibile scegliere tra diverse procedure per creare il database IaaS.

Nota: è possibile attivare SSL sicuro quando si crea o si aggiorna il database SQL. Ad esempio, quando si crea o si aggiorna il database SQL, è possibile utilizzare l'opzione SSL sicuro per richiedere l'applicazione della configurazione SSL già specificata nel server SQL in fase di connessione al database SQL. SSL offre una connessione più sicura tra il server IaaS e il database SQL. Questa opzione, disponibile nell'installazione guidata personalizzata, richiede di aver già configurato SSL sul server SQL. Per informazioni correlate alla configurazione di SSL su SQL Server, vedere KB 316898 *Come abilitare la crittografia SSL per un'istanza di SQL Server utilizzando Microsoft Management Console* sul sito del supporto di Microsoft.

Tavola 4-13. Scelta di uno scenario di database IaaS

Scenario	Procedura
Creare manualmente il database di IaaS utilizzando gli script di database forniti. Questa opzione consente all'amministratore di database di esaminare attentamente i cambiamenti prima di creare il database.	Creazione manuale del database IaaS .
Preparare un database vuoto e utilizzare il programma d'installazione per popolare lo schema del database. Questa opzione consente al programma d'installazione di utilizzare un utente di database con privilegi di dbo per popolare il database e non richiedere privilegi di sysadmin .	Preparazione di un database vuoto .
Utilizzare il programma d'installazione per creare il database. Questa è l'opzione più semplice, ma richiede l'uso dei privilegi di sysadmin nel programma d'installazione.	Creazione del database IaaS utilizzando l'installazione guidata .

Creazione manuale del database IaaS

L'amministratore di sistema di vRealize Automation può creare il database manualmente utilizzando gli script forniti da VMware.

Prerequisiti

- Sull'host di SQL Server deve essere installato .NET 4.5.1 o versione successiva.
- Per connettersi al database, utilizzare l'autenticazione Windows e non l'autenticazione SQL.
- Verificare i prerequisiti d'installazione del database. Vedere [Requisiti del server di database di IaaS](#).
- Scaricare gli script del programma d'installazione del database IaaS dalla vRealize Automation appliance accedendo alla pagina <https://vra-va-hostname.domain.name:5480/installer/>.

Procedura

- 1 Aprire la sottodirectory Database della directory in cui è stato estratto l'archivio ZIP d'installazione.
- 2 Estrarre l'archivio DBInstall.zip in una directory locale.
- 3 Accedere all'host del database Windows con diritti sufficienti a creare ed eliminare database, ovvero con privilegi di **sysadmin** nell'istanza di SQL Server.
- 4 Rivedere gli script di distribuzione del database secondo necessità. In particolare, riesaminare le impostazioni nella sezione DBSettings di CreateDatabase.sql e modificarle se necessario.

Le impostazioni fissate nello script sono quelle consigliate. Sono richiesti solo ALLOW_SNAPSHOT_ISOLATION ON e READ_COMMITTED_SNAPSHOT ON.

- 5 Eseguire il comando seguente utilizzando gli argomenti descritti nella tabella.

```
BuildDB.bat /p:DBServer=db_server;
DBName=db_name;DBDir=db_dir;
LogDir=[log_dir];ServiceUser=service_user;
ReportLogin=web_user;
VersionString=version_string
```

Tavola 4-14. Valori del database

Variabile	Valore
<i>db_server</i>	Specifica l'istanza di SQL Server nel formato dbhostname[,port number]\SQL instance. Immettere un numero di porta solo se si utilizza una porta non predefinita. La porta predefinita di Microsoft SQL è 1433. Il valore predefinito per <i>db_server</i> è localhost.
<i>db_name</i>	Nome del database. Il valore predefinito è vra. I nomi dei database non possono contenere più di 128 caratteri ASCII.
<i>db_dir</i>	Percorso della directory dei dati per il database (escludere la barra finale).
<i>log_dir</i>	Percorso della directory dei registri per il database (escludere la barra finale).
<i>service_user</i>	Nome utente utilizzato per l'esecuzione del servizio di gestione.
<i>Web_user</i>	Nome utente utilizzato per l'esecuzione dei servizi Web.
<i>version_string</i>	Specifica la versione di vRealize Automation. Per la versione 6.1, ad esempio, la stringa di versione è 6.1.0.1200.

Il database è stato creato.

Passi successivi

[Installazione dei componenti di IaaS in una configurazione distribuita.](#)

Preparazione di un database vuoto

Un amministratore di sistema di vRealize Automation può installare lo schema di IaaS su un database vuoto. Questo metodo d'installazione fornisce il massimo controllo sulla sicurezza del database.

Prerequisiti

- Verificare i prerequisiti d'installazione del database. Vedere [Requisiti del server di database di IaaS](#).
- Scaricare gli script del programma d'installazione del database IaaS dalla vRealize Automation appliance accedendo alla pagina <https://vra-va-hostname.domain.name:5480/installer/>.

Procedura

- 1 Aprire la directory Database all'interno della directory in cui è stato estratto l'archivio ZIP d'installazione.
- 2 Estrarre l'archivio DBInstall.zip in una directory locale.
- 3 Accedere all'host del database Windows con privilegi di **sysadmin** nell'istanza di SQL Server.
- 4 Modificare CreateDatabase.sql e sostituire tutte le istanze delle variabili elencate nella tabella con i valori appropriati per il proprio ambiente.

Tavola 4-15. Valori del database

Variabile	Valore
\$(DBName)	Nome del database, ad esempio vra. I nomi dei database non possono contenere più di 128 caratteri ASCII.
\$(DBDir)	Percorso della directory dei dati per il database (escludere la barra finale).
\$(LogDir)	Percorso della directory dei registri per il database (escludere la barra finale).

- 5 Riesaminare le impostazioni nella sezione DB Settings di CreateDatabase.sql e modificarle se necessario.

Le impostazioni fissate nello script sono quelle consigliate per il database di IaaS. Sono richieste solo ALLOW_SNAPSHOT_ISOLATION ON e READ_COMMITTED_SNAPSHOT ON.

- 6 Aprire SQL Server Management Studio.
- 7 Fare clic su **Nuova query**.
Si apre una finestra di SQL Query.
- 8 Nel menu **Query**, verificare che sia selezionata l'opzione **Modalità SQLCMD**.
- 9 Incollare l'intero contenuto modificato di CreateDatabase.sql nel riquadro della query.
- 10 Fare clic su **Esegui**.

Viene eseguito lo script e creato il database.

Passi successivi

[Installazione dei componenti di IaaS in una configurazione distribuita.](#)

Creazione del database IaaS utilizzando l'installazione guidata

vRealize Automation utilizza un database Microsoft SQL Server per conservare le informazioni sulle macchine che gestisce e sui propri elementi e criteri.

La procedura seguente descrive come creare il database IaaS utilizzando il programma d'installazione e come popolare un database vuoto già esistente. È possibile creare il database anche manualmente.

Vedere [Creazione manuale del database IaaS](#).

Prerequisiti

- Se si sta creando il database con l'autenticazione Windows al posto dell'autenticazione SQL, verificare che l'utente che esegue il programma d'installazione abbia diritti di **sysadmin** su SQL Server.
- [Download del programma d'installazione di IaaS.](#)

Procedura

- 1 Fare clic con il pulsante destro del mouse sul file d'installazione `setup__vra-va-hostname.domain.name@5480.exe` e scegliere **Esegui come amministratore**.
- 2 Fare clic su **Avanti**.
- 3 Accettare il contratto di licenza e fare clic su **Avanti**.
- 4 Nella pagina di accesso, inserire le credenziali di amministratore per vRealize Automation appliance e verificare il certificato SSL.
 - a Specificare il nome utente, ovvero **root**, e la password.
Questa è la password che è stata immessa quando è stata distribuita la vRealize Automation appliance.
 - b Selezionare **Accetta certificato**.
 - c Fare clic su **Visualizza certificato**.
Confrontare l'identificazione digitale del certificato con quella impostata per la vRealize Automation appliance. È possibile visualizzare il certificato della vRealize Automation appliance nel browser client quando si accede alla console di gestione sulla porta 5480.
- 5 Fare clic su **Avanti**.
- 6 Selezionare **Installazione personalizzata** nella pagina Tipo di installazione.
- 7 Selezionare **Server IaaS** in Selezione componenti nella pagina Tipo di installazione.
- 8 Accettare la posizione d'installazione radice o fare clic su **Cambia** e selezionare un percorso d'installazione diverso.
- 9 Fare clic su **Avanti**.

10 Nella pagina dell'installazione personalizzata del server IaaS, selezionare **Database**.

11 Nella casella di testo **Database Instance**, specificare l'istanza del database o fare clic su **Scan** e selezionarla dall'elenco di istanze. Se l'istanza del database si trova su una porta non predefinita, includere il numero della porta nella definizione dell'istanza utilizzando la forma `dbhost,SQL_port_number\SQLinstance`. La porta predefinita di Microsoft SQL è 1443.

12 (Facoltativo) Selezionare la casella di controllo **Use SSL for database connection**.

La casella di controllo è selezionata per impostazione predefinita. SSL offre una connessione più sicura tra il server IaaS e il database SQL. Tuttavia è necessario configurare il protocollo SSL sul server SQL per supportare l'opzione. Per informazioni correlate alla configurazione di SSL su SQL Server, vedere l'articolo KB 316898 *How to enable SSL encryption for an instance of SQL Server by using Microsoft Management Console* sul sito del supporto di Microsoft.

13 Selezionare il tipo d'installazione del database dal pannello **Database Name**.

- Selezionare **Use existing empty database** per creare lo schema in un database esistente.
- Immettere il nome di un nuovo database o utilizzare il nome predefinito **vra** per creare un nuovo database. I nomi dei database non possono contenere più di 128 caratteri ASCII.

14 Deselezionare **Use default data and log directories** per specificare posizioni alternative o lasciare l'opzione selezionata per utilizzare le directory predefinite (scelta consigliata).

15 Selezionare un metodo di autenticazione per l'installazione del database dall'elenco **Authentication**.

- Per creare il database utilizzando le credenziali impiegate per eseguire il programma d'installazione, selezionare **User Windows identity**.
- Per utilizzare l'autenticazione SQL, deselezionare **Use Windows identity**. Immettere le credenziali SQL nelle caselle di testo di utente e password.

Per impostazione predefinita, nell'accesso in runtime al database viene utilizzato l'account utente del servizio Windows, il quale deve avere diritti di sysadmin sull'istanza di SQL Server. Le credenziali utilizzate per accedere al database in runtime possono essere configurate per utilizzare credenziali SQL.

16 Fare clic su **Avanti**.

17 Completare il Controllo prerequisiti.

Opzione	Descrizione
Nessun errore	Fare clic su Avanti .
Errori non critici	Fare clic su Bypass .
Errori critici	Se si ignorano gli errori critici, l'installazione non riuscirà. Se vengono visualizzati avvisi, selezionare l'avviso nel riquadro di sinistra e seguire le istruzioni visualizzate a destra. Risolvere tutti gli errori critici e fare clic su Controlla di nuovo per verificare.

18 Fare clic su **Installa**.

19 Alla visualizzazione del messaggio di operazione eseguita, deselezionare **Guide me through initial configuration** e fare clic su **Next**

20 Fare clic su **Fine**.

Il database è pronto per l'uso.

Installazione di un componente sito Web di IaaS e di Model Manager Data

L'amministratore di sistema installa il componente sito Web per permettere di accedere alle funzionalità dell'infrastruttura nella console Web di vRealize Automation. È possibile installare una o più istanze del componente sito Web, ma è necessario configurare Model Manager Data sulla stessa macchina che ospita il primo componente sito Web. Model Manager Data viene installato una sola volta.

Prerequisiti

- Installare il database di IaaS, vedere [Scelta di uno scenario di database IaaS](#).
- Se precedentemente sono stati installati componenti in questo ambiente, assicurarsi di conoscere la passphrase che è stata creata. Vedere [Passphrase di sicurezza](#).
- Se nell'ambiente si utilizzano bilanciamenti del carico, verificare che questi soddisfino i requisiti di configurazione.

Procedura

1 [Installazione del primo componente sito Web di IaaS](#)

Un amministratore di sistema installa un componente sito Web per permettere di accedere alle funzionalità dell'infrastruttura nella console Web di vRealize Automation.

2 [Configurazione di Model Manager Data](#)

Il componente Model Manager viene installato sulla stessa macchina che ospita il primo componente sito Web. Model Manager Data può essere installato una sola volta.

È possibile installare componenti sito Web aggiuntivi o installare il servizio di gestione. Vedere [Installazione di componenti sito Web di IaaS aggiuntivi](#) o [Installazione del servizio di gestione attivo](#).

Installazione del primo componente sito Web di IaaS

Un amministratore di sistema installa un componente sito Web per permettere di accedere alle funzionalità dell'infrastruttura nella console Web di vRealize Automation.

È possibile installare più componenti sito Web, tuttavia solo uno può contenere Model Manager Data. Model Manager Data deve essere installato sul primo componente sito Web creato.

Prerequisiti

- [Creazione del database IaaS utilizzando l'installazione guidata](#).
- Verificare che l'ambiente soddisfi i requisiti descritti in [Requisiti del servizio Web IaaS e del Model Manager Server](#).

- Se precedentemente sono stati installati componenti in questo ambiente, assicurarsi di conoscere la passphrase che è stata creata. Vedere [Passphrase di sicurezza](#).
- Se nell'ambiente si utilizzano bilanciamenti del carico, verificare che questi soddisfino i requisiti di configurazione.

Procedura

- 1 Disabilitare tutti i controlli di integrità del bilanciamento del carico e assicurarsi che il traffico sia diretto al nodo.
- 2 Disabilitare tutti gli altri nodi sotto il bilanciamento del carico.
- 3 Fare clic con il pulsante destro del mouse sul file d'installazione `setup__vra-va-hostname.domain.name@5480.exe` e scegliere **Esegui come amministratore**.
- 4 Fare clic su **Avanti**.
- 5 Accettare il contratto di licenza e fare clic su **Avanti**.
- 6 Nella pagina di accesso, inserire le credenziali di amministratore per vRealize Automation appliance e verificare il certificato SSL.
 - a Specificare il nome utente, ovvero **root**, e la password.
Questa è la password che è stata immessa quando è stata distribuita la vRealize Automation appliance.
 - b Selezionare **Accetta certificato**.
 - c Fare clic su **Visualizza certificato**.
Confrontare l'identificazione digitale del certificato con quella impostata per la vRealize Automation appliance. È possibile visualizzare il certificato della vRealize Automation appliance nel browser client quando si accede alla console di gestione sulla porta 5480.
- 7 Fare clic su **Avanti**.
- 8 Selezionare **Installazione personalizzata** nella pagina Tipo di installazione.
- 9 Selezionare **Server IaaS** in Selezione componenti nella pagina Tipo di installazione.
- 10 Accettare la posizione d'installazione radice o fare clic su **Cambia** e selezionare un percorso d'installazione diverso.
- 11 Fare clic su **Avanti**.
- 12 Selezionare **Sito Web** e **ModelManagerData** nella pagina **Installazione personalizzata server IaaS**.
- 13 Selezionare un sito Web dai siti Web disponibili o accettare il sito Web predefinito nella scheda **Sito Web di amministrazione e Model Manager**.
- 14 Immettere un numero di porta disponibile nella casella di testo **Numero porta** o accettare la porta predefinita 443.
- 15 Fare clic su **Prova binding** per verificare la disponibilità all'uso del numero di porta scelto.

16 Selezionare il certificato per questo componente.

- a Se è stato importato un certificato dopo aver iniziato l'installazione, fare clic su **Aggiorna** per aggiornare l'elenco.
- b Selezionare il certificato da utilizzare da **Certificati disponibili**.
- c Se è stato importato un certificato non dotato di un nome descrittivo e questo non compare nell'elenco, deselezionare **Visualizza certificati con nomi mnemonici** e fare clic su **Aggiorna**.

Se si sta installando in un ambiente che non utilizza bilanciamenti del carico, è possibile selezionare **Genera certificato autofirmato** invece di selezionare un certificato. Se si stanno installando componenti sito Web aggiuntivi dietro a un bilanciamento del carico, non generare certificati autofirmati. Importare il certificato dal server Web IaaS principale per assicurarsi di utilizzare lo stesso certificato su tutti i server dietro al bilanciamento del carico.

17 (Facoltativo) Fare clic su **Visualizza certificato**, visualizzare il certificato e fare clic su **OK** per chiudere la finestra delle informazioni.**18** (Facoltativo) Selezionare **Ignora errori corrispondenza certificati** per eliminare gli errori dei certificati. L'installazione ignorerà gli errori di errata corrispondenza tra i nomi dei certificati e tutti gli errori di corrispondenza negli elenchi certificato-revoca remoti.

Questa è un'opzione meno sicura.

Configurazione di Model Manager Data

Il componente Model Manager viene installato sulla stessa macchina che ospita il primo componente sito Web. Model Manager Data può essere installato una sola volta.

Prerequisiti

[Installazione del primo componente sito Web di IaaS.](#)

Procedura**1** Fare clic sulla scheda **Model Manager Data**.**2** Immettere il nome di dominio completo della vRealize Automation appliance nella casella di testo **Server**.

Gli indirizzi IP non vengono riconosciuti.

Ad esempio **vra.mycompany.com**.

3 Fare clic su **Carica** per visualizzare il **Tenant predefinito SSO**.

Il tenant predefinito vsphere.local viene creato automaticamente quando si configura Single Sign-On. Non modificarlo.

4 Fare clic su **Scarica** per importare il certificato dall'appliance virtuale.

Il download del certificato potrebbe richiedere diversi minuti.

5 (Facoltativo) Fare clic su **Visualizza certificato**, visualizzare il certificato e fare clic su **OK** per chiudere la finestra delle informazioni.

- 6 Far clic su **Accetta certificato**.
- 7 Immettere **administrator@vsphere.local** nella casella di testo **Nome utente** e la password creata quando è stato configurato SSO nelle caselle di testo **Password** e **Conferma**.
- 8 (Facoltativo) Fare clic su **Prova** per verificare le credenziali.
- 9 Immettere il nome di dominio completo del server del sito Web di IaaS nella casella di testo **Server IaaS**.

