

# Installazione e aggiornamento di vRealize Automation

5 ottobre 2018

vRealize Automation 7.4



vmware®

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

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

Il sito Web di VMware fornisce, inoltre, gli ultimi aggiornamenti di prodotto.

In caso di commenti sulla presente documentazione, inviare un messaggio all'indirizzo:

[docfeedback@vmware.com](mailto:docfeedback@vmware.com)

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

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

Copyright © 2017–2018 VMware, Inc. Tutti i diritti riservati. [Informazioni sul copyright e sul marchio commerciale.](#)

# Sommario

<b>1</b>	<b>Installazione o aggiornamento di vRealize Automation</b>	<b>4</b>
	Architettura di riferimento di vRealize Automation	4
	Consigli per le operazioni iniziali di distribuzione e configurazione	4
	Distribuzione di vRealize Automation	5
	Considerazioni sulla distribuzione di vRealize Business for Cloud	7
	Scalabilità di vRealize Automation	8
	Scalabilità di vRealize Business for Cloud	10
	Considerazioni sulla configurazione dell'alta disponibilità di vRealize Automation	11
	Considerazione sull'alta disponibilità di vRealize Business for Cloud	13
	Specifiche hardware e massima capacità di vRealize Automation	13
	Requisiti per una distribuzione piccola di vRealize Automation	15
	Requisiti delle distribuzioni medie vRealize Automation	20
	Requisiti delle grandi distribuzioni vRealize Automation	26
	Distribuzioni di dati di vRealize Automation in più data center	32
	vRealize Automation Secure Configuration	33
	Panoramica su baseline sicura per vRealize Automation	33
	Verifica dell'integrità del supporto di installazione	34
	Proteggere l'infrastruttura software del sistema VMware	35
	Revisione del software installato	36
	Avvisi di sicurezza e patch di VMware	37
	Secure Configuration	37
	Configurazione della sicurezza della rete host	72
	Controllo e registrazione	88
	Installazione di vRealize Automation	88
	Cenni generali sull'installazione di vRealize Automation	88
	Preparazione per l'installazione di vRealize Automation	97
	Distribuzione dell'appliance vRealize Automation	113
	Installazione di vRealize Automation utilizzando l'installazione guidata	119
	Le interfacce di installazione standard di vRealize Automation	146
	Installazione di vRealize Automation invisibile all'utente	225
	Attività post-installazione di vRealize Automation	232
	Risoluzione dei problemi d'installazione di vRealize Automation	250
	Aggiornamento di vRealize Automation	279
	Aggiornamento di vRealize Automation 7.1 o versioni successive alla versione 7.4	282
	Aggiornamento di vRealize Automation 6.2.5 alla versione 7.4	353
	Migrazione a vRealize Automation 7.4	439

# Installazione o aggiornamento di vRealize Automation

1

È possibile installare vRealize Automation per la prima volta oppure aggiornare l'ambiente corrente alla versione più recente.

Questo capitolo include i seguenti argomenti:

- [Architettura di riferimento di vRealize Automation](#)
- [vRealize Automation Secure Configuration](#)
- [Installazione di vRealize Automation](#)
- [Aggiornamento di vRealize Automation](#)

## Architettura di riferimento di vRealize Automation

L'architettura di riferimento descrive la struttura e la configurazione di distribuzioni di vRealize Automation tipiche. Fornisce inoltre informazioni su alta disponibilità, scalabilità e profili di distribuzione.

L'architettura di riferimento include informazioni sui seguenti componenti:

- VMware vRealize Automation
- VMware vRealize Business for Cloud

Per requisiti software, installazioni e piattaforme supportate, vedere la documentazione relativa a ciascun prodotto.

## Consigli per le operazioni iniziali di distribuzione e configurazione

Distribuire e configurare tutti i componenti di VMware vRealize Automation seguendo i consigli forniti da VMware.

Fare in modo che vRealize Automation, vRealize Business for Cloud e vRealize Orchestrator si trovino nello stesso fuso orario e abbiano i relativi orologi sincronizzati.

Installare vRealize Automation, vRealize Business for Cloud e vRealize Orchestrator nello stesso cluster di gestione. Eseguire il provisioning delle macchine in un cluster separato dal cluster di gestione in modo da poter isolare il carico di lavoro dell'utente e quello del server.

Distribuire gli agenti proxy nello stesso data center dell'Endpoint con il quale comunicano. VMware consiglia di non posizionare i DEM Worker in data center remoti a meno che non esista uno scenario di utilizzo basato su un workflow rapido che lo richieda. Tutti i componenti, ad eccezione degli agenti proxy e dei DEM Worker, devono essere distribuiti nello stesso data center o in data center inclusi in una rete MAN (Metro Area Network). La latenza deve essere inferiore a 5 millisecondi e la larghezza di banda tra i data center della rete MAN non deve essere inferiore a 1 GB/s.

Per ulteriori informazioni, inclusa un'informativa sul supporto, vedere l'articolo della knowledge base di VMware *Installing the VMware vRealize Automation on a distributed multi-site instance* all'indirizzo [http://kb.vmware.com/selfservice/microsites/search.do?language=en\\_US&cmd=displayKC&externalId=213484.2](http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=213484.2).

## Distribuzione di vRealize Automation

Utilizzare le raccomandazioni sulle risorse di VMware come punto di partenza per la pianificazione della distribuzione di vRealize Automation.

Dopo il test iniziale e la distribuzione in produzione, continuare a monitorare le prestazioni e se necessario allocare risorse aggiuntive, come descritto in [Scalabilità di vRealize Automation](#).

## Autenticazione

Quando si configura vRealize Automation, è possibile utilizzare il connettore di Gestione directory predefinito per l'autenticazione degli utenti oppure specificare un provider di identità basato su SAML preesistente per supportare un'esperienza Single-Sign On.

Se è richiesta l'autenticazione a due fattori, vRealize Automation supporta l'integrazione con RSA SecurID. Quando è configurato questo punto di integrazione, agli utenti viene richiesta l'immissione di ID utente e passcode.

## Considerazioni sul bilanciamento del carico

Utilizzare i metodi data/ora ultima risposta (Least Response Time) o round-robin per bilanciare il traffico in appliance vRealize Automation e server Web dell'infrastruttura. Attivare l'affinità di sessione o la funzione sessioni permanenti per indirizzare le richieste successive provenienti da ogni sessione univoca allo stesso server Web nel pool di bilanciamenti del carico.

È possibile utilizzare un bilanciamento del carico per gestire il failover per il servizio di gestione, ma non utilizzare un algoritmo di bilanciamento del carico, perché è attivo un solo servizio di gestione alla volta. Inoltre, non utilizzare l'affinità di sessione quando si gestisce il failover con un bilanciamento del carico.

Utilizzare le porte 443 e 8444 quando si esegue il bilanciamento del carico di vRealize Automation Appliance. Per il sito Web dell'infrastruttura e il servizio di gestione dell'infrastruttura, è opportuno applicare il bilanciamento del carico solo alla porta 443.

Sebbene sia possibile utilizzare altri bilanciamenti del carico, si consiglia l'uso di NSX, F5 BIG-IP hardware e F5 BIG-IP Virtual Edition in quanto opportunamente testati.

Consultare la documentazione di vRealize Automation per informazioni dettagliate sulla configurazione dei bilanciamenti del carico.

## Distribuzione database

vRealize Automation inserisce automaticamente in cluster il database dell'appliance nella versione 7.0 e in quelle successive. Tutte le nuove distribuzioni della versione 7.0 e delle versioni successive devono utilizzare il database dell'appliance interno. Le istanze di vRealize Automation che eseguono l'aggiornamento a 7.1 o a versioni successive devono unire i propri database esterni al database dell'appliance. Consultare la documentazione del prodotto vRealize Automation per ulteriori informazioni sul processo di aggiornamento.

Per distribuzioni di produzione dei componenti infrastruttura, utilizzare un server di database dedicato per ospitare i database di Microsoft SQL Server (MSSQL). vRealize Automation richiede che le macchine che comunicano con il server di database server siano configurate per l'uso di Microsoft Distributed Transaction Coordinator (MSDTC). Per impostazione predefinita, MSDTC richiede la porta 135 e le porte da 1024 a 65535.

Per ulteriori informazioni sulla modifica delle porte MSDTC predefinite, consultare l'articolo della Microsoft knowledge base "Configurazione di Microsoft Distributed Transaction Coordinator (DTC) per l'utilizzo tramite un firewall" all'indirizzo <https://support.microsoft.com/it-it/kb/250367>.

L'host del servizio di gestione di IaaS dev'essere in grado di risolvere il nome NETBIOS dell'host del database SQL Server di IaaS. Se non è in grado di risolvere il nome NETBIOS, aggiungere il nome NETBIOS di SQL Server al file `/etc/hosts` della macchina del servizio di gestione e riavviare il servizio di gestione.

vRealize Automation supporta i gruppi SQL AlwaysON solo con Microsoft SQL Server 2016. Quando si installa SQL Server 2016, il database deve essere creato in modalità 100. Se si utilizza una versione precedente di Microsoft SQL Server, utilizzare un'istanza cluster failover con dischi condivisi. Per ulteriori informazioni sulla configurazione dei gruppi SQL AlwaysOn con MSDTC, vedere <https://msdn.microsoft.com/it-it/library/ms366279.aspx>.

## Configurazione della raccolta dati

Le impostazioni di raccolta dati predefinite offrono un buon punto di partenza per la maggior parte delle implementazioni. Dopo la distribuzione in produzione, continuare a monitorare le prestazioni della raccolta dati per stabilire se occorre apportare qualche aggiustamento.

## Agenti proxy

Per ottenere le prestazioni massime, distribuire agenti nello stesso data center dell'endpoint a cui sono associati. È possibile installare agenti aggiuntivi per incrementare velocità di trasferimento e simultaneità del sistema. Le distribuzioni distribuite possono avere agent server multipli distribuiti in tutto il mondo.

Quando gli agenti sono installati nello stesso data center dell'endpoint associato, è possibile riscontrare un miglioramento delle prestazioni nella raccolta dati in media del 200 per cento. Il tempo di raccolta misurato include solo il tempo speso nel trasferimento dei dati tra l'agente proxy e il servizio di gestione. Non è incluso il tempo richiesto dal servizio di gestione per elaborare i dati.

Si supponga ad esempio di distribuire il prodotto in un data center a Palo Alto e di avere endpoint di vSphere a Palo Alto, Boston e Londra. In questa configurazione, gli agenti proxy di vSphere sono distribuiti a Palo Alto, Boston e Londra per i rispettivi endpoint. Se diversamente gli agenti venissero distribuiti solo a Palo Alto, si potrebbe assistere a un aumento del tempo di raccolta dati del 200 per cento per Boston e Londra.

## Configurazione di Distributed Execution Manager

In generale, localizzare i Distributed Execution Manager (DEM) il più vicini possibile all'host di Model Manager. Il DEM Orchestrator deve avere sempre una solida connettività di rete con il Model Manager. Per impostazione predefinita, il programma di installazione colloca i DEM Orchestrator insieme al servizio di gestione. Creare due istanze di DEM Orchestrator, una per failover, e due istanze di DEM Worker nel data center primario.

Se un'istanza di DEM Worker deve eseguire un workflow specifico della posizione, installare l'istanza in quella posizione.

Assegnare le competenze ai workflow corrispondenti e ai DEM in modo che i workflow vengano eseguiti sempre dai DEM nella posizione corretta. Per informazioni sull'assegnazione delle competenze a workflow e DEM utilizzando la console di vRealize Automation Designer, consultare la documentazione di vRealize Automation Extensibility.

Per ottenere prestazioni ottimali, installare DEM e agenti su macchine separate. Per ulteriori informazioni sull'installazione degli agenti di vRealize Automation, vedere [Installazione degli agenti](#).

## vRealize Orchestrator

Utilizzare l'istanza interna di vRealize Orchestrator per tutte le nuove distribuzioni. Se necessario, le distribuzioni legacy possono continuare a utilizzare un vRealize Orchestrator esterno. Vedere [https://kb.vmware.com/selfservice/microsites/search.do?language=en\\_US&cmd=displayKC&externalId=2147109](https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2147109) per le procedure per aumentare la memoria allocata all'istanza di vRealize Orchestrator interna.

Per prestazioni ottimali del prodotto, studiare e implementare le linee guida per la configurazione descritte nella *guida alla progettazione del codice per vRealize Orchestrator* prima di importare i contenuti di vRealize Orchestrator nelle distribuzioni di produzione.

## Considerazioni sulla distribuzione di vRealize Business for Cloud

Distribuire vRealize Business for Cloud, in precedenza noto come vRealize Business Standard Edition, secondo le linee guida di VMware.

## Considerazioni sul bilanciamento del carico

Il bilanciamento del carico non è supportato per le connessioni di raccolta dati. Per ulteriori informazioni, vedere [Scalabilità di vRealize Automation](#). Nell'appliance vRealize Business for Cloud per le connessioni del client API e dell'interfaccia utente, è possibile utilizzare il bilanciamento del carico di vRealize Automation.

## Scalabilità di vRealize Automation

Quando si configura il sistema vRealize Automation, tenere in considerazione tutti i fattori di scalabilità applicabili.

### Utenti

Appliance vRealize Automation è configurata per sincronizzare meno di 100.000 utenti. Se il sistema contiene più utenti, potrebbe essere necessario aggiungere memoria a Gestione directory di vRealize Automation. Per informazioni dettagliate sull'aggiunta di memoria a Gestione directory, vedere [Aggiunta di memoria a Gestione directory](#).

### Scalabilità provisioning simultanei

Per impostazione predefinita, vRealize Automation elabora solo otto provisioning simultanei per endpoint. Per informazioni sull'aumento di questo limite, vedere [Configurazione del provisioning simultaneo di macchine](#).

VMware consiglia di iniziare tutte le distribuzioni con almeno due DEM Worker. Nella versione 6.x, ogni DEM Worker può elaborare 15 workflow contemporaneamente. Il numero è stato aumentato a 30 per vRealize Automation 7.0 e versioni successive.

Se le macchine sono personalizzate tramite stub di workflow, occorre avere 1 DEM Worker per ogni 20 macchine con provisioning eseguito simultaneamente. Ad esempio, un sistema che supporta 100 provisioning simultanei deve avere almeno 5 DEM Worker.

Per ulteriori informazioni su DEM Worker e scalabilità, vedere [Analisi e ottimizzazione delle prestazioni del Distributed Execution Manager](#)

### Scalabilità della raccolta dati

Il tempo di completamento della raccolta dati dipende dalla capacità delle risorse di elaborazione, dal numero di macchine sulla risorsa di elaborazione o sull'endpoint, dal sistema corrente e dal carico della rete, tra le altre variabili. Le prestazioni scalano a un fattore diverso per tipi di raccolta dati differenti.

Ogni tipo di raccolta dati ha un intervallo predefinito che è possibile sostituire o modificare. Gli amministratori dell'infrastruttura possono avviare manualmente la raccolta dei dati per gli endpoint dell'origine delle infrastrutture. Gli amministratori struttura possono avviare manualmente la raccolta dei dati per le risorse di elaborazione. I valori seguenti sono gli intervalli predefiniti per la raccolta dati.

**Tabella 1-1. Intervalli predefiniti raccolta dati**

Tipo di raccolta dati	Intervallo predefinito
Inventario	Ogni 24 ore (giornaliero)
Stato	Ogni 15 minuti
Prestazioni	Ogni 24 ore (giornaliero)



## Analisi e regolazione delle prestazioni

Poiché il numero di risorse che raccolgono dati aumenta, i tempi di completamento della raccolta dati possono diventare più lunghi dell'intervallo tra gli intervalli di raccolta dati, specialmente la raccolta dati di stato. Per determinare se la raccolta dati per una risorsa di elaborazione o endpoint si sta completando in tempo o è in coda, vedere la pagina Raccolta dati. Il valore del campo Data ultimo completamento potrebbe mostrare In coda o In corso invece dell'indicazione dell'ultima data/ora in cui è terminata la raccolta dati. Se si verifica questo problema, è possibile aumentare l'intervallo tra le raccolte dati per ridurre la frequenza di raccolta dati.

In alternativa, è possibile aumentare il limite delle operazioni di raccolta dati simultanee per agente. Per impostazione predefinita, vRealize Automation limita le attività di raccolta dati simultanee a due per agente e accoda le richieste che superano questo limite. Questa limitazione consente di completare rapidamente le attività di raccolta dati, senza influenzare le prestazioni generali. È possibile aumentare il limite per sfruttare la raccolta dati simultanea, ma è necessario valutare questa opzione in relazione al decadimento delle prestazioni generali.

Se si aumenta il limite per agente di vRealize Automation configurato, si potrebbe voler aumentare uno o più di questi intervalli di timeout esecuzione. Per ulteriori informazioni su come configurare la simultaneità della raccolta dati e gli intervalli di timeout, consultare la documentazione Amministrazione di sistema di vRealize Automation. La raccolta dati del servizio di gestione è un'attività che fa un uso intensivo della CPU. L'aumento della potenza di elaborazione dell'host del servizio di gestione può ridurre il tempo necessario per la raccolta dati complessiva.

La raccolta dati per Amazon Elastic Compute Cloud (Amazon AWS), in particolare, può fare un uso intensivo della CPU, specialmente se il sistema raccoglie dati simultaneamente su più regioni e se per queste regioni non sono stati raccolti dati precedentemente. Questo tipo di raccolta dati può causare un decadimento generale delle prestazioni del sito Web. Ridurre la frequenza della raccolta dati di inventario di Amazon AWS se si riscontra un impatto sensibile sulle prestazioni.

## Scalabilità elaborazione workflow

Il tempo di elaborazione workflow medio, da quando il DEM Orchestrator inizia la pre-elaborazione del workflow a quando il workflow termina l'esecuzione, aumenta il numero di workflow simultanei. Il volume del workflow è funzione della quantità di attività di vRealize Automation, incluse le richieste di macchine e alcune attività di raccolta dati.

## Configurazione del servizio di gestione per un volume di dati elevato

Se si prevede di utilizzare un cluster VMware vSphere contenente un numero elevato di oggetti, ad esempio 3000 o più macchine virtuali, è necessario modificare il file di configurazione del servizio di gestione specificando valori più alti. Se non si modifica questa impostazione, potrebbe non essere possibile raccogliere quantità elevate di dati di inventario.

Modificare il valore predefinito delle impostazioni ProxyAgentServiceBinding e maxStringContentLength nel file ManagerService.exe.config.

## Procedura

- 1 Aprire il file `ManagerService.exe.config` in un editor di testo.

Generalmente, questo file si trova nel percorso `C:\Programmi(x86)\VMware\vCAC\Server`.

- 2 Individuare le righe `binding name` e `readerQuotas` nel file.

```
<binding name="ProxyAgentServiceBinding" maxReceivedMessageSize="13107200">
  <readerQuotas maxStringContentLength="13107200" />
```

**Nota** Non confondere queste due righe con righe simili contenente la stringa seguente: `binding name = "ProvisionServiceBinding"`.

- 3 Sostituire i valori numerici assegnati agli attributi `maxReceivedMessageSize` e `maxStringContentLength` con un valore più alto.

La dimensione ottimale dipende da quanti ulteriori oggetti si prevede che saranno contenuti nel cluster VMware vSphere in futuro. È ad esempio possibile incrementare questi numeri di un fattore pari a 10 a scopo di test.

- 4 Salvare le modifiche e chiudere il file.
- 5 Riavviare il servizio di gestione di vRealize Automation.

## Analisi e ottimizzazione delle prestazioni del Distributed Execution Manager

È possibile visualizzare il numero totale di workflow in corso o in sospeso in qualsiasi momento nella pagina Stato Distributed Execution, nonché utilizzare la pagina Cronologia workflow per stabilire la quantità di tempo necessaria per l'esecuzione di un determinato workflow.

Se sono presenti numerosi workflow in sospeso o se il completamento dei workflow sta richiedendo più tempo del previsto, aggiungere ulteriori istanze di DEM (Distributed Execution Manager) Worker per migliorare le prestazioni dei workflow. Ogni istanza di DEM Worker può elaborare 30 workflow simultanei. I workflow in eccesso vengono messi in coda per l'esecuzione.

È possibile modificare le pianificazioni dei workflow in modo da ridurre al minimo il numero di workflow avviati simultaneamente. Ad esempio, anziché pianificare solo workflow su base oraria, ovvero eseguiti a ogni inizio di ora, è possibile scaglionarne gli orari di esecuzione in modo che non debbano contendersi le risorse DEM. Per ulteriori informazioni sui workflow, vedere la documentazione relativa all'estendibilità di vRealize Automation.

Alcuni workflow, in particolare determinati workflow personalizzati, possono richiedere un uso intensivo della CPU. Se il carico della CPU sulle macchine DEM Worker è elevato, provare ad aumentare la potenza di elaborazione della macchina DEM o ad aggiungere ulteriori macchine DEM al proprio ambiente.

## Scalabilità di vRealize Business for Cloud

Configurare l'installazione di vRealize Business for Cloud per la scalabilità secondo le linee guida di VMware.

vRealize Business for Cloud può scalare fino a 20.000 macchine virtuali in dieci istanze di VMware vCenter Server. La prima sincronizzazione della raccolta dati dell'inventario impiega circa tre ore e prevede la sincronizzazione di 20.000 macchine virtuali in tre istanze di VMware vCenter Server. La sincronizzazione delle statistiche da VMware vCenter Server impiega circa un'ora per 20.000 macchine virtuali. Per impostazione predefinita, il processo di calcolo del costo viene eseguito ogni giorno e impiega circa due ore per ogni esecuzione per 20.000 macchine virtuali.

---

**Nota** In vRealize Business for Cloud 1.0, la configurazione dell'appliance virtuale predefinita può supportare fino a 20.000 macchine virtuali. L'incremento dei limiti dell'appliance virtuale oltre la sua configurazione predefinita non aumenta il numero di macchine virtuali che può supportare.

---

## Considerazioni sulla configurazione dell'alta disponibilità di vRealize Automation

Se è necessario un sistema perfettamente affidabile, configurare il sistema vRealize Automation per l'alta disponibilità in base alle linee guida di VMware.

### Appliance vRealize Automation

L'Appliance vRealize Automation supporta l'alta disponibilità attiva-attiva per tutti i componenti ad eccezione del database dell'appliance. A partire dalla release 7.3, il failover del database è automatico se vengono distribuiti tre nodi e la replica sincrona è configurata tra due nodi. Quando Appliance vRealize Automation rileva un errore del database, promuove un server di database appropriato al ruolo di master. È possibile monitorare e gestire il database dell'appliance dalla scheda **Impostazioni vRA > Database** della console di gestione dell'appliance virtuale.

Per abilitare l'alta disponibilità per queste appliance, posizionarle sotto un bilanciamento del carico. Per ulteriori informazioni, vedere [Configurazione del bilanciamento del carico](#). A partire dalla versione 7.0, il database dell'appliance e vRealize Orchestrator vengono inseriti automaticamente in cluster e resi disponibili per l'uso.

### Gestione directory di vRealize Automation

Ogni appliance vRealize Automation include un connettore che supporta l'autenticazione utente, anche se in genere viene configurato un solo connettore per eseguire la sincronizzazione delle directory. Non è importante quale sia il connettore scelto per la sincronizzazione. Per supportare l'alta disponibilità di Gestione directory, è necessario configurare un secondo connettore che corrisponda alla seconda appliance vRealize Automation, si connetta al provider di identità e punti alla stessa istanza di Active Directory. Con questa configurazione, se in un'appliance si verifica un errore, l'altra la sostituisce per la gestione dell'autenticazione degli utenti.

In un ambiente ad alta disponibilità, tutti i nodi devono servire lo stesso set di Active Directory, utenti, metodo di autenticazione e così via. Il metodo più diretto per implementare questa configurazione consiste nel promuovere il provider di identità nel cluster impostando l'host di bilanciamento del carico come host del provider di identità. Con questa configurazione, tutte le richieste di autenticazione vengono indirizzate al bilanciamento del carico, che a sua volta le inoltra al connettore appropriato.

Per ulteriori informazioni sulla configurazione di Gestione directory per l'alta disponibilità, vedere [Configure Directories Management for High Availability](#).

## Server Web infrastruttura

Tutti i componenti del server Web dell'infrastruttura supportano l'alta disponibilità attiva-attiva. Per abilitare l'alta disponibilità per questi componenti, posizionarli sotto un bilanciamento del carico.

## Servizio di gestione dell'infrastruttura

Il componente servizio di gestione supporta l'alta disponibilità attiva-passiva. Per abilitare l'alta disponibilità per questo componente, posizionare due servizi di gestione sotto un bilanciamento del carico. In vRealize Automation 7.3 e versione successiva il failover è automatico.

Se il servizio di gestione attivo ha un problema, arrestare il servizio di Windows, se non già arrestato sotto il bilanciamento del carico. Abilitare il servizio di gestione passivo e riavviare il servizio di Windows sotto il bilanciamento del carico. Vedere [Installazione del servizio di gestione attivo](#).

## Agenti

Gli agenti supportano l'alta disponibilità attiva-attiva. Per informazioni sulla configurazione degli agenti per l'alta disponibilità, consultare la documentazione sulla configurazione di vRealize Automation. Verificare il servizio di destinazione per l'alta disponibilità.

## Distributed Execution Manager Worker

Un Distributed Execution Manager (DEM) in esecuzione con il ruolo di Worker supporta l'alta disponibilità attiva-attiva. Se un'istanza di DEM Worker ha un problema, il DEM Orchestrator rileva il problema e annulla i workflow che l'istanza del DEM Worker sta eseguendo. Quando l'istanza del DEM Worker ritorna online, riconosce che il DEM Orchestrator ha annullato i workflow dell'istanza e ne interrompe l'esecuzione. Per evitare l'annullamento prematuro dei workflow, lasciare l'istanza di un DEM Worker offline per qualche minuto prima di annullare i suoi workflow.

## Distributed Execution Manager Orchestrator

I DEM in esecuzione con il ruolo di Orchestrator supportano l'alta disponibilità attiva-attiva. Quando si avvia, un DEM Orchestrator cerca un altro DEM Orchestrator in esecuzione.

- Se non trova istanze di DEM Orchestrator in esecuzione, inizia l'esecuzione come DEM Orchestrator primario.
- Se trova un altro DEM Orchestrator in esecuzione, monitora l'altro DEM Orchestrator primario per rilevarne un'eventuale interruzione.
- Se rileva un'interruzione, prende il posto di istanza primaria.

Quando l'istanza primaria precedente torna online, rileva che un altro DEM Orchestrator ha preso il posto di istanza primaria e monitora l'istanza primaria di Orchestrator in attesa di eventuali problemi.

## Server di database MSSQL per componenti dell'infrastruttura

vRealize Automation supporta i gruppi SQL AlwaysON solo con Microsoft SQL Server 2016. Quando si installa SQL Server 2016, il database deve essere creato in modalità 100. Se si utilizza una versione precedente di Microsoft SQL Server, utilizzare un'istanza cluster failover con dischi condivisi. Per ulteriori informazioni sulla configurazione dei gruppi SQL AlwaysOn con MSDTC, vedere l'articolo Microsoft <https://msdn.microsoft.com/en-us/library/ms366279.aspx>.

## vRealize Orchestrator

Come parte dell'appliance vRealize Automation viene fornita un'istanza ad alta disponibilità interna di vRealize Orchestrator.

## Considerazione sull'alta disponibilità di vRealize Business for Cloud

Utilizzare la funzione HA di VMware vSphere per l'appliance vRealize Business for Cloud Edition.

Per configurare la funzione HA di VMware vSphere sull'host VMware ESXi, consultare la documentazione di vCenter Server e Host Management.

## Specifiche hardware e massima capacità di vRealize Automation

Installare i componenti appropriati in base alle proprie esigenze di configurazione e capacità su ciascun profilo server di vRealize Automation incluso nell'ambiente.

Ruolo server	Componenti	Specifiche hardware richieste	Specifiche hardware consigliate
Appliance vRealize Automation	Servizi di vRealize Automation, vRealize Orchestrator, database di vRealize Automation Appliance	CPU: 4 vCPU RAM: 18 GB (vedere <a href="#">Scalabilità di vRealize Automation</a> per ulteriori informazioni). Disco: 140 GB Rete: 1 GB/s	Uguali alle specifiche hardware richieste.
Infrastructure Core Server	Sito Web, servizio di gestione, DEM Orchestrator, DEM Worker, agente proxy	CPU: 4 vCPU RAM: 8 GB Disco: 40 GB Rete: 1 GB/s	Uguali alle specifiche hardware richieste.
Server Web infrastruttura	Sito Web	CPU: 2 vCPU RAM: 8 GB Disco: 40 GB Rete: 1 GB/s	CPU: 2 vCPU RAM: 8 GB Disco: 40 GB Rete: 1 GB/s

Ruolo server	Componenti	Specifiche hardware richieste	Specifiche hardware consigliate
Server gestione infrastruttura	Servizio di gestione, DEM Orchestrator	CPU: 2 vCPU RAM: 8 GB Disco: 40 GB Rete: 1 GB/s	CPU: 2 vCPU RAM: 8 GB Disco: 40 GB Rete: 1 GB/s
Web infrastruttura/server di gestione	Web infrastruttura/server di gestione	CPU: 2 vCPU RAM: 8 GB Disco: 40 GB Rete: 1 GB/s	CPU: 2 vCPU RAM: 8 GB Disco: 40 GB Rete: 1 GB/s
Server DEM infrastruttura	(Uno o più) DEM Worker	CPU: 2 vCPU RAM: 8 GB Disco: 40 GB Rete: 1 GB/s per ogni DEM Worker	CPU: 2 vCPU RAM: 8 GB Disco: 40 GB Rete: 1 GB/s per ogni DEM Worker
Server agente infrastruttura	(Uno o più) agente proxy	CPU: 2 vCPU RAM: 8 GB Disco: 40 GB Rete: 1 GB/s	CPU: 2 vCPU RAM: 8 GB Disco: 40 GB Rete: 1 GB/s
Server database MSSQL	Database dell'infrastruttura	CPU: 2 vCPU RAM: 8 GB Disco: 40 GB Rete: 1 GB/s	CPU: 8 vCPU RAM: 16 GB Disco: 80 GB Rete: 1 GB/s
Appliance vRealize Business for Cloud	Server di database vRealize Business for Cloud dei servizi dell'appliance vRealize Business for Cloud	CPU: 2 vCPU RAM: 4 GB Disco: 50 GB Rete: 1 GB/s	Uguali alle specifiche hardware richieste

## Massima capacità consigliata per vRealize Automation

I valori di massima capacità delle risorse riportati di seguito sono applicabili al profilo di distribuzione di grandi dimensioni di vRealize Automation.

**Tabella 1-2. Massima capacità delle risorse di vRealize Automation**

Parametro	Valore massimo
Tenant	100
Endpoint vSphere	20
Risorse di elaborazione	200
Macchine gestite	75.000
Picco richieste simultanee	
costante	50
burst	250
Picco richieste ogni ora	400

**Tabella 1-2. Massima capacità delle risorse di vRealize Automation (Continua)**

Parametro		Valore massimo
Gruppi di business		3000 (con 10 utenti univoci per gruppo di business e nessun utente membro di più di 50 gruppi di business)
Prenotazioni		9.000 (con 3 prenotazioni per gruppo di business)
blueprint		
	Solo CBP	6.000
	CBP + XaaS	8.000
Elementi del catalogo		
	tra più tenant	4.000
	in un singolo tenant	6.000
Sincronizzazione utente/gruppo con 18 GB di memoria predefiniti		
	numero di utenti	95027
	numero di gruppi	20403 (ogni gruppo contiene 4 utenti con un livello di nidificazione)
Utente/gruppo con memoria incrementata a 30 GB		
	numero di utenti	100.000
	numero di gruppi	750 (ogni gruppo contiene 4.000 utenti e ogni utente si trova in 30 gruppi)

## Requisiti per una distribuzione piccola di vRealize Automation

Una distribuzione piccola di vRealize Automation comprende sistemi composti da massimo 10.000 macchine gestite e include le macchine virtuali, i bilanciamenti del carico e le configurazioni di porta appropriati. La distribuzione piccola rappresenta un punto di partenza per una distribuzione di vRealize Automation che consenta di scalare fino a una distribuzione media o grande, conservando il supporto richiesto.

Quando si distribuisce vRealize Automation, utilizzare il processo di distribuzione enterprise per fornire un indirizzo separato per sito Web e servizio di gestione dell'infrastruttura.

## Supporto

Una distribuzione piccola può supportare i seguenti elementi.

- 10.000 macchine gestite
- 500 elementi del catalogo
- 10 provisioning simultanei di macchine

## Requisiti

Una distribuzione piccola deve essere configurata con i componenti appropriati.

- Appliance vRealize Automation: vrava-1.ra.local
- Infrastructure Core Server: inf-1.ra.local.
- Server di database MSSQL: mssql.ra.local
- Appliance vRealize Business for Cloud: vrb.ra.local

## Voci DNS

Voce DNS	Punta a
vrava.ra.local	vrava-1.ra.local
web.ra.local	inf.ra.local
manager.ra.local	inf.ra.local

## Certificati

I nomi host utilizzati in questa tabella sono solo esempi.

Ruolo server	CN o SAN
Appliance vRealize Automation	SAN contiene vra.va.sqa.local e vra.va-1.sqa.local
Infrastructure Core Server	SAN contiene web.ra.local, managers.ra.local e inf-1.ra.local
Server di vRealize Business for Cloud	CN = vrb.ra.local

## Porte

Gli utenti devono poter accedere a determinate porte. Tutte le porte elencate sono predefinite.

Ruolo server	Porta
Appliance vRealize Automation	443, 8444. La porta 8444 è necessaria per la console remota della macchina virtuale. La porta 8283 è necessaria per l'accesso a Control Center di vRealize Orchestrator.

Gli amministratori devono poter accedere a determinate porte, oltre alle porte alle quali devono poter accedere gli utenti.

Ruolo server	Porta
Appliance vRealize Automation	5480, 8443. La porta 8443 è usata per la configurazione della gestione delle identità avanzata. VMware Identity Manager in Active Directory: 389, 636, 3268, 3269 VMware Identity Manager in controller di dominio: 88, 464, 135
vRealize Business for Cloud	5480

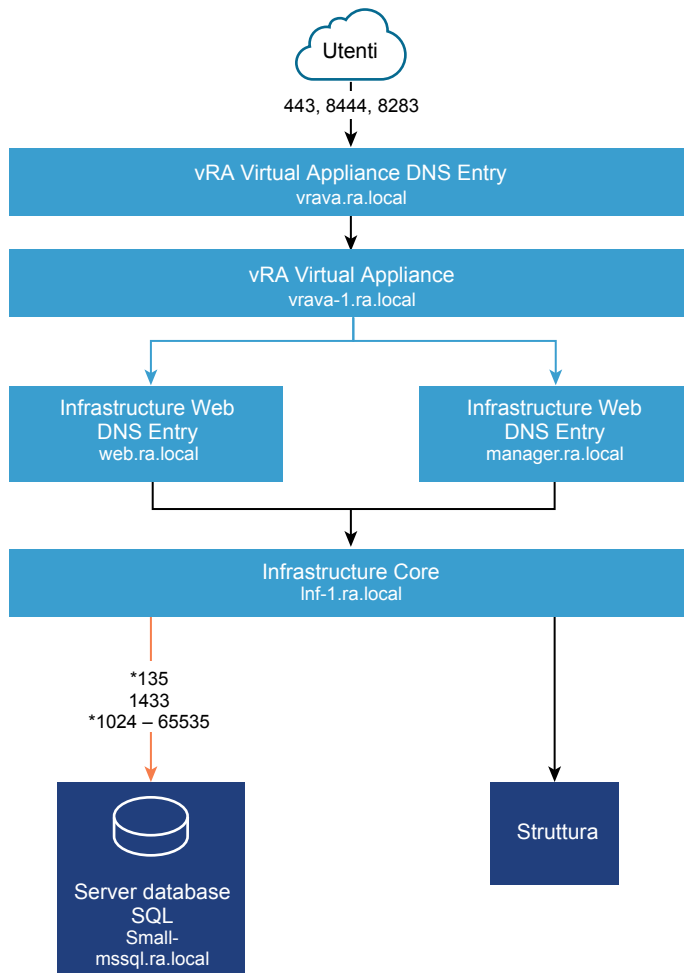


Ruolo server	Porte in entrata	Porte in uscita di servizio/sistema
Appliance vRealize Automation	<p>HTTPS: 443</p> <p>Configurazione adattatore: 8443</p> <p>Proxy console remota: 8444</p> <p>SSH: 22</p> <p>Console gestione appliance virtuale: 5480</p>	<p>LDAP: 389</p> <p>LDAPS:636</p> <p>VMware ESXi: 902</p> <p>Infrastructure Core richiede l'accesso alla porta 443 dell'endpoint vSphere per ottenere un ticket per VMware Remote Console. L'appliance vRealize Automation richiede l'accesso alla porta 902 dell'host ESXi per il proxy del traffico verso il cliente.</p> <p>Infrastructure Core Server: 443</p> <p>Autenticazione Kerberos: 88</p> <p>Rinnovo password oggetto computer: 464</p>
Infrastructure Core Server	<p>HTTPS: 443</p> <p>MSDTC: 135, 1024 - 65535. Per informazioni su come limitare questo intervallo, consultare la sezione relativa alla distribuzione del database di <a href="#">Distribuzione di vRealize Automation</a>.</p>	<p>Appliance virtuale di vRealize Automation: 443, 5480</p> <p>Endpoint vSphere: 443</p> <p>Infrastructure Core richiede l'accesso alla porta 443 dell'endpoint vSphere per ottenere un ticket per VMware Remote Console. L'appliance vRealize Automation richiede l'accesso alla porta 902 dell'host ESXi per il proxy del traffico verso il cliente.</p> <p>MSSQL: 135, 1433, 1024 - 65535</p> <p>MSDTC: 135, 1024 - 65535. Per informazioni su come limitare questo intervallo, consultare la sezione relativa alla distribuzione del database di <a href="#">Distribuzione di vRealize Automation</a>.</p>

Ruolo server	Porte in entrata	Porte in uscita di servizio/sistema
Server database MSSQL	MSSQL: 1433 MSDTC: 135, 1024 - 65535. Per informazioni su come limitare questo intervallo, consultare la sezione relativa alla distribuzione del database di <a href="#">Distribuzione di vRealize Automation</a> .	Infrastructure Core Server: 135, da 1024 a 65535. Per informazioni su come limitare questo intervallo, consultare la sezione relativa alla distribuzione del database di <a href="#">Distribuzione di vRealize Automation</a> . MSDTC: 135, 1024 - 65535. Per informazioni su come limitare questo intervallo, consultare la sezione relativa alla distribuzione del database di <a href="#">Distribuzione di vRealize Automation</a> .
Appliance vRealize Business for Cloud	HTTPS: 443 SSH: 22 Console gestione appliance virtuale: 5480	Appliance virtuale di vRealize Automation: 443 Infrastructure Core: 443
Catalogo globale		Catalogo globale: 3268, 3269

## Dimensioni minime

Figura 1-1. Dimensioni minime per la configurazione ridotta di vRealize Automation



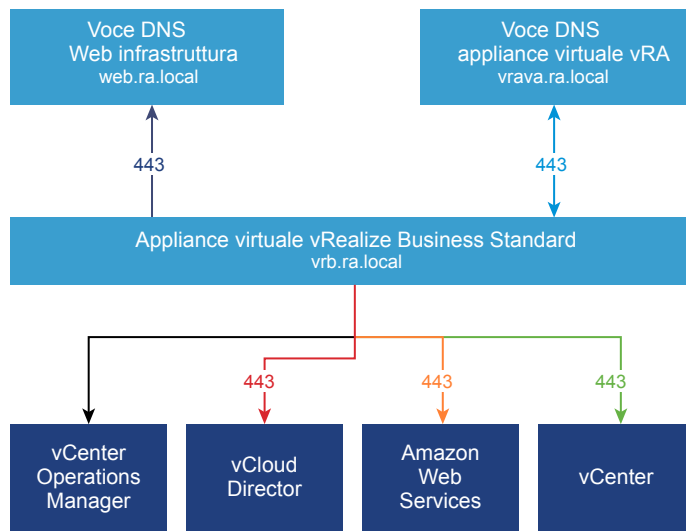
Non visualizzato:  
Tutti i sistemi dell'infrastruttura richiedono l'accesso alla porta 5480 di tutte le appliance vRealize per fare in modo che la raccolta dei registri (Impostazioni vRA > Cluster > Raccogli registri su appliance virtuale:5480) funzioni.

Per la console remota delle macchine virtuali, vRealize Appliance richiede l'accesso alla porta 902 di VMware ESXi, mentre Infrastructure Core Server richiede l'accesso alla porta 443 dell'endpoint vSphere.

\*Vedere la sezione relativa alla distribuzione dei database per informazioni su come ridurre questo intervallo

È inoltre necessaria la comunicazione bidirezionale.

**Figura 1-2. Dimensioni minime per la configurazione ridotta di vRealize Business for Cloud**



## Requisiti delle distribuzioni medie vRealize Automation

Una distribuzione media vRealize Automation comprende sistemi di 30.000 macchine gestite o meno e include macchine virtuali, sistemi di bilanciamento del carico e configurazioni delle porte.

### Supporto

Una distribuzione media può supportare i seguenti elementi.

- 30.000 macchine gestite
- 1000 elementi del catalogo
- 50 provisioning di macchine

### Requisiti

Una distribuzione media deve soddisfare i requisiti di configurazione di sistema appropriati.

#### Appliance virtuali

- Appliance vRealize Automation 1: vrava-1.ra.local
- Appliance vRealize Automation 2: vrava-2.ra.local
- Appliance vRealize Automation 3: vrava-3.ra.local
- vRealize Business for Cloud Appliance: vrb.ra.local

#### Macchine virtuali Windows Server

- Web infrastruttura/server di gestione 1 (Web attivo o DEM-O, gestione attiva): inf-1.ra.local
- Web infrastruttura/server di gestione 2 (Web attivo o DEM-O, gestione attiva): inf-2.ra.local
- Server DEM infrastruttura 1: dem-1.ra.local

- Server DEM infrastruttura 2: dem-2.ra.local
- Server agente infrastruttura 1: agent-1.ra.local
- Server agente infrastruttura 2: agent-2.ra.local

Server di database

- Istanza cluster failover MSSQL: mssql.ra.local

Bilanciamento del carico

- Bilanciamento del carico dell'Appliance vRealize Automation: med-vrava.ra.local
- Bilanciamento del carico Web infrastruttura: med-web.ra.local
- Bilanciamento del carico servizio gestione infrastruttura: med.ra.local

## Certificati

I nomi host usati in questa tabella sono forniti a solo titolo di esempio.

Ruolo server	CN o SAN
Appliance vRealize Automation	SAN contiene i seguenti nomi host: <ul style="list-style-type: none"> <li>▪ vrava.ra.local</li> <li>▪ vrava-1.ra.local</li> <li>▪ vrava-2.ra.local</li> </ul>
Web infrastruttura o server di gestione	SAN contiene i seguenti nomi host: <ul style="list-style-type: none"> <li>▪ web.ra.local</li> <li>▪ manager.ra.local</li> <li>▪ inf-1.ra.local</li> <li>▪ inf-2.ra.local</li> </ul>
Appliance vRealize Business for Cloud	CN = vrb.ra.local

## Porte

Gli utenti devono poter accedere a determinate porte. Tutte le porte elencate sono predefinite.

Ruolo server	Porta
Bilanciamento del carico Appliance vRealize Automation	443, 8444. La porta 8444 è necessaria per la console remota della macchina virtuale.

Gli amministratori devono poter accedere a determinate porte, oltre alle porte alle quali devono poter accedere gli utenti.

Ruolo server	Porta
Appliance vRealize Automation fVAMI	5480, 8443. La porta 8443 è usata per la configurazione della gestione delle identità avanzata. VMware Identity Manager in Active Directory: 389, 636, 3268, 3269 VMware Identity Manager in controller di dominio: 88, 464, 135
Centro di controllo vRealize Appliance Orchestrator	8283
Server di vRealize Business for Cloud	5480

La tabella seguente illustra le comunicazioni tra applicazioni.

Ruolo server	Porte in entrata	Porte in uscita per servizio o sistema
Appliance vRealize Automation	<p>HTTPS:</p> <p>Configurazione adattatore: 8443</p> <p>Proxy console remota: 8444</p> <p>Postgres: 5432</p> <p>RabbitMQ: 4369, 25672, 5671, 5672</p> <p>ElasticSearch: 9300, 40002, 40003</p> <p>Stomp: 61613</p> <p>SSH: 22</p>	<p>LDAP:389</p> <p>LDAPS: 636</p> <p>Appliance vRealize Automation (tutte le altre): 5432, 4369, 25672, 5671, 5672, 9300, 40002, 40003</p> <p>Bilanciamento del carico Web infrastruttura vRealize Automation: 443</p> <p>VMware ESXi: 902. Web infrastruttura o gestione richiede l'accesso alla porta dell'endpoint vSphere 443 per ottenere un ticket per la console remota della macchina virtuale. Appliance vRealize Automation richiede l'accesso alla porta host ESXi 902 per fungere da proxy dei dati console per l'utente.</p> <p>Autenticazione Kerberos: 88</p> <p>Rinnovo password oggetto computer: 464</p>
Web infrastruttura/server di gestione	<p>HTTPS: 443</p> <p>MSDTC: 135, 1024-65535. Per informazioni su come limitare questo intervallo, consultare la sezione relativa alla distribuzione del database di <a href="#">Distribuzione di vRealize Automation</a>.</p>	<p>Bilanciamento del carico Appliance vRealize Automation: 443</p> <p>Bilanciamento del carico Web infrastruttura vRealize Automation: 443</p> <p>Appliance (VA) vRealize Automation: 5480.</p> <p>Endpoint vSphere: 443. Web infrastruttura o gestione richiede l'accesso alla porta dell'endpoint vSphere 443 per ottenere un ticket per la console remota della macchina virtuale. Appliance vRealize Automation richiede l'accesso alla porta host ESXi 902 per fungere da proxy dei dati console per l'utente.</p> <p>MSSQL: 135, 1433, da 1024 a 65535. Per informazioni su come limitare questo intervallo, consultare la sezione relativa alla distribuzione del database di <a href="#">Distribuzione di vRealize Automation</a>.</p>
Server DEM infrastruttura	NA	<p>Bilanciamento del carico appliance vRealize Automation: 443</p> <p>Bilanciamento del carico Web infrastruttura vRealize Automation: 443</p> <p>Bilanciamento del carico gestione infrastruttura vRealize Automation: 443</p> <p>Appliance (VA) vRealize Automation: 5480.</p>

Ruolo server	Porte in entrata	Porte in uscita per servizio o sistema
Server agente infrastruttura	NA	Bilanciamento del carico Web infrastruttura vRealize Automation: 443 Bilanciamento del carico gestione infrastruttura vRealize Automation: 443 Appliance (VA) vRealize Automation: 5480.
Server database MSSQL	MSSQL: 1433 MSDTC: 135, 1024 - 65535. Per informazioni su come limitare questo intervallo, consultare la sezione relativa alla distribuzione del database di <a href="#">Distribuzione di vRealize Automation</a> .	Web infrastruttura/server di gestione: 135, 1024-65535. Per informazioni su come limitare questo intervallo, consultare la sezione relativa alla distribuzione del database di <a href="#">Distribuzione di vRealize Automation</a> .
Server di vRealize Business for Cloud	HTTPS: 443 SSH: 22 Console gestione appliance virtuale: 5480	Bilanciamento del carico appliance vRealize Automation: 443 Bilanciamento del carico Web infrastruttura vRealize Automation: 443
Catalogo globale		Catalogo globale: 3268, 3269

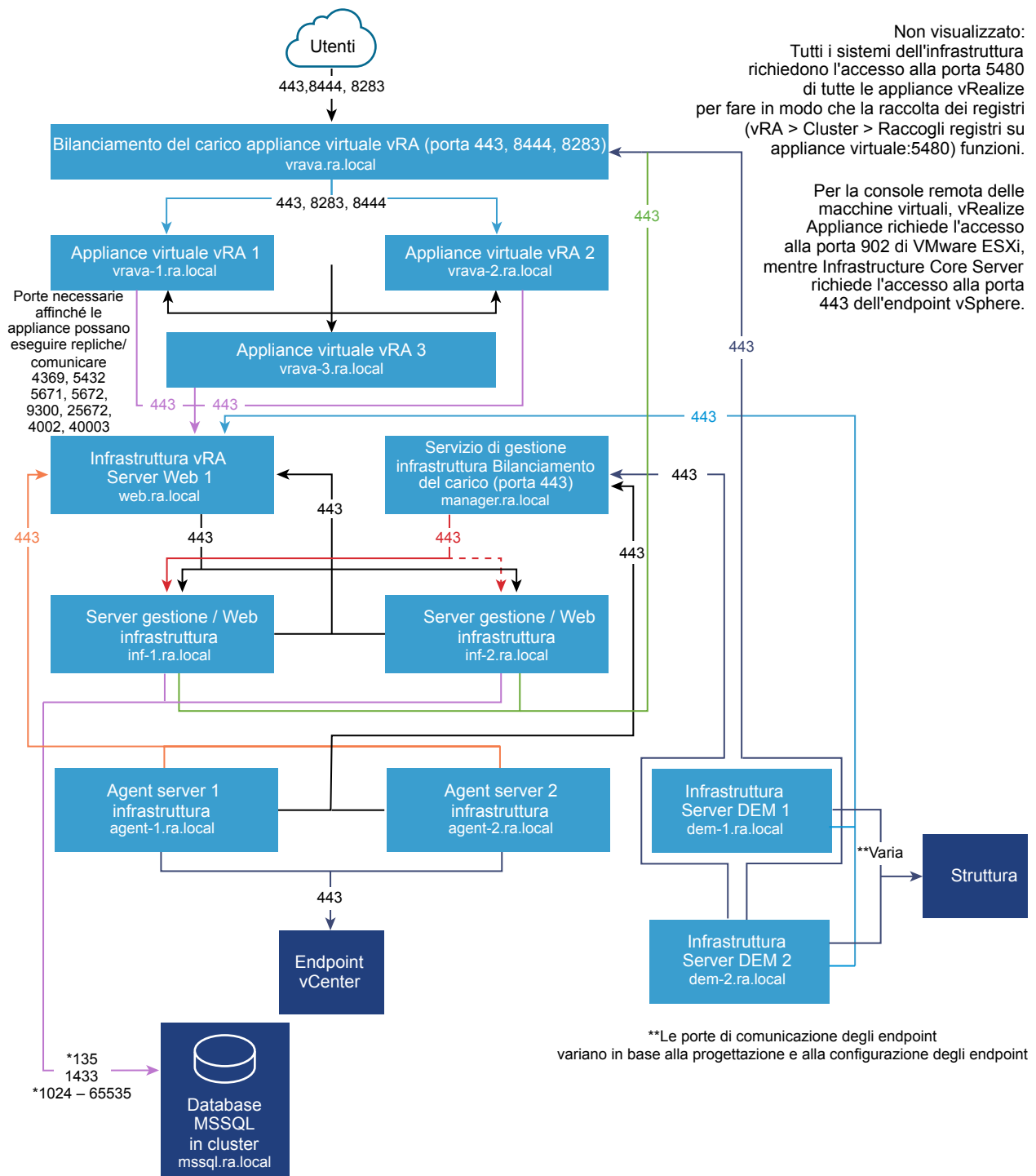
Il bilanciamento del carico richiede l'accesso dalle seguenti porte.

Bilanciamento del carico	Porte bilanciate
Bilanciamento del carico Appliance vRealize Automation	443, 8444
Bilanciamento del carico Web infrastruttura vRealize Automation	443
Bilanciamento del carico servizio manager infrastruttura vRealize Automation	443



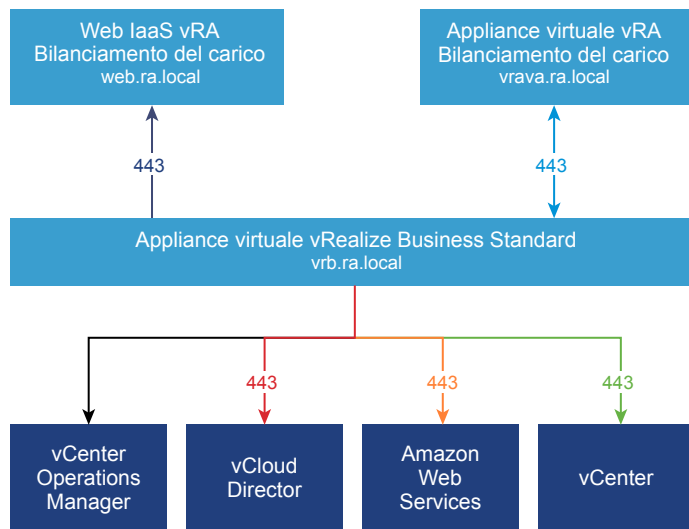
## Grafici

Figura 1-3. Dimensioni minime per configurazione media di vRealize Automation



\*Vedere la sezione relativa alla distribuzione dei database per informazioni su come ridurre questo intervallo. È inoltre necessaria la comunicazione bidirezionale.

**Figura 1-4. Dimensioni minime per configurazione media di vRealize Business for Cloud**



## Requisiti delle grandi distribuzioni vRealize Automation

Una grande distribuzione vRealize Automation comprende sistemi di 50.000 macchine gestite o meno e include macchine virtuali, sistemi di bilanciamento del carico e configurazioni delle porte.

### Supporto

Una grande distribuzione può supportare i seguenti elementi.

- 50.000 macchine gestite
- 2500 elementi del catalogo
- 100 provisioning simultanei di macchine

### Requisiti

Una grande distribuzione deve soddisfare i requisiti di configurazione di sistema appropriati.

#### Appliance virtuali

- vRealize Automation appliance 1: vrava-1.ra.local
- vRealize Automation appliance 2: vrava-2.ra.local
- vRealize Automation appliance 2: vrava-3.ra.local
- vRealize Automation appliance Appliance: vrb.ra.local

#### Macchine virtuali Windows Server

- Server Web infrastruttura 1: web-1.ra.local
- Server Web infrastruttura 2: web-2.ra.local
- Server gestione infrastruttura 1: manager-1.ra.local

- Server gestione infrastruttura 2: manager-2.ra.local
- Server DEM infrastruttura 1: dem-1.ra.local
- Server DEM infrastruttura 2: dem-2.ra.local
- Server agente infrastruttura 1: agent-1.ra.local
- Server agente infrastruttura 2: agent-2.ra.local
- Database MSSQL in cluster: mssql.ra.local

#### Bilanciamento del carico

- Bilanciamento del carico appliance vRealize Automation: vrava.ra.local
- Bilanciamento del carico Web infrastruttura: web.ra.local
- Bilanciamento del carico servizio gestione infrastruttura: manager.ra.local

## Certificati

I nomi host utilizzati in questa tabella sono solo esempi.

Ruolo server	CN o SAN
Appliance vRealize Automation	SAN contiene i seguenti nomi host: <ul style="list-style-type: none"> <li>▪ vrava.ra.local</li> <li>▪ vrava-1.ra.local</li> <li>▪ vrava-2.ra.local</li> </ul>
Server Web infrastruttura	SAN contiene i seguenti nomi host: <ul style="list-style-type: none"> <li>▪ web.ra.local</li> <li>▪ web-1.ra.local</li> <li>▪ web-2.ra.local</li> </ul>
Server gestione infrastruttura	SAN contiene i seguenti nomi host: <ul style="list-style-type: none"> <li>▪ manager.ra.local</li> <li>▪ manager-1.ra.local</li> <li>▪ manager-2.ra.local</li> </ul>
Appliance vRealize Business for Cloud	CN = vrb.ra.local

## Porte

Gli utenti devono poter accedere a determinate porte. Tutte le porte elencate sono predefinite.

Ruolo server	Porta
Bilanciamento del carico appliance vRealize Automation	443, 8444 Porta 88444 necessaria per la VMware Remote Console.

Gli amministratori devono poter accedere a determinate porte, oltre alle porte alle quali devono poter accedere gli utenti.

Ruolo server	Porta
Appliance vRealize Automation	5480, 8443. La porta 8443 è usata per la configurazione della gestione delle identità avanzata. VMware Identity Manager in Active Directory: 389, 636, 3268, 3269 VMware Identity Manager in controller di dominio: 88, 464, 135
Server vRealize Business for Cloud	5480

Il sistema deve supportare le appropriate comunicazioni fra applicazioni.

Ruolo server	Porte in entrata	Porte in uscita per servizio o sistema
vRealize Automation		
Appliance vRealize Automation	HTTPS: 443 Configurazione adattatore: 8443 Proxy console remota: 8444 Postgres: 5432 Rabbit MQ: 4369, 25672, 5671, 5672 ElasticSearch: 9300, 40002, 40003 Stomp: 61613 SSH: 22 Centro di controllo: 8283	LDAP: 389 LDAPS: 636 Appliance vRealize Automation: 5432, 4369, 25672, 5671, 5672, 9300, 40002, 40003. Bilanciamento del carico Web infrastruttura vRealize Automation: 443 VMware ESXi: 902. Web infrastruttura richiede accesso alla porta 443 dell'endpoint vSphere per ottenere un ticket per VMware Remote Console. Appliance vRealize Automation richiede l'accesso alla porta host ESXi 902 per fungere da proxy dei dati console per l'utente. Autenticazione Kerberos: 88 Rinnovo password oggetto computer: 464

Ruolo server	Porte in entrata	Porte in uscita per servizio o sistema
Server Web infrastruttura	HTTPS: 443 MSDTC: 443, 1024-65535. Per informazioni su come limitare questo intervallo, consultare la sezione relativa alla distribuzione del database di <a href="#">Distribuzione di vRealize Automation</a> .	Bilanciamento del carico appliance vRealize Automation: 443 Appliance virtuale appliance vRealize Automation: 5480. Endpoint vSphere: 443. Web infrastruttura richiede accesso alla porta 443 dell'endpoint vSphere per ottenere un ticket per VMware Remote Console. L'appliance vRealize Automation richiede l'accesso alla porta host ESXi 902 per fungere da proxy dei dati console per l'utente. MSSQL: 135, 1433, da 1024 a 65535. Per informazioni su come limitare questo intervallo, consultare la sezione relativa alla distribuzione del database di <a href="#">Distribuzione di vRealize Automation</a> .
Server gestione infrastruttura	HTTPS: 443 MSDTC: 135,1024-65535. Per informazioni su come limitare questo intervallo, consultare la sezione relativa alla distribuzione del database di <a href="#">Distribuzione di vRealize Automation</a> .	Bilanciamento del carico appliance vRealize Automation: 443 Bilanciamento del carico Web infrastruttura vRealize Automation: 443 Appliance di vRealize Automation: 443, 5480 MSSQL: 135, 1433, da 1024 a 65535. Per informazioni su come limitare questo intervallo, consultare la sezione relativa alla distribuzione del database di <a href="#">Distribuzione di vRealize Automation</a> .
Server DEM infrastruttura	NA	Bilanciamento del carico appliance vRealize Automation: 443 Bilanciamento del carico Web infrastruttura vRealize Automation: 443 Bilanciamento del carico gestione infrastruttura vRealize Automation: 443 Bilanciamento del carico vRealize Orchestrator: 8281 Appliance vRealize Automation: 5480.