Opzione	Descrizione
Se si utilizza il bilanciamento del carico	Immettere il nome di dominio completo del bilanciamento del carico per il server del sito Web di IaaS. Ad esempio IaaS-Load-balancer.eng.mycompany.com . Gli indirizzi IP non vengono riconosciuti.
Senza bilanciamento del carico	Immettere il nome di dominio completo del server del sito Web di IaaS. Ad esempio IaaS.eng.mycompany.com . Gli indirizzi IP non vengono riconosciuti.

- 10 Fare clic su **Prova** per verificare la connessione con il server.
- 11 Fare clic su **Avanti**.
- 12 Completare il Controllo prerequisiti.

Opzione	Descrizione
Nessun errore	Fare clic su Avanti .
Errori non critici	Fare clic su Bypass .
Errori critici	Se si ignorano gli errori critici, l'installazione non riuscirà. Se vengono visualizzati avvisi, selezionare l'avviso nel riquadro di sinistra e seguire le istruzioni visualizzate a destra. Risolvere tutti gli errori critici e fare clic su Controlla di nuovo per verificare.

- 13 Immettere il nome utente e la password dell'utente dell'account di servizio, dotato di privilegi amministrativi sul server dell'installazione corrente, nelle caselle di testo **Informazioni installazione server** della pagina Impostazioni server e account.
- 14 Fornire la passphrase utilizzata per generare la chiave di crittografia che protegge il database.

Opzione	Descrizione
Se sono già stati installati componenti in questo ambiente	Immettere la passphrase precedentemente creata nelle caselle di testo Passphrase e Conferma .
Se questa è la prima installazione	Immettere una passphrase nelle caselle di testo Passphrase e Conferma . È necessario utilizzare questa passphrase ogni volta che si installa un nuovo componente.

Conservare la passphrase in un luogo sicuro per uso futuro.

- 15 Specificare il server di database IaaS, il nome del database e il metodo di autenticazione per il server di database nella casella di testo **Informazioni installazione Microsoft SQL Database**.

Si tratta delle informazioni relative a server di database IaaS, nome e autenticazione create precedentemente.

16 Fare clic su **Avanti**.

17 Fare clic su **Installa**.

18 Al termine dell'installazione, deselezionare **Configurazione iniziale guidata** e fare clic su **Avanti**.

Passi successivi

È possibile installare componenti sito Web aggiuntivi o installare il servizio di gestione. Vedere [Installazione di componenti sito Web di IaaS aggiuntivi](#) o [Installazione del servizio di gestione attivo](#). Se non è in programma l'aggiunta di altri nodi sotto il bilanciamento del carico, attivare tutti i controlli di integrità applicabili.

Installazione di componenti sito Web di IaaS aggiuntivi

Il componente sito Web fornisce accesso alle funzionalità dell'infrastruttura nella console Web di vRealize Automation. L'amministratore di sistema può installare una sola o molte istanze del componente sito Web.

Non installare Model Manager Data con il componente sito Web. Solo il primo componente sito Web installato può contenere Model Manager Data.

Prerequisiti

- [Installazione di un componente sito Web di IaaS e di Model Manager Data](#).
- Verificare che l'ambiente soddisfi i requisiti descritti in [Requisiti del servizio Web IaaS e del Model Manager Server](#).
- Se precedentemente sono stati installati componenti in questo ambiente, assicurarsi di conoscere la passphrase che è stata creata. Vedere [Passphrase di sicurezza](#).
- Se nell'ambiente si utilizzano bilanciamenti del carico, verificare che questi soddisfino i requisiti di configurazione.

Procedura

- 1** Disabilitare tutti i controlli di integrità del bilanciamento del carico e assicurarsi che il traffico sia diretto al nodo.
- 2** Fare clic con il pulsante destro del mouse sul file d'installazione `setup__vra-va-hostname.domain.name@5480.exe` e scegliere **Esegui come amministratore**.
- 3** Fare clic su **Avanti**.
- 4** Accettare il contratto di licenza e fare clic su **Avanti**.

- 5 Nella pagina di accesso, inserire le credenziali di amministratore per vRealize Automation appliance e verificare il certificato SSL.

- a Specificare il nome utente, ovvero **root**, e la password.

Questa è la password che è stata immessa quando è stata distribuita la vRealize Automation appliance.

- b Selezionare **Accetta certificato**.
 - c Fare clic su **Visualizza certificato**.

Confrontare l'identificazione digitale del certificato con quella impostata per la vRealize Automation appliance. È possibile visualizzare il certificato della vRealize Automation appliance nel browser client quando si accede alla console di gestione sulla porta 5480.

- 6 Fare clic su **Avanti**.
- 7 Selezionare **Installazione personalizzata** nella pagina Tipo di installazione.
- 8 Selezionare **Server IaaS** in Selezione componenti nella pagina Tipo di installazione.
- 9 Accettare la posizione d'installazione radice o fare clic su **Cambia** e selezionare un percorso d'installazione diverso.
- 10 Fare clic su **Avanti**.
- 11 Selezionare **Sito Web** nella pagina **Installazione personalizzata server IaaS**.
- 12 Selezionare un sito Web dai siti Web disponibili o accettare il sito Web predefinito nella scheda **Sito Web di amministrazione e Model Manager**.
- 13 Immettere un numero di porta disponibile nella casella di testo **Numero porta** o accettare la porta predefinita 443.
- 14 Fare clic su **Prova binding** per verificare la disponibilità all'uso del numero di porta scelto.
- 15 Selezionare il certificato per questo componente.
 - a Se è stato importato un certificato dopo aver iniziato l'installazione, fare clic su **Aggiorna** per aggiornare l'elenco.
 - b Selezionare il certificato da utilizzare da **Certificati disponibili**.
 - c Se è stato importato un certificato non dotato di un nome descrittivo e questo non compare nell'elenco, deselezionare **Visualizza certificati con nomi mnemonici** e fare clic su **Aggiorna**.

Se si sta installando in un ambiente che non utilizza bilanciamenti del carico, è possibile selezionare **Genera certificato autofirmato** invece di selezionare un certificato. Se si stanno installando componenti sito Web aggiuntivi dietro a un bilanciamento del carico, non generare certificati autofirmati. Importare il certificato dal server Web IaaS principale per assicurarsi di utilizzare lo stesso certificato su tutti i server dietro al bilanciamento del carico.
- 16 (Facoltativo) Fare clic su **Visualizza certificato**, visualizzare il certificato e fare clic su **OK** per chiudere la finestra delle informazioni.

- 17 (Facoltativo) Selezionare **Ignora errori corrispondenza certificati** per eliminare gli errori dei certificati. L'installazione ignorerà gli errori di errata corrispondenza tra i nomi dei certificati e tutti gli errori di corrispondenza negli elenchi certificato-revoca remoti.

Questa è un'opzione meno sicura.

- 18 Immettere le informazioni sul server IaaS nella casella di testo **Server IaaS**.

Opzione	Descrizione
Se si utilizza il bilanciamento del carico	Immettere il nome di dominio completo del bilanciamento del carico per il server del sito Web di IaaS. Ad esempio IaaS-load-balancer.eng.mycompany.com .
Senza bilanciamento del carico	Immettere il nome di dominio completo del server del sito Web di IaaS. Ad esempio IaaS.eng.mycompany.com .

- 19 Fare clic su **Prova** per verificare la connessione con il server.

- 20 Fare clic su **Avanti**.

- 21 Completare il Controllo prerequisiti.

Opzione	Descrizione
Nessun errore	Fare clic su Avanti .
Errori non critici	Fare clic su Bypass .
Errori critici	Se si ignorano gli errori critici, l'installazione non riuscirà. Se vengono visualizzati avvisi, selezionare l'avviso nel riquadro di sinistra e seguire le istruzioni visualizzate a destra. Risolvere tutti gli errori critici e fare clic su Controlla di nuovo per verificare.

- 22 Immettere il nome utente e la password dell'utente dell'account di servizio, dotato di privilegi amministrativi sul server dell'installazione corrente, nelle caselle di testo **Informazioni installazione server** della pagina Impostazioni server e account.

- 23 Fornire la passphrase utilizzata per generare la chiave di crittografia che protegge il database.

Opzione	Descrizione
Se sono già stati installati componenti in questo ambiente	Immettere la passphrase precedentemente creata nelle caselle di testo Passphrase e Conferma .
Se questa è la prima installazione	Immettere una passphrase nelle caselle di testo Passphrase e Conferma . È necessario utilizzare questa passphrase ogni volta che si installa un nuovo componente.

Conservare la passphrase in un luogo sicuro per uso futuro.

- 24 Specificare il server di database IaaS, il nome del database e il metodo di autenticazione per il server di database nella casella di testo **Informazioni installazione Microsoft SQL Database**.

Si tratta delle informazioni relative a server di database IaaS, nome e autenticazione create precedentemente.

- 25 Fare clic su **Avanti**.

- 26 Fare clic su **Installa**.

27 Al termine dell'installazione, deselezionare **Configurazione iniziale guidata** e fare clic su **Avanti**.

Passi successivi

[Installazione del servizio di gestione attivo](#). Se non è in programma l'aggiunta di altri nodi sotto il bilanciamento del carico, attivare tutti i controlli di integrità applicabili.

Installazione del servizio di gestione attivo

Il componente servizio di gestione coordina la comunicazione tra agenti e agenti proxy, database, e SMTP. Deve essere installata almeno un'istanza del componente servizio di gestione. È possibile installare un'istanza attiva e un'istanza di backup del componente servizio di gestione per fornire ridondanza in una distribuzione ad alta disponibilità.

Prerequisiti

- Se precedentemente sono stati installati componenti in questo ambiente, assicurarsi di conoscere la passphrase che è stata creata. Vedere [Passphrase di sicurezza](#).
- (Facoltativo) Se si desidera installare il servizio di gestione in un sito Web diverso dal sito Web predefinito, creare prima un sito Web in Internet Information Services.
- Microsoft .NET Framework 4.5.2 sia installato.
- Verificare di avere un certificato da un'autorità di certificazione importato in IIS e che il certificato radice o l'autorità di certificazione sia attendibile. Tutti i componenti sotto il bilanciamento del carico devono avere lo stesso certificato.
- Verificare che il bilanciamento del carico del sito Web sia configurato e che il valore di timeout per il bilanciamento del carico sia impostato ad almeno 180 secondi.
- [Installazione di un componente sito Web di IaaS e di Model Manager Data](#).

Procedura

- 1 Disabilitare tutti i controlli di integrità del bilanciamento del carico e assicurarsi che il traffico sia diretto al nodo.
- 2 Fare clic con il pulsante destro del mouse sul file d'installazione `setup__vra-va-hostname.domain.name@5480.exe` e scegliere **Esegui come amministratore**.
- 3 Accettare il contratto di licenza e fare clic su **Avanti**.

- 4 Nella pagina di accesso, inserire le credenziali di amministratore per vRealize Automation appliance e verificare il certificato SSL.

- a Specificare il nome utente, ovvero **root**, e la password.

Questa è la password che è stata immessa quando è stata distribuita la vRealize Automation appliance.

- b Selezionare **Accetta certificato**.
 - c Fare clic su **Visualizza certificato**.

Confrontare l'identificazione digitale del certificato con quella impostata per la vRealize Automation appliance. È possibile visualizzare il certificato della vRealize Automation appliance nel browser client quando si accede alla console di gestione sulla porta 5480.

- 5 Fare clic su **Avanti**.
- 6 Selezionare **Installazione personalizzata** nella pagina Tipo di installazione.
- 7 Selezionare **Server IaaS** in Selezione componenti nella pagina Tipo di installazione.
- 8 Accettare la posizione d'installazione radice o fare clic su **Cambia** e selezionare un percorso d'installazione diverso.
- 9 Fare clic su **Avanti**.
- 10 Selezionare **Servizio di gestione** nella pagina **Installazione personalizzata server IaaS**.
- 11 Immettere le informazioni sul server IaaS nella casella di testo **Server IaaS**.

Opzione	Descrizione
Se si utilizza il bilanciamento del carico	Immettere il nome di dominio completo del bilanciamento del carico per il server del sito Web di IaaS. Ad esempio IaaS-Load-balancer.eng.mycompany.com .
Senza bilanciamento del carico	Immettere il nome di dominio completo del server del sito Web di IaaS. Ad esempio IaaS.eng.mycompany.com .

- 12 Selezionare **Attiva nodo con tipo di avvio impostato su Automatico**.
- 13 Selezionare un sito Web dai siti Web disponibili o accettare il sito Web predefinito nella scheda **Sito Web di amministrazione e Model Manager**.
- 14 Immettere un numero di porta disponibile nella casella di testo **Numero porta** o accettare la porta predefinita 443.
- 15 Fare clic su **Prova binding** per verificare la disponibilità all'uso del numero di porta scelto.

16 Selezionare il certificato per questo componente.

- a Se è stato importato un certificato dopo aver iniziato l'installazione, fare clic su **Aggiorna** per aggiornare l'elenco.
- b Selezionare il certificato da utilizzare da **Certificati disponibili**.
- c Se è stato importato un certificato non dotato di un nome descrittivo e questo non compare nell'elenco, deselezionare **Visualizza certificati con nomi mnemonici** e fare clic su **Aggiorna**.

Se si sta installando in un ambiente che non utilizza bilanciamenti del carico, è possibile selezionare **Genera certificato autofirmato** invece di selezionare un certificato. Se si stanno installando componenti sito Web aggiuntivi dietro a un bilanciamento del carico, non generare certificati autofirmati. Importare il certificato dal server Web IaaS principale per assicurarsi di utilizzare lo stesso certificato su tutti i server dietro al bilanciamento del carico.

17 (Facoltativo) Fare clic su **Visualizza certificato**, visualizzare il certificato e fare clic su **OK** per chiudere la finestra delle informazioni.**18** Fare clic su **Avanti**.**19** Controllare i prerequisiti e fare clic su **Avanti**.**20** Immettere il nome utente e la password dell'utente dell'account di servizio, dotato di privilegi amministrativi sul server dell'installazione corrente, nelle caselle di testo **Informazioni installazione server** della pagina Impostazioni server e account.**21** Fornire la passphrase utilizzata per generare la chiave di crittografia che protegge il database.

Opzione	Descrizione
Se sono già stati installati componenti in questo ambiente	Immettere la passphrase precedentemente creata nelle caselle di testo Passphrase e Conferma .
Se questa è la prima installazione	Immettere una passphrase nelle caselle di testo Passphrase e Conferma . È necessario utilizzare questa passphrase ogni volta che si installa un nuovo componente.

Conservare la passphrase in un luogo sicuro per uso futuro.

22 Specificare il server di database IaaS, il nome del database e il metodo di autenticazione per il server di database nella casella di testo **Informazioni installazione Microsoft SQL Database**.

Si tratta delle informazioni relative a server di database IaaS, nome e autenticazione create precedentemente.

23 Fare clic su **Avanti**.**24** Fare clic su **Installa**.**25** Al termine dell'installazione, deselezionare **Configurazione iniziale guidata** e fare clic su **Avanti**.**26** Fare clic su **Fine**.

Passi successivi

Per assicurarsi che il servizio di gestione installato sia l'istanza attiva, verificare che il servizio vCloud Automation Center sia in esecuzione e impostarne il tipo di avvio su "Automatico".

È possibile installare un'altra istanza del componente servizio di gestione come backup passivo che può essere avviato manualmente in caso di errore dell'istanza attiva. Vedere [Installazione di un componente servizio di gestione di backup](#).

Gli amministratori di sistema possono cambiare il metodo di autenticazione utilizzato per accedere al database SQL durante il runtime (dopo il completamento dell'installazione). Vedere [Configurazione di un servizio Windows per l'accesso al database IaaS](#).

Installazione di un componente servizio di gestione di backup

È possibile installare un'istanza di backup passiva del componente servizio di gestione che è possibile avviare manualmente per fornire ridondanza in una distribuzione ad alta disponibilità.

Prerequisiti

- Se precedentemente sono stati installati componenti in questo ambiente, assicurarsi di conoscere la passphrase che è stata creata. Vedere [Passphrase di sicurezza](#).
- (Facoltativo) Se si desidera installare il servizio di gestione in un sito Web diverso dal sito Web predefinito, creare prima un sito Web in Internet Information Services.
- Microsoft .NET Framework 4.5.2 sia installato.
- Verificare di avere un certificato da un'autorità di certificazione importato in IIS e che il certificato radice o l'autorità di certificazione sia attendibile. Tutti i componenti sotto il bilanciamento del carico devono avere lo stesso certificato.
- Verificare che sia configurato il bilanciamento del carico del sito Web.
- [Installazione di un componente sito Web di IaaS e di Model Manager Data](#).

Procedura

- 1 Disabilitare tutti i controlli di integrità del bilanciamento del carico e assicurarsi che il traffico sia diretto al nodo.
- 2 Fare clic con il pulsante destro del mouse sul file d'installazione `setup__vra-va-hostname.domain.name@5480.exe` e scegliere **Esegui come amministratore**.
- 3 Fare clic su **Avanti**.
- 4 Accettare il contratto di licenza e fare clic su **Avanti**.

- 5 Nella pagina di accesso, inserire le credenziali di amministratore per vRealize Automation appliance e verificare il certificato SSL.

- a Specificare il nome utente, ovvero **root**, e la password.

Questa è la password che è stata immessa quando è stata distribuita la vRealize Automation appliance.

- b Selezionare **Accetta certificato**.

- c Fare clic su **Visualizza certificato**.

Confrontare l'identificazione digitale del certificato con quella impostata per la vRealize Automation appliance. È possibile visualizzare il certificato della vRealize Automation appliance nel browser client quando si accede alla console di gestione sulla porta 5480.

- 6 Fare clic su **Avanti**.

- 7 Selezionare **Installazione personalizzata** nella pagina Tipo di installazione.

- 8 Selezionare **Server IaaS** in Selezione componenti nella pagina Tipo di installazione.

- 9 Accettare la posizione d'installazione radice o fare clic su **Cambia** e selezionare un percorso d'installazione diverso.

- 10 Fare clic su **Avanti**.

- 11 Selezionare **Servizio di gestione** nella pagina **Installazione personalizzata server IaaS**.

- 12 Immettere le informazioni sul server IaaS nella casella di testo **Server IaaS**.

Opzione	Descrizione
Se si utilizza il bilanciamento del carico	Immettere il nome di dominio completo del bilanciamento del carico per il server del sito Web di IaaS. Ad esempio IaaS-Load-balancer.eng.mycompany.com .
Senza bilanciamento del carico	Immettere il nome di dominio completo del server del sito Web di IaaS. Ad esempio IaaS.eng.mycompany.com .