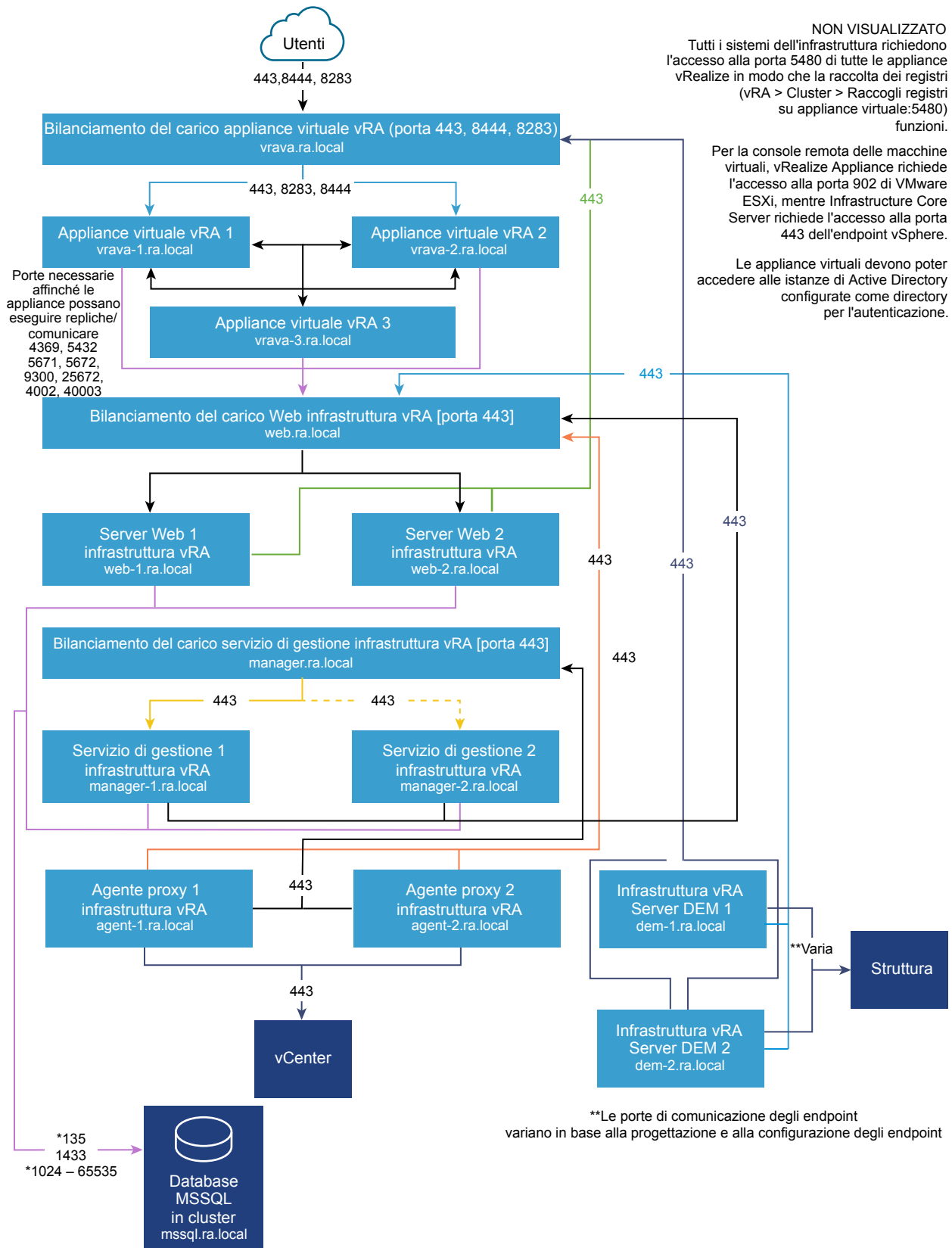
Ruolo server	Porte in entrata	Porte in uscita per servizio o sistema
Server agente infrastruttura	NA	<p>Bilanciamento del carico Web infrastruttura vRealize Automation: 443</p> <p>Bilanciamento del carico gestione infrastruttura vRealize Automation: 443</p> <p>Appliance vRealize Automation: 5480.</p>
Server database MSSQL	<p>MSSQL: 1433</p> <p>MSDTC: 135, 1024-65535. Per informazioni su come limitare questo intervallo, consultare la sezione relativa alla distribuzione del database di <a href="#">Distribuzione di vRealize Automation</a>.</p>	<p>Server Web infrastruttura: 135, 1024-65535. Per informazioni su come limitare questo intervallo, consultare la sezione relativa alla distribuzione del database di <a href="#">Distribuzione di vRealize Automation</a>.</p> <p>Server gestione infrastruttura: 135, 1024-65535. Per informazioni su come limitare questo intervallo, consultare la sezione relativa alla distribuzione del database di <a href="#">Distribuzione di vRealize Automation</a>.</p>
Server vRealize Business for Cloud	<p>HTTPS: 443</p> <p>SSH: 22</p> <p>Console gestione appliance virtuale: 5480</p>	<p>Bilanciamento del carico appliance vRealize Automation: 443</p> <p>Bilanciamento del carico Web infrastruttura vRealize Automation: 443</p>
Catalogo globale		Catalogo globale: 3268, 3269

Il bilanciamento del carico richiede l'accesso dalle seguenti porte.

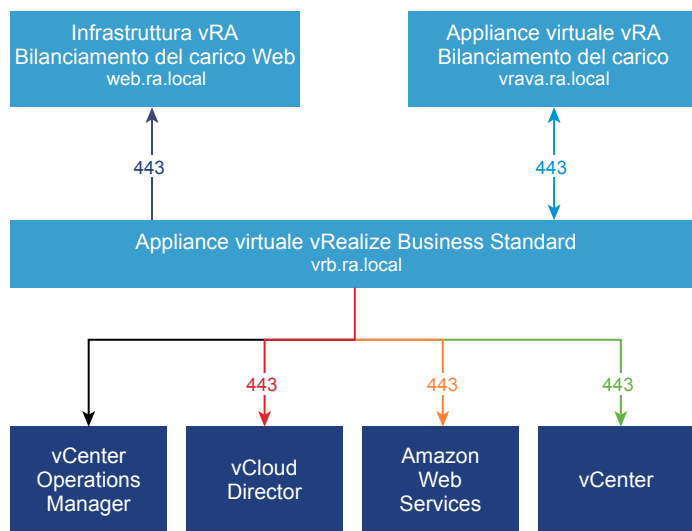
Bilanciamento del carico	Porte bilanciate
Bilanciamento del carico appliance vRealize Automation	443, 8444
Bilanciamento del carico Web infrastruttura vRealize Automation	443
Bilanciamento del carico server gestione vRealize Automation	443

## Grafici

Figura 1-5. Dimensioni minime per configurazione estesa di vRealize Automation



\*Vedere la sezione relativa alla distribuzione dei database per informazioni su come ridurre questo intervallo. È inoltre necessaria la comunicazione bidirezionale.

**Figura 1-6. Dimensioni minime per configurazione estesa di vRealize Business for Cloud**

## Distribuzioni di dati di vRealize Automation in più data center

vRealize Automation supporta la gestione di risorse in data center remoti.

Per gestire risorse di vSphere, HyperV o Xen in data center remoti, distribuire l'agente proxy in una macchina virtuale nel data center remoto.

**Nota** Il diagramma seguente illustra una distribuzione di vSphere. Gli altri endpoint non richiedono alcuna configurazione aggiuntiva.

Poiché è probabile che i workflow di vRealize Orchestrator comunicheranno tramite WAN, è consigliabile seguire le procedure descritte nella *guida alla progettazione del codice di vRealize Orchestrator*.

**Tabella 1-3. Porte necessarie per la comunicazione WAN**

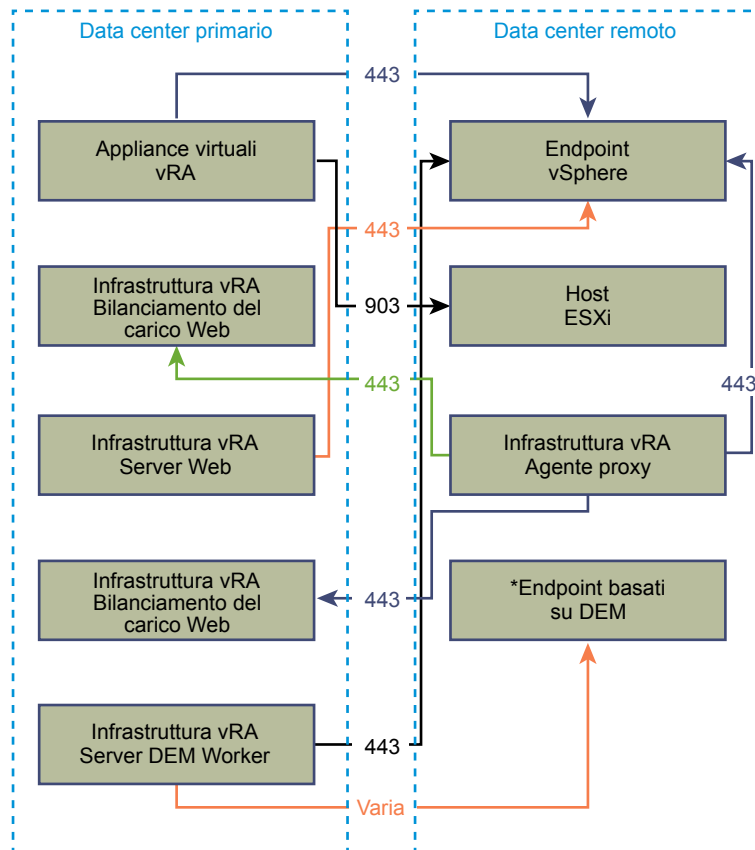
Ruolo	Porte in entrata	Porte in uscita di servizio/sistema
Appliance vRealize Automation, inclusa la versione incorporata di vRealize Orchestrator	N/A	Endpoint vSphere: 443 Host ESXi: 903
Bilanciamento del carico infrastruttura vRealize Automation	Agente proxy infrastruttura vRealize Automation: 443	N/A
Server Web infrastruttura vRealize Automation	N/A	Endpoint vSphere: 443
Bilanciamento del carico gestione infrastruttura vRealize Automation	Agente proxy infrastruttura vRealize Automation: 443	N/A
Server DEM Worker infrastruttura vRealize Automation	N/A	Endpoint: **varia

\* Se i Worker DEM sono installati nella macchina del servizio di gestione o in un altro server, queste porte devono essere aperte tra la macchina e l'endpoint target.



\*\* La porta necessaria per la comunicazione con un endpoint esterno varia a seconda dell'endpoint. Per impostazione predefinita, per vSphere si tratta della porta 443.

**Figura 1-7. Configurazione di vRealize Automation in più siti**



## vRealize Automation Secure Configuration

Secure Configuration descrive come verificare, configurare e aggiornare il profilo di protezione di una distribuzione di vRealize Automation in base alle linee guida di VMware.

Secure Configuration illustra i seguenti argomenti:

- Protezione dell'infrastruttura software
- Protezione della configurazione distribuita
- Protezione della rete host

## Panoramica su baseline sicura per vRealize Automation

VMware fornisce una serie di raccomandazioni complete che consentono di verificare e configurare una baseline sicura per il sistema vRealize Automation.

Utilizzare gli strumenti appropriati e le procedure consigliate da VMware per verificare e mantenere una configurazione della baseline sicura e con protezione avanzata per il sistema vRealize Automation. Alcuni componenti di vRealize Automation sono installati in uno stato di protezione avanzata o protezione avanzata parziale, ma è opportuno riesaminare e verificare la configurazione di ciascun componente alla luce delle raccomandazioni di sicurezza di VMware, dei criteri di protezione dell'azienda e delle minacce note.

## Comportamento della protezione di vRealize Automation

Il comportamento della protezione di vRealize Automation ipotizza un ambiente olisticamente sicuro, basato su configurazione di sistema e rete, criteri di protezione dell'organizzazione e procedure di sicurezza consigliate.

Quando si verifica e si configura la protezione avanzata di un sistema vRealize Automation, tenere in considerazione ognuna delle seguenti aree interessate dalle raccomandazioni di VMware relative alla protezione avanzata.

- Distribuzione sicura
- Secure Configuration
- Sicurezza della rete

Per garantire una protezione avanzata sicura del sistema, considerare le raccomandazioni di VMware e i criteri di protezione locali in relazione ad ognuna di queste aree concettuali.

## Componenti del sistema

Quando si considera la protezione avanzata e la configurazione sicura del proprio sistema vRealize Automation, assicurarsi di comprendere tutti i componenti e come interagiscono per supportare le funzionalità del sistema.

Quando si pianifica e si implementa un sistema sicuro, tenere in considerazione i seguenti componenti.

- Appliance vRealize Automation
- Componente IaaS

Per familiarizzare con vRealize Automation e con il modo in cui i componenti operano insieme, vedere [Nozioni fondamentali e concetti](#) nel centro documentazione di VMware vRealize Automation. Per informazioni sulle distribuzioni e sull'architettura tipiche di vRealize Automation, vedere [Architettura di riferimento di vRealize Automation](#).

## Verifica dell'integrità del supporto di installazione

Gli utenti dovrebbero sempre verificare l'integrità del supporto di installazione prima di installare un prodotto VMware.

Verificare sempre l'hash SHA1 dopo aver scaricato una ISO, un bundle offline o una patch per assicurarsi che i file scaricati siano integri e autentici. Se si ottiene un supporto fisico da VMware e il sigillo di sicurezza risulta danneggiato, restituire il software a VMware affinché venga sostituito.

Dopo aver scaricato il supporto, utilizzare il valore della somma MD5/SHA1 per verificare l'integrità del download. Confrontare l'output dell'hash MD5/SHA1 con il valore pubblicato sul sito Web di VMware. L'hash SHA1 o MD5 deve coincidere.

Per ulteriori informazioni sulla verifica dell'integrità del supporto di installazione, vedere <http://kb.vmware.com/kb/1537>.

## Proteggere l'infrastruttura software del sistema VMware

Durante le operazioni di protezione, valutare l'infrastruttura del software distribuito che supporta il sistema VMware e verificare che soddisfi le linee guida per la protezione di VMware.

Prima di proteggere il sistema VMware, esaminare e risolvere le vulnerabilità della sicurezza nell'infrastruttura del software di supporto per creare un ambiente sicuro e completamente protetto. Gli elementi dell'infrastruttura software da considerare includono i componenti del sistema operativo, il software di supporto e il software del database. Provare a risolvere i problemi di sicurezza in questi e negli altri componenti seguendo i suggerimenti del produttore e utilizzando altri protocolli di sicurezza pertinenti.

### Proteggere l'ambiente VMware vSphere®

Valutare l'ambiente VMware vSphere® e verificare che siano state applicate e mantenute le linee guida appropriate per la protezione di vSphere.

Per ulteriori istruzioni sulla protezione, vedere <http://www.vmware.com/security/hardening-guides.html>.

Essendo integrata in un ambiente completamente protetto, l'infrastruttura VMware vSphere® deve soddisfare le linee guida per la sicurezza stabilite da VMware.

### Proteggere l'host Infrastructure as a Service

Verificare che la macchina host Infrastructure as a Service Microsoft Windows sia protetta in base alle linee guida di VMware.

Consultare i suggerimenti nelle linee guida pertinenti delle procedure consigliate di protezione e sicurezza di Microsoft Windows e verificare che l'host Windows Server sia protetto in modo appropriato. La mancata applicazione dei suggerimenti per la protezione potrebbe comportare l'esposizione a vulnerabilità della sicurezza note per i componenti non protetti delle versioni di Windows.

Per verificare che la versione in uso sia supportata, fare riferimento alla [Matrice di supporto di vRealize Automation](#).

Per istruzioni corrette sulle procedure di protezione dei prodotti Microsoft, contattare il rivenditore Microsoft.

### Proteggere Microsoft SQL Server

Verificare che il database Microsoft SQL Server soddisfi le linee guida per la sicurezza stabilite da Microsoft e VMware.

Consultare i suggerimenti contenuti nelle linee guida pertinenti delle procedure consigliate di sicurezza e protezione di Microsoft SQL Server. Leggere tutti i bollettini di sicurezza Microsoft relativi alla versione installata di Microsoft SQL Server. La mancata applicazione dei suggerimenti per la protezione potrebbe comportare l'esposizione a vulnerabilità della sicurezza note per i componenti non protetti delle versioni di Microsoft SQL Server.

Per verificare che la versione di Microsoft SQL Server in uso sia supportata, fare riferimento alla [Matrice di supporto di vRealize Automation](#).

Per istruzioni sulle procedure di protezione per i prodotti Microsoft, contattare il rivenditore Microsoft.

## Proteggere Microsoft .NET

Essendo integrato in un ambiente completamente protetto, Microsoft .NET deve soddisfare le linee guida per la sicurezza stabilite da Microsoft e VMware.

Consultare i suggerimenti contenuti nelle linee guida pertinenti delle procedure consigliate di sicurezza e protezione di .NET. Leggere inoltre tutti i bollettini Microsoft sulla sicurezza relativi alla versione di Microsoft SQL Server in uso. La mancata applicazione dei suggerimenti per la protezione potrebbe comportare l'esposizione a vulnerabilità della sicurezza note per i componenti Microsoft.NET non protetti.

Per verificare che la versione di Microsoft.NET in uso sia supportata, fare riferimento alla [Matrice di supporto di vRealize Automation](#).

Per istruzioni sulle procedure di protezione per i prodotti Microsoft, contattare il rivenditore Microsoft.

## Proteggere Microsoft Internet Information Services (IIS)

Verificare che Microsoft Internet Information Services (IIS) rispetti tutte le linee guida per la sicurezza stabilite da Microsoft e VMware.

Consultare i suggerimenti contenuti nelle linee guida delle procedure consigliate per la sicurezza e la protezione di Microsoft IIS. Leggere inoltre tutti i bollettini Microsoft sulla sicurezza relativi alla versione di IIS in uso. La mancata applicazione dei suggerimenti per la protezione potrebbe comportare l'esposizione a vulnerabilità della sicurezza note.

Per verificare che la versione in uso sia supportata, fare riferimento alla [Matrice di supporto di vRealize Automation](#).

Per istruzioni sulle procedure di protezione per i prodotti Microsoft, contattare il rivenditore Microsoft.

## Revisione del software installato

Poiché le vulnerabilità nel software di terze parti o inutilizzato aumentano il rischio di accessi non autorizzati al sistema e interruzione della disponibilità, è importante rivedere tutto il software installato nelle macchine host di VMware e valutarne l'utilizzo.

Non installare software che non è necessario per il funzionamento sicuro del sistema nelle macchine host di VMware. Disinstallare il software estraneo o inutilizzato.

## Software non supportato installato in inventario

Valutare la propria distribuzione di VMware e l'inventario dei prodotti installati per verificare che non sia installato software estraneo non supportato.

Per ulteriori informazioni sui criteri di supporto per i prodotti di terze parti, vedere l'articolo sul supporto di VMware all'indirizzo <https://www.vmware.com/support/policies/thirdparty.html>.

## Verificare il software di terze parti

VMware non supporta né consiglia l'installazione di software di terze parti che non sia stato testato e verificato. Software di terze parti non sicuro, senza le patch o non autenticato, installato in macchine host di VMware, può esporre il sistema al rischio di accessi non autorizzati e interruzione della disponibilità. Se è necessario utilizzare software di terze parti non supportato, consultare il fornitore terzo per conoscere la configurazione sicura e i requisiti di applicazione delle patch.

## Avvisi di sicurezza e patch di VMware

Per garantire la massima protezione del sistema, attenersi agli avvisi di sicurezza rilasciati da VMware e applicare tutte le patch pertinenti.

VMware rilascia avvisi di sicurezza per i prodotti. Monitorare questi avvisi per assicurarsi che il prodotto sia protetto dalle minacce note.

Esaminare la cronologia delle installazioni, delle applicazioni delle patch e degli aggiornamenti di vRealize Automation e verificare che gli avvisi di sicurezza rilasciati da VMware vengano seguiti e implementati.

Per ulteriori informazioni sugli avvisi di sicurezza correnti di VMware, vedere <http://www.vmware.com/security/advisories/>.

## Secure Configuration

Verificare e aggiornare le impostazioni di sicurezza per le appliance virtuali di vRealize Automation e il componente Infrastructure as a Service nel modo appropriato in base alla configurazione del sistema. Inoltre, verificare e aggiornare la configurazione di altri componenti e applicazioni.

Per configurare in modo sicuro un'installazione di vRealize Automation, è necessario agire sia sulla configurazione di ciascun componente singolarmente, sia sull'interazione dei componenti. Considerare la configurazione di tutti i componenti del sistema nel loro insieme per ottenere una baseline ragionevolmente sicura.

## Protezione dell'appliance vRealize Automation

Verificare e aggiornare le impostazioni di sicurezza dell'appliance vRealize Automation in base alle esigenze della configurazione del sistema.

Configurare le impostazioni di sicurezza delle appliance virtuali e dei relativi sistemi operativi host. Inoltre, impostare o verificare la configurazione di altri componenti e applicazioni correlati. In alcuni casi è necessario verificare le impostazioni esistenti, mentre in altri è necessario modificare o aggiungere impostazioni per ottenere una configurazione appropriata.

### Modifica della password root

È possibile modificare la password root di Appliance vRealize Automation per soddisfare i requisiti di sicurezza applicabili.

Modificare la password root nell'Appliance vRealize Automation tramite l'interfaccia di gestione dell'appliance virtuale. Verificare che la password root soddisfi i requisiti aziendali di complessità delle password.

#### Procedura

- 1 Aprire l'interfaccia di gestione dell'appliance virtuale dell'istanza di Appliance vRealize Automation in uso.  
`https://vRealizeAppliance-url:5480`
- 2 Selezionare la scheda **Amministrazione** dell'interfaccia di gestione dell'appliance virtuale.
- 3 Selezionare il sottomenu **Amministrazione**.
- 4 Immettere la password esistente nella casella di testo **Password amministratore corrente**.
- 5 Immettere la nuova password nella casella di testo **Nuova password amministratore**.
- 6 Immettere la nuova password nella casella di testo **Ridigita la nuova password amministratore**.
- 7 Fare clic su **Salva impostazioni** per salvare le modifiche.

### Verifica dell'hash e della complessità della password root

Verificare che la password root soddisfi i requisiti aziendali di complessità delle password.

È necessario controllare la complessità della password root perché per l'utente root non viene eseguito il controllo di complessità della password del modulo pam\_cracklib, applicato agli account utente.

La password dell'account deve iniziare con \$6\$, che indica un hash sha512. Questo è l'hash standard per tutte le appliance con protezione avanzata.

#### Procedura

- 1 Per verificare l'hash della password root, accedere come root ed eseguire il comando `# more /etc/shadow`.

Vengono visualizzate le informazioni dell'hash.

**Figura 1-8. Risultati hash password**

```
vcac148-084-111:~ $ more /etc/shadow
bin:!:16332:0:60:7:::
daemon:!:16332:0:60:7:::
haldaemon:!:16332:0:60:7:::
mail:!:15870:0:60:::
man:!:16332:0:60:7:::
messagebus:!:16332:0:60:7:::
nobody:!:15870:0:60:::
ntp:!:16332:0:60:7:::
polkituser:!:16332:0:60:7:::
postfix:!:16332:0:60:7:::
root:$6$PHxGPY5A$ba8KzK4SS44UEHPfAtgs
P/:16346:0:365:7:::
```

- 2 Se la password root non contiene un hash sha512, eseguire il comando `passwd` per modificarla.

Tutte le appliance con protezione avanzata abilitano `enforce_for_root` per il modulo `pw_history`, che si trova nel file `/etc/pam.d/common-password`. Per impostazione predefinita, il sistema ricorda le ultime cinque password. Le password precedenti di ciascun utente vengono memorizzate nel file `/etc/securetty/passwd`.

### Verifica della cronologia delle password root

Verificare che per l'account root venga applicata la cronologia delle password.

Tutte le appliance con protezione avanzata abilitano `enforce_for_root` per il modulo `pw_history`, che si trova nel file `/etc/pam.d/common-password`. Per impostazione predefinita, il sistema ricorda le ultime cinque password. Le password precedenti di ciascun utente vengono memorizzate nel file `/etc/securetty/passwd`.

### Procedura

- 1 Eseguire il comando seguente.

```
cat /etc/pam.d/common-password-vmware.local | grep pam_pwhistory.so
```

- 2 Assicurarsi che nei risultati restituiti sia presente `enforce_for_root`.

```
password required pam_pwhistory.so enforce_for_root remember=5 retry=3
```

### Gestione della scadenza delle password

Configurare le scadenze delle password di tutti gli account in base ai criteri di protezione dell'organizzazione.

Per impostazione predefinita, la protezione avanzata di tutti gli account dell'appliance virtuale VMware prevede una durata della password di 60 giorni. Nella maggior parte delle appliance con protezione avanzata, la durata della password impostata per l'account root è di 365 giorni. È consigliabile verificare che per tutti gli account la durata impostata soddisfi gli standard dei requisiti di sicurezza e di quelli operativi.

Se la password root scade, non è possibile ripristinarla. È necessario implementare criteri specifici per i siti per impedire la scadenza delle password degli account amministrativi e root.

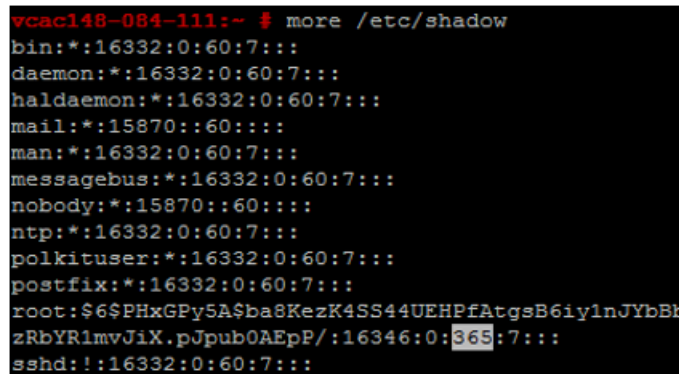
## Procedura

- 1 Accedere alle macchine dell'appliance virtuale come utente root ed eseguire il seguente comando per verificare la scadenza delle password per tutti gli account.

```
# cat /etc/shadow
```

La scadenza della password è specificata nel quinto campo (i campi sono separati da due punti) del file shadow. La scadenza dell'account root è impostata in giorni.

**Figura 1-9. Campo scadenza password**



```
vcac148-084-111:~ # more /etc/shadow
bin:!:16332:0:60:7:::
daemon:!:16332:0:60:7:::
haldaemon:!:16332:0:60:7:::
mail:!:15870::60:::
man:!:16332:0:60:7:::
messagebus:!:16332:0:60:7:::
nobody:!:15870::60:::
ntp:!:16332:0:60:7:::
polkituser:!:16332:0:60:7:::
postfix:!:16332:0:60:7:::
root:$6$PHxGPY5A$ba8KzK4SS44UEHPfAtgsB6iy1nJYbBk
zRbYR1mvJiX.pJpub0AEpP/:16346:0:365:7:::
sshd:!:16332:0:60:7:::
```

- 2 Per modificare la scadenza dell'account root, eseguire un comando del tipo seguente.

```
# passwd -x 365 root
```

In questo comando, il valore 365 specifica il numero di giorni della durata della password. Utilizzare lo stesso comando per modificare qualsiasi altro utente, sostituendo "root" con l'account specifico e il numero di giorni in base agli standard di scadenza stabiliti per l'organizzazione.

## Gestione degli account SSH e amministrativi

Per le connessioni remote, tutte le appliance con protezione avanzata includono il protocollo Secure Shell (SSH). Utilizzare SSH solo se necessario e gestirlo in modo appropriato per preservare la sicurezza del sistema.

SSH è un ambiente interattivo da riga di comando che supporta le connessioni remote alle appliance virtuali VMware. Per impostazione predefinita, l'accesso a SSH richiede credenziali di account utente con privilegi elevati. In genere, le attività SSH dell'utente root escludono il controllo degli accessi in base al ruolo (RBAC) e i controlli delle appliance virtuali.

È consigliabile disattivare SSH negli ambienti di produzione e attivarlo solo per la risoluzione dei problemi che non possono essere risolti in altro modo. Lasciarlo abilitato solo per il tempo necessario a raggiungere uno scopo specifico e nel rispetto dei criteri di protezione dell'organizzazione. Nell'appliance vRealize Automation SSH è disabilitato per impostazione predefinita. In base alla configurazione di vSphere in uso, SSH può essere abilitato o disabilitato quando si distribuisce il proprio modello OVF (Open Virtualization Format).

Per sapere se in una macchina è abilitato SSH, è sufficiente provare ad aprire una connessione utilizzando il protocollo SSH. Se la connessione viene stabilita e vengono richieste le credenziali, significa che SSH è abilitato e disponibile per le connessioni.



## Account utente root di SSH

Poiché le appliance VMware non includono account utente preconfigurati, l'account root può utilizzare SSH per accedere direttamente per impostazione predefinita. Disabilitare SSH come root non appena possibile.

Per rispettare gli standard di conformità per il non ripudio, il server SSH in tutte le appliance con protezione avanzata è preconfigurato con la voce AllowGroups wheel per limitare l'accesso SSH al gruppo wheel secondario. Per separare i compiti, è possibile modificare la voce AllowGroups wheel nel file `/etc/ssh/sshd_config` in modo che utilizzi un altro gruppo, ad esempio `sshd`.

Il gruppo wheel è abilitato con il modulo `pam_wheel` per l'accesso superuser, pertanto i membri del gruppo wheel possono utilizzare `su-root` quando è richiesta la password di root. La separazione dei gruppi consente agli utenti di connettersi all'appliance tramite SSH, ma non di utilizzare `su-to-root`. Non rimuovere o modificare le altre voci nel campo AllowGroups per assicurare il corretto funzionamento dell'appliance. Dopo aver apportato una modifica, è necessario riavviare il daemon SSH eseguendo il comando: `# service sshd restart`.

## Abilitare o disabilitare il servizio SS nelle appliance di vRealize Automation

Abilitare il servizio SSH (Secure Shell) nell'appliance vRealize Automation solo per la risoluzione dei problemi. Durante le normali operazioni di produzione, disabilitare SSH in questi componenti.

È possibile abilitare o disabilitare SSH nell'appliance vRealize Automation utilizzando la console di gestione dell'appliance virtuale.

### Procedura

- 1 Passare alla console di gestione dell'appliance virtuale per l'appliance vRealize Automation in uso.  
: `https://vRealizeAppliance url:5480`
- 2 Fare clic sulla scheda **Amministrazione**.
- 3 Fare clic sul menu secondario **Amministrazione**.
- 4 Selezionare la casella di controllo di abilitazione del servizio SSH per abilitare SSH o deselezionarla per disabilitarlo.
- 5 Fare clic su **Salva impostazioni** per salvare le modifiche.