- 13 Selezionare **Nodo standby a freddo disaster recovery**.

- 14 Selezionare un sito Web dai siti Web disponibili o accettare il sito Web predefinito nella scheda **Sito Web di amministrazione e Model Manager**.

- 15 Immettere un numero di porta disponibile nella casella di testo **Numero porta** o accettare la porta predefinita 443.

- 16 Fare clic su **Prova binding** per verificare la disponibilità all'uso del numero di porta scelto.

17 Selezionare il certificato per questo componente.

- a Se è stato importato un certificato dopo aver iniziato l'installazione, fare clic su **Aggiorna** per aggiornare l'elenco.
- b Selezionare il certificato da utilizzare da **Certificati disponibili**.
- c Se è stato importato un certificato non dotato di un nome descrittivo e questo non compare nell'elenco, deselezionare **Visualizza certificati con nomi mnemonici** e fare clic su **Aggiorna**.

Se si sta installando in un ambiente che non utilizza bilanciamenti del carico, è possibile selezionare **Genera certificato autofirmato** invece di selezionare un certificato. Se si stanno installando componenti sito Web aggiuntivi dietro a un bilanciamento del carico, non generare certificati autofirmati. Importare il certificato dal server Web IaaS principale per assicurarsi di utilizzare lo stesso certificato su tutti i server dietro al bilanciamento del carico.

18 (Facoltativo) Fare clic su **Visualizza certificato**, visualizzare il certificato e fare clic su **OK** per chiudere la finestra delle informazioni.**19** Fare clic su **Avanti**.**20** Controllare i prerequisiti e fare clic su **Avanti**.**21** Immettere il nome utente e la password dell'utente dell'account di servizio, dotato di privilegi amministrativi sul server dell'installazione corrente, nelle caselle di testo **Informazioni installazione server** della pagina Impostazioni server e account.**22** Fornire la passphrase utilizzata per generare la chiave di crittografia che protegge il database.

Opzione	Descrizione
Se sono già stati installati componenti in questo ambiente	Immettere la passphrase precedentemente creata nelle caselle di testo Passphrase e Conferma .
Se questa è la prima installazione	Immettere una passphrase nelle caselle di testo Passphrase e Conferma . È necessario utilizzare questa passphrase ogni volta che si installa un nuovo componente.

Conservare la passphrase in un luogo sicuro per uso futuro.

23 Specificare il server di database IaaS, il nome del database e il metodo di autenticazione per il server di database nella casella di testo **Informazioni installazione Microsoft SQL Database**.

Si tratta delle informazioni relative a server di database IaaS, nome e autenticazione create precedentemente.

24 Fare clic su **Avanti**.**25** Fare clic su **Installa**.**26** Al termine dell'installazione, deselezionare **Configurazione iniziale guidata** e fare clic su **Avanti**.**27** Fare clic su **Fine**.

Passi successivi

Se non si aggiungeranno altri nodi sotto il bilanciamento del carico WEB, attivare tutti i controlli di integrità applicabili.

Per assicurarsi che il servizio di gestione installato sia un'istanza di backup passiva, verificare che il servizio vRealize Automation non sia in esecuzione e impostarlo sul tipo di avvio "Manuale".

Gli amministratori di sistema possono cambiare il metodo di autenticazione utilizzato per accedere al database SQL durante il runtime (dopo il completamento dell'installazione). Vedere [Configurazione di un servizio Windows per l'accesso al database IaaS](#).

Installazione dei Distributed Execution Manager

Distributed Execution Manager può essere installato con due ruoli: DEM Orchestrator e DEM Worker. È necessario installare almeno un'istanza di DEM per ogni ruolo, quindi è possibile installare istanze aggiuntive di DEM per motivi di failover e alta disponibilità.

L'amministratore di sistema deve scegliere le macchine dell'installazione che soddisfano requisiti di sistema predefiniti. Il DEM Orchestrator e il Worker possono risiedere sulla stessa macchina.

Se si pianifica di installare Distributed Execution Manager, tenere in considerazione i seguenti aspetti:

- I DEM Orchestrator supportano l'alta disponibilità attiva-attiva. In genere si installa un DEM Orchestrator su ogni macchina del servizio di gestione.
- Installare l'Orchestrator su una macchina con una solida connettività di rete che le consenta di comunicare con l'host di Model Manager.
- Installare un secondo DEM Orchestrator su una macchina differente per garantire il failover.
- Di solito si installano i DEM Worker sul server del servizio di gestione di IaaS o su un server separato. Installare l'Orchestrator su una macchina con una solida connettività di rete che le consenta di comunicare con l'host di Model Manager.
- È possibile installare istanze di DEM aggiuntive per ridondanza e scalabilità, incluse istanze multiple sulla stessa macchina.

Esistono requisiti specifici dell'installazione dei DEM che dipendono dagli endpoint utilizzati. Vedere [Requisiti di Distributed Execution Manager](#).

Installazione dei Distributed Execution Manager

Un amministratore di sistema installa almeno un DEM Worker e un DEM Orchestrator. La procedura d'installazione è la stessa per entrambi i ruoli.

I DEM Orchestrator supportano l'alta disponibilità attiva-attiva. In genere si installa un singolo DEM Orchestrator su ogni macchina del servizio di gestione. È possibile installare i DEM Orchestrator e i DEM worker sulla stessa macchina.

Prerequisiti

[Download del programma d'installazione di IaaS](#).

Procedura

- 1 Fare clic con il pulsante destro del mouse sul file d'installazione `setup__vra-va-hostname.domain.name@5480.exe` e scegliere **Esegui come amministratore**.
- 2 Fare clic su **Avanti**.
- 3 Accettare il contratto di licenza e fare clic su **Avanti**.
- 4 Nella pagina di accesso, inserire le credenziali di amministratore per vRealize Automation appliance e verificare il certificato SSL.
 - a Specificare il nome utente, ovvero **root**, e la password.
Questa è la password che è stata immessa quando è stata distribuita la vRealize Automation appliance.
 - b Selezionare **Accetta certificato**.
 - c Fare clic su **Visualizza certificato**.
Confrontare l'identificazione digitale del certificato con quella impostata per la vRealize Automation appliance. È possibile visualizzare il certificato della vRealize Automation appliance nel browser client quando si accede alla console di gestione sulla porta 5480.
- 5 Fare clic su **Avanti**.
- 6 Selezionare **Installazione personalizzata** nella pagina Tipo di installazione.
- 7 Selezionare **Distributed Execution Manager** dalla sezione Selezione componenti della pagina Tipo di installazione.
- 8 Accettare la posizione d'installazione radice o fare clic su **Cambia** e selezionare un percorso d'installazione diverso.
- 9 Fare clic su **Avanti**.
- 10 Controllare i prerequisiti e fare clic su **Avanti**.
- 11 Immettere le credenziali di accesso con le quali verrà eseguito il servizio. Queste devono appartenere a un account amministratore locale.
- 12 Fare clic su **Avanti**.
- 13 Selezionare il tipo di installazione dal menu a discesa **Ruolo DEM**.

Opzione	Descrizione
Worker	Il Worker si occupa di eseguire i workflow.
Orchestrator	L'Orchestrator supervisiona le attività del DEM Worker, inclusa la pianificazione e la pre-elaborazione dei workflow, e monitora lo stato online del DEM Worker.

- 14 Specificare un nome univoco che identifichi questo DEM nella casella di testo **Nome DEM**.

Se si pianifica di utilizzare lo strumento di migrazione, questo nome deve corrispondere esattamente al nome utilizzato nell'installazione di vCloud Automation Center 5.2.3. Il nome non può includere spazi e non può superare i 128 caratteri. Se si specifica un nome utilizzato precedentemente, viene visualizzato il seguente messaggio: "Nome DEM già esistente. Fare clic su Sì per specificare un nome diverso per questo DEM. Se si sta ripristinando o reinstallando un DEM con lo stesso nome, fare clic su No".

- 15 (Facoltativo) Immettere una descrizione per questa istanza di **Descrizione DEM**.
- 16 Specificare i nomi host e le porte nelle caselle di testo **Nome host servizio di gestione** e **Nome host servizio Web di Model Manager**.

Opzione	Descrizione
Se si utilizza il bilanciamento del carico	Immettere il nome di dominio completo dei bilanciamenti del carico per il servizio di gestione e il servizio Web di Model Manager. Ad esempio <code>manager-load-balancer.eng.mycompany.com:443</code> e <code>web-load-balancer.eng.mycompany.com:443</code> .
Senza bilanciamento del carico	Immettere il nome di dominio completo del servizio di gestione e del servizio Web di Model Manager. Ad esempio <code>manager-service.eng.mycompany.com:443</code> e <code>model-manager.eng.mycompany.com:443</code> .

- 17 (Facoltativo) Fare clic su **Prova** per provare le connessioni al servizio di gestione e al servizio Web di Model Manager.
- 18 Fare clic su **Aggiungi**.
- 19 Fare clic su **Avanti**.
- 20 Fare clic su **Installa**.
- 21 Al termine dell'installazione, deselezionare **Configurazione iniziale guidata** e fare clic su **Avanti**.
- 22 Fare clic su **Fine**.

Passi successivi

Verificare che il servizio sia in esecuzione e che il registro non contenga errori. Il nome del servizio è VMware DEM *Ruolo* - *Nome* dove Ruolo corrisponde a Orchestrator o Worker. La posizione del registro è *Posizione installazione*\Distributed Execution Manager\Name\Logs.

Ripetere questa procedura per installare istanze DEM aggiuntive.

Configurazione di DEM per la connessione a SCVMM su un percorso d'installazione non standard

Per impostazione predefinita, il file di configurazione di DEM Worker (DynamicOps.DEM.exe.config) punta al percorso d'installazione standard della console di Microsoft System Center Virtual Machine Manager (SCVMM): {ProgramFiles}\Microsoft System Center 2012\Virtual Machine Manager\bin. Se il programma viene installato in una posizione diversa, l'amministratore di sistema dovrà cambiare il percorso.

Questa procedura è necessaria solo quando si hanno endpoint e agenti SCVMM.

Prerequisiti

- Se la console di SCVMM è stata installata in una posizione diversa, il file di configurazione del DEM Worker (situato in Programmi (x86)VMware\VCAC\Distributed Execution Manager*InstanceName*\DynamicOps.DEM.exe.config deve essere aggiornato cambiando il percorso predefinito nella sezione `assemblyLoadConfiguration` affinché punti alla nuova cartella.

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

Procedura

- 1 Arrestare il DEM Worker.
- 2 Determinare il percorso d'installazione.
- 3 Aggiornare il file `DynamicOps.DEM.exe.config`.
- 4 Riavviare il DEM Worker.

Il percorso predefinito del DEM Worker viene aggiornato alla nuova cartella.

Configurazione di un servizio Windows per l'accesso al database IaaS

Gli amministratori di sistema possono cambiare il metodo di autenticazione utilizzato per accedere al database SQL durante il runtime (dopo il completamento dell'installazione). Per impostazione predefinita, la connessione al database dopo la sua installazione viene eseguita utilizzando l'identità Windows dell'account correntemente connesso al sistema.

Abilitazione dell'accesso al database IaaS da parte dell'utente del servizio

Se il database SQL è installato in un host separato dal servizio di gestione, è necessario abilitare l'accesso al database dal servizio di gestione. Se l'utente sotto cui viene eseguito il servizio di gestione coincide con il proprietario del database, non è richiesta alcuna azione. Se l'utente non è il proprietario del database, l'amministratore di sistema deve concedere l'accesso.

Prerequisiti

- [Scelta di uno scenario di database IaaS](#).
- Verificare che l'utente sotto cui viene eseguito il servizio di gestione non coincida con il proprietario del database.

Procedura

- 1 Aprire la sottodirectory Database all'interno della directory in cui è stato estratto l'archivio ZIP d'installazione.
- 2 Estrarre l'archivio DBInstall.zip in una directory locale.
- 3 Accedere all'host del database con un utente avente il ruolo di **sysadmin** nell'istanza di SQL Server.
- 4 Modificare VMPSOpsUser.sql e sostituire tutte le ricorrenze di \$(Service User) con l'utente (dal passaggio 3) sotto cui viene eseguito il servizio di gestione.
Non sostituire ServiceUser nella riga che termina con WHERE name = N'ServiceUser').
- 5 Aprire SQL Server Management Studio.
- 6 Selezionare il database (vCAC per impostazione predefinita) in **Databases** nel riquadro di sinistra.
- 7 Fare clic su **Nuova query**.
Si apre una finestra di SQL Query nel riquadro di destra.
- 8 Incollare il contenuto modificato di VMPSOpsUser.sql nella finestra della query.
- 9 Fare clic su **Esegui**.

L'accesso al database è abilitato dal servizio di gestione.

Configurazione dell'account dei servizi Windows per l'utilizzo dell'autenticazione SQL

Per impostazione predefinita, in fase di runtime è l'account dei servizi Windows che accede al database, anche se il database è stato creato utilizzando l'autenticazione SQL. Un amministratore di sistema può cambiare il metodo di autenticazione in runtime da Windows a SQL, ad esempio quando il database si trova in un dominio non attendibile.

Prerequisiti

[Scelta di uno scenario di database IaaS.](#)

Procedura

- 1 Accedere all'host del servizio di gestione come utente locale con privilegi di **amministratore**.
- 2 Arrestare il servizio di vCloud Automation Center.
- 3 Aprire la directory Server.
C:\Programmi (x86) \VMware\vCAC\Server\
- 4 Aprire il file ManagerService.exe.config in un editor di testo.
- 5 Nella sezione connectionStrings e nella sezione serviceConfiguration serviceURI, sostituire **Integrated Security=True** con **User Id=DATABASE_USER;Password=DATABASE_PASSWORD**.
- 6 Salvare e chiudere il file.
- 7 Passare alla directory C:\Programmi (x86)\VMware\vCAC\Server\Model Manager Web\.

- 8 Aprire il file `Web.config` in un editor di testo.
- 9 Individuare la sezione `repository server`.

```
<repository server="localhost" database="vCAC" store="https://vcac.example.com/" />
```

- 10 Aggiungere il comando `user` del database.

`user=DATABASE_USER password=DATABASE_PASSWORD`. Ad esempio:

```
<repository server="localhost" database="vCAC" user="sqlUser" password="sqlPassword"
store="https://vcac.example.com/" />
```

- 11 Salvare e chiudere il file.
- 12 Avviare il servizio di vCloud Automation Center.

Da questo momento, in fase di runtime verrà utilizzata l'autenticazione del server SQL.

Passi successivi

Riavviare Internet Information Service.

Verifica dei servizi di IaaS

Dopo l'installazione, l'amministratore di sistema verifica che i servizi di IaaS siano in esecuzione. Se i servizi sono in esecuzione, l'installazione ha esito positivo.

Procedura

- 1 Dal desktop Windows della macchina IaaS, selezionare **Strumenti di amministrazione > Servizi**.
- 2 Individuare i seguenti servizi e verificare che il loro stato sia **Avviato** e che il Tipo di avvio impostato sia **Automatico**.
 - VMware DEM – Orchestrator – *Nome* dove *Nome* è la stringa specificata nella casella **DEM Name** durante l'installazione.
 - VMware DEM – Worker – *Nome* dove *Nome* è la stringa specificata nella casella **DEM Name** durante l'installazione.
 - VMware vCloud Automation Center Agent *Nome agente*
 - VMware vCloud Automation Center Service
- 3 Chiudere la finestra **Servizi**.

Installazione degli agenti

vRealize Automation utilizza gli agenti per integrarsi con i sistemi esterni. Un amministratore di sistema può selezionare agenti da installare per comunicare con altre piattaforme di virtualizzazione.

vRealize Automation utilizza i tipi di agenti seguenti per gestire sistemi esterni:

- agenti Hypervisor proxy (vSphere, server Citrix Xen e server Microsoft Hyper-V)
- agenti di integrazione External Provisioning Infrastructure (EPI)
- agenti Virtual Desktop Infrastructure (VDI)
- agenti Windows Management Instrumentation (WMI)

È possibile installare più agenti per un singolo endpoint a scopo di alta disponibilità. Installare ciascun agente ridondante su un server diverso, ma denominare e configurare gli agenti in modo identico. Agenti ridondanti offrono un certo grado di tolleranza agli errori, ma non offrono failover. Se ad esempio si installano due agenti di vSphere, uno sul server A e uno sul server B, e il server A diventa non disponibile, l'agente installato sul B continua a elaborare gli elementi di lavoro. Ma l'agente del server B non può completare l'elaborazione di un elemento di lavoro che l'agente del server A ha già iniziato.

È possibile installare un agente di vSphere come parte dell'installazione minima, ma dopo l'installazione è possibile anche aggiungere altri agenti, incluso un altro agente di vSphere. In una distribuzione distribuita è possibile procedere con l'installazione di tutti gli agenti dopo aver completato l'installazione distribuita di base. Gli agenti installati dipendono dalle risorse presenti nell'infrastruttura.

Per informazioni sull'uso degli agenti di vSphere, vedere [Requisiti dell'agente di vSphere](#).

Impostare i criteri di esecuzione di PowerShell su RemoteSigned

È necessario impostare i criteri di esecuzione della PowerShell da Restricted a RemoteSigned o Unrestricted per consentire l'esecuzione degli script della PowerShell locale.

Prerequisiti

- Accedere come amministratore di Windows.
- Verificare che Microsoft PowerShell sia installato sull'host d'installazione prima di installare l'agente. La versione richiesta dipende dal sistema operativo dell'host d'installazione. Consultare la Guida e supporto tecnico di Microsoft.
- Per ulteriori informazioni sui criteri di esecuzione di MS PowerShell, eseguire `help about_signing` o `help Set-ExecutionPolicy` al prompt dei comandi di PowerShell.

Procedura

- 1 Scegliere **Start > Tutti i programmi > Windows PowerShell versione > Windows PowerShell**.
- 2 Per RemoteSigned, eseguire `Set-ExecutionPolicy RemoteSigned`.
- 3 Per Unrestricted, eseguire `Set-ExecutionPolicy Unrestricted`.
- 4 Verificare che il comando non restituisca errori.
- 5 Digitare **Exit** al prompt dei comandi della PowerShell.

Scelta dello scenario d'installazione degli agenti

Gli agenti che è necessario installare dipendono dai sistemi esterni con cui si pianifica di integrare.