## Creazione di un account amministratore locale per Secure Shell

Come procedura consigliata per la sicurezza, creare e configurare account amministrativi locali per Secure Shell nelle macchine host dell'appliance virtuale. Rimuovere inoltre l'accesso SSH root dopo aver creato gli account appropriati.

Creare account amministrativi locali per SSH o membri del gruppo wheel secondario o entrambi. Prima di disabilitare l'accesso root diretto, verificare che gli amministratori autorizzati possano accedere a SSH mediante AllowGroups e che possano eseguire `su-to-root` usando il gruppo wheel.

## Procedura

- 1 Accedere all'appliance virtuale come root ed eseguire i seguenti comandi con il nome utente appropriato.

```
# useradd -g users <username> -G wheel -m -d /home/username
# passwd username
```

Wheel è il gruppo specificato in AllowGroups per l'accesso ssh. Per aggiungere più gruppi secondari, usare `-G wheel,sshd`.

- 2 Passare all'utente e fornire una nuova password per applicare il controllo della complessità della password.

```
# su -username
# username@hostname:~>passwd
```

Se i requisiti di complessità della password sono soddisfatti, la password viene aggiornata. Se i requisiti di complessità della password non sono soddisfatti, viene ripristinata la password originale ed è necessario eseguire di nuovo il comando della password.

- 3 Per rimuovere l'accesso diretto a SSH, modificare il file `/etc/ssh/sshd_config` sostituendo `(#)PermitRootLogin yes` con `PermitRootLogin no`.

In alternativa, è possibile abilitare/disabilitare SSH nell'interfaccia di gestione dell'appliance virtuale (Virtual Appliance Management Interface, VAMI) selezionando o deselezionando la casella di controllo **Accesso SSH amministratore abilitato** nella scheda **Amministrazione**.

## Operazioni successive

Disabilitare gli accessi diretti come root. Per impostazione predefinita, le appliance con protezione avanzata consentono l'accesso diretto a root tramite la console. Dopo aver creato gli account amministrativi per il non ripudio e averli provati per l'accesso wheel su-root, disabilitare gli accessi root diretti modificando il file `/etc/security` come root e sostituendo la voce `tty1` con `console`.

- 1 Aprire il file `/etc/securetty` in un editor di testo.
- 2 Individuare `tty1` e sostituirlo con `console`.
- 3 Salvare il file e chiuderlo.

## Proteggere la configurazione del server Secure Shell

Laddove possibile, tutte le appliance VMware hanno una configurazione protetta predefinita. Gli utenti possono verificare il livello di protezione della configurazione esaminando le impostazioni dei servizi del server e del client nella sezione delle opzioni globali del file di configurazione.

## Procedura

- 1 Aprire il file di configurazione del server `/etc/ssh/sshd_config` nell'appliance VMware e verificare che le impostazioni siano corrette.

Impostazione	Stato
Server Daemon Protocol	Protocollo 2
CBC Ciphers	aes256-ctr e aes128-ctr
TCP Forwarding	AllowTCPForwarding - No
Server Gateway Ports	Porte gateway - No
X11 Forwarding	X11Forwarding - No
SSH Service	Utilizzare il campo AllowGroups e specificare un gruppo con autorizzazione di accesso. Aggiungere i membri corretti a questo gruppo.
GSSAPI Authentication	GSSAPIAuthentication - No, se inutilizzata
Keberos Authentication	KeberosAuthentication - No, se inutilizzata
Local Variables (AcceptEnv global option)	Impostare su <code>disabled by commenting out</code> o su <code>enabled for LC_* or LANG variables</code>
Tunnel Configuration	PermitTunnel - No
Network Sessions	MaxSessions 1
User Concurrent Connections	Impostare su 1 per l'utente root e qualsiasi altro utente. È necessario configurare anche il file <code>/etc/security/limits.conf</code> con la stessa impostazione.
Strict Mode Checking	Strict Modes - Yes
Privilege Separation	UsePrivilegeSeparation - Yes
rhosts RSA Authentication	RhostsESAAuthentication - No
Compression	Compression delayed o Compression no
Message Authentication code	MACs hmac-sha1
User Access Restriction	PermitUserEnvironment - No

- 2 Salvare le modifiche e chiudere il file.

## Proteggere la configurazione del client Secure Shell

Durante le operazioni di potenziamento della protezione del sistema, verificare il livello di protezione del client SSH esaminandone il file di configurazione nelle macchine host dell'appliance virtuale per assicurarsi che sia configurato in base alle linee guida di VMware.

## Procedura

- 1 Aprire il file di configurazione del client SSH, `/etc/ssh/ssh_config` e verificare che le impostazioni nella sezione delle opzioni globali siano corrette.

Impostazione	Stato
Client Protocol	Protocollo 2
Client Gateway Ports	Porte gateway - No
GSSAPI Authentication	GSSAPIAuthentication - No
Local Variables (SendEnv global option)	Specificare solo variabili LC_* o LANG
CBC Ciphers	Solo aes256-ctr e aes128-ctr
Message Authentication Codes	Utilizzati solo nella voce MACs hmac-sha1

- 2 Salvare le modifiche e chiudere il file.

## Verifica delle autorizzazioni del file della chiave di SSH

Per ridurre al minimo la possibilità di attacchi dannosi, gestire in modo appropriato le autorizzazioni del file della chiave di Secure Shell (SSH) nelle macchine host dell'appliance virtuale.

Dopo aver configurato o aggiornato la configurazione di SSH, verificare sempre che le seguenti autorizzazioni del file della chiave di SSH non vengano modificate.

- I file delle chiavi degli host pubblici contenuti in `/etc/ssh/*key.pub` sono di proprietà dell'utente root e hanno le autorizzazioni impostate su 0644 (-rw-r--r--).
- I file delle chiavi degli host privati inclusi in `/etc/ssh/*key` sono di proprietà dell'utente root e hanno le autorizzazioni impostate su 0600 (-rw-----).

## Verifica delle autorizzazioni dei file di chiave SSH

Verificare che le autorizzazioni SSH vengano applicate sia ai file di chiave privata che di chiave pubblica.

## Procedura

- 1 Per verificare i file di chiave pubblica SSH, eseguire il comando seguente: `ls -l /etc/ssh/*key.pub`
- 2 Verificare che il proprietario sia di tipo root, che il proprietario del gruppo sia di tipo root e che le autorizzazioni dei file siano impostate su 0644 (-rw-r--r--).
- 3 Correggere eventuali problemi eseguendo i comandi riportati di seguito.
 

```
chown root /etc/ssh/*key.pub
chgrp root /etc/ssh/*key.pub
chmod 644 /etc/ssh/*key.pub
```
- 4 Per verificare i file di chiave privata SSH, eseguire il comando seguente: `ls -l /etc/ssh/*key`

- 5 Correggere eventuali problemi eseguendo i comandi riportati di seguito.

```
chown root /etc/ssh/*key
```

```
chgrp root /etc/ssh/*key
```

```
chmod 644 /etc/ssh/*key
```

### Modifica dell'utente dell'interfaccia di gestione dell'appliance virtuale

È possibile aggiungere ed eliminare utenti nell'interfaccia di gestione dell'appliance virtuale per creare il livello appropriato di sicurezza.

L'account utente root per l'interfaccia di gestione dell'appliance virtuale utilizza PAM per l'autenticazione, pertanto vengono applicati anche i livelli di ritaglio impostati da PAM. Se non è stata isolata in modo corretto l'interfaccia di gestione dell'appliance virtuale, è possibile che si verifichi un blocco dell'account root di sistema se un utente malintenzionato tenta di accedere effettuando un attacco di forza bruta. Inoltre, quando l'account root è considerato insufficiente al non ripudio da parte di più persone nella propria organizzazione, si può scegliere di cambiare l'utente amministratore per l'interfaccia di gestione.

#### Prerequisiti

#### Procedura

- 1 Eseguire il comando seguente per creare un nuovo utente e aggiungerlo al gruppo dell'interfaccia di gestione dell'appliance virtuale.

```
useradd -G vami,root user
```

- 2 Creare una password per l'utente.

```
passwd user
```

- 3 (Facoltativo) Eseguire il comando seguente per disattivare l'accesso root nell'interfaccia di gestione dell'appliance virtuale.

```
usermod -R vami root
```

---

**Nota** La disattivazione dell'accesso root all'interfaccia di gestione dell'appliance virtuale disattiva anche la possibilità di aggiornare la password dell'amministratore, ovvero la password root, dalla scheda Amministrazione.

---

### Impostazione dell'autenticazione del caricatore di avvio

Per fornire un livello di sicurezza adeguato, configurare l'autenticazione del caricatore di avvio nelle appliance virtuali VMware.

Se il caricatore di avvio del sistema non richiede alcuna autenticazione, gli utenti che dispongono dei diritti di accesso alla console del sistema possono alterare la configurazione di avvio del sistema o avviare il sistema in modalità utente singolo o in modalità di manutenzione, esponendolo al rischio di attacchi DoS (Denial of Service) o di accessi non autorizzati. Poiché l'autenticazione del caricatore di avvio non è impostata in modo predefinito nelle appliance virtuali VMware, è necessario creare una password GRUB per configurarla.

**Procedura**

- 1 Verificare se esiste una password di avvio individuando la riga `password --md5 <password-hash>` nel file `/boot/grub/menu.lst` nelle appliance virtuali.
- 2 Se non esiste alcuna password, eseguire il comando `# /usr/sbin/grub-md5-crypt` nell'appliance virtuale.  
Viene generata una password MD5 e il comando fornisce come output l'hash md5.
- 3 Aggiungere la password al file `menu.lst` eseguendo il comando `# password --md5 <hash from grub-md5-crypt>`.

**Configurazione del protocollo NTP**

Per il reperimento critico dell'ora, disabilitare la sincronizzazione dell'ora dell'host e usare il protocollo NTP (Network Time Protocol) nell'appliance vRealize Automation.

Il daemon NTP nell'appliance vRealize Automation fornisce servizi orari sincronizzati. Poiché il protocollo NTP è disabilitato per impostazione predefinita, è necessario configurarlo manualmente. Se possibile, negli ambienti di produzione usare NTP per monitorare le azioni degli utenti, nonché rilevare intrusioni e attacchi potenzialmente dannosi mediante accurati controlli e compilazioni dei registri. Per informazioni sugli avvisi di sicurezza relativi a NTP, consultare il sito Web di NTP.

Il file di configurazione di NTP si trova nella cartella `/etc/` delle singole appliance. È possibile abilitare il servizio NTP per l'appliance vRealize Automation e aggiungere server orari nella scheda

**Amministrazione** dell'interfaccia di gestione dell'appliance virtuale.

**Procedura**

- 1 Aprire il file di configurazione `/etc/ntp.conf` nella macchina host dell'appliance virtuale in un editor di testo.
- 2 Impostare la proprietà del file su **root:root**.
- 3 Impostare le autorizzazioni su **0640**.
- 4 Per ridurre il rischio di un attacco con amplificazione Denial of Service nel servizio NTP, aprire il file `/etc/ntp.conf` e verificare che siano presenti le righe di limitazione.

```
restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery
restrict 127.0.0.1
restrict -6 ::1
```

- 5 Salvare le eventuali modifiche e chiudere i file.

**Configurazione del protocollo TLS per i dati in transito dell'appliance vRealize Automation**

Assicurarsi che la distribuzione di vRealize Automation usi protocolli TLS complessi per proteggere i canali di trasmissione dei componenti dell'appliance vRealize Automation.

Per quanto riguarda le prestazioni, TLS non è abilitato per le connessioni localhost tra alcuni servizi delle applicazioni. Se è necessario applicare la difesa in profondità, abilitare TLS in tutte le comunicazioni localhost.

---

**Importante** Se si arresta TLS nel bilanciamento del carico, disabilitare i protocolli non sicuri, come SSLv2, SSLv3 e TLS 1.0, in tutti i bilanciamenti del carico.

---

## Abilitare TLS nella configurazione localhost

Per impostazione predefinita, alcune comunicazioni localhost non utilizzano TLS. È possibile abilitare TLS in tutte le connessioni localhost per fornire una protezione avanzata.

### Procedura

- 1 Connettersi all'Appliance vRealize Automation utilizzando il servizio SSH.
- 2 Impostare le autorizzazioni per l'archivio chiavi vcac eseguendo i comandi seguenti.

```
usermod -A vco,coredump,pivotal vco
chown vcac.pivotal /etc/vcac/vcac.keystore
chmod 640 /etc/vcac/vcac.keystore
```

- 3 Aggiornare la configurazione HAProxy.

- a Aprire il file di configurazione HAProxy che si trova in `/etc/haproxy/conf.d` e scegliere il servizio `20-vcac.cfg`.
- b Individuare le righe contenenti la stringa seguente:

```
server local 127.0.0.1... e aggiungere quanto segue alla fine di queste righe: ssl verify
none
```

Questa sezione contiene altre righe, ad esempio:

backend-horizon	backend-vro
backend-vra	backend-artifactory
backend-vra-health	

- c Modificare la porta di backend-horizon da 8080 a 8443.
- 4 Ottenere la password di keystorePass.

- a Individuare la proprietà `certificate.store.password` nel file `/etc/vcac/security.properties`.

Ad esempio `certificate.store.password=s2enc~iom0GXATG+RB8ff7Wdm4Bg==`

- b Decrittografare il valore utilizzando il comando seguente:

```
vcac-config prop-util -d --p VALUE
```

Ad esempio `vcac-config prop-util -d --p s2enc~iom0GXATG+RB8ff7Wdm4Bg==`

**5 Configurare il servizio vRealize Automation.**

- a Aprire il file `/etc/vcac/server.xml`.
- b Aggiungere l'attributo seguente al tag Connector, sostituendo `certificate.store.password` con il valore della password dell'archivio di certificati disponibile in `etc/vcac/security.properties`.

```
scheme="https" secure="true" SSLEnabled="true" sslProtocol="TLS"
keystoreFile="/etc/vcac/vcac.keystore" keyAlias="apache"
keystorePass="certificate.store.password"
```

**6 Configurare il servizio vRealize Orchestrator.**

- a Aprire il file `/etc/vco/app-server.xml`
- b Aggiungere l'attributo seguente al tag Connector, sostituendo `certificate.store.password` con il valore della password dell'archivio di certificati disponibile in `etc/vcac/security.properties`.

```
scheme="https" secure="true" SSLEnabled="true" sslProtocol="TLS"
keystoreFile="/etc/vcac/vcac.keystore" keyAlias="apache"
keystorePass="certificate.store.password"
```

**7 Riavviare vRealize Orchestrator, vRealize Automation e i servizi haproxy.**

```
service vcac-server restart
service vco-server restart
service haproxy restart
```

---

**Nota** Se il server vco non viene riavviato, riavviare il computer host.

---

**8 Configurare l'interfaccia di gestione dell'appliance virtuale.**

- a Aprire il file `/opt/vmware/share/htdocs/service/café-services/services.py`.
- b Sostituire la riga `conn = httpLib.HTTP()` con `conn = httpLib.HTTPS()` per una maggiore protezione.

**Abilitare la conformità a FIPS (Federal Information Processing Standard) 140-2**

L'appliance vRealize Automation ora utilizza la versione certificata FIPS (Federal Information Processing Standard) 140-2 di OpenSSL per i dati in transito su TLS in tutto il traffico di rete in entrata e in uscita.

È possibile abilitare o disabilitare la modalità FIPS nell'interfaccia di gestione dell'appliance vRealize Automation. È inoltre possibile configurare FIPS dalla riga di comando quando si accede come utente root, utilizzando i comandi seguenti:

```
vcac-vami fips enable
vcac-vami fips disable
vcac-vami fips status
```



Se FIPS è abilitato, il traffico di rete dell'Appliance vRealize Automation in entrata e in uscita sulla porta 443 utilizza la crittografia conforme a FIPS 140–2. Indipendentemente dall'impostazione di FIPS, vRealize Automation utilizza AES–256 per tutelare i dati protetti archiviati nell'appliance vRealize Automation.

---

**Nota** Attualmente, vRealize Automation abilita solo in parte la conformità a FIPS, poiché alcuni componenti interni non utilizzano ancora i moduli di crittografia certificati. Nei casi in cui i moduli certificati non sono ancora stati implementati, viene utilizzata la crittografia basata su AES–256 in tutti gli algoritmi di crittografia.

---

**Nota** La procedura seguente consentirà di riavviare la macchina fisica quando si modifica la configurazione.

---

#### Procedura

- 1 Accedere come root all'interfaccia di gestione dell'appliance vRealize Automation.  
`https:// vrealize-automation-appliance-FQDN:5480`
- 2 Selezionare **Impostazioni vRA > Impostazioni host**.
- 3 Fare clic sul pulsante sotto l'intestazione Azioni in alto a destra per abilitare o disabilitare la modalità FIPS.
- 4 Fare clic su **Sì** per riavviare l'appliance vRealize Automation.

#### Verifica dello stato di disabilitazione di SSLv3, TLS 1.0 e TLS 1.1

Nell'ambito del processo dell'applicazione della protezione avanzata, assicurarsi che Appliance vRealize Automation utilizzi canali di trasmissione sicuri.

---

**Nota** Non è possibile eseguire l'operazione di unione cluster una volta disabilitato TLS 1.0/1.1 e abilitato TLS 1.2

---

#### Prerequisiti

Completare la procedura [Abilitare TLS nella configurazione localhost](#).

## Procedura

- 1 Verificare che SSLv3, TLS 1.0 e TLS 1.1 siano disabilitati nei gestori https HAProxy in Appliance vRealize Automation.

File da esaminare	Parametro che deve essere presente	Nella riga appropriata corrispondente
/etc/haproxy/conf.d/20-vcac.cfg	no-ssl3 no-tls10 no-tls11 force-tls12	bind 0.0.0.0:443 ssl crt /etc/apache2/server.pem ciphers !aNULL:!eNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH no-ssl3 no-tls10 no-tls11
/etc/haproxy/conf.d/30-vro-config.cfg	no-ssl3 no-tls10 no-tls11 force-tls12	bind :::8283 v4v6 ssl crt /opt/vmware/etc/lighttpd/server.pem ciphers !aNULL:!eNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH no-ssl3 no-tls10 no-tls11

- 2 Riavviare il servizio.

```
service haproxy restart
```

- 3 Aprire il file /opt/vmware/etc/lighttpd/lighttpd.conf e verificare che contenga le voci di disabilitazione corrette.

**Nota** Non sono disponibili direttive per la disabilitazione di TLS 1.0 o TLS 1.1 in Lighttpd. La restrizione sull'utilizzo di TLS 1.1 e TLS 1.0 può essere parzialmente mitigata facendo in modo che OpenSSL non utilizzi le suite di crittografia di TLS 1.0 e TLS 1.1.

```
ssl.use-ssl2 = "disable"
ssl.use-ssl3 = "disable"
```

- 4 Verificare che SSLv3, TLS 1.0 e TLS 1.1 siano disabilitati per il proxy della console in Appliance vRealize Automation.

- a Modificare il file /etc/vcac/security.properties aggiungendo o modificando la riga seguente:

```
consoleproxy.ssl.server.protocols = TLSv1.2
```

- b Riavviare il server eseguendo il comando seguente:

```
service vcac-server restart
```

- 5 Verificare che SSLv3, TLS 1.0 e TLS 1.1 siano disabilitati per il servizio vCO.
  - a Individuare il tag <Connector> nel file /etc/vco/app-server/server.xml e aggiungere il seguente attributo:
 

```
sslEnabledProtocols = "TLSv1.2"
```
  - b Riavviare il servizio vCO con il seguente comando.
 

```
service vco-server restart
```
- 6 Verificare che SSLv3, TLS 1.0 e TLS 1.1 siano disabilitati per il servizio vRealize Automation.
  - a Aggiungere i seguenti attributi al tag <Connector> nel file /etc/vcac/server.xml.
 

```
sslEnabledProtocols = "TLSv1.2"
```
  - b Riavviare il servizio vRealize Automation mediante il seguente comando:
 

```
service vcac-server restart
```
- 7 Verificare che SSLv3, TLS 1.0 e TLS 1.1 siano disabilitati per RabbitMQ.
 

Aprire il file /etc/rabbitmq/rabbitmq.config e verificare che {versions, ['tlsv1.2', 'tlsv1.1']} sia presente nelle sezioni ssl e ssl\_options.

```
[
  {ssl, [
    {versions, ['tlsv1.2', 'tlsv1.1']},
    {ciphers, ["AES256-SHA", "AES128-SHA"]}
  ]},
  {rabbit, [
    {tcp_listeners, [{"127.0.0.1", 5672}]},
    {frame_max, 262144},
    {ssl_listeners, [5671]},
    {ssl_options, [
      {cacertfile, "/etc/rabbitmq/certs/ca/cacert.pem"},
      {certfile, "/etc/rabbitmq/certs/server/cert.pem"},
      {keyfile, "/etc/rabbitmq/certs/server/key.pem"},
      {versions, ['tlsv1.2', 'tlsv1.1']},
      {ciphers, ["AES256-SHA", "AES128-SHA"]},
      {verify, verify_peer},
      {fail_if_no_peer_cert, false}
    ]},
    {mnesia_table_loading_timeout, 600000},
    {cluster_partition_handling, autoheal},
    {heartbeat, 600}
  ]},
  {kernel, [{net_ticktime, 120}]}
].
```

- 8 Riavviare il server RabbitMQ.
 

```
# service rabbitmq-server restart
```

- 9 Verificare che SSLv3, TLS 1.0 e TLS 1.1 siano disabilitati per il servizio vIDM.

Aprire il file `opt/vmware/horizon/workspace/conf/server.xml` per ogni istanza del connettore contenente `SSLEnabled="true"` e assicurarsi che sia presente la seguente riga.

```
sslEnabledProtocols="TLSv1.2"
```

### Configurazione di pacchetti di crittografia TLS per i componenti vRealize Automation

Per ottenere la massima protezione, è necessario configurare i componenti di vRealize Automation in modo che usino crittografie complesse.

L'algoritmo di crittografia negoziato tra il server e il browser determina la complessità della crittografia usata in una sessione TLS.

Per assicurare che vengano selezionate solo crittografie complesse, disabilitare le crittografie vulnerabili nei componenti di vRealize Automation. Configurare il server in modo che supporti solo crittografie complesse e utilizzi dimensioni di chiave sufficientemente grandi. Configurare inoltre tutte le crittografie in un ordine adeguato.

Disabilitare i pacchetti di crittografia che non offrono autenticazione, come i pacchetti di crittografia NULL, ovvero aNULL o eNULL. Disabilitare inoltre lo scambio di chiavi Diffie-Hellman anonimo (ADH), le crittografie a livello di esportazione (EXP, crittografie che contengono DES), le dimensioni di chiave inferiori a 128 bit per la codifica del traffico del payload, l'uso di MD5 come meccanismo di hashing per il traffico del payload, i pacchetti di crittografia IDEA e i pacchetti di crittografia RC4. Assicurarsi inoltre che i pacchetti di crittografia che usano lo scambio di chiavi Diffie-Hellman (DHE) siano disabilitati

### Disabilitare i pacchetti di crittografia deboli nel proxy HA

Esaminare i pacchetti di crittografia del servizio proxy HA dell'appliance vRealize Automation facendo riferimento all'elenco di pacchetti accettabili e disabilitare tutti quelli considerati deboli.

Disabilitare i pacchetti di crittografia che non offrono autenticazione, come i pacchetti di crittografia NULL, ovvero aNULL o eNULL. Disabilitare inoltre lo scambio di chiavi Diffie-Hellman anonimo (ADH), le crittografie a livello di esportazione (EXP, crittografie che contengono DES), le dimensioni di chiave inferiori a 128 bit per la codifica del traffico del payload, l'uso di MD5 come meccanismo di hashing per il traffico del payload, i pacchetti di crittografia IDEA e i pacchetti di crittografia RC4.

### Procedura

- 1 Esaminare la voce della direttiva di binding relativa ai pacchetti di crittografia del file `/etc/haproxy/conf.d/20-vcac.cfg` e disabilitare tutti quelli considerati deboli.

```
bind 0.0.0.0:443 ssl crt /etc/apache2/server.pem ciphers !aNULL:!eNULL:kECDH
+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH no-ssl3 no-
tlsv10 no-tlsv11
```

- 2 Esaminare la voce della direttiva di binding relativa ai pacchetti di crittografia del file `/etc/haproxy/conf.d/30-vro-config.cfg` e disabilitare tutti quelli considerati deboli.

```
bind :::8283 v4v6 ssl crt /opt/vmware/etc/httpsd/server.pem ciphers !aNULL:!
eNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH
no-ssl3 no-tlsv10 no-tlsv11
```

## Disabilitazione dei pacchetti di crittografia deboli nel servizio proxy della console dell'appliance vRealize Automation

Esaminare i pacchetti di crittografia del servizio proxy della console dell'appliance vRealize Automation facendo riferimento all'elenco di pacchetti accettabili e disabilitare tutti quelli considerati deboli.

Disabilitare i pacchetti di crittografia che non offrono autenticazione, come i pacchetti di crittografia NULL, ovvero aNULL o eNULL. Disabilitare inoltre lo scambio di chiavi Diffie-Hellman anonimo (ADH), le crittografie a livello di esportazione (EXP, crittografie che contengono DES), le dimensioni di chiave inferiori a 128 bit per la codifica del traffico del payload, l'uso di MD5 come meccanismo di hashing per il traffico del payload, i pacchetti di crittografia IDEA e i pacchetti di crittografia RC4.

### Procedura

- 1 Aprire il file `/etc/vcac/security.properties` in un editor di testo.
- 2 Aggiungere una riga al file per disabilitare i pacchetti di crittografia indesiderati.

Utilizzare una variante della riga seguente:

```
consoleproxy.ssl.ciphers.disallowed=pacchetto_crittografia_1, pacchetto_crittografia_2 e così via
```

Ad esempio, per disabilitare i pacchetti di crittografia AES 128 e AES 256, aggiungere la riga seguente:

```
consoleproxy.ssl.ciphers.disallowed=TLS_DH_DSS_WITH_AES_128_CBC_SHA,
TLS_DH_DSS_WITH_AES_256_CBC_SHA, TLS_DH_RSA_WITH_AES_256_CBC_SHA,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA, TLS_DHE_DSS_WITH_AES_256_CBC_SHA,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA
```

- 3 Riavviare il server con il comando seguente.

```
service vcac-server restart
```

## Disabilitare i pacchetti di crittografia deboli nel servizio vCO di Appliance vRealize Automation

Esaminare i pacchetti di crittografia del servizio vCO di Appliance vRealize Automation facendo riferimento all'elenco di pacchetti accettabili e disabilitare tutti quelli considerati deboli.

Disabilitare i pacchetti di crittografia che non offrono autenticazione, come i pacchetti di crittografia NULL, ovvero aNULL o eNULL. Disabilitare inoltre lo scambio di chiavi Diffie-Hellman anonimo (ADH), le crittografie a livello di esportazione (EXP, crittografie che contengono DES), le dimensioni di chiave inferiori a 128 bit per la codifica del traffico del payload, l'uso di MD5 come meccanismo di hashing per il traffico del payload, i pacchetti di crittografia IDEA e i pacchetti di crittografia RC4.

### Procedura

- 1 Individuare il tag `<Connector>` nel file `/etc/vco/app/server/server.xml`.

- 2 Modificare o aggiungere l'attributo di crittografia in modo che vengano utilizzati i pacchetti di crittografia desiderati.

Fare riferimento all'esempio seguente:

```
ciphers="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
```

## Disabilitare i pacchetti di crittografia deboli nel servizio RabbitMQ di Appliance vRealize Automation

Esaminare i pacchetti di crittografia del servizio RabbitMQ di Appliance vRealize Automation facendo riferimento all'elenco di pacchetti di crittografia accettabili e disabilitare tutti quelli considerati deboli.

Disabilitare i pacchetti di crittografia che non offrono autenticazione, come i pacchetti di crittografia NULL, ovvero aNULL o eNULL. Disabilitare inoltre lo scambio di chiavi Diffie-Hellman anonimo (ADH), le crittografie a livello di esportazione (EXP, crittografie che contengono DES), le dimensioni di chiave inferiori a 128 bit per la codifica del traffico del payload, l'uso di MD5 come meccanismo di hashing per il traffico del payload, i pacchetti di crittografia IDEA e i pacchetti di crittografia RC4.

### Procedura

- 1 Valutare i pacchetti di crittografia supportati eseguendo il comando `# /usr/sbin/rabbitmqctl eval 'ssl:cipher_suites()'`.

I pacchetti di crittografia restituiti nell'esempio seguente sono solo quelli supportati. Il server RabbitMQ non utilizza né comunica questi pacchetti di crittografia, a meno che non sia stato configurato a questo scopo nel file `rabbitmq.config`.

```
[ "ECDHE-ECDSA-AES256-GCM-SHA384", "ECDHE-RSA-AES256-GCM-SHA384",
  "ECDHE-ECDSA-AES256-SHA384", "ECDHE-RSA-AES256-SHA384",
  "ECDH-ECDSA-AES256-GCM-SHA384", "ECDH-RSA-AES256-GCM-SHA384",
  "ECDH-ECDSA-AES256-SHA384", "ECDH-RSA-AES256-SHA384",
  "DHE-RSA-AES256-GCM-SHA384", "DHE-DSS-AES256-GCM-SHA384",
  "DHE-RSA-AES256-SHA256", "DHE-DSS-AES256-SHA256", "AES256-GCM-SHA384",
  "AES256-SHA256", "ECDHE-ECDSA-AES128-GCM-SHA256",
  "ECDHE-RSA-AES128-GCM-SHA256", "ECDHE-ECDSA-AES128-SHA256",
  "ECDHE-RSA-AES128-SHA256", "ECDH-ECDSA-AES128-GCM-SHA256",
  "ECDH-RSA-AES128-GCM-SHA256", "ECDH-ECDSA-AES128-SHA256",
  "ECDH-RSA-AES128-SHA256", "DHE-RSA-AES128-GCM-SHA256",
  "DHE-DSS-AES128-GCM-SHA256", "DHE-RSA-AES128-SHA256", "DHE-DSS-AES128-SHA256",
  "AES128-GCM-SHA256", "AES128-SHA256", "ECDHE-ECDSA-AES256-SHA",
  "ECDHE-RSA-AES256-SHA", "DHE-RSA-AES256-SHA", "DHE-DSS-AES256-SHA",
  "ECDH-ECDSA-AES256-SHA", "ECDH-RSA-AES256-SHA", "AES256-SHA",
  "ECDHE-ECDSA-DES-CBC3-SHA", "ECDHE-RSA-DES-CBC3-SHA", "EDH-RSA-DES-CBC3-SHA",
  "EDH-DSS-DES-CBC3-SHA", "ECDH-ECDSA-DES-CBC3-SHA", "ECDH-RSA-DES-CBC3-SHA",
  "DES-CBC3-SHA", "ECDHE-ECDSA-AES128-SHA", "ECDHE-RSA-AES128-SHA",
  "DHE-RSA-AES128-SHA", "DHE-DSS-AES128-SHA", "ECDH-ECDSA-AES128-SHA",
  "ECDH-RSA-AES128-SHA", "AES128-SHA"]
```

- 2 Selezionare i pacchetti di crittografia supportati che soddisfano i requisiti di protezione della propria organizzazione.

Ad esempio, per consentire solo la crittografia ECDHE-ECDSA-AES128-GCM-SHA256 & ECDHE-ECDSA-AES256-GCM-SHA384, esaminare il file `/etc/rabbitmq/rabbitmq.config` e aggiungere la riga seguente a `ssl` e `ssl_options`:

```
{ciphers, ["ECDHE-ECDSA-AES128-GCM-SHA256", "ECDHE-ECDSA-AES256-GCM-SHA384"]}
```

- 3 Riavviare il server RabbitMQ eseguendo il comando seguente:

```
service rabbitmq-server restart
```

### Verifica della protezione dei dati inattivi

Verificare la protezione degli utenti e degli account del database utilizzati con vRealize Automation.

#### Utente Postgres

L'account utente postgres di Linux è legato al ruolo dell'account superuser del database postgres ed è un account bloccato per impostazione predefinita. Questa è la configurazione più sicura per questo utente poiché è accessibile solo dall'account utente root. Non sbloccare questo account utente.

#### Ruoli degli account utente del database

I ruoli predefiniti degli account utente postgres non dovrebbero essere utilizzati per finalità esterne alle funzionalità dell'applicazione. Per poter supportare attività non predefinite di analisi e creazione report del database, è consigliabile creare un account e una password aggiuntivi, adeguatamente protetti.

Eseguire lo script seguente dalla riga di comando:

```
vcac-vami add-db-user newUsername newPassword
```

Verrà aggiunto un nuovo utente e una password fornita dall'utente.

---

**Nota** Lo script deve essere eseguito in relazione al database postgres master nei casi in cui è implementata una configurazione di postgres HA master-slave.

---

### Configurazione dell'autenticazione del client PostgreSQL

Assicurarsi che nel database PostgreSQL dell'appliance vRealize Automation non sia configurata l'autenticazione trust locale. Questa configurazione consente a qualsiasi utente locale, incluso il superuser del database, di connettersi in qualità di qualsiasi utente PostgreSQL senza dover specificare una password.

---

**Nota** L'account superuser di Postgres deve rimanere come trust locale.

---

È consigliabile utilizzare il metodo di autenticazione md5 perché invia password crittografate.

Le impostazioni di configurazione dell'autenticazione del client si trovano nel file `/storage/db/pgdata/pg_hba.conf`.

```
# TYPE DATABASE USER ADDRESS METHOD

# "local" is for Unix domain socket connections only
local all postgres trust
# IPv4 local connections:
#host all all 127.0.0.1/32 md5
hostssl all all 127.0.0.1/32 md5
# IPv6 local connections:
#host all all ::1/128 md5
hostssl all all ::1/128 md5

# Allow remote connections for VCAC user.
#host vcac vcac 0.0.0.0/0 md5
hostssl vcac vcac 0.0.0.0/0 md5
hostssl vcac vcac ::0/0 md5
# Allow remote connections for VCAC replication user.
#host vcac vcac_replication 0.0.0.0/0 md5
hostssl vcac vcac_replication 0.0.0.0/0 md5
hostssl vcac vcac_replication ::0/0 md5
# Allow replication connections by a user with the replication privilege.
#host replication vcac_replication 0.0.0.0/0 md5
hostssl replication vcac_replication 0.0.0.0/0 md5
hostssl replication vcac_replication ::0/0 md5
```

Se si modifica il file `pg_hba.conf`, è necessario riavviare il server Postgres utilizzando i comandi seguenti per rendere effettive le modifiche.

```
# cd /opt/vmware/vpostgres/9.2/bin
# su postgres
# ./pg_ctl restart -D /storage/db/pgdata/ -m fast
```

## Configurazione delle risorse applicazione di vRealize Automation

Controllare le risorse applicazione di vRealize Automation e limitare le autorizzazioni per i file.

### Procedura

- 1 Eseguire il comando seguente per verificare che i file con i bit SUID e GUID impostati siano definiti correttamente.

```
find / -path /proc -prune -o -type f -perm +6000 -ls
```

Dovrebbe venire visualizzato il seguente elenco.

```
2197357 24 -rwsr-xr-x 1 polkituser root 23176 Mar 31 2015 /usr/lib/PolicyKit/polkit-
set-default-helper
2197354 16 -rwxr-sr-x 1 root polkituser 14856 Mar 31 2015 /usr/lib/PolicyKit/polkit-
read-auth-helper
2197353 12 -rwsr-x--- 1 root polkituser 10744 Mar 31 2015 /usr/lib/PolicyKit/polkit-
grant-helper-pam
2197352 20 -rwxr-sr-x 1 root polkituser 19208 Mar 31 2015 /usr/lib/PolicyKit/polkit-
```



```

grant-helper
2197351 20 -rwxr-sr-x 1 root polkituser 19008 Mar 31 2015 /usr/lib/PolicyKit/polkit-
explicit-grant-helper
2197356 24 -rwxr-sr-x 1 root polkituser 23160 Mar 31 2015 /usr/lib/PolicyKit/polkit-
revoke-helper
2188203 460 -rws--x--x 1 root root 465364 Apr 21 22:38 /usr/lib64/ssh/ssh-keysign
2138858 12 -rwxr-sr-x 1 root tty 10680 May 10 2010 /usr/sbin/utempter
2142482 144 -rwsr-xr-x 1 root root 142890 Sep 15 2015 /usr/bin/passwd
2142477 164 -rwsr-xr-x 1 root shadow 161782 Sep 15 2015 /usr/bin/chage
2142467 156 -rwsr-xr-x 1 root shadow 152850 Sep 15 2015 /usr/bin/chfn
1458298 364 -rwsr-xr-x 1 root root 365787 Jul 22 2015 /usr/bin/sudo
2142481 64 -rwsr-xr-x 1 root root 57776 Sep 15 2015 /usr/bin/newgrp
1458249 40 -rwsr-x--- 1 root trusted 40432 Mar 18 2015 /usr/bin/crontab
2142478 148 -rwsr-xr-x 1 root shadow 146459 Sep 15 2015 /usr/bin/chsh
2142480 156 -rwsr-xr-x 1 root shadow 152387 Sep 15 2015 /usr/bin/gpasswd
2142479 48 -rwsr-xr-x 1 root shadow 46967 Sep 15 2015 /usr/bin/expiry
311484 48 -rwsr-x--- 1 root messagebus 47912 Sep 16 2014 /lib64/dbus-1/dbus-daemon-
launch-helper
876574 36 -rwsr-xr-x 1 root shadow 35688 Apr 10 2014 /sbin/unix_chkpwd
876648 12 -rwsr-xr-x 1 root shadow 10736 Dec 16 2011 /sbin/unix2_chkpwd
49308 68 -rwsr-xr-x 1 root root 63376 May 27 2015 /opt/likewise/bin/ksu
1130552 40 -rwsr-xr-x 1 root root 40016 Apr 16 2015 /bin/su
1130511 40 -rwsr-xr-x 1 root root 40048 Apr 15 2011 /bin/ping
1130600 100 -rwsr-xr-x 1 root root 94808 Mar 11 2015 /bin/mount
1130601 72 -rwsr-xr-x 1 root root 69240 Mar 11 2015 /bin/umount
1130512 36 -rwsr-xr-x 1 root root 35792 Apr 15 2011 /bin/ping6
2012 /lib64/dbus-1/dbus-daemon-launch-helper

```

- 2 Eseguire il comando seguente per verificare che tutti i file nell'appliance virtuale abbiano un proprietario.

```
find / -path /proc -prune -o -nouser -o -nogroup
```

- 3 Eseguire il comando seguente per rivedere le autorizzazioni per tutti i file nell'appliance virtuale e verificare che nessuno di essi sia scrivibile da chiunque.

```
find / -name ".*" -type f -perm -a+w | xargs ls -ldb
```

- 4 Eseguire il comando seguente per verificare che solo l'utente vcac possieda i file corretti.

```
find / -name "proc" -prune -o -user vcac -print | egrep -v -e "*/vcac/*" | egrep
-v -e "*/vmware-vcac/*"
```

Se non viene visualizzato alcun risultato, tutti i file corretti appartengono unicamente all'utente vcac.

- 5 Verificare che i seguenti file siano scrivibili solo dall'utente vcac.

```

/etc/vcac/vcac/security.properties
/etc/vcac/vcac/solution-users.properties
/etc/vcac/vcac/sso-admin.properties
/etc/vcac/vcac/vcac.keystore
/etc/vcac/vcac/vcac.properties

```

Verificare anche i seguenti file e le relative sottodirectory

`/var/log/vcac/*`

`/var/lib/vcac/*`

`/var/cache/vcac/*`

- 6 Verificare che solo l'utente vcac o l'utente root possa leggere i file corretti nelle seguenti directory e relative sottodirectory.

`/etc/vcac/*`

`/var/log/vcac/*`

`/var/lib/vcac/*`

`/var/cache/vcac/*`

- 7 Verificare che i file corretti appartengano solo all'utente vco o all'utente root, come illustrato nelle seguenti directory e relative sottodirectory.

`/etc/vco/*`

`/var/log/vco/*`

`/var/lib/vco/*`

`/var/cache/vco/*`

- 8 Verificare che i file corretti siano scrivibili solo dall'utente vco o dall'utente root, come illustrato nelle seguenti directory e relative sottodirectory.

`/etc/vco/*`

`/var/log/vco/*`

`/var/lib/vco/*`

`/var/cache/vco/*`

- 9 Verificare che i file corretti siano leggibili solo dall'utente vco o dall'utente root, come mostrato nelle seguenti directory e relative sottodirectory.

`/etc/vco/*`

`/var/log/vco/*`

`/var/lib/vco/*`

`/var/cache/vco/*`

## Personalizzazione della configurazione del proxy della console

È possibile personalizzare la configurazione della console remota per vRealize Automation per semplificare la risoluzione dei problemi e le procedure organizzative.

Quando si installa, si configura o si gestisce vRealize Automation, è possibile modificare alcune impostazioni per abilitare la risoluzione dei problemi ed eseguire il debug dell'installazione. Catalogare e controllare ogni modifica apportata per assicurarsi che i componenti applicabili siano protetti in modo adeguato in base all'utilizzo che se ne deve fare. Non passare alla produzione se non si è sicuri che le modifiche della configurazione non siano opportunamente protette.

### **Personalizzazione della scadenza del ticket di VMware Remote Console**

È possibile personalizzare il periodo di validità dei ticket della console remota usati per stabilire le connessioni di VMware Remote Console.

Quando un utente esegue connessioni di VMware Remote Console, il sistema crea e restituisce credenziali monouso che stabiliscono una connessione specifica a una macchina virtuale. È possibile impostare la scadenza del ticket per un intervallo di tempo specificato in minuti.

#### **Procedura**

- 1 Aprire il file `/etc/vcac/security.properties` in un editor di testo.
- 2 Aggiungere una riga al file del modulo `consoleproxy.ticket.validitySec=30`.  
In questa riga, il valore numerico specifica il numero di minuti che devono trascorrere prima che il ticket scada.
- 3 Salvare il file e chiuderlo.
- 4 Riavviare il server `vcac` usando il comando `/etc/init.d/vcac-server restart`.

Il valore della scadenza del ticket viene reimpostato sull'intervallo di tempo specificato in minuti.

### **Personalizzazione della porta del server proxy della console**

È possibile personalizzare la porta su cui il proxy della console di VMware Remote Console è in ascolto per i messaggi.

#### **Procedura**

- 1 Aprire il file `/etc/vcac/security.properties` in un editor di testo.
- 2 Aggiungere una riga al file del modulo `consoleproxy.service.port=8445`.  
Il valore numerico specifica il numero della porta del servizio proxy della console, in questo caso 8445.
- 3 Salvare il file e chiuderlo.
- 4 Riavviare il server `vcac` usando il comando `/etc/init.d/vcac-server restart`.

La porta del servizio proxy ha ora il numero di porta specificato.

### **Configurazione dell'intestazione della risposta X-XSS-Protection**

Aggiungere l'intestazione della risposta X-XSS-Protection al file di configurazione `haproxy`.

## Procedura

- 1 Aprire `/etc/haproxy/conf.d/20-vcac.cfg` per modificarlo.
- 2 Aggiungere le seguenti righe in una sezione del front end:

```
rspdel X-XSS-Protection:\ 1;\ mode=block
      rspadd X-XSS-Protection:\ 1;\ mode=block
```

- 3 Ricaricare la configurazione HAProxy utilizzando il comando seguente.
- ```
/etc/init.d/haproxy reload
```

## Configurazione dell'intestazione della risposta HTTP Strict Transport Security

Aggiungere l'intestazione della risposta HTTP Strict Transport (HSTS) alla configurazione HAProxy.

## Procedura

- 1 Aprire `/etc/haproxy/conf.d/20-vcac.cfg` per modificarlo.
- 2 Aggiungere le seguenti righe in una sezione del front end:

```
rspdel Strict-Transport-Security:\ max-age=31536000
      rspadd Strict-Transport-Security:\ max-age=31536000
```

- 3 Ricaricare la configurazione HAProxy utilizzando il comando seguente.
- ```
/etc/init.d/haproxy reload
```

## Configurazione dell'intestazione della risposta X-Frame-Options

In alcuni casi, l'intestazione della risposta X-Frame-Options può essere visualizzata due volte.

L'intestazione della risposta X-Frame-Options può essere visualizzata due volte perché il servizio vIDM aggiunge questa intestazione al back end oltre che ad HAProxy. Una configurazione appropriata può evitare la doppia visualizzazione.

## Procedura

- 1 Aprire `/etc/haproxy/conf.d/20-vcac.cfg` per modificarlo.
  - 2 Individuare la riga seguente nella sezione front end:
 

```
rspadd X-Frame-Options:\ SAMEORIGIN
```
  - 3 Aggiungere le righe seguenti prima della riga individuata nel passaggio precedente:
 

```
rspdel X-Frame-Options:\ SAMEORIGIN
```
  - 4 Ricaricare la configurazione HAProxy utilizzando il comando seguente.
- ```
/etc/init.d/haproxy reload
```

## Configurazione delle intestazioni di risposta dei server

Come procedura di sicurezza consigliata, configurare il sistema vRealize Automation per limitare le informazioni disponibili per i potenziali utenti malintenzionati.

Per quanto possibile, ridurre al minimo la quantità di informazioni che il sistema condivide sulla sua identità e la sua versione. Gli utenti malintenzionati e i pirati informatici possono usare queste informazioni per creare attacchi mirati contro il server Web o una sua specifica versione.

### Configurazione dell'intestazione della risposta del server Lighttpd

È consigliabile creare un'intestazione del server vuota per il server Lighttpd dell'appliance vRealize Automation.

#### Procedura

- 1 Aprire il file `/opt/vmware/etc/lighttpd/lighttpd.conf` in un editor di testo.
- 2 Aggiungere `server.tag = " "` al file.
- 3 Salvare le modifiche e chiudere il file.
- 4 Riavviare il server Lighttpd eseguendo il comando `# /opt/vmware/etc/init.d/vami-lighttpd restart`.

### Configurazione dell'intestazione della risposta TCServer per l'appliance vRealize Automation

È consigliabile creare un'intestazione del server vuota personalizzata per l'intestazione della risposta TCServer utilizzata con l'appliance vRealize Automation per limitare la possibilità che un utente malintenzionato ottenga informazioni preziose.

#### Procedura

- 1 Aprire il file `/etc/vco/app-server/server.xml` in un editor di testo.
- 2 In ciascun elemento `<Connector>`, aggiungere `server=" "`.  
Ad esempio: `<Connector protocol="HTTP/1.1" server="" ..... />`
- 3 Salvare le modifiche e chiudere il file.
- 4 Riavviare il server con il comando seguente.  
`service vco-server restart`

### Configurazione dell'intestazione della risposta del server Internet Information Services

Come procedura consigliata, creare un'intestazione del server vuota personalizzata per il server Internet Information Services (IIS) usato con Identity Appliance per limitare la possibilità che utenti malintenzionati ottengano informazioni preziose.

#### Procedura

- 1 Aprire il file `C:\Windows\System32\inetsrv\urlscan\UrlScan.ini` in un editor di testo.
- 2 Cercare la voce `RemoveServerHeader=0` e sostituirla con `RemoveServerHeader=1`.

- 3 Salvare le modifiche e chiudere il file.
- 4 Riavviare il server eseguendo il comando `iisreset`.

### Operazioni successive

Disabilitare l'intestazione IIS X-Powered By rimuovendo le intestazioni di risposta HTTP dall'elenco nella console Gestione IIS.

- 1 Aprire la console Gestione IIS.
- 2 Aprire l'intestazione della risposta HTTP e rimuoverla dall'elenco.
- 3 Riavviare il server eseguendo il comando `iisreset`.

### Impostazione del timeout della sessione di Appliance vRealize Automation

Configurare l'impostazione del timeout della sessione in Appliance vRealize Automation in base al criterio di protezione dell'azienda.

Il timeout della sessione predefinito di Appliance vRealize Automation in caso di inattività dell'utente è 30 minuti. Per modificare questo valore di timeout e adattarlo al criterio di protezione della propria organizzazione, modificare il file `web.xml` nella macchina host di Appliance vRealize Automation.

#### Procedura

- 1 Aprire il file `/usr/lib/vcac/server/webapps/vcac/WEB-INF/web.xml` in un editor di testo.
- 2 Trovare `session-config` e impostare il valore `session-timeout`. Vedere il seguente esempio di codice.

```
<!-- 30 minutes session expiration time -->
<session-config>
    <session-timeout>30</session-timeout>
    <tracking-mode>COOKIE</tracking-mode>
    <cookie-config>
        <path>/</path>
    </cookie-config>
</session-config>
```

- 3 Riavviare il server eseguendo il comando seguente.

```
service vcac-server restart
```

### Gestione del software non essenziale

Per ridurre al minimo i rischi di sicurezza, rimuovere o configurare il software non essenziale dalle macchine host vRealize Automation.

Per ridurre al minimo la possibilità che crei problemi di sicurezza, configurare tutto il software che non si intende rimuovere in base alle raccomandazioni dei produttori e in conformità alle procedure di sicurezza consigliate.

## Sicurezza del gestore di archiviazione di massa USB

Garantire la sicurezza del gestore di archiviazione di massa USB per impedirne l'uso come gestore dei dispositivi USB con le macchine host dell'appliance virtuale VMware. Utenti potenzialmente malintenzionati possono sfruttare questo gestore per compromettere il sistema.

### Procedura

- 1 Aprire il file `/etc/modprobe.conf.local` in un editor di testo.
- 2 Assicurarsi che nel file sia presente la riga `install usb-storage /bin/true`.
- 3 Salvare il file e chiuderlo.

## Sicurezza del gestore del protocollo Bluetooth

Garantire la sicurezza del gestore del protocollo Bluetooth nelle macchine host dell'appliance virtuale per evitare che utenti potenzialmente malintenzionati lo sfruttino.

Il binding del protocollo Bluetooth allo stack della rete non è necessario e può aumentare la superficie di attacco dell'host.

### Procedura

- 1 Aprire il file `/etc/modprobe.conf.local` in un editor di testo.
- 2 Assicurarsi che nel file sia presente la riga seguente.  
`install bluetooth /bin/true`
- 3 Salvare il file e chiuderlo.

## Sicurezza di Stream Control Transmission Protocol

Impedire il caricamento predefinito di Stream Control Transmission Protocol (SCTP) nel sistema. Utenti potenzialmente malintenzionati possono sfruttare questo protocollo per compromettere il sistema.

Configurare il sistema per evitare il caricamento di Stream Control Transmission Protocol (SCTP) a meno che non sia assolutamente necessario. SCTP è un protocollo di livello trasporto standard IETF inutilizzato. Il binding di questo protocollo allo stack della rete aumenta la superficie di attacco dell'host. Processi locali senza privilegi possono fare in modo che il kernel carichi dinamicamente un gestore del protocollo utilizzando il protocollo per aprire un socket.

### Procedura

- 1 Aprire il file `/etc/modprobe.conf.local` in un editor di testo.
- 2 Assicurarsi che nel file sia presente la riga seguente.  
`install sctp /bin/true`
- 3 Salvare il file e chiuderlo.

## Sicurezza di Datagram Congestion Protocol

Come parte delle attività di protezione avanzata del sistema, evitare il caricamento predefinito del protocollo Datagram Congestion Control Protocol (DCCP) nelle macchine host dell'appliance virtuale. Utenti potenzialmente malintenzionati possono sfruttare questo protocollo per compromettere il sistema.

Evitare il caricamento del modulo Datagram Congestion Control Protocol (DCCP) a meno che non sia assolutamente necessario. DCCP è un protocollo del livello trasporto proposto, che non viene utilizzato. Il binding di questo protocollo allo stack della rete aumenta la superficie di attacco dell'host. Processi locali senza privilegi possono fare in modo che il kernel carichi dinamicamente un gestore del protocollo utilizzando il protocollo per aprire un socket.

### Procedura

- 1 Aprire il file `/etc/modprobe.conf.local` in un editor di testo.
- 2 Assicurarsi che nel file siano presenti le righe DCCP.

```
install dccp/bin/true
install dccp_ipv4/bin/true
install dccp_ipv6/bin/true
```

- 3 Salvare il file e chiuderlo.

## Sicurezza del bridging di rete

Impedire il caricamento predefinito del modulo di bridging di rete nel sistema. Utenti potenzialmente malintenzionati possono sfruttarlo per compromettere il sistema.

Configurare il sistema per evitare il caricamento della rete a meno che non sia assolutamente necessario. Utenti potenzialmente malintenzionati possono sfruttarlo per aggirare il partizionamento e la protezione della rete.

### Procedura

- 1 Eseguire il comando seguente su tutte le macchine host dell'appliance virtuale VMware.

```
# rmmod bridge
```

- 2 Aprire il file `/etc/modprobe.conf.local` in un editor di testo.
- 3 Assicurarsi che nel file sia presente la riga seguente.

```
install bridge /bin/false
```

- 4 Salvare il file e chiuderlo.

## Sicurezza del protocollo Reliable Datagram Sockets

Come parte delle attività di protezione avanzata del sistema, evitare il caricamento predefinito del protocollo Reliable Datagram Sockets (RDS) nelle macchine host dell'appliance virtuale. Utenti potenzialmente malintenzionati possono sfruttare questo protocollo per compromettere il sistema.



Il binding del protocollo Reliable Datagram Sockets (RDS) allo stack della rete aumenta la superficie di attacco dell'host. Processi locali senza privilegi possono fare in modo che il sistema carichi dinamicamente un gestore del protocollo utilizzando il protocollo per aprire un socket.

#### **Procedura**

- 1 Aprire il file `/etc/modprobe.conf.local` in un editor di testo.
- 2 Assicurarsi che nel file sia presente la riga `install rds /bin/true`.
- 3 Salvare il file e chiuderlo.

#### **Sicurezza del protocollo Transparent Inter-Process Communication**

Come parte delle attività di protezione avanzata del sistema, evitare il caricamento predefinito del protocollo Transparent Inter-Process Communication (TIPC) nelle macchine host dell'appliance virtuale. Utenti potenzialmente malintenzionati possono sfruttare questo protocollo per compromettere il sistema.

Il binding del protocollo Transparent Inter-Process Communication (TIPC) allo stack della rete aumenta la superficie di attacco dell'host. Processi locali senza privilegi possono fare in modo che il kernel carichi dinamicamente un gestore del protocollo utilizzando il protocollo per aprire un socket.

#### **Procedura**

- 1 Aprire il file `/etc/modprobe.conf.local` in un editor di testo.
- 2 Assicurarsi che nel file sia presente la riga `install tipc /bin/true`.
- 3 Salvare il file e chiuderlo.

#### **Sicurezza di Internetwork Packet Exchange Protocol**

Impedire il caricamento predefinito di Internetwork Packet Exchange (IPX) Protocol nel sistema. Utenti potenzialmente malintenzionati possono sfruttare questo protocollo per compromettere il sistema.

Evitare il caricamento del modulo Internetwork Packet Exchange (IPX) Protocol a meno che non sia assolutamente necessario. Il protocollo IPX è un protocollo a livello di rete obsoleto. Il binding di questo protocollo allo stack della rete aumenta la superficie di attacco dell'host. Processi locali senza privilegi possono fare in modo che il sistema carichi dinamicamente un gestore di protocollo utilizzando il protocollo per aprire un socket.

#### **Procedura**

- 1 Aprire il file `/etc/modprobe.conf.local` in un editor di testo.
- 2 Assicurarsi che nel file sia presente la riga seguente.  
`install ipx /bin/true`
- 3 Salvare il file e chiuderlo.

#### **Sicurezza di Appletalk Protocol**

Impedire il caricamento predefinito di Appletalk Protocol nel sistema. Utenti potenzialmente malintenzionati possono sfruttare questo protocollo per compromettere il sistema.

Evitare il caricamento del modulo Appletalk Protocol a meno che non sia assolutamente necessario. Il binding di questo protocollo allo stack della rete aumenta la superficie di attacco dell'host. Processi locali senza privilegi possono fare in modo che il sistema carichi dinamicamente un gestore di protocollo utilizzando il protocollo per aprire un socket.

#### **Procedura**

- 1 Aprire il file `/etc/modprobe.conf.local` in un editor di testo.
- 2 Assicurarsi che nel file sia presente la riga seguente.  

```
install appletalk /bin/true
```
- 3 Salvare il file e chiuderlo.

#### **Sicurezza di DECnet Protocol**

Impedire il caricamento predefinito di DECnet Protocol nel sistema. Utenti potenzialmente malintenzionati possono sfruttare questo protocollo per compromettere il sistema.

Evitare il caricamento del modulo DECnet Protocol a meno che non sia assolutamente necessario. Il binding di questo protocollo allo stack della rete aumenta la superficie di attacco dell'host. Processi locali senza privilegi possono fare in modo che il sistema carichi dinamicamente un gestore di protocollo utilizzando il protocollo per aprire un socket.

#### **Procedura**

- 1 Aprire il file `/etc/modprobe.conf.local` di DECnet Protocol in un editor di testo.
- 2 Assicurarsi che nel file sia presente la riga seguente.  

```
install decnet /bin/true
```
- 3 Salvare il file e chiuderlo.

#### **Sicurezza del modulo Firewire**

Impedire il caricamento predefinito del modulo Firewire nel sistema. Utenti potenzialmente malintenzionati possono sfruttare questo protocollo per compromettere il sistema.

Evitare il caricamento del modulo Firewire a meno che non sia assolutamente necessario.

#### **Procedura**

- 1 Aprire il file `/etc/modprobe.conf.local` in un editor di testo.
- 2 Assicurarsi che nel file sia presente la riga seguente.  

```
install ieee1394 /bin/true
```
- 3 Salvare il file e chiuderlo.

## Protezione del componente Infrastructure as a Service

Quando si applica la protezione avanzata al sistema, garantire la sicurezza del componente Infrastructure as a Service (IaaS) di vRealize Automation e della sua macchina host per evitare che utenti potenzialmente malintenzionati lo sfruttino.

È necessario configurare le impostazioni di sicurezza per il componente Infrastructure as a Service (IaaS) di vRealize Automation e per l'host in cui si trova. È necessario impostare o verificare la configurazione degli altri componenti e applicazioni correlati. In alcuni casi, è possibile verificare le impostazioni esistenti, mentre in altri sarà necessario cambiare o aggiungere impostazioni per una configurazione appropriata.

### Disabilitare il servizio Ora di Windows

Come procedura consigliata di sicurezza, utilizzare server di riferimento ora autorizzati anziché la sincronizzazione con l'ora dell'host in un ambiente di produzione di vRealize Automation.

In un ambiente di produzione, disabilitare la sincronizzazione con l'ora dell'host e utilizzare server di riferimento ora autorizzati per garantire il monitoraggio accurato delle azioni utente, nonché l'identificazione di intrusioni e attacchi potenzialmente dannosi tramite le funzionalità di auditing e registrazione.

### Configurazione del protocollo TLS per i dati in transito di Infrastructure as a Service

Assicurarsi che la distribuzione di vRealize Automation usi protocolli TLS complessi per proteggere i canali di trasmissione dei componenti di Infrastructure as a Service.

Secure Sockets Layer (SSL) e Transport Layer Security (TLS) sviluppato più di recente, sono protocolli di crittografia che contribuiscono a garantire la sicurezza durante le comunicazioni di rete tra i diversi componenti del sistema. Il protocollo SSL è uno standard datato e molte delle sue implementazioni non forniscono più una protezione adeguata da potenziali attacchi. Sono state identificate gravi debolezze nei protocolli SSL precedenti, tra cui SSLv2 e SSLv3. Questi protocolli non sono più considerati sicuri.

In base ai criteri di sicurezza dell'organizzazione, potrebbe essere preferibile disabilitare anche TLS 1.0.

---

**Nota** Quando si interrompe TLS nel bilanciamento del carico, disabilitare anche i protocolli vulnerabili come SSLv2, SSLv3 e, se necessario, anche TLS 1.0.