Tavola 4-16. Scelta dello scenario per un agente

Scenario di integrazione	Requisiti dell'agente e procedura
Provisioning di macchine cloud tramite l'integrazione con un ambiente cloud quale Amazon Web Services o Red Hat Enterprise Linux OpenStack Platform.	Non è necessario installare un agente.
Provisioning di macchine virtuali tramite l'integrazione con un ambiente vSphere.	Installazione e configurazione dell'agente proxy per vSphere
Provisioning di macchine virtuali tramite l'integrazione con un ambiente Microsoft Hyper-V Server.	Installazione dell'agente proxy per Hyper-V o XenServer
Provisioning di macchine virtuali tramite l'integrazione con un ambiente XenServer.	<ul style="list-style-type: none"> ■ Installazione dell'agente proxy per Hyper-V o XenServer ■ Installazione dell'agente EPI per Citrix
Provisioning di macchine virtuali tramite l'integrazione con un ambiente XenDesktop.	<ul style="list-style-type: none"> ■ Installazione dell'agente VDI per XenDesktop ■ Installazione dell'agente EPI per Citrix
Esecuzione di script Visual Basic per eseguire passaggi aggiuntivi nel processo di provisioning, prima o dopo il provisioning di una macchina o in fase di deprovisioning.	Installazione dell'agente EPI per Visual Basic Scripting
Raccolta di dati da macchine Windows di cui è stato eseguito il provisioning, ad esempio lo stato di Active Directory del proprietario di una macchina.	Installazione dell'agente WMI per le richieste WMI remote
Provisioning di macchine virtuali tramite l'integrazione con qualsiasi altra piattaforma virtuale supportata.	Non è necessario installare un agente.

Posizione d'installazione dell'agente e requisiti

Gli amministratori di sistema in genere installano gli agenti sul server vRealize Automation che ospita il componente del servizio di gestione attivo.

Se un agente viene installato su un altro host, la configurazione di rete deve consentire la comunicazione tra l'agente e la macchina d'installazione dei servizi di gestione.

Ciascun agente viene installato sotto un nome univoco nella propria directory, `Agents\nomeagente`, sotto la directory d'installazione di vRealize Automation (in genere `Programmi (x86)\VMware\vCAC`), con la rispettiva configurazione memorizzata nel file `VRMAgent.exe.config` in quella stessa directory.

Installazione e configurazione dell'agente proxy per vSphere

Gli amministratori di sistema possono installare gli agenti proxy per comunicare con istanze server di vSphere. Gli agenti rilevano la presenza di lavoro disponibile, recuperano informazioni sugli host e riportano gli elementi di lavoro completati e altri cambi di stato degli host.

Requisiti dell'agente di vSphere

Le credenziali dell'endpoint vSphere, o le credenziali con cui viene eseguito il servizio dell'agente, devono consentire l'accesso amministrativo all'host d'installazione. Agenti di vSphere multipli devono soddisfare i requisiti di configurazione di vRealize Automation.

Credenziali

Quando si crea un endpoint che rappresenta l'istanza di vCenter Server da gestire mediante un agente di vSphere, l'agente può utilizzare le credenziali con cui è eseguito il servizio per interagire con vCenter Server o specificare credenziali separate per l'endpoint.

La tabella seguente elenca dettagliatamente le autorizzazioni che devono avere le credenziali dell'endpoint vSphere per gestire un'istanza di vCenter Server.

Tavola 4-17. Autorizzazioni richieste per consentire all'agente di vSphere di gestire l'istanza di vCenter Server

Valore attributo		Autorizzazione
Datastore		Spazio allocato
		Sfoglia datastore
Cartella		Crea cartella
		Elimina cartella
Globale		Gestisci attributi personalizzati
		Imposta attributo personalizzato
Rete		Assegna rete
Autorizzazioni		Modifica autorizzazione
Risorsa		Assegna VM a pool di risorse
		Migrazione macchina virtuale spenta
		Migrazione macchina virtuale accesa
Macchina virtuale	Inventario	Crea da esistente
		Crea nuovo
		Migrazione macchina virtuale accesa
		Sposta
		Rimuovi
	Interazione	Configura supporto CD
		Interazione console
		Connessione dispositivo
		Spegni
		Accendi
		Reimposta
		Sospendi

Tavola 4-17. Autorizzazioni richieste per consentire all'agente di vSphere di gestire l'istanza di vCenter Server (Continua)

Valore attributo	Autorizzazione
Configurazione	Installazione strumenti
	Aggiungi disco esistente
	Aggiungi nuovo disco
	Aggiungi o rimuovi
	Rimuovi disco
	Avanzate
	Cambia numero CPU
	Cambia risorsa
	Impostazioni disco virtuale estese dispositivo
	Traccia cambiamenti disco
	Memoria
	Modifica impostazioni dispositivo
	Rinomina
	Imposta annotazione (versione 5.0 e successive)
	Impostazioni
Provisioning	Posizionamento file di swap
	Personalizza
	Clona modello
	Clona macchina virtuale
	Distribuisci modello
Stato	Leggi specifiche di personalizzazione
	Crea snapshot
	Rimuovi snapshot
	Ripristina snapshot

Disabilitare o riconfigurare qualsiasi software di terze parti esterno a vRealize Automation in grado di cambiare lo stato di alimentazione delle macchine virtuali. Cambiamenti di questo tipo possono interferire con la gestione del ciclo di vita delle macchine tramite vRealize Automation.

Installazione dell'agente di vSphere

Installare un agente di vSphere per gestire istanze di vCenter Server. Per ottenere alta disponibilità, è possibile installare un secondo agente di vSphere ridondante per la stessa istanza di vCenter Server. È necessario denominare e configurare esattamente allo stesso modo entrambi gli agenti di vSphere, installandoli su macchine differenti.

Prerequisiti

- Siano installati i componenti di IaaS, inclusi il servizio di gestione e il sito Web.
- Verificare di aver completato tutti i [Requisiti dell'agente di vSphere](#).
- Se è stato già creato un endpoint di vSphere da utilizzare con questo agente, prendere nota del nome dell'endpoint.
- [Download del programma d'installazione di IaaS](#).

Procedura

- 1 Fare clic con il pulsante destro del mouse sul file d'installazione `setup__vra-va-hostname.domain.name@5480.exe` e scegliere **Esegui come amministratore**.
- 2 Fare clic su **Avanti**.
- 3 Accettare il contratto di licenza e fare clic su **Avanti**.
- 4 Nella pagina di accesso, inserire le credenziali di amministratore per vRealize Automation appliance e verificare il certificato SSL.
 - a Specificare il nome utente, ovvero **root**, e la password.
Questa è la password che è stata immessa quando è stata distribuita la vRealize Automation appliance.
 - b Selezionare **Accetta certificato**.
 - c Fare clic su **Visualizza certificato**.
Confrontare l'identificazione digitale del certificato con quella impostata per la vRealize Automation appliance. È possibile visualizzare il certificato della vRealize Automation appliance nel browser client quando si accede alla console di gestione sulla porta 5480.
- 5 Selezionare **Installazione personalizzata** nella pagina Tipo di installazione.
- 6 Selezionare **Selezione componenti** on the Tipo di installazione page.
- 7 Accettare la posizione d'installazione radice o fare clic su **Cambia** e selezionare un percorso d'installazione diverso.
- 8 Fare clic su **Avanti**.
- 9 Accedere con privilegi di **amministratore** per i servizi Windows sulla macchina d'installazione.
Il servizio deve essere in esecuzione sulla stessa macchina d'installazione.
- 10 Fare clic su **Avanti**.
- 11 Selezionare vSphere dall'elenco **Tipo di agente**.

12 Inserire un identificatore per questo agente nella casella di testo **Nome agente**.

Mantenere un registro contenente il nome dell'agente, le credenziali, il nome dell'endpoint e l'istanza della piattaforma per ciascun agente. Queste informazioni sono necessarie per configurare gli endpoint e aggiungere host in futuro.

Importante: non duplicare i nomi degli agenti, se non nel caso di un'installazione di agenti ridondanti configurati in modo identico a scopo di alta disponibilità.

Opzione	Descrizione
Installazione di agenti ridondanti	Installare gli agenti ridondanti su server diversi, ma denominarli e configurarli in modo identico per fornire alta disponibilità.
Installazione di un agente singolo	Selezionare un nome univoco per questo agente.

13 Configurare una connessione al componente servizio di gestione.

Opzione	Descrizione
Se si utilizza il bilanciamento del carico	Specificare il nome di dominio completo e il numero di porta del bilanciamento del carico relativo al componente servizio di gestione. Ad esempio manager-load-balancer.eng.mycompany.com:443 . Gli indirizzi IP non vengono riconosciuti.
Senza bilanciamento del carico	Specificare il nome di dominio completo e il numero di porta della macchina su cui è stato installato il componente servizio di gestione. Ad esempio manager_service.mycompany.com:443 . Gli indirizzi IP non vengono riconosciuti.

La porta predefinita è 443.

14 Configurare una connessione al componente sito Web del Manager.

Opzione	Descrizione
Se si utilizza il bilanciamento del carico	Specificare il nome di dominio completo e il numero di porta del bilanciamento del carico relativo al componente servizio Web del Manager. Ad esempio website-load-balancer.eng.mycompany.com:443 . Gli indirizzi IP non vengono riconosciuti.
Senza bilanciamento del carico	Specificare il nome di dominio completo e il numero di porta della macchina su cui è stato installato il componente sito Web del Manager. Ad esempio website_component.mycompany.com:443 . Gli indirizzi IP non vengono riconosciuti.

La porta predefinita è 443.

15 Fare clic su **Prova** per verificare la connettività con ciascun host.**16** Specificare il nome dell'endpoint.

Il nome dell'endpoint configurato in vRealize Automation deve corrispondere al nome dell'endpoint fornito all'agente proxy di vSphere durante l'installazione o l'endpoint non potrà funzionare.

17 Fare clic su **Aggiungi**.**18** Fare clic su **Avanti**.

19 Fare clic su **Installa** per iniziare l'installazione.

Dopo qualche minuto viene visualizzato il messaggio di installazione eseguita.

20 Fare clic su **Avanti**.

21 Fare clic su **Fine**.

22 Verificare che l'operazione di installazione sia stata eseguita correttamente.

23 (Facoltativo) Aggiungere più agenti con configurazioni differenti e un endpoint sullo stesso sistema.

Passi successivi

[Configurazione dell'agente di vSphere.](#)

Configurazione dell'agente di vSphere

È possibile utilizzare l'utilità degli agenti proxy per modificare le configurazioni iniziali crittografate nei file di configurazione degli agenti, oppure per cambiare il criterio di eliminazione delle macchine per le piattaforme di virtualizzazione.

Prerequisiti

Accedere in qualità di **amministratore di sistema** alla macchina in cui è stato installato l'agente.

Procedura

1 Aprire una console di comando di Windows come amministratore.

2 Aprire la directory d'installazione degli agenti.

Ad esempio `cd Program Files (x86)\VMware\VCAC\CD_Agents\agent_name`.

3 (Facoltativo) Immettere il comando `DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config get` per visualizzare le impostazioni di configurazione correnti.

Il seguente è un esempio dell'output del comando:

```
managementEndpointName: VCendpoint doDeletes: True
```

4 (Facoltativo) Immettere il comando `set managementEndpointName` per cambiare il nome dell'endpoint generico configurato durante l'installazione.

Ad esempio `DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set managementEndpointName My Endpoint`.

Modificando questa proprietà è possibile rinominare l'endpoint generico all'interno di vRealize Automation invece di modificare gli endpoint.

- 5 (Facoltativo) Immettere il comando `set doDeletes` per configurare il criterio di eliminazione delle macchine virtuali.

Ad esempio, `DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set doDeletes false`.

Opzione	Descrizione
true	(Predefinito) Le macchine virtuali eliminate in vRealize Automation da vCenter Server vengono cancellate.
false	Le macchine virtuali eliminate in vRealize Automation vengono spostate nella directory <code>VRMDeleted</code> in vCenter Server.

- 6 Scegliere **Start > Strumenti di amministrazione > Servizi** e riavviare il servizio vRealize Automation Agent – *agentname*.

Passi successivi

È possibile installare e configurare un agente ridondante per l'endpoint a scopo di alta disponibilità. Installare ciascun agente ridondante su un server diverso, ma denominare e configurare gli agenti in modo identico.

Installazione dell'agente proxy per Hyper-V o XenServer

Gli amministratori di sistema possono installare gli agenti proxy per comunicare con istanze server di Hyper-V e XenServer. Gli agenti rilevano la presenza di lavoro disponibile, recuperano informazioni sugli host e riportano gli elementi di lavoro completati e altri cambi di stato degli host.

Requisiti di Hyper-V e XenServer

Per installare gli agenti proxy Hypervisor di Hyper-V sono necessarie le credenziali di amministratore di sistema.

Le credenziali con cui eseguire il servizio dell'agente devono consentire l'accesso amministrativo all'host d'installazione.

Sono necessarie credenziali di livello amministrativo per tutte le istanze di XenServer o Hyper-V sugli host che dovranno essere gestiti mediante l'agente.

Se si utilizzano pool Xen, tutti i nodi all'interno del pool Xen devono essere identificati dai propri nomi di dominio completi.

Nota: per impostazione predefinita, Hyper-V non è configurato per la gestione remota. Un agente proxy Hyper-V di vRealize Automation non può comunicare con un server Hyper-V se non è stata attivata la gestione remota.

Consultare la documentazione di Microsoft Windows Server per informazioni su come configurare Hyper-V per la gestione remota.

Installazione dell'agente di Hyper-V o XenServer

L'agente di Hyper-V gestisce le istanze server di Hyper-V. L'agente di XenServer gestisce le istanze server di XenServer.

Prerequisiti

- Siano installati i componenti di IaaS, inclusi il servizio di gestione e il sito Web.
- [Download del programma d'installazione di IaaS](#).
- Verificare che gli agenti proxy Hypervisor di Hyper-V abbiano credenziali di amministratore di sistema.
- Verificare che le credenziali con cui eseguire il servizio dell'agente abbiano accesso amministrativo all'host d'installazione.
- Verificare che tutte le istanze di XenServer o Hyper-V sugli host da gestire mediante l'agente abbiano credenziali di livello amministrativo.
- Se si utilizzano pool Xen, tenere presente che tutti i nodi all'interno del pool Xen devono essere identificati dai propri nomi di dominio completi.

vRealize Automation non può gestire né comunicare con qualsiasi nodo che non sia identificato dal proprio nome di dominio completo all'interno del pool Xen.

- Configurare Hyper-V per la gestione remota per abilitare la comunicazione del server di Hyper-V con gli agenti proxy Hyper-V di vRealize Automation.

Consultare la documentazione di Microsoft Windows Server per informazioni su come configurare Hyper-V per la gestione remota.

Procedura

- 1 Fare clic con il pulsante destro del mouse sul file d'installazione `setup__vra-va-hostname.domain.name@5480.exe` e scegliere **Esegui come amministratore**.
- 2 Fare clic su **Avanti**.
- 3 Accettare il contratto di licenza e fare clic su **Avanti**.

- 4 Nella pagina di accesso, inserire le credenziali di amministratore per vRealize Automation appliance e verificare il certificato SSL.

- a Specificare il nome utente, ovvero **root**, e la password.

Questa è la password che è stata immessa quando è stata distribuita la vRealize Automation appliance.

- b Selezionare **Accetta certificato**.

- c Fare clic su **Visualizza certificato**.

Confrontare l'identificazione digitale del certificato con quella impostata per la vRealize Automation appliance. È possibile visualizzare il certificato della vRealize Automation appliance nel browser client quando si accede alla console di gestione sulla porta 5480.

- 5 Selezionare **Installazione personalizzata** nella pagina Tipo di installazione.

- 6 Selezionare **Selezione componenti** on the Tipo di installazione page.

- 7 Accettare la posizione d'installazione radice o fare clic su **Cambia** e selezionare un percorso d'installazione diverso.

- 8 Fare clic su **Avanti**.

- 9 Accedere con privilegi di **amministratore** per i servizi Windows sulla macchina d'installazione.

Il servizio deve essere in esecuzione sulla stessa macchina d'installazione.

- 10 Fare clic su **Avanti**.

- 11 Selezionare l'agente dall'elenco **Tipo di agente**.

- Xen
- Hyper-V

- 12 Inserire un identificatore per questo agente nella casella di testo **Nome agente**.

Mantenere un registro contenente il nome dell'agente, le credenziali, il nome dell'endpoint e l'istanza della piattaforma per ciascun agente. Queste informazioni sono necessarie per configurare gli endpoint e aggiungere host in futuro.

Importante: non duplicare i nomi degli agenti, se non nel caso di un'installazione di agenti ridondanti configurati in modo identico a scopo di alta disponibilità.

Opzione	Descrizione
Installazione di agenti ridondanti	Installare gli agenti ridondanti su server diversi, ma denominarli e configurarli in modo identico per fornire alta disponibilità.
Installazione di un agente singolo	Selezionare un nome univoco per questo agente.

- 13 Comunicare il **Nome agente** all'amministratore di IaaS che configura gli endpoint.

Per consentire l'accesso e la raccolta dati, l'endpoint deve essere collegato all'agente che è stato configurato per esso.

14 Configurare una connessione al componente servizio di gestione.

Opzione	Descrizione
Se si utilizza il bilanciamento del carico	Specificare il nome di dominio completo e il numero di porta del bilanciamento del carico relativo al componente servizio di gestione. Ad esempio manager-load-balancer.eng.mycompany.com:443 . Gli indirizzi IP non vengono riconosciuti.
Senza bilanciamento del carico	Specificare il nome di dominio completo e il numero di porta della macchina su cui è stato installato il componente servizio di gestione. Ad esempio manager_service.mycompany.com:443 . Gli indirizzi IP non vengono riconosciuti.

La porta predefinita è 443.

15 Configurare una connessione al componente sito Web del Manager.

Opzione	Descrizione
Se si utilizza il bilanciamento del carico	Specificare il nome di dominio completo e il numero di porta del bilanciamento del carico relativo al componente servizio Web del Manager. Ad esempio website-load-balancer.eng.mycompany.com:443 . Gli indirizzi IP non vengono riconosciuti.
Senza bilanciamento del carico	Specificare il nome di dominio completo e il numero di porta della macchina su cui è stato installato il componente sito Web del Manager. Ad esempio website_component.mycompany.com:443 . Gli indirizzi IP non vengono riconosciuti.