---

### Disabilitare SSLv3 in Internet Information Services

Come procedura consigliata di sicurezza, disabilitare SSLv3 in Internet Information Services (IIS) nella macchina del server host IaaS (Infrastructure as a Service).

#### Procedura

- 1 Eseguire l'editor del Registro di sistema di Windows come amministratore.
- 2 Passare a `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\` nella finestra del Registro di sistema.
- 3 Fare clic con il pulsante destro del mouse su **Protocolli** e scegliere **Nuovo > Chiave**.

- 4 Immettere **SSL 3.0**.
- 5 Nell'albero di spostamento, fare clic con il pulsante destro del mouse sulla chiave **SSL 3.0** appena creata e nel menu a comparsa scegliere **Nuovo > Chiave**, quindi immettere **Client**.
- 6 Nell'albero di spostamento, fare clic con il pulsante destro del mouse sulla chiave **SSL 3.0** appena creata e nel menu a comparsa scegliere **Nuovo > Chiave**, quindi immettere **Server**.
- 7 Nell'albero di spostamento, sotto SSL 3.0, fare clic con il pulsante destro del mouse su **Client** e scegliere **Nuovo > Valore DWORD (32 bit)**, quindi immettere **DisabledByDefault**.
- 8 Nell'albero di spostamento, sotto SSL 3.0, selezionare **Client** e nel riquadro destro fare doppio clic su **DisabledByDefault**, quindi immettere **1**.
- 9 Nell'albero di spostamento, sotto SSL 3.0, fare clic con il pulsante destro del mouse su **Server** e scegliere **Nuovo > Valore DWORD (32 bit)**, quindi immettere **Abilitato**.
- 10 Nell'albero di spostamento, sotto SSL 3.0, selezionare **Server** e nel riquadro destro fare doppio clic sul valore **DWORD** abilitato, quindi immettere **0**.
- 11 Riavviare Windows Server.

### Disabilitare TLS 1.0 per IaaS

Per garantire la massima sicurezza, configurare IaaS in modo che utilizzi il pooling e disabilitare TLS 1.0.

Per ulteriori informazioni, vedere l'articolo della Knowledge Base di Microsoft all'indirizzo

<https://support.microsoft.com/en-us/kb/245030>.

### Procedura

- 1 Configurare IaaS per l'utilizzo del pooling anziché dei socket Web.
  - a Aggiornare il file di configurazione dei servizi di gestione  
`C:\Programmi(x86)\VMware\VCAC\Server\ManagerService.exe.config` aggiungendo i valori seguenti nella sezione <appSettings>:
 

```
<add key="Extensibility.Client.RetrievalMethod" value="Polling"/>
<add key="Extensibility.Client.PollingInterval" value="2000"/>
<add key="Extensibility.Client.PollingMaxEvents" value="128"/>
```
  - b Riavviare il servizio di gestione (VMware vCloud Automation Center Service).
- 2 Verificare che TLS 1.0 sia disabilitato nel server IaaS.
  - a Eseguire l'editor del Registro di sistema come amministratore.
  - b Nella finestra del Registro di sistema, passare a  
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\`
  - c Fare clic con il pulsante destro del mouse su Protocolli e scegliere **Nuovo > Chiave**, quindi immettere **TLS 1.0**.

- d Nell'albero di spostamento, fare clic con il pulsante destro del mouse sulla chiave TLS 1.0 appena creata e nel menu a comparsa scegliere **Nuovo > Chiave**, quindi immettere **Client**.
- e Nell'albero di spostamento, fare clic con il pulsante destro del mouse sulla chiave TLS 1.0 appena creata e nel menu a comparsa scegliere **Nuovo > Chiave**, quindi immettere **Server**.
- f Nell'albero di spostamento, sotto TLS 1.0, fare clic con il pulsante destro del mouse su **Client**, quindi fare clic su **Nuovo > Valore DWORD (32 bit)** e immettere **DisabledByDefault**.
- g Nell'albero di spostamento, sotto TLS 1.0, selezionare **Client** e nel riquadro destro fare doppio clic su **DisabledByDefault** DWORD, quindi immettere **1**.
- h Nell'albero di spostamento, sotto TLS 1.0, fare clic con il pulsante destro del mouse su **Server** e scegliere **Nuovo > Valore DWORD (32 bit)**, quindi immettere **Abilitato**.
- i Nell'albero di spostamento, sotto TLS 1.0, selezionare **Server** e nel riquadro destro fare doppio clic su **Abilitato** DWORD, quindi immettere **0**.
- j Riavviare Windows Server.

### Configurazione dei pacchetti di crittografia TLS

Per ottenere la massima protezione, è necessario configurare i componenti di vRealize Automation in modo che usino crittografie complesse. L'algoritmo di crittografia negoziato tra il server e il browser determina la complessità della crittografia usata in una sessione TLS. Per assicurare che vengano selezionate solo crittografie complesse, disabilitare le crittografie vulnerabili nei componenti di vRealize Automation. Configurare il server in modo che supporti solo crittografie complesse e utilizzi dimensioni di chiave sufficientemente grandi. Configurare inoltre tutte le crittografie in un ordine adeguato.

### Pacchetti di crittografia non accettabili

Disabilitare i pacchetti di crittografia che non offrono autenticazione, come i pacchetti di crittografia NULL, ovvero aNULL o eNULL. Disabilitare inoltre lo scambio di chiavi Diffie-Hellman anonimo (ADH), le crittografie a livello di esportazione (EXP, crittografie che contengono DES), le dimensioni di chiave inferiori a 128 bit per la codifica del traffico del payload, l'uso di MD5 come meccanismo di hashing per il traffico del payload, i pacchetti di crittografia IDEA e i pacchetti di crittografia RC4. Assicurarsi inoltre che i pacchetti di crittografia che usano lo scambio di chiavi Diffie-Hellman (DHE) siano disabilitati.

### Verifica della protezione del server host

Come procedura di sicurezza consigliata, verificare la configurazione della protezione delle macchine del server host di Infrastructure as a Service (IaaS).

Microsoft fornisce diversi strumenti che consentono di verificare gli aspetti legati alla sicurezza nelle macchine del server host. Per informazioni su come utilizzare al meglio questi strumenti, rivolgersi al proprio fornitore Microsoft.

## Verifica della baseline sicura del server host

Eseguire lo strumento Microsoft Baseline Security Analyzer (MBSA) per verificare rapidamente che nel server siano stati installati gli aggiornamenti e gli hotfix più recenti. È possibile utilizzare MBSA per installare le patch di sicurezza mancanti rilasciate da Microsoft e mantenere aggiornato il server con le raccomandazioni di protezione fornite da Microsoft.

Scaricare la versione più recente dello strumento MBSA dal sito Web di Microsoft.

## Verificare la configurazione della protezione del server host

Utilizzare Configurazione guidata impostazioni di sicurezza di Windows e il toolkit Microsoft Security Compliance Manager (SCM) per verificare che il server host sia configurato in modo sicuro.

Eseguire SCW dagli strumenti di amministrazione nel server Windows. Questo strumento è in grado di identificare i ruoli del server e le funzionalità installate, incluse le impostazioni di rete, del firewall di Windows e del Registro di sistema. Confrontare il report con le istruzioni più recenti per l'applicazione della protezione avanzata dal toolkit SCM relativo al server Windows in uso. In base ai risultati è possibile ottimizzare le impostazioni della protezione per ogni funzionalità, ad esempio i servizi di rete, le impostazioni degli account e i firewall di Windows, quindi applicare le impostazioni al server.

Sul sito Web di Microsoft Technet sono disponibili ulteriori informazioni sullo strumento SCW.

## Protezione delle risorse applicazione

Come procedura di sicurezza consigliata, verificare che tutti i file di Infrastructure as a Service rilevanti dispongano delle autorizzazioni appropriate.

Esaminare i file Infrastructure as a Service rispetto all'installazione di Infrastructure as a Service. Nella maggior parte dei casi, sottocartelle e file per ogni cartella dovrebbero avere le stesse impostazioni della cartella.

Directory o file	Gruppo o utenti	Controllo		Lettura ed esecuzione	Lettura	Scrittura
		completo	Modifica			
VMware\vmCAC\Agents\ <nome_agente> logs	SYSTEM	X	X	X	X	X
	Amministratore	X	X	X	X	X
	Amministratori	X	X	X	X	X
VMware\vmCAC\Agents\ <nome_agente> \temp	SYSTEM	X	X	X	X	X
	Amministratore	X	X	X	X	X
	Amministratori	X	X	X	X	X
VMware\vmCAC\Agents\	SYSTEM	X	X	X	X	X
	Amministratori	X	X	X	X	X
	Utenti			X	X	
VMware\vmCAC\Distributed Execution Manager\	SYSTEM	X	X	X	X	X
	Amministratori	X	X	X	X	X

Directory o file	Gruppo o utenti	Controllo completo	Modifica	Lettura ed esecuzione	Lettura	Scrittura
	Utenti			X	X	
VMware\VCAC\Distributed Execution Manager\DEM\Logs	SYSTEM	X	X	X	X	X
	Amministratore	X	X	X	X	X
	Amministratori	X	X	X	X	X
VMware\VCAC\Distributed Execution Manager\DEO\Logs	SYSTEM	X	X	X	X	X
	Amministratore	X	X	X	X	X
	Amministratori	X	X	X	X	X
VMware\VCAC\Management Agent\	SYSTEM	X	X	X	X	X
	Amministratori	X	X	X	X	X
	Utenti			X	X	
VMware\VCAC\Server\	SYSTEM	X	X	X	X	X
	Amministratori	X	X	X	X	X
	Utenti			X	X	
VMware\VCAC\Web API	SYSTEM	X	X	X	X	X
	Amministratori	X	X	X	X	X
	Utenti			X	X	

### Protezione della macchina host Infrastructure as a Service (IaaS)

Come procedura consigliata per la sicurezza, esaminare le impostazioni di base nella macchina host Infrastructure as a Service (IaaS) per assicurarsi che sia conforme alle linee guida sulla sicurezza.

Proteggere vari account, applicazioni, porte e servizi nella macchina host Infrastructure as a Service (IaaS).

#### Verificare le impostazioni dell'account utente server

Verificare che non siano presenti account utente e impostazioni utente, di dominio o locali, non necessari. Limitare tutti gli account utente che non sono correlati alle funzionalità dell'applicazione a quelli necessari per l'amministrazione, la manutenzione e la risoluzione dei problemi. Limitare l'accesso remoto dagli account utente del dominio al minimo indispensabile per la manutenzione del server. Controllare e verificare con precisione questi account.

#### Eliminare le applicazioni non necessarie

Eliminare tutte le applicazioni non necessarie dai server host. Le applicazioni non necessarie aumentano il rischio di esposizione a causa delle loro vulnerabilità non note o prive di patch.

## Disabilitare le porte e i servizi non necessari

Esaminare l'elenco delle porte aperte nel firewall del server host. Bloccare tutte le porte che non sono necessarie per il componente IaaS o per il funzionamento del sistema critico. Vedere [Configurazione di porte e protocolli](#). Controllare i servizi in esecuzione rispetto al server host e disabilitare quelli che non sono necessari.

## Configurazione della sicurezza della rete host

Per offrire la massima protezione dalle minacce note alla sicurezza, configurare le impostazioni dell'interfaccia di rete e della comunicazione in tutte le macchine host VMware.

Nell'ambito di un piano di sicurezza completo, configurare le impostazioni di sicurezza dell'interfaccia di rete per le appliance virtuali VMware e i componenti Infrastructure as a Service in base alle linee guida stabilite per la sicurezza.

## Configurazione delle impostazioni di rete per le appliance VMware

Per assicurarsi che le macchine host dell'appliance virtuale VMware supportino solo comunicazioni sicure ed essenziali, esaminare e modificare le impostazioni di comunicazione di rete corrispondenti.

Esaminare la configurazione del protocollo IP delle macchine host VMware e configurare le impostazioni di rete in base alle linee guida di sicurezza. Disabilitare tutti i protocolli di comunicazione non essenziali.

## Evitare il controllo delle interfacce di rete da parte degli utenti

Come procedura di sicurezza consigliata, concedere agli utenti solo i privilegi di sistema di cui hanno strettamente bisogno per eseguire il proprio lavoro nelle macchine host dell'appliance VMware.

Concedendo agli account degli utenti i privilegi per manipolare le interfacce di rete, si espone la rete ad attacchi quali l'aggiornamento dei meccanismi di sicurezza della rete o DoS (Denial of Service). Consentire di modificare le impostazioni delle interfacce di rete solo agli utenti con privilegi.

### Procedura

- 1 Eseguire il comando seguente in ogni macchina host dell'appliance VMware.

```
# grep -i '^USERCONTROL=' /etc/sysconfig/network/ifcfg*
```

- 2 Assicurarsi che ogni interfaccia sia impostata su NO.

## Impostazione della dimensione della coda di backlog TCP

Per fornire un livello di difesa contro gli attacchi dannosi, configurare una dimensione per la coda di backlog TCP predefinita nelle macchine host dell'appliance VMware.

Se si imposta la dimensione della coda di backlog TCP su un valore predefinito adeguato, è possibile mitigare l'impatto degli attacchi Denial of Service del protocollo TCP. L'impostazione predefinita consigliata è 1280.



## Procedura

- 1 Eseguire il comando seguente in ogni macchina host dell'appliance VMware.

```
# cat /proc/sys/net/ipv4/tcp_max_syn_backlog
```

- 2 Aprire il file `/etc/sysctl.conf` in un editor di testo.
- 3 Impostare la dimensione della coda di backlog TCP predefinita aggiungendo la voce seguente al file.  
`net.ipv4.tcp_max_syn_backlog=1280`
- 4 Salvare le modifiche e chiudere il file.

## Negare le richieste eco ICMPv4 inviate a un indirizzo di broadcast

Come procedura consigliata di sicurezza, verificare che le macchine host dell'appliance VMware ignorino le richieste echo inviate agli indirizzi di broadcast ICMP.

Le risposte alle richieste eco ICMP (Internet Control Message Protocol) inviate a un indirizzo di broadcast forniscono un vettore di attacco per gli attacchi con amplificazione e possono facilitare la mappatura della rete da parte di agenti dannosi. La configurazione delle macchine host dell'appliance in modo che ignorino le richieste eco ICMPv4 garantisce protezione da questi tipi di attacchi.

## Procedura

- 1 Eseguire il comando `# cat /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts` nelle macchine host dell'appliance virtuale VMware per verificare che siano configurate in modo da negare le richieste eco agli indirizzi di broadcast IPv4.

Se le macchine host sono configurate per negare i reindirizzamenti IPv4, questo comando restituirà il valore 0 per `/proc/sys/net/ipv4/icmp_echo_ignore_broadcasts`.

- 2 Per configurare una macchina host dell'appliance virtuale in modo che neghi le richieste eco inviate agli indirizzi di broadcast ICMPv4, aprire il file `/etc/sysctl.conf` in un editor di testo nella macchina host Windows.
- 3 Individuare la voce `net.ipv4.icmp_echo_ignore_broadcasts=0`. Se il valore di questa voce non è impostato su 0 o se la voce non esiste, aggiungerla o aggiornare la voce esistente nel modo appropriato.
- 4 Salvare le modifiche e chiudere il file.

## Disabilitare il protocollo ARP del proxy IPv4

Verificare che il protocollo ARP del proxy IPv4 sia disabilitato a meno che non sia necessario nelle macchine host dell'appliance VMware per impedire la condivisione non autorizzata delle informazioni.

Il protocollo ARP del proxy IPv4 consente a un sistema di inviare risposte alle richieste ARP in un'interfaccia per conto degli host connessi a un'altra interfaccia. Disabilitarlo se non è necessario per impedire la dispersione di informazioni di identificazione tra i segmenti di rete collegati.

**Procedura**

- 1 Eseguire il comando `# grep [01] /proc/sys/net/ipv4/conf/*/proxy_arp | egrep "default|all"` nelle macchine host dell'appliance virtuale VMware per verificare che il protocollo ARP del proxy IPv4 sia disabilitato.

Se è disabilitato, questo comando restituisce il valore 0.

```
/proc/sys/net/ipv4/conf/all/proxy_arp:0
/proc/sys/net/ipv4/conf/default/proxy_arp:0
```

Se le macchine host sono configurate correttamente, non è necessario eseguire ulteriori operazioni.

- 2 Se è necessario configurare il protocollo ARP del proxy IPv6 nelle macchine host, aprire il file `/etc/sysctl.conf` in un editor di testo.
- 3 Controllare le voci seguenti:

```
net.ipv4.conf.default.proxy_arp=0
net.ipv4.conf.all.proxy_arp=0
```

Se queste voci non esistono o se i loro valori non sono impostati su 0, aggiungere le voci o aggiornare le voci esistenti nel modo appropriato.

- 4 Salvare le modifiche apportate e chiudere il file.

**Negare i messaggi di reindirizzamento IPv4 ICMP**

Come procedura consigliata di sicurezza, verificare che le macchine host dell'appliance virtuale VMware neghino i messaggi di reindirizzamento IPv4 ICMP.

I router utilizzano i messaggi di reindirizzamento ICMP per comunicare agli host che per una determinata destinazione esiste una route più diretta. Un messaggio di reindirizzamento ICMP dannoso può favorire un attacco di tipo man-in-the-middle. Questi messaggi modificano la tabella di routing dell'host e non sono autenticati. Verificare che il sistema sia configurato in modo da ignorarli se non sono necessari.

**Procedura**

- 1 Eseguire il comando `# grep [01] /proc/sys/net/ipv4/conf/*/accept_redirects | egrep "default|all"` nelle macchine host dell'appliance VMware per verificare che siano configurate in modo da negare i messaggi di reindirizzamento IPv4.

Se le macchine host sono configurate per negare i reindirizzamenti IPv4, questo comando restituisce i seguenti valori:

```
/proc/sys/net/ipv4/conf/all/accept_redirects:0
/proc/sys/net/ipv4/conf/default/accept_redirects:0
```

- 2 Se è necessario configurare una macchina host dell'appliance virtuale in modo che neghi i messaggi di reindirizzamento IPv4, aprire il file `/etc/sysctl.conf` in un editor di testo.

### 3 Controllare i valori delle righe che iniziano con `net.ipv4.conf`.

Se i valori delle voci elencate di seguito non sono impostati su 0 o se le voci non esistono, aggiungerle al file o aggiornare le voci esistenti nel modo appropriato.

```
net.ipv4.conf.all.accept_redirects=0
net.ipv4.conf.default.accept_redirects=0
```

### 4 Salvare le modifiche apportate e chiudere il file.

## Negare i messaggi di reindirizzamento IPv6 ICMP

Come procedura consigliata di sicurezza, verificare che le macchine host dell'appliance virtuale VMware neghino i messaggi di reindirizzamento IPv6 ICMP.

I router utilizzano i messaggi di reindirizzamento ICMP per comunicare agli host che per una determinata destinazione esiste una route più diretta. Un messaggio di reindirizzamento ICMP dannoso può favorire un attacco di tipo man-in-the-middle. Questi messaggi modificano la tabella di routing dell'host e non sono autenticati. Verificare che il sistema sia configurato in modo da ignorarli a meno che non siano necessari.

### Procedura

#### 1 Eseguire il comando `# grep [01] /proc/sys/net/ipv6/conf/*/accept_redirects | grep "default|all"` nelle macchine host dell'appliance virtuale VMware per verificare che siano configurate in modo da negare i messaggi di reindirizzamento IPv6.

Se le macchine host sono configurate per negare i reindirizzamenti IPv6, questo comando restituisce i seguenti valori:

```
/proc/sys/net/ipv6/conf/all/accept_redirects:0
/proc/sys/net/ipv6/conf/default/accept_redirects:0
```

#### 2 Per configurare una macchina host dell'appliance virtuale in modo che neghi i messaggi di reindirizzamento IPv4, aprire il file `/etc/sysctl.conf` in un editor di testo.

### 3 Controllare i valori delle righe che iniziano con `net.ipv6.conf`.

Se i valori delle voci elencate di seguito non sono impostati su 0 o se le voci non esistono, aggiungerle al file o aggiornare le voci esistenti nel modo appropriato.

```
net.ipv6.conf.all.accept_redirects=0
net.ipv6.conf.default.accept_redirects=0
```

### 4 Salvare le modifiche e chiudere il file.

## Registrazione dei pacchetti martian IPv4

Come procedura di sicurezza consigliata, verificare che le macchine host dell'appliance virtuale VMware registrino i pacchetti martian IPv4.

I pacchetti martian contengono gli indirizzi che sono stati riconosciuti dal sistema come non validi. Configurare le macchine host per la registrazione di questi messaggi in modo da poter identificare le configurazioni errate e gli attacchi in corso.

### Procedura

- 1 Eseguire il comando `# grep [01] /proc/sys/net/ipv4/conf/*/log_martians | egrep "default|all"` nelle macchine host dell'appliance VMware per verificare che registrino i pacchetti martian IPv4.

Se le macchine virtuali sono configurate per registrare i pacchetti martian, restituiranno il seguente output:

```
/proc/sys/net/ipv4/conf/all/log_martians:1
/proc/sys/net/ipv4/conf/default/log_martians:1
```

Se le macchine host sono configurate correttamente, non è necessario eseguire ulteriori operazioni.

- 2 Se è necessario configurare le macchine virtuali per la registrazione dei pacchetti martian IPv4, aprire il file `/etc/sysctl.conf` in un editor di testo.
- 3 Controllare i valori delle righe che iniziano con `net.ipv4.conf`.

Se i valori delle voci seguenti non sono impostati su 1 o se non esistono, aggiungerli al file o aggiornare le voci esistenti di conseguenza.

```
net.ipv4.conf.all.log_martians=1
net.ipv4.conf.default.log_martians=1
```

- 4 Salvare le modifiche e chiudere il file.

### Uso del filtro del percorso inverso IPv4

Come procedura consigliata, verificare che le macchine host dell'appliance virtuale VMware utilizzino il filtro del percorso inverso IPv4.

Il filtro del percorso inverso protegge da indirizzi di origine falsificati facendo in modo che il sistema ignori i pacchetti con indirizzi di origine privi di percorso o con un percorso che non punta all'interfaccia di origine. Configurare le macchine host in modo che utilizzino il filtro del percorso inverso ogni volta che è possibile. In alcuni casi, a seconda del ruolo di sistema, il filtro del percorso inverso può fare in modo che il sistema ignori traffico lecito. Se si verificano tali problemi, potrebbe essere necessario usare una modalità più permissiva o disattivare del tutto il filtro del percorso inverso.

**Procedura**

- 1 Eseguire il comando `# grep [01] /proc/sys/net/ipv4/conf/*/rp_filter | egrep "default|all"` nelle macchine host dell'appliance virtuale VMware per verificare che utilizzino il filtro del percorso inverso IPv4.

Se le macchine virtuali usano il filtro del percorso inverso IPv4, il comando restituisce quanto segue:

```
/proc/sys/net/ipv4/conf/all/rp_filter:1
/proc/sys/net/ipv4/conf/default/rp_filter:1
```

Se le macchine virtuali sono configurate correttamente, non sono richieste ulteriori azioni.

- 2 Se è necessario configurare il filtro del percorso inverso IPv4 nelle macchine host, aprire il file `/etc/sysctl.conf` in un editor di testo.
- 3 Controllare i valori delle righe che iniziano con `net.ipv4.conf`.

Se i valori delle voci seguenti non sono impostati su 1 o se non esistono, aggiungerli al file o aggiornare le voci esistenti di conseguenza.

```
net.ipv4.conf.all.rp_filter=1
net.ipv4.conf.default.rp_filter=1
```

- 4 Salvare le modifiche e chiudere il file.

**Negare l'inoltro IPv4**

Verificare che le macchine host dell'appliance VMware neghino l'inoltro IPv4.

Se il sistema è configurato in modo da eseguire l'inoltro IP e non è un router designato, gli autori degli attacchi potrebbero utilizzarlo per aggirare la sicurezza della rete fornendo un percorso per le comunicazioni non filtrate dai dispositivi di rete. Per evitare questo rischio, configurare le macchine host dell'appliance virtuale in modo che neghino l'inoltro IPv4.

**Procedura**

- 1 Eseguire il comando `# cat /proc/sys/net/ipv4/ip_forward` nelle macchine host dell'appliance VMware per verificare che siano configurate in modo da negare l'inoltro IPv4.

Se le macchine host sono configurate per negare l'inoltro IPv4, questo comando restituirà il valore 0 per `/proc/sys/net/ipv4/ip_forward`. Se le macchine virtuali sono configurate correttamente, non è necessario eseguire ulteriori operazioni.

- 2 Per configurare una macchina host dell'appliance virtuale in modo che neghi l'inoltro IPv4, aprire il file `/etc/sysctl.conf` in un editor di testo.
- 3 Individuare la voce `net.ipv4.ip_forward=0`. Se il valore di questa voce non è impostato su 0 o se la voce non esiste, aggiungerla o aggiornare la voce esistente nel modo appropriato.
- 4 Salvare le modifiche e chiudere il file.

## Negare l'inoltro IPv6

Come procedura consigliata di sicurezza, verificare che i sistemi host dell'appliance VMware neghino l'inoltro IPv6.

Se il sistema è configurato in modo da eseguire l'inoltro IP e non è un router designato, gli autori degli attacchi potrebbero utilizzarlo per aggirare la sicurezza della rete fornendo un percorso per le comunicazioni non filtrate dai dispositivi di rete. Per evitare questo rischio, configurare le macchine host dell'appliance virtuale in modo che neghino l'inoltro IPv6.

### Procedura

- 1 Eseguire il comando `# grep [01] /proc/sys/net/ipv6/conf/*/forwarding | egrep "default|all"` nelle macchine host dell'appliance VMware per verificare che siano configurate in modo da negare l'inoltro IPv6.

Se le macchine host sono configurate per negare l'inoltro IPv6, questo comando restituisce i seguenti valori:

```
/proc/sys/net/ipv6/conf/all/forwarding:0
/proc/sys/net/ipv6/conf/default/forwarding:0
```

Se le macchine host sono configurate correttamente, non è necessario eseguire ulteriori operazioni.

- 2 Se è necessario configurare una macchina host in modo che neghi l'inoltro IPv6, aprire il file `/etc/sysctl.conf` in un editor di testo.
- 3 Controllare i valori delle righe che iniziano con `net.ipv6.conf`.

Se i valori delle voci elencate di seguito non sono impostati su 0 o se le voci non esistono, aggiungerle o aggiornare le voci esistenti nel modo appropriato.

```
net.ipv6.conf.all.accept_redirects=0
net.ipv6.conf.default.accept_redirects=0
```

- 4 Salvare le modifiche apportate e chiudere il file.

## Uso dei SYN cookie TCP IPv4

Verificare che le macchine host dell'appliance VMware utilizzino i SYN cookie TCP IPv4.

Un attacco flood SYN TCP può causare un Denial of Service riempiendo la tabella delle connessioni TCP di un sistema con connessioni nello stato SYN\_RCVD. I SYN cookie impediscono il monitoraggio di una connessione finché non si riceve un ACK successivo, assicurandosi in tal modo che l'iniziatore stia tentando una connessione valida e non si tratti dell'origine di un attacco flood. Questa tecnica non funziona in modo pienamente conforme agli standard, ma viene attivata solo durante una condizione di flood e permette di difendere il sistema continuando a rispondere alle richieste valide.

**Procedura**

- 1 Eseguire il comando `# cat /proc/sys/net/ipv4/tcp_syncookies` nelle macchine host dell'appliance VMware per verificare che utilizzino i SYN cookie TCP IPv4.

Se le macchine host sono configurate per negare l'inoltro IPv4, il comando restituisce il valore 1 per `/proc/sys/net/ipv4/tcp_syncookies`. Se le macchine virtuali sono configurate correttamente, non è necessario eseguire ulteriori operazioni.

- 2 Se è necessario configurare un'appliance virtuale per l'utilizzo dei SYN cookie TCP IPv4, aprire il file `/etc/sysctl.conf` in un editor di testo.

- 3 Individuare la voce `net.ipv4.tcp_syncookies=1`.

Se il valore di questa voce non è attualmente impostato su uno o se la voce non esiste, aggiungere la voce o aggiornare quella esistente di conseguenza.

- 4 Salvare le modifiche apportate e chiudere il file.

**Negare gli annunci del router IPv6**

Verificare che le macchine host VMware neghino l'accettazione degli annunci del router e i reindirizzamenti ICMP a meno che non siano necessari per il funzionamento del sistema.

IPv6 consente ai sistemi di configurare i dispositivi di rete utilizzando automaticamente le informazioni fornite dalla rete. Dal punto di vista della sicurezza, configurare manualmente informazioni di configurazione importanti è preferibile rispetto ad accettarle dalla rete in modalità non autenticata.

**Procedura**

- 1 Eseguire il comando `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra | egrep "default|all"` nelle macchine host dell'appliance VMware per verificare che siano configurate in modo da negare gli annunci del router.

Se le macchine host sono configurate per negare gli annunci del router IPv6, questo comando restituisce il valore 0.

```
/proc/sys/net/ipv6/conf/all/accept_ra:0
/proc/sys/net/ipv6/conf/default/accept_ra:0
```

Se le macchine host sono configurate correttamente, non è necessario eseguire ulteriori operazioni.

- 2 Se è necessario configurare una macchina host in modo che neghi gli annunci del router IPv6, aprire il file `/etc/sysctl.conf` in un editor di testo.

- 3 Controllare le voci seguenti:

```
net.ipv6.conf.all.accept_ra=0
net.ipv6.conf.default.accept_ra=0
```

Se queste voci non esistono o se i loro valori non sono impostati su 0, aggiungere le voci o aggiornare le voci esistenti nel modo appropriato.

- 4 Salvare le modifiche apportate e chiudere il file.

### Negare le richieste del router IPv6

Come procedura consigliata di sicurezza, verificare che le macchine host dell'appliance VMware neghino le richieste del router IPv6 a meno che non siano necessarie per il funzionamento del sistema.

L'impostazione relativa alle richieste del router determina quante richieste del router vengono inviate quando viene visualizzata l'interfaccia. Se gli indirizzi vengono assegnati in modo statico, non è necessario inviare alcuna richiesta.

#### Procedura

- 1 Eseguire il comando `# grep [01] /proc/sys/net/ipv6/conf/*/router_sollicitations | grep "default|all"` nelle macchine host dell'appliance VMware per verificare che siano configurate in modo da negare le richieste del router IPv6.

Se le macchine host sono configurate per negare gli annunci del router IPv6, questo comando restituisce i seguenti valori:

```
/proc/sys/net/ipv6/conf/all/router_sollicitations:0
/proc/sys/net/ipv6/conf/default/router_sollicitations:0
```

Se le macchine host sono configurate correttamente, non è necessario eseguire ulteriori operazioni.

- 2 Se è necessario configurare le macchine host in modo che neghino le richieste del router IPv6, aprire il file `/etc/sysctl.conf` in un editor di testo.
- 3 Controllare le voci seguenti:

```
net.ipv6.conf.all.router_sollicitations=0
net.ipv6.conf.default.router_sollicitations=0
```

Se queste voci non esistono o se i loro valori non sono impostati su 0, aggiungere le voci o aggiornare le voci esistenti nel modo appropriato.

- 4 Salvare le modifiche e chiudere il file.

### Negare la preferenza del router IPv6 nelle richieste del router

Verificare che le macchine host dell'appliance VMware neghino le richieste del router IPv6 a meno che non siano necessarie per il funzionamento del sistema.

La preferenza del router nell'impostazione delle richieste determina le preferenze del router. Se gli indirizzi vengono assegnati in modo statico, non è necessario ricevere alcuna preferenza del router per le richieste.



**Procedura**

- 1 Eseguire il comando `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_rtr_pref | egrep "default|all"` nelle macchine host dell'appliance VMware per verificare che siano configurate in modo da negare le richieste del router IPv6.

Se le macchine host sono configurate per negare gli annunci del router IPv6, questo comando restituisce i seguenti valori:

```
/proc/sys/net/ipv6/conf/all/accept_ra_rtr_pref:0
/proc/sys/net/ipv6/conf/default/accept_ra_rtr_pref:0
```

Se le macchine host sono configurate correttamente, non è necessario eseguire ulteriori operazioni.

- 2 Se è necessario configurare le macchine host in modo che neghino le richieste del router IPv6, aprire il file `/etc/sysctl.conf` in un editor di testo.
- 3 Controllare le voci seguenti:

```
net.ipv6.conf.all.accept_ra_rtr_pref=0
net.ipv6.conf.default.accept_ra_rtr_pref=0
```

Se queste voci non esistono o se i loro valori non sono impostati su 0, aggiungere le voci o aggiornare le voci esistenti nel modo appropriato.

- 4 Salvare le modifiche apportate e chiudere il file.

**Negare il prefisso del router IPv6**

Verificare che le macchine host dell'appliance VMware neghino le informazioni sul prefisso del router IPv6 a meno che non siano necessarie per il funzionamento del sistema.

L'impostazione `accept_ra_pinfo` controlla se il sistema accetta informazioni sul prefisso dal router. Se gli indirizzi vengono assegnati in modo statico, non è necessario ricevere alcuna informazione sul prefisso del router.

**Procedura**

- 1 Eseguire il comando `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_pinfo | egrep "default|all"` nelle macchine host dell'appliance VMware per verificare che siano configurate in modo da negare le informazioni sul prefisso del router IPv6.

Se le macchine host sono configurate per negare gli annunci del router IPv6, questo comando restituisce i seguenti valori:

```
/proc/sys/net/ipv6/conf/all/accept_ra_pinfo:0
/proc/sys/net/ipv6/conf/default/accept_ra_pinfo:0
```

Se le macchine host sono configurate correttamente, non è necessario eseguire ulteriori operazioni.

- 2 Se è necessario configurare le macchine host in modo che neghino le informazioni sul prefisso del router IPv6, aprire il file `/etc/sysctl.conf` in un editor di testo.

### 3 Controllare le voci seguenti:

```
net.ipv6.conf.all.accept_ra_pinfo=0
net.ipv6.conf.default.accept_ra_pinfo=0
```

Se queste voci non esistono o se i loro valori non sono impostati su 0, aggiungere le voci o aggiornare le voci esistenti nel modo appropriato.

### 4 Salvare le modifiche e chiudere il file.

## Negare le impostazioni del limite di hop degli annunci del router IPv6

Verificare che le macchine host dell'appliance VMware neghino le impostazioni relative al limite di hop del router IPv6 a meno che non siano necessarie.

L'impostazione `accept_ra_defrtr` controlla se il sistema accetterà le impostazioni del limite di hop da un annuncio del router. Impostando il valore 0 si impedisce che un router modifichi il limite di hop IPv6 predefinito per i pacchetti in uscita.

### Procedura

- 1 Eseguire il comando `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_defrtr | egrep "default|all"` nelle macchine host dell'appliance VMware per verificare che siano configurate in modo da negare le impostazioni del limite di hop del router IPv6.

Se le macchine host sono configurate per negare le impostazioni del limite di hop del router IPv6, questo comando restituisce il valore 0.

```
/proc/sys/net/ipv6/conf/all/accept_ra_defrtr:0
/proc/sys/net/ipv6/conf/default/accept_ra_defrtr:0
```

Se le macchine host sono configurate correttamente, non è necessario eseguire ulteriori operazioni.

- 2 Se è necessario configurare una macchina host in modo che neghi le impostazioni del limite di hop del router IPv6, aprire il file `/etc/sysctl.conf` in un editor di testo.
- 3 Controllare le voci seguenti:

```
net.ipv6.conf.all.autoconf=0
net.ipv6.conf.default.autoconf=0
```

Se queste voci non esistono o se i loro valori non sono impostati su 0, aggiungere le voci o aggiornare le voci esistenti nel modo appropriato.

- 4 Salvare le modifiche apportate e chiudere il file.

## Negare le impostazioni di configurazione automatica degli annunci del router IPv6

Verificare che le macchine host dell'appliance VMware neghino le impostazioni di configurazione automatica del router IPv6 a meno che non siano necessarie.

L'impostazione `autoconf` controlla se gli annunci del router possono fare in modo che il sistema assegni un indirizzo unicast globale a un'interfaccia.

**Procedura**

- 1 Eseguire il comando `# grep [01] /proc/sys/net/ipv6/conf/*/autoconf | egrep "default|all"` nelle macchine host dell'appliance VMware per verificare che siano configurate in modo da negare le impostazioni di configurazione automatica del router IPv6.

Se le macchine host sono configurate per negare le impostazioni di configurazione automatica del router IPv6, questo comando restituisce il valore 0.

```
/proc/sys/net/ipv6/conf/all/autoconf:0
/proc/sys/net/ipv6/conf/default/autoconf:0
```

Se le macchine host sono configurate correttamente, non è necessario eseguire ulteriori operazioni.

- 2 Se è necessario configurare una macchina host in modo che neghi le impostazioni di configurazione automatica del router IPv6, aprire il file `/etc/sysctl.conf` in un editor di testo.
- 3 Controllare le voci seguenti:

```
net.ipv6.conf.all.autoconf=0
net.ipv6.conf.default.autoconf=0
```

Se queste voci non esistono o se i loro valori non sono impostati su 0, aggiungere le voci o aggiornare le voci esistenti nel modo appropriato.

- 4 Salvare le modifiche apportate e chiudere il file.

**Negare le richieste del router adiacente IPv6**

Verificare che le macchine host dell'appliance VMware neghino le richieste del router adiacente IPv6 a meno che non siano necessarie.

L'impostazione `dad_transmits` determina quante richieste del router adiacente inviare per ogni indirizzo (globale e locale rispetto al collegamento) quando si visualizza un'interfaccia, per garantire che l'indirizzo desiderato sia univoco nella rete.

**Procedura**

- 1 Eseguire il comando `# grep [01] /proc/sys/net/ipv6/conf/*/dad_transmits | egrep "default|all"` nelle macchine host dell'appliance VMware per verificare che siano configurate in modo da negare le richieste del router adiacente IPv6.

Se le macchine host sono configurate per negare le richieste del router adiacente IPv6, questo comando restituisce il valore 0.

```
/proc/sys/net/ipv6/conf/all/dad_transmits:0
/proc/sys/net/ipv6/conf/default/dad_transmits:0
```

Se le macchine host sono configurate correttamente, non è necessario eseguire ulteriori operazioni.

- 2 Se è necessario configurare una macchina host in modo che neghi le richieste del router adiacente IPv6, aprire il file `/etc/sysctl.conf` in un editor di testo.

### 3 Controllare le voci seguenti:

```
net.ipv6.conf.all.dad_transmits=0
net.ipv6.conf.default.dad_transmits=0
```

Se queste voci non esistono o se i loro valori non sono impostati su 0, aggiungere le voci o aggiornare le voci esistenti nel modo appropriato.

### 4 Salvare le modifiche apportate e chiudere il file.

## Limitazione del numero massimo di indirizzi IPv6

Verificare che nelle impostazioni delle macchine host dell'appliance VMware, il numero massimo di indirizzi IPv6 sia limitato alla quantità minima necessaria per consentire il corretto funzionamento del sistema.

L'impostazione del numero massimo di indirizzi determina quanti indirizzi IPv6 unicast globali sono disponibili per ogni interfaccia. Il valore predefinito è 16, ma è consigliabile impostare il numero di indirizzi globali configurati statisticamente richiesti per il sistema specifico.

### Procedura

- 1 Eseguire il comando `# grep [1] /proc/sys/net/ipv6/conf/*/max_addresses | egrep "default|all"` nelle macchine host dell'appliance VMware per verificare che limitino in modo appropriato il numero massimo di indirizzi IPv6.

Se le macchine host sono configurate per limitare il numero massimo di indirizzi IPv6, il comando restituisce valori 1.

```
/proc/sys/net/ipv6/conf/all/max_addresses:1
/proc/sys/net/ipv6/conf/default/max_addresses:1
```

Se le macchine host sono configurate correttamente, non è necessario eseguire ulteriori operazioni.

- 2 Se è necessario configurare il numero massimo di indirizzi IPv6 nelle macchine host, aprire il file `/etc/sysctl.conf` in un editor di testo.
- 3 Controllare le voci seguenti:

```
net.ipv6.conf.all.max_addresses=1
net.ipv6.conf.default.max_addresses=1
```

Se le voci non esistono o se i loro valori non sono impostati su 1, aggiungere le voci o aggiornare le voci esistenti di conseguenza.

- 4 Salvare le modifiche apportate e chiudere il file.

## Configurazione delle impostazioni di rete per l'host IaaS

Come procedura consigliata per la sicurezza, configurare le impostazioni di comunicazione di rete nella macchina host del componente Infrastructure as a Service (IaaS) VMware in base alle linee guida e ai requisiti di VMware.

Impostare la configurazione di rete della macchina host Infrastructure as a Service (IaaS) per il supporto completo delle funzioni di vRealize Automation con la protezione appropriata.

Vedere [Protezione del componente Infrastructure as a Service](#).

## Configurazione di porte e protocolli

Come procedura di sicurezza consigliata, configurare le porte e i protocolli di tutti i componenti e le appliance vRealize Automation in conformità con le linee guida di VMware.

Configurare le porte in ingresso e uscita per i componenti di vRealize Automation come richiesto per il funzionamento in produzione dei componenti di sistema critici. Disabilitare tutte le porte e i protocolli non necessari. Vedere [Architettura di riferimento di vRealize Automation](#).

### Porte richieste per gli utenti

Come procedura di sicurezza consigliata, configurare le porte utente di vRealize Automation in base alle linee guida di VMware.

Esporre le porte necessarie solo in una rete sicura.

SERVER	PORTE
Appliance vRealize Automation	443, 8443

### Porte necessarie per l'amministratore

Come procedura consigliata per la sicurezza, configurare le porte dell'amministratore di vRealize Automation in base alle linee guida di VMware.

Esporre le porte necessarie solo in una rete sicura.

SERVER	PORTE
Server vRealize Application Services	5480

### Porte dell'appliance vRealize Automation

Come procedura di sicurezza consigliata, configurare le porte in ingresso e uscita per Appliance vRealize Automation in conformità alle raccomandazioni di VMware.

### Porte in ingresso

Configurare il numero minimo di porte in ingresso richieste per Appliance vRealize Automation. Configurare porte facoltative se necessarie per la configurazione del sistema.

**Tabella 1-4. Porte in ingresso minime richieste**

PORTA	PROTOCOLLO	COMMENTI
443	TCP	Consente di accedere alla console di vRealize Automation e alle chiamate API.
8443	TCP	Proxy console (VMRC).
5480	TCP	Consente di accedere alla console di gestione Web dell'appliance virtuale.

**Tabella 1-4. Porte in ingresso minime richieste (Continua)**

PORTA	PROTOCOLLO	COMMENTI
5488, 5489	TCP	Interne. Utilizzate da Appliance vRealize Automation per gli aggiornamenti.
5672	TCP	Messaggistica RabbitMQ.  <b>Nota</b> Quando si configurano istanze di Appliance vRealize Automation in cluster, potrebbe essere necessario configurare le porte 4369 e 25672 aperte.
40002	TCP	Richiesta per il servizio vIDM. Questa porta è bloccata dal firewall per tutto il traffico esterno ad eccezione del traffico proveniente da altri nodi di Appliance vRealize Automation quando vengono aggiunti nella configurazione HA.

Se necessario, configurare le porte in ingresso facoltative.

**Tabella 1-5. Porte in ingresso facoltative**

PORTA	PROTOCOLLO	COMMENTI
22	TCP	(Facoltativa) SSH. In un ambiente di produzione, disabilitare il servizio SSH in ascolto sulla porta 22 e chiudere la porta 22.
80	TCP	(Facoltativa) Reindirizza a 443.

## Porte in uscita

Configurare le porte in uscita richieste.

**Tabella 1-6. Porte in uscita minime richieste**

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.
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.
443	TCP	Servizio di gestione di Infrastructure as a Service mediante protocollo HTTPS.

Se necessario, configurare le porte in uscita facoltative.

**Tabella 1-7. Porte in uscita opzionali**

PORTA	PROTOCOLLO	COMMENTI
80	TCP	(Facoltativa) Per il recupero degli aggiornamenti software. È possibile scaricare e applicare gli aggiornamenti separatamente.
123	TCP, UDP	(Facoltativa) Per la connessione diretta a NTP anziché utilizzare l'orario dell'host.

## Porte Infrastructure as a Service

Come procedura consigliata di sicurezza, configurare le porte in ingresso e in uscita per i componenti Infrastructure as a Service (IaaS) in base alle linee guida di VMware.

### Porte in ingresso

Configurare le porte in ingresso minime richieste per i componenti IaaS.

**Tabella 1-8. Porte in ingresso minime richieste**

COMPONENTE	PORTA	PROTOCOLLO	COMMENTI
Servizio di gestione	443	TCP	Comunicazione con i componenti di IaaS e con l'appliance vRealize Automation 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.

### Porte in uscita

Configurare le porte in uscita minime richieste per i componenti IaaS.

**Tabella 1-9. Porte in uscita minime richieste**

COMPONENTE	PORTA	PROTOCOLLO	COMMENTI
Tutto	53	TCP, UDP	DNS.
Tutto		TCP, UDP	DHCP.
Servizio di gestione	443	TCP	Comunicazione con l'appliance vRealize Automation su 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.

Se necessario, configurare le porte in uscita opzionali.

**Tabella 1-10. Porte in uscita opzionali**

COMPONENTE	PORTA	PROTOCOLLO	COMMENTI
Tutto	123	TCP, UDP	NTP è opzionale.

## Controllo e registrazione

Come procedura consigliata per la sicurezza, configurare il controllo e la registrazione nel sistema vRealize Automation in base alle raccomandazioni di VMware.

La registrazione remota in un host di file di registro centrale fornisce un archivio sicuro per i file di registro. Raccogliendo i file di registro in un host centrale, è possibile monitorare l'ambiente con un solo strumento. È inoltre possibile eseguire analisi aggregate e cercare la prova di minacce quali attacchi coordinati a più entità all'interno dell'infrastruttura. La registrazione in un server di file di registro centralizzato e protetto può impedire la manomissione dei file di registro e fornisce inoltre una registrazione di controllo a lungo termine.

### Assicurarsi che il server di registrazione remota sia protetto

Spesso, dopo aver violato la sicurezza del computer host, gli autori degli attacchi possono cercare e manomettere i file di registro per coprire le loro tracce e mantenere il controllo senza essere scoperti. Proteggere in modo adeguato il server di registrazione remota contribuisce a scoraggiare la manomissione del registro.

### Utilizzare un server NTP autorizzato

Assicurarsi che tutte le macchine host utilizzino la stessa origine ora relativa, incluso lo stesso offset di localizzazione pertinente, e che sia possibile correlare l'origine ora relativa a uno standard orario concordato, come l'ora UTC (Coordinated Universal Time). Un approccio disciplinato alle origini ora consente di individuare rapidamente e correlare le azioni di un intruso quando si esaminano i file di registro pertinenti. Impostazioni orarie errate possono rendere difficoltosa l'ispezione e la correlazione dei file di registro allo scopo di rilevare gli attacchi e possono rendere imprecisi i controlli.

Usare almeno tre server NTP di origini ora esterne oppure configurare alcuni server NTP locali in una rete affidabile che a sua volta riceva l'ora da almeno tre origini ora esterne.

## Installazione di vRealize Automation

Attenersi alle istruzioni fornite per installare una nuova istanza di vRealize Automation.

### Cenni generali sull'installazione di vRealize Automation

È possibile installare vRealize Automation per il supporto di ambienti prototipo minimi o in configurazioni enterprise distribuite di dimensioni differenti, in grado di gestire i carichi di lavoro di produzione.

L'installazione può essere interattiva o invisibile all'utente.

Al termine dell'installazione, iniziare a utilizzare vRealize Automation personalizzando le impostazioni e configurando i tenant, per fornire agli utenti l'accesso al provisioning self-service e alla gestione del ciclo di vita dei servizi cloud.

### Informazioni sull'installazione di vRealize Automation

È possibile installare vRealize Automation con diversi metodi, ognuno con livelli diversi di interattività.



Per eseguire l'installazione si distribuisce un'appliance vRealize Automation e si completa quindi l'installazione utilizzando una delle opzioni seguenti:

- Un'installazione guidata consolidata basata su Web
- Una configurazione dell'appliance separata, basata su browser e installazioni separate di Windows per i componenti server IaaS
- Un programma di installazione invisibile all'utente, basato sulla riga di comando che accetta input da un file di proprietà di risposta
- Un API REST di installazione che accetta input in formato JSON

È anche possibile installare vRealize Automation utilizzando vRealize Suite Lifecycle Manager. Consultare la [documentazione di vRealize Suite](#).

## Novità di questa installazione di vRealize Automation

Se sono state installate le versioni precedenti di vRealize Automation, prestare attenzione alle modifiche alla procedura di installazione apportate in questa release prima di avviare il processo.

- Questa versione semplifica il processo di ridenominazione dell'appliance vRealize Automation. Vedere [Modifica del nome host dell'appliance vRealize Automation](#).
- In questa versione, l'appliance vRealize Automation utilizza TLS 1.2 per impostazione predefinita. L'interfaccia di amministrazione include un'opzione per abilitare temporaneamente TLS 1.0 e 1.1, necessari per aggiornare gli agenti esistenti a questa versione.
- L'interfaccia di amministrazione dell'appliance vRealize Automation ora include una pagina per l'installazione e la gestione delle patch. Vedere [Gestione delle patch di accesso](#).
- Questa versione descrive come modificare la porta predefinita del proxy per VMware Remote Console. Vedere [Modifica della porta del proxy di VMware Remote Console](#).
- In questa versione sono stati corretti alcuni collegamenti alla guida interrotti nell'installazione guidata.

## Componenti d'installazione di vRealize Automation

Un'installazione tipica di vRealize Automation include un'appliance vRealize Automation e uno o più server Windows che insieme forniscono Infrastructure as a Service (IaaS) di vRealize Automation.

### Appliance vRealize Automation

L'appliance vRealize Automation è un'appliance virtuale Linux preconfigurata. L'appliance vRealize Automation viene fornita come file di virtualizzazione aperto da distribuire in un'infrastruttura virtualizzata esistente come vSphere.

L'appliance vRealize Automation esegue diverse funzioni centrali di vRealize Automation.

- L'appliance contiene il server che ospita il portale di prodotto di vRealize Automation in cui gli utenti inseriscono le credenziali per accedere al provisioning self-service e alla gestione dei servizi cloud.
- L'appliance gestisce il single Sign-On (SSO) per l'autorizzazione e l'autenticazione degli utenti.

- Il server dell'appliance ospita un'interfaccia di gestione per le impostazioni dell'appliance vRealize Automation.
- L'appliance include un database PostgreSQL preconfigurato utilizzato per le operazioni interne dell'appliance vRealize Automation.

Nelle distribuzioni di grandi dimensioni con appliance ridondanti, i database delle appliance secondarie fungono da replica per fornire l'alta disponibilità.

- L'appliance include un'istanza preconfigurata di vRealize Orchestrator. vRealize Automation utilizza i workflow e le azioni di vRealize Orchestrator per ampliare le proprie capacità.

Ora è consigliata l'istanza incorporata di vRealize Orchestrator. Nelle distribuzioni precedenti o in casi particolari, tuttavia, gli utenti possono invece collegare vRealize Automation a un vRealize Orchestrator esterno.

- L'appliance contiene il programma di installazione scaricabile dell'agente di gestione. Tutti i server Windows che compongono vRealize Automation IaaS devono installare l'agente di gestione.

L'agente di gestione registra i server Windows di IaaS nell'appliance vRealize Automation, automatizza l'installazione e la gestione dei componenti IaaS e raccoglie le informazioni relative a supporto e telemetria.

### **Infrastructure as a Service (IaaS)**

Il servizio IaaS di vRealize Automation consiste in uno o più server Windows che lavorano insieme per modellare ed eseguire il provisioning di sistemi all'interno di infrastrutture cloud private, pubbliche o ibride.

I componenti del servizio IaaS di vRealize Automation vengono installati su uno o più server Windows virtuali o fisici. Dopo l'installazione, le operazioni di IaaS vengono visualizzate sulla scheda Infrastruttura dell'interfaccia del prodotto.

IaaS consiste nei seguenti componenti, che possono essere installati insieme o separatamente, in base alle dimensioni della distribuzione.

#### **Server Web**

Il server Web IaaS fornisce le funzionalità di amministrazione dell'infrastruttura e di creazione dei servizi all'interfaccia del prodotto vRealize Automation. Il componente server Web comunica con il servizio di gestione, che fornisce aggiornamenti di Distributed Execution Manager (DEM), database SQL Server e agenti.

#### **Model Manager**

I modelli di vRealize Automation favoriscono l'integrazione con sistemi e database esterni e implementano la logica di business utilizzata dal DEM.

Il Model Manager fornisce servizi e utilità per rendere permanenti, gestire le versioni, proteggere e distribuire elementi dei modelli. Model Manager è ospitato in uno dei server Web IaaS e comunica con i DEM, il database SQL Server e il sito Web dell'interfaccia del prodotto.

## Servizio di gestione

Il servizio di gestione è un servizio Windows che coordina le comunicazioni tra DEM IaaS, database SQL Server, agenti e SMTP. Inoltre, il servizio di gestione comunica con il server Web attraverso il Model Manager e deve essere eseguito con un account di dominio con privilegi di amministratore su tutti i server IaaS Windows.

A meno che non si abiliti il failover automatico del servizio di gestione, IaaS richiede che tale servizio venga eseguito attivamente su una sola macchina Windows alla volta. Per il backup o l'alta disponibilità, è possibile distribuire ulteriori macchine del servizio di gestione, ma l'approccio basato su failover manuale richiede che sulle macchine di backup il servizio sia interrotto e configurato per l'avvio manuale.

Per ulteriori informazioni, vedere [Informazioni sul failover automatico del servizio di gestione](#).

## Database di SQL Server

IaaS utilizza un database Microsoft SQL Server per conservare le informazioni sulle macchine che gestisce e sui propri elementi e criteri. La maggior parte degli utenti consente a vRealize Automation di creare il database durante l'installazione. In alternativa, è possibile creare il database separatamente in base ai criteri del sito.

## Distributed Execution Manager

Il componente IaaS DEM esegue la logica di business di modelli personalizzati, interagendo con il database IaaS SQL Server e con database e sistemi esterni. Un approccio comune consiste nell'installare DEM sul server Windows IaaS che ospita il servizio di gestione attivo, ma non si tratta di un'azione obbligatoria.

Ciascuna istanza di DEM agisce come Worker o Orchestrator. I ruoli possono essere installati sullo stesso server o su server separati.

DEM Worker: il DEM worker ha un'unica funzione che consiste nell'eseguire i workflow. Più DEM Worker incrementano la capacità e possono essere installati sullo stesso server o in server separati.

DEM Orchestrator: il DEM orchestrator svolge le seguenti funzioni di supervisione.

- Monitoraggio dei DEM worker. Se un worker si interrompe o perde la connessione a Model Manager, il DEM orchestrator trasferisce il workflow a un altro DEM worker.
- Pianifica i workflow creando istanze dei workflow all'orario pianificato.
- Garantisce che in un dato momento sia in esecuzione una sola istanza di un workflow pianificato.
- Pre-elabora i workflow prima che vengano eseguiti. La pre-elaborazione include il controllo delle precondizioni per i workflow e la creazione della cronologia di esecuzione dei workflow.

Il DEM orchestrator attivo richiede una solida connessione di rete all'host Model Manager. Nelle grandi distribuzioni con più istanze di DEM Orchestrator in server distinti, le istanze di Orchestrator secondarie fungono da backup. Le istanze di DEM Orchestrator secondarie monitorano l'istanza di DEM Orchestrator attiva e forniscono ridondanza e failover quando si verifica un problema relativo all'istanza di DEM Orchestrator attiva. Per questo tipo di configurazione di failover, può essere opportuno installare il DEM orchestrator attivo con l'host di gestione del servizio attivo e i DEM orchestrator secondari con gli host del servizio di gestione standby.

## Agenti

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

Un approccio comune consiste nell'installare agenti vRealize Automation sul server IaaS Windows che ospita il servizio di gestione. Non si tratta di un'azione obbligatoria. Più agenti incrementano la capacità e possono essere installati sullo stesso server o in server separati.

## Agenti proxy di virtualizzazione

vRealize Automation crea e gestisce macchine virtuali su host di virtualizzazione. Gli agenti proxy di virtualizzazione inviano comandi e raccolgono dati sia con host vSphere ESX Server, XenServer e Hyper-V sia con le macchine virtuali di cui è stato effettuato il provisioning su di essi.

Un agente proxy di virtualizzazione ha le seguenti caratteristiche.

- Richiede di norma i privilegi di amministratore sulla piattaforma di virtualizzazione che gestisce.
- Comunica con il servizio di gestione IaaS
- Viene installato separatamente con un proprio file di configurazione.

Nella maggior parte delle distribuzioni di vRealize Automation viene installato l'agente proxy vSphere. A seconda delle risorse di virtualizzazione disponibili, è possibile installare altri agenti proxy.

## Agenti Virtual Desktop Integration

Gli agenti della PowerShell di Virtual Desktop Integration (VDI) consentono a vRealize Automation di integrarsi con i sistemi desktop virtuali esterni. Per gli agenti VDI è necessario disporre di privilegi di amministratore per i sistemi esterni.

È possibile registrare macchine virtuali di cui vRealize Automation ha eseguito il provisioning con XenDesktop su un Desktop Delivery Controller (DDC) Citrix, che consente all'utente di accedere all'interfaccia Web di XenDesktop da vRealize Automation.

## Agenti External Provisioning Integration

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.

Per gli agenti EPI è necessario disporre di privilegi di amministratore nei sistemi esterni con cui interagiscono.

### **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 di Windows e consente di gestire server remoti Windows da una posizione centrale. L'agente WMI consente inoltre di raccogliere dati dai server Windows gestiti da vRealize Automation.

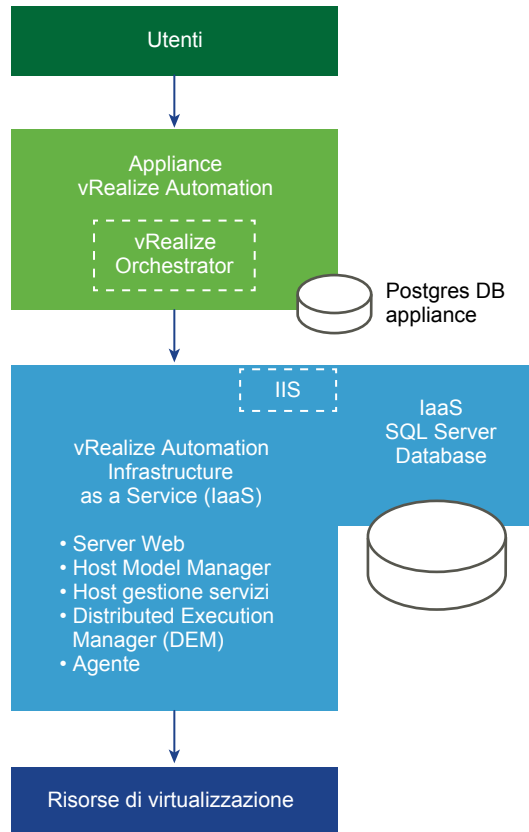
## **Tipo di distribuzione**

È possibile installare una distribuzione minima di vRealize Automation come distribuzione minima per un'implementazione di prototipazione o sviluppo, oppure in una configurazione distribuita adatta per carichi di lavoro di produzione da medi ad alti.

### **Distribuzioni minime di vRealize Automation**

Le distribuzioni minime includono un'appliance vRealize Automation e un server Windows che ospita i componenti IaaS. In una distribuzione minima, il database SQL Server di vRealize Automation può trovarsi sullo stesso server Windows IaaS con i componenti IaaS oppure su un server Windows separato.