La porta predefinita è 443.

16 Fare clic su **Prova** per verificare la connettività con ciascun host.**17** Inserire le credenziali di un utente dotato di autorizzazioni di livello amministrativo sull'istanza del server gestito.**18** Fare clic su **Aggiungi**.**19** Fare clic su **Avanti**.**20** (Facoltativo) Aggiungere un altro agente.

Ad esempio, è possibile aggiungere un agente XEN se precedentemente è stato aggiunto l'agente Hyper-V.

21 Fare clic su **Installa** per iniziare l'installazione.

Dopo qualche minuto viene visualizzato il messaggio di installazione eseguita.

22 Fare clic su **Avanti**.**23** Fare clic su **Fine**.**24** Verificare che l'operazione di installazione sia stata eseguita correttamente.

Passi successivi

È possibile installare e configurare un agente ridondante per l'endpoint a scopo di alta disponibilità. Installare ciascun agente ridondante su un server diverso, ma denominare e configurare gli agenti in modo identico.

[Configurazione dell'agente Hyper-V o XenServer.](#)

Configurazione dell'agente Hyper-V o XenServer

Un amministratore di sistema può modificare le impostazioni di configurazione degli agenti proxy, come ad esempio il criterio di eliminazione per le piattaforme virtualizzate. È possibile utilizzare l'utilità degli agenti proxy per modificare le configurazioni iniziali crittografate nei file di configurazione degli agenti.

Prerequisiti

Accedere in qualità di **amministratore di sistema** alla macchina in cui è stato installato l'agente.

Procedura

- 1 Cambiare la directory d'installazione degli agenti, dove *agent_name* è la directory contenente l'agente proxy, che è anche il nome sotto cui è installato l'agente.

```
cd Programmi (x86)\VMware\VCAC Agents\agent_name
```

- 2 Visualizzare le impostazioni di configurazione correnti.

```
Immettere DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config get
```

Il seguente è un esempio dell'output del comando:

```
Username: XSadmin
```

- 3 Immettere il comando set per cambiare una proprietà, dove *property* è una delle opzioni elencate nella tabella.

```
DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set property value
```

Se si omette *value*, l'utilità visualizza la richiesta di un nuovo valore.

Proprietà	Descrizione
username	Nome utente che rappresenta le credenziali di livello amministrativo per il server XenServer o Hyper-V con cui comunica l'agente.
password	Password relativa al nome utente di livello amministrativo.

- 4 Scegliere **Start > Strumenti di amministrazione > Servizi** e riavviare il servizio vRealize Automation Agent – *agentname*.

Esempio: Cambiare le credenziali di livello amministrativo

Immettere il comando seguente per cambiare le credenziali di livello amministrativo per la piattaforma di virtualizzazione specificata durante l'installazione dell'agente.

```
DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set username jsmith
```

```
DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set password
```

Passi successivi

È possibile installare e configurare un agente ridondante per l'endpoint a scopo di alta disponibilità. Installare ciascun agente ridondante su un server diverso, ma denominare e configurare gli agenti in modo identico.

Installazione dell'agente VDI per XenDesktop

vRealize Automation utilizza gli agenti della PowerShell di Virtual Desktop Integration (VDI) per registrare le macchine XenDesktop di cui esegue il provisioning con sistemi di gestione desktop esterni.

L'agente di integrazione di VDI offre ai proprietari di macchine registrate una connessione diretta all'interfaccia Web di XenDesktop. È possibile installare un agente VDI come agente dedicato per interagire con un singolo Desktop Delivery Controller (DDC) o come agente generale che può interagire con più DDC.

Requisiti di XenDesktop

Gli amministratori di sistema possono installare un agente Virtual Desktop Infrastructure (VDI) per integrare i server XenDesktop in vRealize Automation.

È possibile installare un agente VDI generale per interagire con server multipli. Se si installa un agente dedicato per server per ragioni di bilanciamento del carico o autorizzazione, è necessario fornire il nome del server XenDesktop DDC quando si installa l'agente. Un agente dedicato può gestire solo richieste di registrazione indirizzate al server specificato nella sua configurazione.

Consultare *Matrice di supporto di vRealize Automation* sul sito Web di VMware per conoscere le versioni supportate di XenDesktop per server XenDesktop DDC.

Installazione di host e credenziali

Le credenziali con cui viene eseguito l'agente devono consentire l'accesso amministrativo a tutti i server XenDesktop DDC con cui interagisce.

Requisiti di XenDesktop

Il nome fornito all'host di XenServer sul server XenDesktop deve coincidere con l'UUID del pool Xen in XenCenter. Vedere [Impostazione del nome host di XenServer](#) per ulteriori informazioni.

Ogni server XenDesktop DDC con cui si intende registrare macchine deve essere configurato nel modo seguente:

- Il tipo di gruppo/catalogo deve essere impostato su **Esistente** per l'uso con vRealize Automation.

- Il nome di un host di vCenter Server su un server DDC deve corrispondere al nome delle istanze vCenter Server come immesse nell'endpoint vSphere di vRealize Automation, senza il dominio. L'endpoint deve essere configurato con un nome di dominio completo e non con un indirizzo IP. Se ad esempio l'indirizzo dell'endpoint è `https://virtual-center27.domain/sdk`, il nome dell'host sul server DDC deve essere impostato su `virtual-center27`.

Se l'endpoint di vSphere di vRealize Automation è stato configurato con un indirizzo IP, è necessario cambiarlo per utilizzare un nome di dominio completo. Vedere *Configurazione IaaS* per ulteriori informazioni sulla configurazione degli endpoint.

Requisiti dell'host dell'agente XenDesktop

Il SDK di Citrix XenDesktop deve essere installato. Il SDK di XenDesktop è incluso nel disco d'installazione di XenDesktop.

Verificare che Microsoft PowerShell sia installato sull'host d'installazione prima di installare l'agente. La versione richiesta dipende dal sistema operativo dell'host d'installazione. Consultare la Guida e supporto tecnico di Microsoft.

I criteri di esecuzione di MS PowerShell siano impostati su `RemoteSigned` o `Unrestricted`. Vedere [Impostare i criteri di esecuzione di PowerShell su RemoteSigned](#).

Per ulteriori informazioni sui criteri di esecuzione di MS PowerShell, eseguire `help about_signing` o `help Set-ExecutionPolicy` al prompt dei comandi di PowerShell.

Impostazione del nome host di XenServer

In XenDesktop, il nome fornito all'host XenServer sul server XenDesktop deve corrispondere all'UUID del Xen Pool in XenCenter. Se non è configurato alcun XenPool, il nome deve corrispondere all'UUID dello stesso XenServer.

Procedura

- 1 In Citrix XenCenter, selezionare XenPool o XenServer autonomo e fare clic sulla scheda **General**. Registrare l'UUID.
- 2 Quando si aggiunge lo XenServer Pool o l'host autonomo a XenDesktop, digitare l'UUID registrato nel passaggio precedente come nome della **Connection**.

Installazione dell'agente di XenDesktop

Gli agenti della PowerShell di Virtual Desktop Integration (VDI) si integrano con un sistema desktop virtuale esterno, ad esempio XenDesktop e Citrix. Utilizzare un agente della PowerShell di VDI per gestire la macchina XenDesktop.

Prerequisiti

- Siano installati i componenti di IaaS, inclusi il servizio di gestione e il sito Web.
- Verificare che l'ambiente soddisfi i [Requisiti di XenDesktop](#).
- [Download del programma d'installazione di IaaS](#).

Procedura

- 1 Fare clic con il pulsante destro del mouse sul file d'installazione `setup__vra-va-hostname.domain.name@5480.exe` e scegliere **Esegui come amministratore**.
- 2 Fare clic su **Avanti**.
- 3 Accettare il contratto di licenza e fare clic su **Avanti**.
- 4 Nella pagina di accesso, inserire le credenziali di amministratore per vRealize Automation appliance e verificare il certificato SSL.
 - a Specificare il nome utente, ovvero **root**, e la password.
 Questa è la password che è stata immessa quando è stata distribuita la vRealize Automation appliance.
 - b Selezionare **Accetta certificato**.
 - c Fare clic su **Visualizza certificato**.
 Confrontare l'identificazione digitale del certificato con quella impostata per la vRealize Automation appliance. È possibile visualizzare il certificato della vRealize Automation appliance nel browser client quando si accede alla console di gestione sulla porta 5480.
- 5 Fare clic su **Avanti**.
- 6 Selezionare **Installazione personalizzata** nella pagina Tipo di installazione.
- 7 Selezionare **Agenti proxy** nel riquadro di selezione dei componenti.
- 8 Accettare la posizione d'installazione radice o fare clic su **Cambia** e selezionare un percorso d'installazione diverso.
- 9 Fare clic su **Avanti**.
- 10 Accedere con privilegi di **amministratore** per i servizi Windows sulla macchina d'installazione.
 Il servizio deve essere in esecuzione sulla stessa macchina d'installazione.
- 11 Fare clic su **Avanti**.
- 12 Selezionare **VdiPowerShell** dall'elenco **Tipo di agente**.

13 Inserire un identificatore per questo agente nella casella di testo **Nome agente**.

Mantenere un registro contenente il nome dell'agente, le credenziali, il nome dell'endpoint e l'istanza della piattaforma per ciascun agente. Queste informazioni sono necessarie per configurare gli endpoint e aggiungere host in futuro.

Importante: non duplicare i nomi degli agenti, se non nel caso di un'installazione di agenti ridondanti configurati in modo identico a scopo di alta disponibilità.

Opzione	Descrizione
Installazione di agenti ridondanti	Installare gli agenti ridondanti su server diversi, ma denominarli e configurarli in modo identico per fornire alta disponibilità.
Installazione di un agente singolo	Selezionare un nome univoco per questo agente.

14 Configurare una connessione al componente servizio di gestione.

Opzione	Descrizione
Se si utilizza il bilanciamento del carico	Specificare il nome di dominio completo e il numero di porta del bilanciamento del carico relativo al componente servizio di gestione. Ad esempio manager-load-balancer.eng.mycompany.com:443 . Gli indirizzi IP non vengono riconosciuti.
Senza bilanciamento del carico	Specificare il nome di dominio completo e il numero di porta della macchina su cui è stato installato il componente servizio di gestione. Ad esempio manager_service.mycompany.com:443 . Gli indirizzi IP non vengono riconosciuti.

La porta predefinita è 443.

15 Configurare una connessione al componente sito Web del Manager.

Opzione	Descrizione
Se si utilizza il bilanciamento del carico	Specificare il nome di dominio completo e il numero di porta del bilanciamento del carico relativo al componente servizio Web del Manager. Ad esempio website-load-balancer.eng.mycompany.com:443 . Gli indirizzi IP non vengono riconosciuti.
Senza bilanciamento del carico	Specificare il nome di dominio completo e il numero di porta della macchina su cui è stato installato il componente sito Web del Manager. Ad esempio website_component.mycompany.com:443 . Gli indirizzi IP non vengono riconosciuti.

La porta predefinita è 443.

16 Fare clic su **Prova** per verificare la connettività con ciascun host.**17** Selezionare la **Versione VDI**.**18** Immettere il nome di dominio completo del server gestito nella casella di testo **Server VDI**.**19** Fare clic su **Aggiungi**.**20** Fare clic su **Avanti**.

21 Fare clic su **Installa** per iniziare l'installazione.

Dopo qualche minuto viene visualizzato il messaggio di installazione eseguita.

22 Fare clic su **Avanti**.

23 Fare clic su **Fine**.

24 Verificare che l'operazione di installazione sia stata eseguita correttamente.

25 (Facoltativo) Aggiungere più agenti con configurazioni differenti e un endpoint sullo stesso sistema.

Passi successivi

È possibile installare e configurare un agente ridondante per l'endpoint a scopo di alta disponibilità. Installare ciascun agente ridondante su un server diverso, ma denominare e configurare gli agenti in modo identico.

Installazione dell'agente EPI per Citrix

Gli agenti della PowerShell di External Provisioning Integration (EPI) consentono di integrare macchine esterne Citrix nel processo di provisioning. L'agente EPI fornisce lo streaming on-demand delle immagini dei dischi Citrix da cui le macchine vengono avviate ed eseguite.

L'agente EPI dedicato interagisce con un singolo server di provisioning esterno. È necessario installare un agente EPI per ogni istanza di server di provisioning Citrix.

Requisiti di Citrix Provisioning Server

Utilizzando agenti EPI (External Provisioning Infrastructure), gli amministratori di sistema possono integrare Citrix Provisioning Server e abilitare l'utilizzo di script Visual Basic nel processo di provisioning.

Posizione d'installazione e credenziali

Installare l'agente sull'host PVS per istanze Citrix Provisioning Services. Verificare che l'host d'installazione soddisfi i [Requisiti dell'host dell'agente Citrix](#) prima di installare l'agente.

Sebbene generalmente un agente EPI possa interagire con più server, Citrix Provisioning Server richiede un agente EPI dedicato. È necessario installare un agente EPI per ogni istanza di Citrix Provisioning Server, fornendo il nome del server che lo esegue. Le credenziali con cui viene eseguito l'agente devono consentire l'accesso amministrativo all'istanza di Citrix Provisioning Server.

Consultare la *Matrice di supporto di vRealize Automation* per conoscere le versioni di Citrix PVS supportate.

Requisiti dell'host dell'agente Citrix

Prima di installare l'agente, è necessario che sull'host d'installazione siano presenti PowerShell e Citrix Provisioning Services SDK. Consultare la *Matrice di supporto di vRealize Automation* sul sito Web di VMware per i dettagli.

Verificare che Microsoft PowerShell sia installato sull'host d'installazione prima di installare l'agente. La versione richiesta dipende dal sistema operativo dell'host d'installazione. Consultare la Guida e supporto tecnico di Microsoft.

È necessario assicurarsi che sia installato anche lo snap-in di PowerShell. Per ulteriori informazioni, vedere la *Citrix Provisioning Services PowerShell Programmer's Guide* sul sito Web di Citrix.

I criteri di esecuzione di MS PowerShell siano impostati su RemoteSigned o Unrestricted. Vedere [Impostare i criteri di esecuzione di PowerShell su RemoteSigned](#).

Per ulteriori informazioni sui criteri di esecuzione di MS PowerShell, eseguire `help about_signing` o `help Set-ExecutionPolicy` al prompt dei comandi di PowerShell.

Installazione dell'agente di Citrix

Gli agenti della PowerShell di External Provisioning Integration (EPI) integrano sistemi esterni nel processo di provisioning delle macchine. Utilizzare l'agente della PowerShell di EPI per integrare con il server di provisioning Citrix e consentire il provisioning di macchine mediante streaming di dischi on-demand.

Prerequisiti

- Siano installati i componenti di IaaS, inclusi il servizio di gestione e il sito Web.
- Verificare di aver soddisfatto tutti i [Requisiti di Citrix Provisioning Server](#).
- [Download del programma d'installazione di IaaS](#).

Procedura

- 1 Fare clic con il pulsante destro del mouse sul file d'installazione `setup__vra--va--hostname.domain.name@5480.exe` e scegliere **Esegui come amministratore**.
- 2 Fare clic su **Avanti**.
- 3 Accettare il contratto di licenza e fare clic su **Avanti**.
- 4 Nella pagina di accesso, inserire le credenziali di amministratore per vRealize Automation appliance e verificare il certificato SSL.
 - a Specificare il nome utente, ovvero **root**, e la password.
Questa è la password che è stata immessa quando è stata distribuita la vRealize Automation appliance.
 - b Selezionare **Accetta certificato**.
 - c Fare clic su **Visualizza certificato**.
Confrontare l'identificazione digitale del certificato con quella impostata per la vRealize Automation appliance. È possibile visualizzare il certificato della vRealize Automation appliance nel browser client quando si accede alla console di gestione sulla porta 5480.
- 5 Selezionare **Installazione personalizzata** nella pagina Tipo di installazione.

- 6 Selezionare **Selezione componenti** on the Tipo di installazione page.
- 7 Accettare la posizione d'installazione radice o fare clic su **Cambia** e selezionare un percorso d'installazione diverso.
- 8 Fare clic su **Avanti**.
- 9 Accedere con privilegi di **amministratore** per i servizi Windows sulla macchina d'installazione.
Il servizio deve essere in esecuzione sulla stessa macchina d'installazione.
- 10 Fare clic su **Avanti**.

- 11 Selezionare **EPIPowerShell** dall'elenco Tipo di agente.

- 12 Inserire un identificatore per questo agente nella casella di testo **Nome agente**.

Mantenere un registro contenente il nome dell'agente, le credenziali, il nome dell'endpoint e l'istanza della piattaforma per ciascun agente. Queste informazioni sono necessarie per configurare gli endpoint e aggiungere host in futuro.

Importante: non duplicare i nomi degli agenti, se non nel caso di un'installazione di agenti ridondanti configurati in modo identico a scopo di alta disponibilità.

Opzione	Descrizione
Installazione di agenti ridondanti	Installare gli agenti ridondanti su server diversi, ma denominarli e configurarli in modo identico per fornire alta disponibilità.
Installazione di un agente singolo	Selezionare un nome univoco per questo agente.

- 13 Configurare una connessione al componente servizio di gestione.

Opzione	Descrizione
Se si utilizza il bilanciamento del carico	Specificare il nome di dominio completo e il numero di porta del bilanciamento del carico relativo al componente servizio di gestione. Ad esempio manager-load-balancer.eng.mycompany.com:443 . Gli indirizzi IP non vengono riconosciuti.
Senza bilanciamento del carico	Specificare il nome di dominio completo e il numero di porta della macchina su cui è stato installato il componente servizio di gestione. Ad esempio manager_service.mycompany.com:443 . Gli indirizzi IP non vengono riconosciuti.

La porta predefinita è 443.

14 Configurare una connessione al componente sito Web del Manager.

Opzione	Descrizione
Se si utilizza il bilanciamento del carico	Specificare il nome di dominio completo e il numero di porta del bilanciamento del carico relativo al componente servizio Web del Manager. Ad esempio website-load-balancer.eng.mycompany.com:443 . Gli indirizzi IP non vengono riconosciuti.
Senza bilanciamento del carico	Specificare il nome di dominio completo e il numero di porta della macchina su cui è stato installato il componente sito Web del Manager. Ad esempio website_component.mycompany.com:443 . Gli indirizzi IP non vengono riconosciuti.

La porta predefinita è 443.

15 Fare clic su **Prova** per verificare la connettività con ciascun host.

16 Selezionare il tipo di EPI.

17 Immettere il nome di dominio completo del server gestito nella casella di testo **Server EPI**.

18 Fare clic su **Aggiungi**.

19 Fare clic su **Avanti**.

20 Fare clic su **Installa** per iniziare l'installazione.

Dopo qualche minuto viene visualizzato il messaggio di installazione eseguita.

21 Fare clic su **Avanti**.

22 Fare clic su **Fine**.

23 Verificare che l'operazione di installazione sia stata eseguita correttamente.

24 (Facoltativo) Aggiungere più agenti con configurazioni differenti e un endpoint sullo stesso sistema.

Passi successivi

È possibile installare e configurare un agente ridondante per l'endpoint a scopo di alta disponibilità. Installare ciascun agente ridondante su un server diverso, ma denominare e configurare gli agenti in modo identico.

Installazione dell'agente EPI per Visual Basic Scripting

Un amministratore di sistema può indicare script Visual Basic per eseguire passaggi aggiuntivi nel processo di provisioning, prima o dopo il provisioning di una macchina o in fase di deprovisioning di una macchina. Per poter eseguire script Visual Basic è necessario installare la PowerShell di External Provisioning Integration (EPI).

Gli script Visual Basic vengono specificati nel blueprint da cui viene eseguito il provisioning delle macchine. Questi script hanno accesso a tutte le proprietà personalizzate associate alla macchina e possono aggiornarne i valori. Il passaggio successivo nel workflow avrà quindi accesso a questi nuovi valori.

Ad esempio è possibile utilizzare uno script per generare certificati o token di sicurezza prima del provisioning e quindi utilizzare questi ultimi nel provisioning della macchina.

Per abilitare gli script nel provisioning è necessario installare un tipo di agente EPI specifico e collocare gli script da utilizzare all'interno del sistema su cui è installato l'agente.

Quando si esegue uno script, l'agente EPI passa allo script tutte le proprietà personalizzate delle macchine come argomenti. Per restituire valori delle proprietà aggiornati, inserire queste proprietà in un dizionario e chiamare una funzione di vRealize Automation. Nella sottodirectory degli script della directory d'installazione dell'agente EPI si può trovare uno script di esempio. Lo script è articolato in un'intestazione in cui vengono caricati tutti gli argomenti in un dizionario, un corpo in cui è possibile includere le proprie funzioni e una sezione finale per la restituzione dei valori delle proprietà personalizzate aggiornate.

Nota: è possibile installare più agenti EPI/VBScripts su server multipli ed eseguire il provisioning utilizzando un agente specifico e gli script Visual Basic sull'host di quell'agente. Se è questa la configurazione richiesta, contattare l'assistenza clienti di VMware.

Requisiti di Visual Basic Scripting

Gli amministratori di sistema possono installare agenti EPI (External Provisioning Infrastructure) per consentire l'impiego di script Visual Basic nel processo di provisioning.

Nella tabella seguente sono elencati i requisiti necessari per installare un agente EPI e consentire così l'uso di script Visual Basic nel processo di provisioning.

Tavola 4-18. Agenti EPI per Visual Basic Scripting

Requisito	Descrizione
Credenziali	Le credenziali con cui sarà eseguito l'agente devono consentire l'accesso amministrativo all'host d'installazione.
Microsoft PowerShell	Prima dell'installazione dell'agente è necessario installare Microsoft PowerShell sull'host d'installazione: la versione richiesta dipende dal sistema operativo dell'host d'installazione e potrebbe essere stata installata insieme al sistema operativo. Per ulteriori informazioni, visitare http://support.microsoft.com .
Criteri di esecuzione di MS PowerShell	<p>I criteri di esecuzione di MS PowerShell devono essere impostati su RemoteSigned o Unrestricted.</p> <p>Per informazioni sui criteri di esecuzione di PowerShell, eseguire uno dei seguenti comandi al prompt dei comandi della PowerShell:</p> <pre>help about_signing help Set-ExecutionPolicy</pre>

Installazione dell'agente per Visual Basic Scripting

Gli agenti della PowerShell di External Provisioning Integration (EPI) consentono di integrare sistemi esterni nel processo di provisioning delle macchine. Utilizzare un agente EPI per eseguire script Visual Basic e attuare operazioni aggiuntive durante il processo di provisioning.

Prerequisiti

- Siano installati i componenti di IaaS, inclusi il servizio di gestione e il sito Web.
- Verificare di aver soddisfatto tutti i [Requisiti di Visual Basic Scripting](#).
- [Download del programma d'installazione di IaaS](#).

Procedura

- 1 Fare clic con il pulsante destro del mouse sul file d'installazione `setup__vra-va-hostname.domain.name@5480.exe` e scegliere **Esegui come amministratore**.
- 2 Fare clic su **Avanti**.
- 3 Accettare il contratto di licenza e fare clic su **Avanti**.
- 4 Nella pagina di accesso, inserire le credenziali di amministratore per vRealize Automation appliance e verificare il certificato SSL.
 - a Specificare il nome utente, ovvero **root**, e la password.
Questa è la password che è stata immessa quando è stata distribuita la vRealize Automation appliance.
 - b Selezionare **Accetta certificato**.
 - c Fare clic su **Visualizza certificato**.
Confrontare l'identificazione digitale del certificato con quella impostata per la vRealize Automation appliance. È possibile visualizzare il certificato della vRealize Automation appliance nel browser client quando si accede alla console di gestione sulla porta 5480.
- 5 Selezionare **Installazione personalizzata** nella pagina Tipo di installazione.
- 6 Selezionare **Selezione componenti** on the Tipo di installazione page.
- 7 Accettare la posizione d'installazione radice o fare clic su **Cambia** e selezionare un percorso d'installazione diverso.
- 8 Fare clic su **Avanti**.
- 9 Accedere con privilegi di **amministratore** per i servizi Windows sulla macchina d'installazione.
Il servizio deve essere in esecuzione sulla stessa macchina d'installazione.
- 10 Fare clic su **Avanti**.
- 11 Selezionare **EPIPowerShell** dall'elenco Tipo di agente.

12 Inserire un identificatore per questo agente nella casella di testo **Nome agente**.

Mantenere un registro contenente il nome dell'agente, le credenziali, il nome dell'endpoint e l'istanza della piattaforma per ciascun agente. Queste informazioni sono necessarie per configurare gli endpoint e aggiungere host in futuro.

Importante: non duplicare i nomi degli agenti, se non nel caso di un'installazione di agenti ridondanti configurati in modo identico a scopo di alta disponibilità.

Opzione	Descrizione
Installazione di agenti ridondanti	Installare gli agenti ridondanti su server diversi, ma denominarli e configurarli in modo identico per fornire alta disponibilità.
Installazione di un agente singolo	Selezionare un nome univoco per questo agente.

13 Configurare una connessione al componente servizio di gestione.

Opzione	Descrizione
Se si utilizza il bilanciamento del carico	Specificare il nome di dominio completo e il numero di porta del bilanciamento del carico relativo al componente servizio di gestione. Ad esempio manager-load-balancer.eng.mycompany.com:443 . Gli indirizzi IP non vengono riconosciuti.
Senza bilanciamento del carico	Specificare il nome di dominio completo e il numero di porta della macchina su cui è stato installato il componente servizio di gestione. Ad esempio manager_service.mycompany.com:443 . Gli indirizzi IP non vengono riconosciuti.

La porta predefinita è 443.

14 Configurare una connessione al componente sito Web del Manager.

Opzione	Descrizione
Se si utilizza il bilanciamento del carico	Specificare il nome di dominio completo e il numero di porta del bilanciamento del carico relativo al componente servizio Web del Manager. Ad esempio website-load-balancer.eng.mycompany.com:443 . Gli indirizzi IP non vengono riconosciuti.
Senza bilanciamento del carico	Specificare il nome di dominio completo e il numero di porta della macchina su cui è stato installato il componente sito Web del Manager. Ad esempio website_component.mycompany.com:443 . Gli indirizzi IP non vengono riconosciuti.

La porta predefinita è 443.

15 Fare clic su **Prova** per verificare la connettività con ciascun host.**16** Selezionare il tipo di EPI.**17** Immettere il nome di dominio completo del server gestito nella casella di testo **Server EPI**.**18** Fare clic su **Aggiungi**.**19** Fare clic su **Avanti**.

20 Fare clic su **Installa** per iniziare l'installazione.

Dopo qualche minuto viene visualizzato il messaggio di installazione eseguita.

21 Fare clic su **Avanti**.

22 Fare clic su **Fine**.

23 Verificare che l'operazione di installazione sia stata eseguita correttamente.

24 (Facoltativo) Aggiungere più agenti con configurazioni differenti e un endpoint sullo stesso sistema.

Installazione dell'agente WMI per le richieste WMI remote

Per rendere operativa la gestione di dati e operazioni, l'amministratore di sistema abilita il protocollo Windows Management Instrumentation (WMI) e installa l'agente WMI su tutte le macchine Windows gestite. L'agente è deputato alla raccolta dei dati dalle macchine Windows, ad esempio lo stato di Active Directory del proprietario di una macchina.

Abilitazione delle richieste WMI remote su macchine Windows

Per utilizzare gli agenti WMI, sui server Windows gestiti è necessario abilitare le richieste WMI remote.

Procedura

- 1** In ogni dominio che contiene macchine virtuali Windows fornite in provisioning e gestite, creare un gruppo di Active Directory e aggiungervi le credenziali di servizio degli agenti WMI che eseguono richieste WMI remote sulle macchine di cui viene eseguito il provisioning.
- 2** Abilitare le richieste WMI remote per i gruppi di Active Directory contenenti le credenziali degli agenti su ogni macchina Windows fornita in provisioning.

Installazione dell'agente WMI

L'agente Windows Management Instrumentation (WMI) consente di raccogliere dati dalle macchine gestite Windows.

Prerequisiti

- Siano installati i componenti di IaaS, inclusi il servizio di gestione e il sito Web.
- Verificare che tutti i requisiti siano soddisfatti, vedere [Abilitazione delle richieste WMI remote su macchine Windows](#).
- [Download del programma d'installazione di IaaS](#).

Procedura

- 1** Fare clic con il pulsante destro del mouse sul file d'installazione `setup__vra-va-hostname.domain.name@5480.exe` e scegliere **Esegui come amministratore**.
- 2** Fare clic su **Avanti**.
- 3** Accettare il contratto di licenza e fare clic su **Avanti**.

- 4 Nella pagina di accesso, inserire le credenziali di amministratore per vRealize Automation appliance e verificare il certificato SSL.

- a Specificare il nome utente, ovvero **root**, e la password.

Questa è la password che è stata immessa quando è stata distribuita la vRealize Automation appliance.

- b Selezionare **Accetta certificato**.

- c Fare clic su **Visualizza certificato**.

Confrontare l'identificazione digitale del certificato con quella impostata per la vRealize Automation appliance. È possibile visualizzare il certificato della vRealize Automation appliance nel browser client quando si accede alla console di gestione sulla porta 5480.

- 5 Selezionare **Installazione personalizzata** nella pagina Tipo di installazione.
- 6 Selezionare **Selezione componenti** on the Tipo di installazione page.
- 7 Accettare la posizione d'installazione radice o fare clic su **Cambia** e selezionare un percorso d'installazione diverso.
- 8 Fare clic su **Avanti**.
- 9 Accedere con privilegi di **amministratore** per i servizi Windows sulla macchina d'installazione.
Il servizio deve essere in esecuzione sulla stessa macchina d'installazione.
- 10 Fare clic su **Avanti**.
- 11 Selezionare **WMI** dall'elenco **Tipo di agente**.
- 12 Inserire un identificatore per questo agente nella casella di testo **Nome agente**.

Mantenere un registro contenente il nome dell'agente, le credenziali, il nome dell'endpoint e l'istanza della piattaforma per ciascun agente. Queste informazioni sono necessarie per configurare gli endpoint e aggiungere host in futuro.

Importante: non duplicare i nomi degli agenti, se non nel caso di un'installazione di agenti ridondanti configurati in modo identico a scopo di alta disponibilità.

Opzione	Descrizione
Installazione di agenti ridondanti	Installare gli agenti ridondanti su server diversi, ma denominarli e configurarli in modo identico per fornire alta disponibilità.
Installazione di un agente singolo	Selezionare un nome univoco per questo agente.

13 Configurare una connessione al componente servizio di gestione.

Opzione	Descrizione
Se si utilizza il bilanciamento del carico	Specificare il nome di dominio completo e il numero di porta del bilanciamento del carico relativo al componente servizio di gestione. Ad esempio manager-load-balancer.eng.mycompany.com:443 . Gli indirizzi IP non vengono riconosciuti.
Senza bilanciamento del carico	Specificare il nome di dominio completo e il numero di porta della macchina su cui è stato installato il componente servizio di gestione. Ad esempio manager_service.mycompany.com:443 . Gli indirizzi IP non vengono riconosciuti.

La porta predefinita è 443.

14 Configurare una connessione al componente sito Web del Manager.

Opzione	Descrizione
Se si utilizza il bilanciamento del carico	Specificare il nome di dominio completo e il numero di porta del bilanciamento del carico relativo al componente servizio Web del Manager. Ad esempio website-load-balancer.eng.mycompany.com:443 . Gli indirizzi IP non vengono riconosciuti.
Senza bilanciamento del carico	Specificare il nome di dominio completo e il numero di porta della macchina su cui è stato installato il componente sito Web del Manager. Ad esempio website_component.mycompany.com:443 . Gli indirizzi IP non vengono riconosciuti.

La porta predefinita è 443.

15 Fare clic su **Prova** per verificare la connettività con ciascun host.**16** Fare clic su **Aggiungi**.**17** Fare clic su **Avanti**.**18** Fare clic su **Installa** per iniziare l'installazione.

Dopo qualche minuto viene visualizzato il messaggio di installazione eseguita.

19 Fare clic su **Avanti**.**20** Fare clic su **Fine**.**21** Verificare che l'operazione di installazione sia stata eseguita correttamente.**22** (Facoltativo) Aggiungere più agenti con configurazioni differenti e un endpoint sullo stesso sistema.

Configurazione dell'accesso per il tenant predefinito

5

È necessario assegnare ai membri del proprio team i diritti di accesso al tenant predefinito per poter consentire loro di iniziare a configurare vRealize Automation.

Il tenant predefinito viene creato automaticamente quando si configura Single Sign-On nell'installazione guidata. Non è possibile modificare i dettagli del tenant, come il nome o il token dell'URL, ma è possibile creare nuovi utenti locali e nominare altri amministratori del tenant o di IaaS in qualsiasi momento.

Procedura

- 1 Accedere alla console di vRealize Automation come amministratore di sistema del tenant predefinito.
 - a Accedere alla console di vRealize Automation.

Opzione	Descrizione
Senza bilanciamento del carico	https://vrealize-appliance-hostname.domain.name/vcac

- b Accedere con il nome utente **administrator** e la password definita per questo utente quando è stato configurato SSO.
- 2 Selezionare **Amministrazione > Tenant**.
 - 3 Fare clic sul nome del tenant predefinito **vsphere.local**.
 - 4 Fare clic sulla scheda **Utenti locali**.
 - 5 Creare gli account utente locali per il tenant predefinito di vRealize Automation.

Gli utenti locali sono specifici del tenant e possono accedere solo al tenant in cui sono stati creati.

 - a Fare clic sull'icona **Aggiungi** (+).
 - b Specificare i dettagli relativi all'utente responsabile dell'amministrazione dell'infrastruttura.
 - c Fare clic su **Aggiungi**.
 - d Ripetere questo passaggio per aggiungere altri utenti responsabili della configurazione del tenant predefinito.
 - 6 Fare clic sulla scheda **Amministratori**.

7 Assegnare gli utenti locali ai ruoli di amministratore tenant e amministratore IaaS.

- a Specificare un nome utente nella casella di ricerca **Amministratori tenant** e premere Invio.
- b Specificare un nome utente nella casella di ricerca **Amministratori IaaS** e premere Invio.

L'amministratore di IaaS è responsabile della creazione e della gestione degli endpoint dell'infrastruttura in vRealize Automation. Solo l'amministratore di sistema può assegnare questo ruolo.

8 Fare clic su **Aggiorna**.

Passi successivi

Fornire al proprio team l'URL e le informazioni di accesso per gli account utente creati in modo che possano iniziare la configurazione di vRealize Automation.

- Gli amministratori tenant configurano impostazioni quali quelle relative all'autenticazione degli utenti, inclusa la configurazione di Gestione directory per l'alta disponibilità. Vedere *Configurazione di vRealize Automation*.
- Gli amministratori IaaS preparano le risorse esterne per il provisioning. Vedere *Configurazione di vRealize Automation*.
- Se durante l'installazione è stata configurata la creazione del contenuto iniziale, l'amministratore della configurazione può richiedere l'elemento di catalogo Contenuto iniziale per popolare rapidamente un'implementazione di prototipazione. Per un esempio di come richiedere l'elemento e completare l'azione utente manuale, vedere *Installazione e configurazione di vRealize Automation per lo scenario Rainpole*.

Sostituzione di certificati autofirmati con certificati forniti da un'autorità

6

Se vRealize Automation è stato installato con certificati autofirmati, potrebbe essere preferibile sostituirli con certificati emessi da un'autorità di certificazione prima della distribuzione in produzione.

Per ulteriori informazioni sull'aggiornamento dei certificati, vedere *Gestione di vRealize Automation*.

Risoluzione dei problemi

Nella risoluzione dei problemi di vRealize Automation sono descritte le procedure che consentono di risolvere i problemi che si possono verificare durante l'installazione o la configurazione di vRealize Automation.

Questo capitolo include i seguenti argomenti:

- [Posizioni predefinite dei registri](#)
- [Rollback di un'installazione non riuscita](#)
- [Creazione di un bundle di supporto per vRealize Automation](#)
- [Risoluzione dei problemi correlati all'installazione generale](#)
- [Risoluzione dei problemi delle appliance vRealize Automation](#)
- [Risoluzione dei problemi relativi ai componenti IaaS](#)
- [Risoluzione degli errori di accesso](#)

Posizioni predefinite dei registri

Consultare i file dei registri di sistema e prodotti per avere maggiori informazioni su un'installazione non riuscita.

I percorsi dei file sono percorsi predefiniti. Se IaaS è stato installato in un'altra directory, sostituire la directory predefinita con quella dell'installazione personalizzata.

Nota: il vRealize Log Insight Content Pack di VMware vRealize™ Automation (vRA) offre un riepilogo consolidato di eventi di registro in tutti i componenti di vRealize Automation. Per ulteriori informazioni, vedere la descrizione di vRA 6.1+ Log Insight Content Pack su VMware Solution Exchange all'indirizzo https://solutionexchange.vmware.com/store/products/vra-6-1-log-insight-content-pack#.VU0r3_PD-Ht.

Registri di Windows

Utilizzare quanto segue per trovare i file di registro relativi agli eventi di Windows.

Registro	Posizione
Registri del Visualizzatore eventi di Windows	Start > Pannello di controllo > Strumenti di amministrazione > Visualizzatore eventi

Registri d'installazione

I registri delle installazioni si trovano nelle seguenti posizioni.

Registro	Posizione predefinita
Registri d'installazione	C:\Programmi (x86)\vCAC\InstallLogs C:\Programmi (x86)\VMware\vCAC\Server\ConfigTool\Log
Registri d'installazione di WAPI	C:\Programmi (x86)\VMware\vCAC\Web API\ConfigTool\Logfilename WapiConfiguration-<XXX>

Registri di IaaS

I registri IaaS si trovano nelle seguenti posizioni.

Registro	Posizione predefinita
Registri del sito Web	C:\Programmi (x86)\VMware\vCAC\Server\Website\Logs
Registro del repository	C:\Programmi (x86)\VMware\vCAC\Server\Model Manager Web\Logs
Registri del servizio di gestione	C:\Programmi (x86)\VMware\vCAC\Server\Logs
Registri DEM Orchestrator	C:\Users\<user-name>\AppData\Local\Temp\VMware\vCAC\Distributed Execution Manager\<system-name> DEO \Logs
Registri degli agenti	C:\Users\<user-name>\AppData\Local\Temp\VMware\vCAC\Agents\<agent-name>\logs

vRealize Automation Registri del framework

Le voci di registro per i framework di vRealize Automation si trovano nella posizione che segue.

Registro	Posizione predefinita
Registri del framework	/var/log/vmware

Registri di provisioning dei componenti software

I registri di provisioning dei componenti software si trovano nella posizione che segue.

Registro	Posizione predefinita
Registro di avvio automatico dell'agente software	/opt/vmware-appdirector (per Linux) o \opt\vmware-appdirector (per Windows)
Registri degli script del ciclo di vita del software	/tmp/taskId (per Linux) \Users\darwin\AppData\Local\Temp\taskId (per Windows)

Raccolta dei registri delle distribuzioni distribuite

È possibile creare un file ZIP contenente tutti i registri relativi ai componenti di una distribuzione distribuita. .

Rollback di un'installazione non riuscita

Quando un'installazione non riesce e viene ripristinata con il rollback, è necessario che l'amministratore di sistema verifichi che tutti i file richiesti siano stati disinstallati prima di avviare un'altra installazione. Alcuni file devono essere disinstallati manualmente.

Rollback di un'installazione minima

L'amministratore di sistema deve rimuovere manualmente alcuni file e ripristinare il database per disinstallare completamente un'installazione di IaaS vRealize Automation non riuscita.

Procedura

- 1 Se sono presenti i seguenti componenti, disinstallarli utilizzando il programma d'installazione di Windows.

- Agenti di vRealize Automation
- DEM Worker di vRealize Automation
- DEM Orchestrator di vRealize Automation
- Server di vRealize Automation
- vRealize Automation WAPI

Nota: se viene visualizzato il messaggio seguente, riavviare la macchina e attenersi alla seguente procedura: Errore durante l'apertura del file di registro. Verificare che il file di registro specificato sia presente e che sia scrivibile.

Nota: se il sistema Windows è stato ripristinato o se è stato disinstallato IaaS, è necessario eseguire il comando `iisreset` prima di reinstallare IaaS di vRealize Automation.

- 2 Riportare il database allo stato in cui era prima che venisse avviata l'installazione. Il metodo utilizzato dipende dalla modalità d'installazione originale del database.
- 3 In IIS (Gestione Internet Information Services) selezionare il Sito Web predefinito (o il proprio sito personalizzato) e fare clic su **Binding**. Rimuovere il binding https (predefinito sulla porta 443).
- 4 Verificare che Applications Repository, vRealize Automation e WAPI siano stati eliminati e che anche i pool di applicazioni RepositoryAppPool, vCACAppPool, WapiAppPool siano stati eliminati.

L'installazione è stata completamente rimossa.

Rollback di un'installazione distribuita

L'amministratore di sistema deve rimuovere manualmente alcuni file e ripristinare il database per disinstallare completamente un'installazione di IaaS non riuscita.

Procedura

- 1 Se sono presenti i seguenti componenti, disinstallarli utilizzando il programma d'installazione di Windows.
 - Server di vRealize Automation
 - vRealize Automation WAPI

Nota: se viene visualizzato il messaggio seguente, riavviare la macchina e attenersi alla seguente procedura: Errore durante l'apertura del file di registro. Verificare che il file di registro specificato sia presente e che sia scrivibile.

Nota: se il sistema Windows è stato ripristinato o se è stato disinstallato IaaS, è necessario eseguire il comando `iisreset` prima di reinstallare IaaS di vRealize Automation.

- 2 Riportare il database allo stato in cui era prima che venisse avviata l'installazione. Il metodo utilizzato dipende dalla modalità d'installazione originale del database.
- 3 In IIS (Gestione Internet Information Services) selezionare il Sito Web predefinito (o il proprio sito personalizzato) e fare clic su **Binding**. Rimuovere il binding https (predefinito sulla porta 443).
- 4 Verificare che Applications Repository, vCAC e WAPI siano stati eliminati e che anche i pool di applicazioni RepositoryAppPool, vCACAppPool, WapiAppPool siano stati eliminati.

Tavola 7-1. Rollback dei punti di errore

Punto di errore	Azione
Installazione del servizio di gestione	Se presente, disinstallare vCloud Automation Center Server.
Installazione di DEM Orchestrator	Se presente, disinstallare il DEM Orchestrator
Installazione di DEM Worker	Se presenti, disinstallare tutti i DEM Worker
Installazione di un agente	Se presenti, disinstallare tutti gli agenti di vRealize Automation

Creazione di un bundle di supporto per vRealize Automation

Un utente root può creare un bundle di supporto nella console di gestione di vRealize Automation appliance o in relazione a componenti di IaaS. Questi bundle possono aiutare gli addetti al supporto di VMware nell'identificazione dei problemi che possono presentarsi.

Per informazioni sulla creazione di un bundle di supporto per un componente IaaS, vedere l'articolo della knowledgebase di VMware *Collecting VMware vRealize Automation logs using the log collection utility (2078179)* all'indirizzo <http://kb.vmware.com/kb/2078179>.

Attenersi alla seguente procedura per creare un bundle di supporto per vRealize Automation appliance.

Procedura

- 1 Accedere alla console di gestione della vRealize Automation appliance utilizzando il suo nome di dominio completo, `https://vra-va-hostname.domain.name:5480/`.
- 2 Effettuare l'accesso e passare ad **Amministrazione > Registri**.
- 3 Fare clic su **Crea bundle di supporto**.
- 4 Fare clic su **Download** e salvare il file nel sistema.

Il bundle di supporto può essere utilizzato per risolvere autonomamente i problemi o inviato al rappresentante del servizio assistenza di VMware.

Risoluzione dei problemi correlati all'installazione generale

Gli argomenti che trattano la risoluzione dei problemi delle vRealize Automation appliance offrono le soluzioni alle potenziali problematiche di installazione che possono verificarsi nell'uso di vRealize Automation.

Installazione o aggiornamento non riuscito con un errore di timeout del bilanciamento del carico

Un'installazione o un aggiornamento di vRealize Automation per una distribuzione distribuita con un bilanciamento del carico si interrompe con un errore 503 servizio non disponibile.

Problema

L'installazione o l'aggiornamento non riesce perché l'impostazione del timeout del bilanciamento del carico non concede un tempo sufficiente per completare l'attività.

Causa

Un'impostazione di timeout del bilanciamento del carico insufficiente può causare un errore. È possibile correggere il problema aumentando l'impostazione del timeout del bilanciamento del carico a 100 secondi o più ed eseguendo nuovamente l'attività.

Soluzione

- 1 Aumentare il valore di timeout del bilanciamento del carico ad almeno 100 secondi. Ad esempio, modificare l'impostazione di timeout del bilanciamento del carico in `ssl.conf`, `httpd.conf` o altro file di configurazione Web, a seconda del bilanciamento del carico utilizzato.
- 2 Eseguire nuovamente l'installazione o l'aggiornamento.

Gli orari dei server non sono sincronizzati

Se i server orari di IaaS non sono sincronizzati con la vRealize Automation appliance, un'installazione potrebbe avere esito negativo.

Problema

Non è possibile accedere dopo l'installazione o l'installazione termina con esito negativo quando è ormai prossima al completamento.

Causa

I server orari su tutti i server potrebbero non essere sincronizzati.

Soluzione

Per ogni server vRealize Automation appliance e per tutti i server Windows in cui saranno installati componenti di IaaS, attivare la sincronizzazione di data e ora come descritto nei seguenti argomenti:

- [Attivazione della sincronizzazione di data e ora su vRealize Automation Appliance](#)
- [Attivazione della sincronizzazione di data e ora su Windows Server](#)

Per una trattazione generale sulla sincronizzazione di data e ora per vRealize Automation, vedere [Sincronizzazione di data e ora](#).

Quando si utilizza Internet Explorer 9 o 10 su Windows 7 possono presentarsi pagine vuote

Quando si utilizza Internet Explorer 9 o 10 su Windows 7 ed è attivata la modalità compatibilità, alcune pagine potrebbero apparire senza contenuti.

Problema

Quando si utilizza Internet Explorer 9 o 10 su Windows 7, le pagine seguenti non mostrano alcun contenuto:

- Infrastruttura
- Cartella predefinita del tenant nella pagina di Orchestrator
- Configurazione del server nella pagina di Orchestrator

Causa

Il problema potrebbe essere correlato alla modalità di compatibilità attivata. È possibile disattivare la modalità compatibilità di Internet Explorer attenendosi alla procedura seguente.

Soluzione

Prerequisiti

Verificare che sia visibile la barra dei menu. Se si utilizza Internet Explorer 9 o 10, premere Alt per visualizzare la barra dei menu (o fare clic con il pulsante destro del mouse sulla barra Indirizzo e scegliere **Barra dei menu**).

Procedura

- 1 Selezionare **Strumenti > Impostazioni Visualizzazione Compatibilità**.

- 2 Deselezionare l'opzione **Visualizza siti Intranet in Visualizzazione Compatibilità**.
- 3 Fare clic su **Chiudi**.

Impossibile stabilire una relazione basata sulla fiducia per il canale sicuro SSL/TLS

Potrebbe essere visualizzato il messaggio "Impossibile stabilire una relazione basata sulla fiducia per il canale sicuro SSL/TLS durante l'aggiornamento dei certificati di sicurezza per vCloud Automation Center".

Problema

Se si verifica un problema di certificato con vcac-config.exe durante l'aggiornamento di un certificato di sicurezza, potrebbe essere visualizzato il messaggio seguente:

La connessione sottostante è stata chiusa: impossibile stabilire una relazione basata sulla fiducia per il canale sicuro SSL/TLS

La procedura seguente consente di ottenere ulteriori informazioni sulla causa del problema.

Soluzione

- 1 Aprire il file `vcac-config.exe.config` e individuare l'indirizzo del repository: `<add key="repositoryAddress" value=" https://[Indirizzo IaaS]:443/repository/" />`
- 2 Accedere all'indirizzo utilizzando il browser Internet Explorer.
- 3 Continuare nonostante eventuali messaggi di errore relativi a problemi di attendibilità con i certificati.
- 4 Ottenere un rapporto sulla sicurezza da Internet Explorer e utilizzarlo per comprendere la natura del problema di non attendibilità del certificato.

Se i problemi persistono, ripetere la procedura accedendo con il browser all'indirizzo da registrare, l'indirizzo dell'endpoint utilizzato per la registrazione con vcac-config.exe.

Connessione alla rete attraverso un server proxy

Alcuni siti potrebbero connettersi a Internet attraverso un server proxy.

Problema

Non è possibile connettersi a Internet con la propria distribuzione. Ad esempio, non è possibile accedere a siti Web, cloud pubblici sotto la propria gestione o agli indirizzi dei fornitori da cui si scaricano software o aggiornamenti.

Causa

È possibile che il proprio sito si connetta a Internet attraverso un server proxy.

Soluzione

Prerequisiti

Procurarsi i nomi, numeri di porta e credenziali per il server proxy dall'amministratore del sito.

Procedura

- 1 Puntare un browser Web alla console di gestione di vRealize Automation appliance:
`https://appliance-FQDN-or-IP-address:5480`
- 2 Accedere con il nome utente **root** e la password impostata quando è stata effettuata la distribuzione dell'appliance.
- 3 Fare clic sulla scheda **Rete**.
- 4 Immettere l'indirizzo FQDN o IP del server proxy del sito e il numero di porta.
- 5 Se il server proxy richiede credenziali, immettere nome utente e password.
- 6 Fare clic su **Salva impostazioni**.

Passi successivi

La configurazione per l'uso di un proxy potrebbe influire sull'accesso degli utenti a VMware Identity Manager. Per correggere il problema, vedere [Il proxy impedisce l'accesso di utenti di VMware Identity Manager](#)

Il proxy impedisce l'accesso di utenti di VMware Identity Manager

La configurazione per l'utilizzo di un proxy potrebbe impedire agli utenti di VMware Identity Manager di accedere.

Problema

vRealize Automation viene configurato per accedere alla rete tramite un server proxy e gli utenti di VMware Identity Manager visualizzano il seguente errore quando tentano di accedere.

Error Unable to get metadata

Soluzione

Prerequisiti

Configurare vRealize Automation per accedere alla rete tramite un server proxy. Vedere [Connessione alla rete attraverso un server proxy](#).

Procedura

- 1 Accedere alla console di vRealize Automation appliance come radice.
- 2 Aprire il seguente file in un editor di testo.
`/etc/sysconfig/proxy`

- 3 Aggiornare la riga NO_PROXY per ignorare il server proxy per gli accessi a VMware Identity Manager.

`NO_PROXY=vra-hostname`

Ad esempio: `NO_PROXY=localhost, 127.0.0.1, vra.system.mycompany.com"`

- 4 Salvare e chiudere il proxy.
- 5 Riavviare il servizio dell'area di lavoro Horizon immettendo il seguente comando.
`service horizon-workspace restart`

Risoluzione dei problemi delle appliance vRealize Automation

Negli argomenti relativi alla risoluzione dei problemi delle appliance vRealize Automation vengono fornite soluzioni per i potenziali problemi di installazione che potrebbero verificarsi quando si utilizzano le appliance vRealize Automation.

Download non riuscito dei programmi d'installazione

Il download di programmi d'installazione dalla vRealize Automation appliance non è riuscito.

Problema

All'esecuzione di `setup__vra-va-hostname.domain.name.exe`, i programmi d'installazione non vengono scaricati.

Causa

- Problemi di connettività di rete durante la connessione alla macchina della vRealize Automation appliance.
- Impossibilità di connettersi alla macchina della vRealize Automation appliance perché non è possibile raggiungere la macchina o la stessa non risponde prima del timeout di connessione.

Soluzione

- 1 Verificare che sia possibile connettersi alla vRealize Automation appliance immettendo il seguente URL in un browser.
`https://vra-va-hostname.domain.name`
- 2 Consultare gli altri argomenti di risoluzione dei problemi della vRealize Automation appliance.
- 3 Scaricare il file d'installazione e riconnettersi alla vRealize Automation appliance.

Il file Encryption.key ha autorizzazioni errate

Quando si assegnano autorizzazioni errate al file Encryption.key per un'appliance virtuale, può verificarsi un errore di sistema.

Problema

All'accesso alla vRealize Automation appliance viene visualizzata la pagina Tenant. Dopo che la pagina ha iniziato il caricamento, viene visualizzato il messaggio System Error.

Causa

Ci sono autorizzazioni errate sul file Encryption.key o è stato commesso un errore nell'assegnazione del gruppo o del livello utente del proprietario.

Soluzione**Prerequisiti**

Accedere alla appliance virtuale che visualizza l'errore.

Nota: se le appliance virtuali sono in esecuzione sotto un bilanciamento del carico, è necessario controllare ogni appliance virtuale.

Procedura

- 1 Visualizzare il file di registro /var/log/vcac/catalina.out e cercare il messaggio Cannot write to /etc/vcac/Encryption.key.
- 2 Passare alla directory /etc/vcac/ e controllare autorizzazioni e proprietà del file Encryption.key. Dovrebbe esserci una riga simile a quella seguente:

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

Le autorizzazioni di lettura (r) e scrittura (w) sono necessarie e proprietario e gruppo del file devono essere vcac.

- 3 Se l'output è diverso da questo, cambiare le autorizzazioni o la proprietà del file come richiesto.

Passi successivi

Accedere alla pagina Tenant per accertarsi di poter accedere senza l'errore.

Identity Manager non si avvia dopo il riavvio di Horizon Workspace

In un ambiente vRealize Automation a disponibilità elevata, Identity Manager potrebbe non avviarsi dopo il riavvio del servizio Horizon Workspace.

Problema

Il servizio Horizon Workspace non si avvia a causa di un errore simile al seguente:

Error creating bean with name 'liquibase' defined in class path resource [spring/datastore-wireup.xml]: Invocation of init method failed; nested exception is liquibase.exception.LockException: Could not acquire change log lock. Currently locked by fe80:0:0:0:250:56ff:fea8:7d0c%eth0 (fe80:0:0:0:250:56ff:fea8:7d0c%eth0) since 10/29/15 (Errore di creazione bean con nome 'liquibase' definito nella risorsa del percorso delle classi [spring/datastore-wireup.xml]: invocazione del metodo init non riuscita; eccezione nidificata liquibase.exception.LockException: impossibile acquisire il blocco del registro delle modifiche.)

Causa

Identity Manager potrebbe non avviarsi in un ambiente a disponibilità elevata a causa di problemi con l'utilità di gestione dei dati liquibase utilizzata da vRealize Automation.

Soluzione

- 1 Accedere a vRealize Automation appliance come root utilizzando SSH.
- 2 Eseguire il comando `service horizon-workspace` per interrompere il servizio Horizon Workspace.
- 3 Eseguire il comando `su postgres` per diventare un utente postgres.
- 4 Eseguire il comando `psql vcac`.
- 5 Eseguire la seguente query SQL: `"update "databasechangelock" set locked=FALSE, lockgranted=NULL, lockedby=NULL where id=1;"`
- 6 Eseguire la query SQL `select *` da `databasechangelock`.
L'output dovrebbe avere il valore "f" per "locked".
- 7 Avviare il servizio Horizon Workspace con il comando `service horizon-workspace start`.

Risoluzione dei problemi relativi ai componenti IaaS

Negli argomenti relativi alla risoluzione dei problemi dei componenti IaaS vRealize Automation vengono fornite soluzioni per i potenziali problemi di installazione che potrebbero verificarsi quando si utilizza vRealize Automation.

Convalida dei certificati del server per IaaS

È possibile utilizzare il comando `vcac-Config.exe` per verificare che un server IaaS accetti certificati di vRealize Automation appliance e appliance SSO.

Problema

Quando si utilizzano funzionalità di IaaS vengono generati errori di autenticazione.

Causa

Gli errori di autenticazione possono verificarsi quando IaaS non riconosce i certificati di sicurezza provenienti da altri componenti.

Soluzione

- 1 Aprire il prompt dei comandi in qualità di utente amministratore e passare alla directory Cafe in `<vra-installation-dir>\Server\Model Manager Data\Cafe`, di solito `C:\Programmi (x86)\VMware\VCAC\Server\Model Manager Data\Cafe`.
- 2 Digitare il comando nella forma
Vcac-Config.exe CheckServerCertificates -d [vra-database] -s [vRA SQL server] -v.
 I parametri opzionali sono `-su [SQL user name]` e `-sp [password]`.

L'esito positivo del comando è segnalato dalla visualizzazione del seguente messaggio:

```
Certificates validated successfully.  
Command succeeded."
```

Se il comando non riesce viene visualizzato un messaggio di errore dettagliato.

Nota: il comando è disponibile solo sul nodo del componente Model Manager Data.

Errore di credenziali quando si esegue il programma d'installazione di IaaS

Quando si installano componenti di IaaS, si ottiene un errore all'immissione delle proprie credenziali dell'appliance virtuale.

Problema

Dopo aver fornito le credenziali nel programma d'installazione di IaaS, viene visualizzato l'errore `org.xml.sax.SAXParseException`.

Causa

Sono state utilizzate credenziali errate o queste sono state espresse in un formato non valido.

Soluzione

- ◆ Assicurarsi di utilizzare valori di tenant e nome utente corretti.
 Ad esempio, il tenant predefinito SSO utilizza un nome di dominio come `vsphere.local`, non `administrator@vsphere.local`.

Visualizzazione di un avviso di salvataggio impostazioni durante l'installazione di IaaS

Durante l'installazione di IaaS compare il seguente messaggio. Warning: Could not save settings to the virtual appliance during IaaS installation.

Problema

Durante l'installazione di IaaS compare un messaggio di errore che indica che le impostazioni dell'utente non sono state salvate.

Causa

In caso di problemi di comunicazione o di rete, questo messaggio può essere visualizzato per errore.

Soluzione

Ignorare il messaggio di errore e continuare l'installazione. Il messaggio non dovrebbe pregiudicare il buon esito dell'installazione.

Installazione del server del sito Web e dei Distributed Execution Manager non riuscita

L'installazione del server del sito Web dell'infrastruttura e dei Distributed Execution Manager di vRealize Automation appliance non può continuare quando la password dell'account del servizio di IaaS contiene virgolette doppie.

Problema

Viene visualizzato un messaggio che informa che l'installazione dei Distributed Execution Manager (DEM) e del server del sito Web di vRealize Automation appliance non è riuscita a causa di parametri msixexec non validi.

Causa

La password dell'account del servizio IaaS contiene un carattere virgolette doppie.

Soluzione

- 1 Assicurarsi che la password dell'account del servizio IaaS non contenga le virgolette doppie.
- 2 Se la password contiene virgolette doppie, creare una nuova password.
- 3 Riavviare l'installazione.

L'autenticazione di IaaS non riesce durante l'installazione dei componenti di gestione modelli e Web di IaaS

Quando si esegue il Controllo prerequisiti, viene visualizzato un messaggio che attesta l'esito negativo del controllo dell'autenticazione di IIS.

Problema

Il messaggio attesta che l'autenticazione non è attivata, ma la casella di controllo dell'autenticazione di IIS è selezionata.

Soluzione

- 1 Deselezionare la casella di controllo dell'autenticazione Windows.
- 2 Fare clic su **Salva**.
- 3 Selezionare la casella di controllo dell'autenticazione Windows.
- 4 Fare clic su **Salva**.

5 Rieseguire il Controllo prerequisiti.

Installazione di Model Manager Data e componenti Web non riuscita

L'installazione di vRealize Automation può non riuscire se il programma d'installazione di IaaS non riesce a salvare il componente Model Manager Data e il componente Web.

Problema

L'installazione non riesce e viene visualizzato il messaggio seguente:

```
Impossibile salvare i componenti Model Manager Data e Web da parte del programma d'installazione di IaaS.
```

Causa

Sono diverse le cause possibili di questo errore.

- Problemi di connettività a vRealize Automation appliance e problemi di connettività tra le appliance. Un tentativo di connessione non riesce perché non c'è risposta o perché è impossibile stabilire la connessione.
- Problemi con i certificati attendibili in IaaS quando si utilizza una configurazione distribuita.
- Mancata corrispondenza tra i nomi dei certificati in una configurazione distribuita.
- Il certificato potrebbe essere non valido o potrebbe esserci un errore nella catena di certificati.
- L'avvio del servizio del repository non riesce.
- Configurazione errata del bilanciamento del carico in un ambiente distribuito.

Soluzione

- Connettività

Verificare che sia possibile connettersi a vRealize Automation appliance immettendo il seguente URL in un browser: `https://vra-va-hostname.domain.name`.

- Problemi con i certificati attendibili

- In IaaS, aprire Microsoft Management Console con il comando `mmc.exe` e verificare che il certificato utilizzato nell'installazione sia stato aggiunto all'archivio dei certificati radice attendibili nella macchina.
- Utilizzando un browser, aprire `https://<ip-web>/repository/data/MetaModel.svc` e verificare che nel browser non si presentino errori di certificati.

- Errata corrispondenza nomi dei certificati

Questo errore può verificarsi quando il certificato viene emesso a un particolare nome e poi viene utilizzato per un nome o un indirizzo IP diverso. È possibile eliminare l'errore di mancata corrispondenza del nome del certificato durante l'installazione selezionando **Elimina mancata corrispondenza certificato**.

L'opzione Elimina mancata corrispondenza certificato consente anche di ignorare gli errori di corrispondenza degli elenchi di revoca dei certificati remoti.

- Certificato non valido

Aprire Microsoft Management Console con il comando `mmc.exe`. Verificare che il certificato non sia scaduto e che lo stato sia corretto. Eseguire questa procedura per tutti i certificati della catena di certificati. Potrebbe essere necessario importare altri certificati nella catena nell'archivio dei certificati radice attendibili quando si utilizza una gerarchia di certificati.

- Servizio del repository

Attenersi alla procedura seguente per controllare lo stato del servizio del repository.

- Dall'interno di un browser, controllare lo stato del servizio MetaModel all'indirizzo `https://<ip-web>/repository/data/MetaModel.svc`.
- Verificare l'eventuale presenza di errore nel registro `Repository.log`.
- Reimpostare IIS (`iisreset`) se si riscontrano problemi con le applicazioni in hosting sul sito Web (Repository, vRealize Automation o WAPI).
- Controllare i registri del sito Web in `%SystemDrive%\inetpub\logs\LogFiles` per informazioni di registrazione aggiuntive.
- Verificare che Controllo prerequisiti fornisca esito positivo nel controllo dei requisiti.
- In Windows 2012, verificare che i servizi WCF sotto .NET Framework siano installati e che l'attivazione HTTP sia installata.

L'aggiunta di un endpoint XaaS causa un errore interno

Quando si tenta di creare un endpoint XaaS viene visualizzato un messaggio di errore interno.

Problema

La creazione di un endpoint ha esito negativo e viene emesso il seguente messaggio di errore interno, Si è verificato un errore interno. Se il problema persiste, contattare l'amministratore di sistema. Per contattare l'amministratore, usare questo riferimento: `c0DD0C01`. I codici di riferimento sono generati in modo casuale e non sono collegati a un particolare messaggio di errore.

Soluzione

- 1 Aprire il file di registro dell'appliance vRealize Automation.

`/var/log/vcac/catalina.out`

- 2 Individuare il codice di riferimento nel messaggio di errore.

In questo esempio è *c0DD0C01*.

- 3 Cercare il codice di riferimento nel file di registro per individuare la voce associata.
- 4 Analizzare le voci che compaiono prima e dopo la voce associata per acquisire ogni elemento utile a risolvere il problema.

La voce di registro associata non chiarisce in modo specifico l'origine del problema.

Disinstallazione di un agente proxy non riuscita

La rimozione di un agente proxy può non riuscire se è attivata la registrazione del programma d'installazione di Windows.

Problema

Quando si tenta di disinstallare un agente proxy dal Pannello di controllo di Windows, la disinstallazione non riesce e viene visualizzato il seguente errore:

```
Error opening installation log file. Verify that the
specified log file location exists and is writable
```

Causa

Il problema può verificarsi quando è attivata la registrazione del programma d'installazione di Windows, ma il motore del programma d'installazione di Windows non può scrivere correttamente il file del registro di disinstallazione. Per ulteriori informazioni, vedere l'articolo della Knowledge Base di Microsoft all'indirizzo <http://support.microsoft.com/kb/2564571>.

Soluzione

- 1 Riavviare la macchina o riavviare explorer.exe da Gestione attività.
- 2 Disinstallare l'agente.

Le richieste delle macchine non riescono quando le transazioni remote sono disabilite

Le richieste di macchine non riescono quando le transazioni remote di Microsoft Distributed Transaction Coordinator (DTC) sono disabilite su macchine server Windows.

Problema

Se si esegue il provisioning di una macchina quando le transazioni remote sono disabilite sul portale di Model Manager o su SQL Server, la richiesta non verrà completata. La raccolta dati ha esito negativo e la richiesta della macchina resta nello stato CloneWorkflow.

Causa

Le transazioni remote di DTC sono disabilite nell'istanza SQL di IaaS utilizzata dal sistema vRealize Automation.

Soluzione

- 1 Avviare Server Manager di Windows per abilitare DTC su tutti i server vRealize e sui server SQL associati.

In Windows 7, scegliere **Start > Strumenti di amministrazione > Servizi componenti**.

Nota: assicurarsi che tutti i server Windows abbiano un SID univoco per la configurazione di MSDTC.

- 2 Aprire tutti i nodi per individuare il DTC locale o il DTC in cluster se si utilizza un sistema in cluster.
Passare a **Servizi componenti > Computer > Computer locale > Distributed Transaction Coordinator**.
- 3 Fare clic con il pulsante destro del mouse sul DTC locale o in cluster e scegliere **Proprietà**.
- 4 Fare clic sulla scheda Sicurezza.
- 5 Selezionare l'opzione **Accesso di rete DTC**.
- 6 Selezionare le opzioni **Consenti client remoti** e **Consenti amministrazione remota**.
- 7 Selezionare le opzioni **Consenti connessioni in ingresso** e **Consenti connessioni in uscita**.
- 8 Immettere o selezionare NT AUTHORITY\Network Service nel campo **Account** del riquadro Account di accesso DTC.
- 9 Fare clic su **OK**.
- 10 Rimuovere le macchine bloccate nello stato Clone Workflow.
 - a Accedere a vRealize Automation appliance.
`https://virtualappliance/vcac/tenantname`
 - b Selezionare **Infrastruttura > Macchine gestite**.
 - c Fare clic con il pulsante destro del mouse sulla macchina di destinazione.
 - d Scegliere **Elimina** per rimuovere la macchina.

Errore di comunicazione nel servizio di gestione

I nodi IaaS clonati da un modello in cui è installato MS DTC contengono identificatori duplicati per MS DTC che impediscono la comunicazione tra i nodi.

Problema

Si verifica un errore del servizio di gestione IaaS e nel registro viene visualizzato il seguente errore.

```
Communication with the underlying transaction manager has failed. --->
System.Runtime.InteropServices.COMException: The MSDTC transaction manager was unable to pull the
transaction from the source transaction manager due to communication problems. Possible causes are: a
firewall is present and it doesn't have an exception for the MSDTC process, the two machines cannot
find each other by their NetBIOS names, or the support for network transactions is not enabled for one
of the two transaction managers. (Comunicazione con il gestore della transazione sottostante non
```

riuscita. ----> System.Runtime.InteropServices.COMException: il gestore della transazione MSDTC non è stato in grado di richiamare la transazione dal gestore della transazione di origine a causa di problemi di comunicazione. Possibili cause: presenza di un firewall in cui non è stata impostata un'eccezione per il processo MSDTC, le due macchine non possono individuarsi mediante il rispettivo nome NetBIOS, oppure il supporto di transazioni di rete non è abilitato per uno dei due gestori di transazione.)

Causa

Quando si clona un nodo IaaS in cui è installato MS DTC, entrambi i cloni utilizzano lo stesso identificatore univoco per MS DTC. Pertanto la comunicazione tra i nodi non riesce.

Soluzione

- 1 Aprire un prompt di comandi per amministratore.
- 2 Eseguire il seguente comando: **msdtc -uninstall**
- 3 Riavviare la macchina virtuale.
- 4 Aprire un altro prompt di comandi ed eseguire il comando seguente:
msdtc -install <manager-service-host>.

Il comportamento della personalizzazione email è cambiato

In vRealize Automation 6.0 o versioni successive, è possibile personalizzare solo le notifiche generate dal componente IaaS usando la funzionalità del modello email delle versioni precedenti.

Soluzione

È possibile usare i seguenti modelli XSLT:

- ArchivePeriodExpired
- EpiRegister
- EpiUnregister
- LeaseAboutToExpire
- LeaseExpired
- LeaseExpiredPowerOff
- ManagerLeaseAboutToExpire
- ManagerLeaseExpired
- ManagerReclamationExpiredLeaseModified
- ManagerReclamationForcedLeaseModified
- ReclamationExpiredLeaseModified
- ReclamationForcedLeaseModified
- VdiRegister

- VdiUnregister

I modelli email si trovano nella directory `\Templates` sotto la directory di installazione del server, in genere `%SystemDrive%\Programmi x86\VMware\VCAC\Server`. La directory `\Templates` include inoltre i modelli XSLT non più supportati che non possono essere modificati.

Risoluzione degli errori di accesso

Gli argomenti che trattano la risoluzione degli errori di accesso per vRealize Automation offrono le soluzioni alle potenziali problematiche di installazione che possono verificarsi nell'uso di vRealize Automation.

I tentativi di accedere come amministratore di IaaS con credenziali in formato UPN errate terminano con esito negativo senza fornire dettagli

Nel tentativo di accedere a vRealize Automation come amministratore di IaaS si viene reindirizzati alla pagina di accesso senza alcuna spiegazione.

Problema

Se si tenta di accedere a vRealize Automation come amministratore IaaS con credenziali UPN che non includono la porzione `@yourdomain` del nome utente, l'uscita dall'SSO è immediata e l'utente viene reindirizzato alla pagina di accesso senza alcuna spiegazione.

Causa

L'UPN immesso deve aderire a un formato `tuonome.admin@tuodominio`, ad esempio se si accede usando `jsmith.admin@sqa.local` come nome utente ma l'UPN nell'Active Directory è impostato solo come `jsmith.admin`, l'accesso non riesce.

Soluzione

Per risolvere il problema, modificare il valore `userPrincipalName` per includere il contenuto `@yourdomain` necessario e provare di nuovo ad accedere. In questo esempio, il nome dell'UPN deve essere `jsmith.admin@sqa.local`. È possibile trovare questa informazione nel file di registro della cartella `log/vcac`.

Impossibile accedere a un tenant o scomparsa degli archivi identità dei tenant

Novanta giorni dopo una distribuzione, non è possibile accedere a un tenant o l'archivio identità di un tenant scompare.

Problema

- All'atto dell'accesso a un tenant, viene visualizzata una pagina vuota con un pulsante **Invia** nell'angolo superiore sinistro.

- Viene visualizzato un errore Eccezione di sistema quando si accede alla pagina di configurazione dell'archivio identità del tenant.
- La configurazione dell'archivio identità scompare.
- Impossibile accedere a un tenant utilizzando un account LDAP.
- Il registro `catalina.out` che si trova in `/var/log/vmware/vcac/` mostra un errore simile a quello seguente:

```
12:40:49,190 [tomcat-http--34] [authentication] INFO
com.vmware.vim.sso.client.impl.SecurityTokenServiceImpl
$RequestResponseProcessor.handleFaultCondition:922 - Failed trying to retrieve
token: ns0:RequestFailed: Error occurred looking for solution user ::
Insufficient access YYYY-03-18 12:40:49,201 [tomcat-http--34] [authentication]
ERROR
com.vmware.vcac.platform.service.rest.resolver.ApplicationExceptionHandler.handle
UnexpectedException:820 - Failed trying to retrieve token: ns0:RequestFailed:
Error occurred looking for solution user :: Insufficient access
com.vmware.vim.sso.client.exception.InternalError: Failed trying to retrieve
token: ns0:RequestFailed: Error occurred looking for solution user ::
Insufficient access
```

Causa

Per impostazione predefinita, la password dell'amministratore tenant interno di SSO scade dopo 90 giorni. Il problema è interno a vRealize Automation e non influisce sugli archivi identità di Active Directory esterni.

Si tratta di un problema noto, dovuto al fatto che l'interfaccia utente di vRealize Automation non informa dell'avvicinarsi della scadenza della password dell'amministratore tenant. La soluzione alternativa a questo problema consiste nel disabilitare la scadenza della password per l'account dell'amministratore tenant.

Per le istruzioni passo passo su come risolvere il problema, vedere l'articolo della knowledgebase di VMware all'indirizzo <http://kb.vmware.com/kb/2075011>.