**Figura 1-10. Distribuzione minima di vRealize Automation**



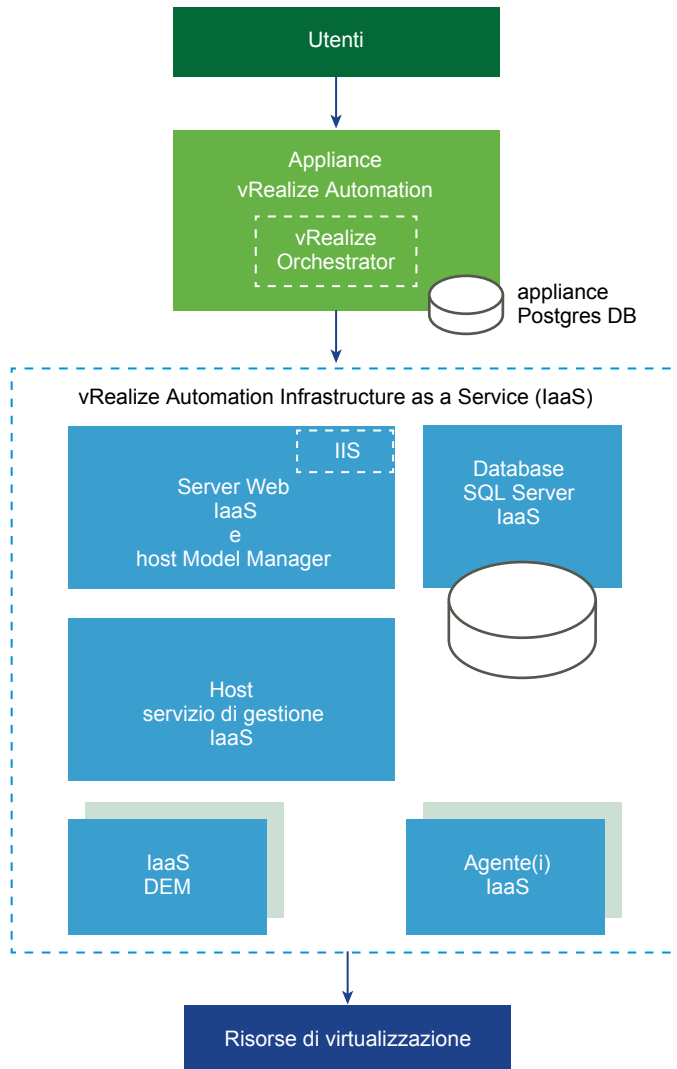
Non è possibile convertire una distribuzione minima in una distribuzione enterprise. Per ampliare una distribuzione, iniziare con una distribuzione enterprise di piccole dimensioni e aggiungervi componenti. Non è possibile iniziare con una distribuzione minima.

**Nota** La documentazione di vRealize Automation include uno scenario completo di distribuzione minima di esempio, con una procedura guidata per installare e iniziare a utilizzare il prodotto per la prototipazione. Vedere *Installazione e configurazione di vRealize Automation per lo scenario Rainpole*.

### Distribuzioni di vRealize Automation distribuite

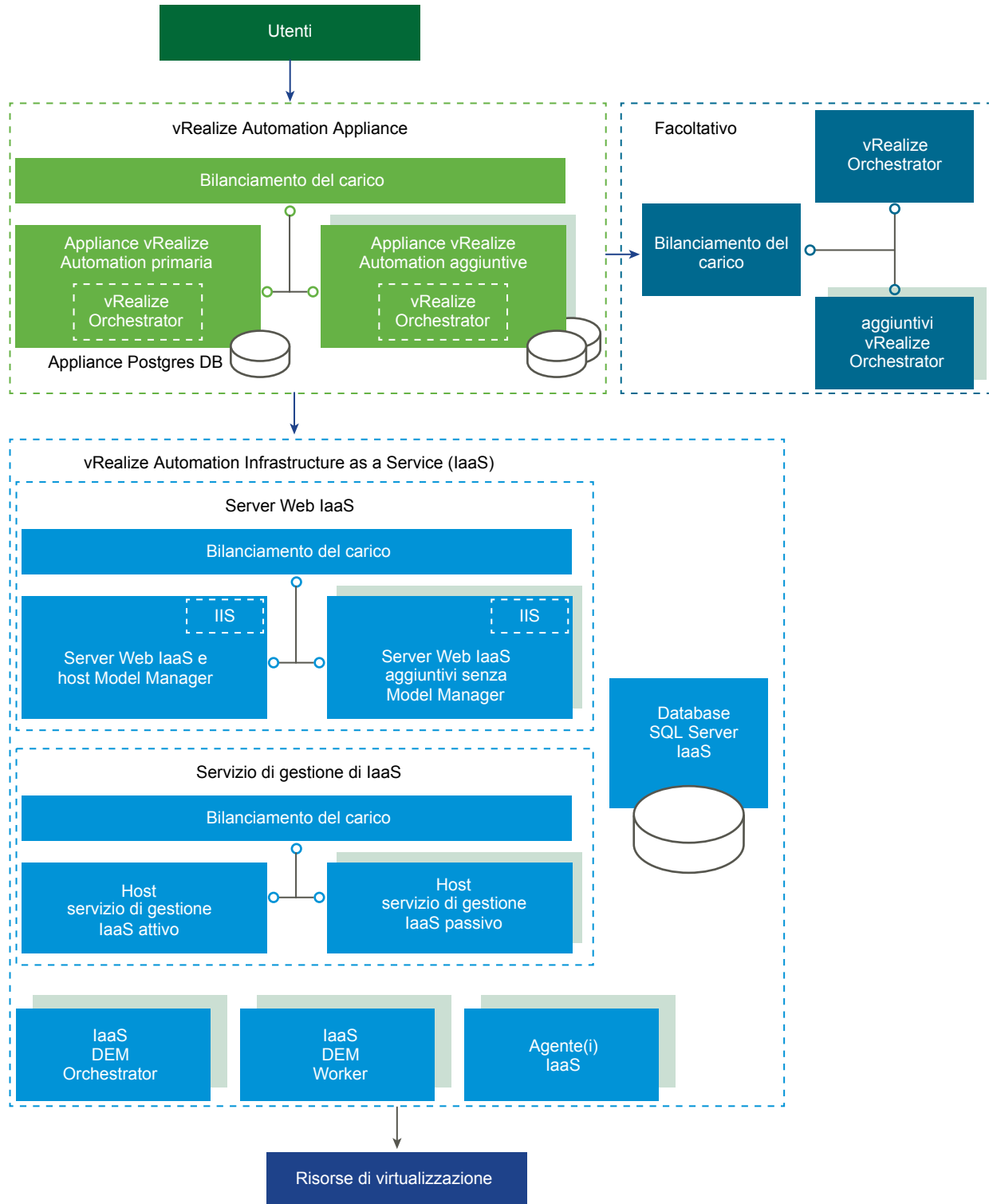
Le dimensioni delle distribuzioni enterprise distribuite possono essere varie. Una distribuzione distribuita di base può migliorare vRealize Automation semplicemente ospitando componenti IaaS in server Windows, come mostrato nell'illustrazione seguente.

**Figura 1-11. Distribuzione vRealize Automation distribuita**



Diverse distribuzioni di produzione si spingono più avanti, con appliance e server ridondanti, uniti al bilanciamento del carico per una maggiore capacità. Le distribuzioni distribuite di grandi dimensioni offrono maggiore scalabilità, alta disponibilità e disaster recovery. Tenere presente che ora l'istanza incorporata di vRealize Orchestrator è consigliata, ma nelle distribuzioni più datate vRealize Automation potrebbe essere connesso a un vRealize Orchestrator esterno.

**Figura 1-12. Distribuzione di vRealize Automation distribuita di grandi dimensioni con bilanciamento del carico.**



Per informazioni sulla scalabilità e sull'alta disponibilità, vedere la guida *Architettura di riferimento di vRealize Automation*.



## Scelta del metodo d'installazione

L'installazione guidata di vRealize Automation è lo strumento principale per le nuove installazioni di vRealize Automation. In alternativa è possibile eseguire i processi di installazione separati manuali o un'installazione invisibile all'utente.

- L'installazione guidata è un modo semplice e rapido per eseguire le installazioni, sia che si tratti di distribuzioni minime o di distribuzioni enterprise distribuite, con o senza bilanciamenti del carico. La maggior parte degli utenti esegue l'installazione guidata.
- Se si desidera espandere una distribuzione vRealize Automation o se l'installazione guidata si è arrestata per qualsiasi motivo, è necessario eseguire i passaggi d'installazione manuali. Una volta iniziata un'installazione manuale, non è più possibile tornare indietro e scegliere di eseguire l'installazione guidata.
- In base alle esigenze del sito, è possibile sfruttare le caratteristiche dell'installazione invisibile all'utente, da riga di comando o basata su API.

## Preparazione per l'installazione di vRealize Automation

vRealize Automation viene installato nell'infrastruttura di virtualizzazione esistente. Prima di iniziare un'installazione, è necessario assicurarsi che siano rispettati determinati requisiti di sistema e ambientali.

### Preparazione generale

Prima di installare vRealize Automation, è opportuno tenere presenti alcuni aspetti che riguardano la distribuzione in generale.

Per ulteriori informazioni sui requisiti degli ambienti di livello superiore, inclusi il sistema operativo e le versioni del browser supportati, vedere la [matrice di supporto di vRealize Automation](#).

### Browser Web utente

Non sono supportate le schede e le finestre multiple dei browser. vRealize Automation supporta un'unica sessione per utente.

Le console remote di VMware Remote Console di cui viene eseguito il provisioning su vSphere supportano solo un sottoinsieme dei browser supportati da vRealize Automation.

### Software di terze parti

I software di terze parti devono sempre includere le patch del fornitore più recenti. Tra i software di terze parti sono inclusi Microsoft Windows e SQL Server.

### Sincronizzazione di data e ora

Tutte le appliance di vRealize Automation e dei server IaaS Windows devono essere sincronizzate con la stessa origine ora. È possibile utilizzare una sola origine tra quelle indicate di seguito. Non utilizzare più origini ora diverse.

- L'host dell'appliance di vRealize Automation

- Un server NTP (Network Time Protocol) esterno

Per utilizzare l'host dell'appliance di vRealize Automation, è necessario eseguire NTP sull'host ESXi. Per ulteriori informazioni sulla sincronizzazione di data e ora, vedere [Articolo della Knowledge Base VMware 1318](#).

È possibile selezionare l'origine ora nella pagina dei prerequisiti d'installazione dell'installazione guidata.

## Account e password

Prima di installare vRealize Automation, potrebbe essere necessario creare o impostare diversi account utente e password.

### Account del servizio IaaS

IaaS installa diversi servizi Windows che devono essere eseguiti con un unico account utente.

- L'account deve essere un utente di dominio.
- Non è necessario che l'account sia un amministratore di dominio, tuttavia prima dell'installazione deve disporre delle autorizzazioni di amministratore locale per tutti i server IaaS Windows.
- La password dell'account non può contenere il carattere virgolette doppie (").
- Il programma di installazione dell'agente di gestione per i server Windows IaaS chiede di specificare le credenziali dell'account.
- L'account deve disporre dell'autorizzazione **Accedi come servizio** che consente l'avvio del servizio di gestione, che genera i file di registro.
- L'account deve disporre dell'autorizzazione dbo per il database IaaS.

Se si utilizza il programma di installazione per creare il database, aggiungere l'accesso dell'account a SQL Server prima dell'installazione. Il programma di installazione concede l'autorizzazione dbo dopo aver creato il database.

- Se si utilizza il programma di installazione per creare il database, in SQL aggiungere il ruolo sysadmin all'account prima dell'installazione.

Il ruolo sysadmin non è necessario se si sceglie di utilizzare un database vuoto preesistente.

### Identità pool di applicazioni IIS

L'account utilizzato come identità del pool di applicazioni IIS per il servizio Web di gestione dei modelli deve disporre dell'autorizzazione **Accesso come processo batch**.

### Credenziali del database IaaS

Il database può essere creato dal programma di installazione di vRealize Automation oppure è possibile crearlo separatamente utilizzando SQL Server. Quando il programma di installazione di vRealize Automation crea il database, vengono applicati i requisiti riportati di seguito.

- Per il programma di installazione di vRealize Automation, se si seleziona Autenticazione di Windows, l'account che esegue l'agente di gestione sul server Web IaaS primario deve disporre del ruolo sysadmin in SQL per poter creare il database e modificarne le dimensioni.

- Per il programma di installazione di vRealize Automation, anche se non si seleziona Autenticazione di Windows, l'account che esegue l'agente di gestione sul server Web IaaS primario deve disporre del ruolo sysadmin in SQL poiché le credenziali vengono utilizzate in runtime.
- Se si crea il database separatamente, le credenziali dell'utente Windows o dell'utente SQL specificate devono disporre dell'autorizzazione dbo per il database.

### **Passphrase di sicurezza del database IaaS**

La passphrase di sicurezza del database genera una chiave di crittografia che protegge i dati nel database SQL IaaS. La passphrase di sicurezza viene specificata nella pagina Host IaaS dell'installazione guidata.

- È consigliabile utilizzare la stessa passphrase di sicurezza del database per l'intera installazione in modo che ciascun componente abbia la stessa chiave di crittografia.
- Registrare la passphrase, in quanto sarà necessaria per ripristinare il database in caso di errore o se si desidera aggiungere componenti dopo l'installazione.
- La passphrase di sicurezza del database non può contenere il carattere virgolette doppie ("). La passphrase verrebbe accettata al momento della creazione ma causerebbe un errore di installazione.

### **Endpoint vSphere**

Se si intende eseguire il provisioning in un endpoint vSphere, è necessario un dominio o un account locale con autorizzazioni sufficienti a eseguire le operazioni nel target. È inoltre necessario che l'account disponga del livello appropriato di autorizzazioni configurato in vRealize Orchestrator.

### **Password dell'amministratore di vRealize Automation**

Dopo l'installazione, la password dell'amministratore di vRealize Automation permette di accedere al tenant predefinito. È necessario specificare la password dell'amministratore nella pagina Single Sign-On dell'installazione guidata.

La password dell'amministratore di vRealize Automation non può terminare con il simbolo di uguaglianza (=). La password verrebbe accettata al momento della creazione ma causerebbe errori nell'esecuzione di operazioni quali il salvataggio di endpoint.

### **Nomi host e indirizzi IP**

vRealize Automation richiede di assegnare un nome agli host nella propria installazione in base ad alcuni requisiti.

- Tutte le macchine vRealize Automation della propria installazione devono essere in grado di risolverli a vicenda mediante un nome di dominio completamente qualificato (FQDN).

Durante l'installazione, immettere sempre il nome di dominio completo quando si identifica o si seleziona una macchina vRealize Automation. Non immettere indirizzi IP o nomi di macchina brevi.

- Oltre al requisito FQDN, le macchine Windows che eseguono l'hosting del servizio Model Manager Web, del servizio di gestione e del database di Microsoft SQL Server devono essere in grado di risolversi a vicenda attraverso il nome del Windows Internet Name Service (WINS).

Configurare il DNS (Domain Name System) per risolvere questi nomi host WINS brevi.

- Pianificare anticipatamente la denominazione di domini e macchine in modo che i nomi delle macchine vRealize Automation inizino con lettere (a-z, A-Z), terminino con lettere o numeri (0-9) e abbiano nel mezzo solo lettere, numeri o trattini (-). Il carattere di sottolineatura (\_) non è consentito nel nome host o in qualsiasi punto dell'FQDN.

Per ulteriori informazioni sui nomi consentiti, esaminare le specifiche del nome host dell'Internet Engineering Task Force. Vedere [www.ietf.org](http://www.ietf.org).

- In generale, si consiglia di mantenere i nomi host e gli FQDN pianificati per i sistemi vRealize Automation. Non sempre è possibile modificare un nome host. Anche laddove sia possibile, la procedura richiesta potrebbe essere complessa.
- È consigliabile riservare e utilizzare indirizzi IP statici per tutte le appliance vRealize Automation e i server Windows di IaaS. vRealize Automation supporta DHCP, ma gli indirizzi IP statici sono consigliati per distribuzioni a lungo termine come gli ambienti di produzione.
  - L'indirizzo IP viene applicato all'appliance vRealize Automation durante una distribuzione OVF o OVA.
  - Per i server Windows IaaS, si segue il processo del sistema operativo abituale. Impostare l'indirizzo IP prima d'installare vRealize Automation IaaS.

## Latenza e larghezza di banda

vRealize Automation supporta più siti e l'installazione distribuita, ma volume e velocità di trasmissione dati devono soddisfare dei prerequisiti minimi.

vRealize Automation richiede un ambiente con una latenza di rete di 5 ms o inferiore e una larghezza di banda di 1 GB o superiore tra i seguenti componenti.

- Appliance vRealize Automation
- Server Web IaaS
- Host Model Manager IaaS
- Host del servizio di gestione IaaS
- Database di SQL Server IaaS
- DEM Orchestrator IaaS

Il componente seguente potrebbe funzionare in un sito a latenza superiore, ma la procedura non è consigliata.

- DEM Worker IaaS

È possibile installare il componente seguente nel sito dell'endpoint con cui esso comunica.

- Agente proxy IaaS

## Appliance vRealize Automation

La maggior parte dei requisiti dell'appliance vRealize Automation sono preconfigurati nell'OVF o OVA distribuito. Gli stessi prerequisiti si applicano alle appliance vRealize Automation autonoma, master o replica.

L'hardware minimo della macchina virtuale su cui è possibile distribuire è Versione 7, ESX/ESXi 4.x o versioni successive. Vedere [Articolo della Knowledge Base VMware 2007240](#). Per via della richiesta di risorse hardware, non distribuire su VMware Workstation.

Dopo la distribuzione, è possibile utilizzare vSphere per configurare le impostazioni hardware dell'appliance vRealize Automation per far sì che soddisfino i requisiti di Active Directory. Vedere la tabella seguente.

**Tabella 1-11. Requisiti hardware dell'appliance vRealize Automation per Active Directory**

Appliance vRealize Automation per piccole istanze di Active Directory	Appliance vRealize Automation per grandi istanze di Active Directory
<ul style="list-style-type: none"> <li>■ 4 CPU</li> <li>■ 18 GB di memoria</li> <li>■ 60 GB di spazio su disco</li> </ul>	<ul style="list-style-type: none"> <li>■ 4 CPU</li> <li>■ 22 GB di memoria</li> <li>■ 60 GB di spazio su disco</li> </ul>

Una piccola istanza di Active Directory contiene fino a 25.000 utenti nell'unità organizzativa da sincronizzare nella configurazione archivio identità. Una grande istanza di Active Directory contiene più di 25.000 utenti nell'unità organizzativa.

## Porte dell'appliance vRealize Automation

Le porte dell'appliance vRealize Automation sono in genere preconfigurate in OVF o OVA distribuito.

Le porte seguenti vengono utilizzate dall'appliance vRealize Automation.

**Tabella 1-12. Porte in ingresso**

Porta	Protocollo	Commenti
22	TCP	Facoltativi. Accesso alle sessioni SSH.
80	TCP	Facoltativi. Reindirizza alla 443.
88	TCP, (UDP facoltativo)	Autenticazione Kerberos KDC cloud dai dispositivi mobili esterni.
443	TCP	Consente di accedere alla console di vRealize Automation e alle chiamate API. Accesso alle macchine per scaricare l'agente guest e l'agente di avvio automatico software. Accesso per il bilanciamento del carico, browser.
4369, 5671, 5672, 25672	TCP	Messaggistica RabbitMQ.
5480	TCP	Consente di accedere all'interfaccia di gestione dell'appliance virtuale.

**Tabella 1-12. Porte in ingresso (Continua)**

Porta	Protocollo	Commenti
		Utilizzata dall'agente di gestione.
5488, 5489	TCP	Utilizzata internamente dall'appliance vRealize Automation per gli aggiornamenti.
8230, 8280, 8281, 8283	TCP	Istanza di vRealize Orchestrator interna.
8443	TCP	Accesso per il browser. Porta dell'amministratore di Identity Manager su HTTPS.
8444	TCP	Comunicazione proxy della console per connessioni a VMware Remote Console di vSphere.
9300-9400	TCP	Accesso ai controlli di Identity Manager.
54328	UDP	

**Tabella 1-13. Porte in uscita**

Porta	Protocollo	Commenti
25, 587	TCP, UDP	SMTP per l'invio di notifiche via email in uscita.
53	TCP, UDP	Server 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.
88, 464, 135	TCP, UDP	Controller di dominio.
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.
389	TCP	Accesso al server delle connessioni View.
389, 636, 3268, 3269	TCP	Active Directory. Porte predefinite visualizzate, ma è possibile configurarle.
443	TCP	Comunicazione con il servizio di gestione dell'IaaS e gli host degli endpoint di infrastruttura su protocollo HTTPS.
		Comunicazione con il servizio software vRealize Automation su HTTPS.
		Accesso al server di aggiornamento di Identity Manager.
		Accesso al server delle connessioni View.
445	TCP	Accesso al repository ThinApp per Identity Manager.
902	TCP	Operazioni di copia dei file di rete ESXi e connessioni a VMware Remote Console.
5050	TCP	Facoltativi. Per la comunicazione con vRealize Business for Cloud.
5432	TCP, UDP	Facoltativi. Per la comunicazione con un altro database PostgreSQL dell'appliance.
5500	TCP	Sistema RSA SecurID. Porte predefinite visualizzate, ma è possibile configurarla.
8281	TCP	Facoltativi. Per la comunicazione con un'istanza di vRealize Orchestrator esterna.

**Tabella 1-13. Porte in uscita (Continua)**

Porta	Protocollo	Commenti
9300-9400	TCP	Accesso ai controlli di Identity Manager.
54328	UDP	

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.

## Server Windows IaaS

Tutti i server Windows che ospitano componenti IaaS devono rispettare requisiti specifici. Esaminare e verificare i requisiti prima di avviare l'installazione guidata di vRealize Automation o il programma d'installazione Windows standard.

- Includere tutti i server Windows IaaS nello stesso dominio. Non utilizzare workgroup.
- Ogni server richiede il seguente hardware minimo.
  - 2 CPU
  - 8 GB di memoria
  - 40 GB di spazio su disco

Un server che ospita il database SQL insieme ai componenti IaaS potrebbe richiedere hardware aggiuntivo.

- Per via della richiesta di risorse hardware, non distribuire su VMware Workstation.
- Installare Microsoft .NET Framework 3.5.
- Installare Microsoft .NET Framework 4.5.2 o versione successiva.

Una copia di .NET è disponibile in qualsiasi appliance vRealize Automation:

<https://vrealize-automation-appliance-fqdn:5480/installer/>

Se si utilizza Internet Explorer per il download, verificare che la configurazione di sicurezza avanzata sia disabilitata. Passare a <res://iesetup.dll/SoftAdmin.htm> nel server Windows.

- Installare Microsoft PowerShell 2.0, 3.0 o 4.0, in base alla versione di Windows in oggetto.
 

Si noti che alcuni aggiornamenti o migrazioni di vRealize Automation potrebbero richiedere una versione precedente o più recente di PowerShell, oltre a quella attualmente in esecuzione.
- Se si installa più di un componente IaaS sullo stesso server Windows, pianificarne l'installazione all'interno della stessa cartella. Non utilizzare percorsi diversi.
- I server IaaS utilizzano TLS per l'autenticazione, che è abilitata per impostazione predefinita su alcuni server Windows.

Alcuni siti disabilitano TLS per motivi di sicurezza, ma è necessario lasciare abilitato almeno un protocollo TLS. Questa versione di vRealize Automation supporta TLS 1.2.

- Attivare il servizio DTC (Distributed Transaction Coordinator). 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](#).

Attivare DTC anche sul server che ospita il database SQL, se questo è separato da IaaS. Per ulteriori informazioni sull'abilitazione di DTC, vedere [Articolo della Knowledge Base VMware 2038943](#).

- Verificare che il servizio Accesso secondario sia in esecuzione. Se desiderato, è possibile arrestare il servizio una volta completata l'installazione.

### Porte dei server IaaS Windows

È necessario configurare le porte dei server IaaS Windows prima dell'installazione di vRealize Automation.

Aprire le porte tra tutti i server IaaS Windows in base alle tabelle riportate di seguito. Includere il server che ospita il database SQL, se è separato da IaaS. In alternativa, se i criteri del sito lo consentono, è possibile disabilitare i firewall tra i server Windows di IaaS e SQL Server.

**Tabella 1-14. Porte in ingresso**

Porta	Protocollo	Componente	Commenti
443	TCP	Servizio di gestione	Comunicazione con i componenti di IaaS e con l'appliance vRealize Automation su protocollo HTTPS.
443	TCP	Appliance vRealize Automation	Comunicazione con i componenti di IaaS e con l'appliance vRealize Automation su protocollo HTTPS.
443	TCP	Host degli endpoint di infrastruttura	Comunicazione con i componenti di IaaS e con l'appliance vRealize Automation su protocollo HTTPS. In genere 443 è la porta di comunicazione predefinita per host di endpoint dell'infrastruttura virtuale e nel cloud; consultare tuttavia la documentazione fornita dai propri host di infrastruttura per conoscere l'elenco completo delle porte predefinite e necessarie
443	TCP	Agente guest agente di avvio automatico software	Comunicazione con il servizio di gestione su protocollo HTTPS.
443	TCP	DEM Worker	Comunicazione con NSX Manager
1433	TCP	Istanza di SQL Server	MSSQL.

**Tabella 1-15. Porte in uscita**

Porta	Protocollo	Componente	Commenti
53	TCP, UDP	Tutto	DNS.
67, 68, 546, 547	TCP, UDP	Tutto	DHCP



**Tabella 1-15. Porte in uscita (Continua)**

Porta	Protocollo	Componente	Commenti
123	TCP, UDP	Tutto	Facoltativi. NTP
443	TCP	Servizio di gestione	Comunicazione con l'appliance vRealize Automation su protocollo HTTPS.
443	TCP	Distributed Execution Manager	Comunicazione con il servizio di gestione su protocollo HTTPS.
443	TCP	Agenti proxy	Comunicazione con il servizio di gestione e gli host degli endpoint di infrastruttura su protocollo HTTPS
443	TCP	Agente di gestione	Comunicazione con l'appliance vRealize Automation
443	TCP	Agente guest agente di avvio automatico software	Comunicazione con il servizio di gestione su protocollo HTTPS.
1433	TCP	Servizio di gestione Sito Web	MSSQL.
5480	TCP	Tutto	Comunicazione con l'appliance vRealize Automation.

Inoltre, poiché si abilita DTC tra tutti i server, DTC richiede la porta 135 su TCP e una porta casuale tra 1024 e 65535. Si noti che Controllo prerequisiti verifica che DTC sia in esecuzione e che le porte necessarie siano aperte.

## Server Web IaaS

Un server Windows che ospita il componente Web deve soddisfare altri requisiti, oltre a quelli relativi a tutti i server IaaS Windows.

I requisiti sono gli stessi, indipendentemente dal fatto che il componente Web ospiti il servizio di gestione dei modelli.

- Configurare Java.
  - Installare l'aggiornamento 161 di Java 1.8 a 64 bit o versione successiva. Non utilizzare l'edizione a 32 bit.
  - JRE è sufficiente. Non è necessario JDK completo.
  - Impostare la variabile di ambiente JAVA\_HOME sulla cartella di installazione Java.
  - Verificare che %JAVA\_HOME%\bin\java.exe sia disponibile.
- Configurare Internet Information Services (IIS) in base alla seguente tabella.

È necessario IIS 7.5 per le varianti di Windows 2008, IIS 8 per Windows 2012, IIS 8.5 per Windows 2012 R2 e IIS 10 per Windows 2016.

Oltre alle impostazioni di configurazione, evitare l'hosting di siti Web aggiuntivi in IIS. vRealize Automation imposta il binding sulla sua porta di comunicazione a tutti gli indirizzi IP non assegnati, evitando ulteriori binding possibili. La porta di comunicazione predefinita di vRealize Automation è 443.

**Tabella 1-16. Internet Information Services host servizio di gestione IaaS**

Componente IIS	Impostazione
Ruoli di Internet Information Services (IIS)	<ul style="list-style-type: none"> <li>■ Autenticazione Windows</li> <li>■ Contenuto statico</li> <li>■ Documento predefinito</li> <li>■ ASP.NET 3.5 e ASP.NET 4.5</li> <li>■ Estensioni ISAPI</li> <li>■ Filtro ISAPI</li> </ul>
Ruoli del servizio Attivazione processo Windows di IIS	<ul style="list-style-type: none"> <li>■ API di configurazione</li> <li>■ Ambiente di rete</li> <li>■ Modello di processo</li> <li>■ Attivazione WCF (solo varianti di Windows 2008)</li> <li>■ Attivazione HTTP</li> <li>■ Attivazione non HTTP (solo varianti di Windows 2008)</li> </ul> <p>(Varianti di Windows 2012: passare a Funzionalità &gt; Funzionalità di .Net Framework 3.5 &gt; Attivazione non HTTP)</p>
Impostazioni di autenticazione IIS	<p>Configurare le seguenti impostazioni non predefinite.</p> <ul style="list-style-type: none"> <li>■ Autenticazione Windows attivata</li> <li>■ Autenticazione anonima disabilitata</li> </ul> <p>Non modificare le seguenti impostazioni predefinite.</p> <ul style="list-style-type: none"> <li>■ Provider negoziazione attivata</li> <li>■ Provider NTLM attivata</li> <li>■ Modalità kernel autenticazione Windows attivata</li> <li>■ Protezione estesa autenticazione Windows disattivata</li> <li>■ Per i certificati che utilizzano SHA512, è necessario disabilitare TLS1.2 sulle varianti di Windows 2012</li> </ul>

## Host del servizio di gestione di IaaS

Un server Windows che ospita il componente servizio di gestione deve soddisfare requisiti aggiuntivi rispetto a quelli richiesti per tutti i server Windows IaaS.

I requisiti sono gli stessi, indipendentemente dal fatto che l'host del servizio di gestione sia primario o di backup.

- Non possono esserci firewall tra un host del servizio di gestione e un host del DEM. Per informazioni sulla porta, vedere [Porte dei server IaaS Windows](#).

- L'host del servizio di gestione dev'essere in grado di risolvere il nome NETBIOS dell'host del database SQL Server. Se non può risolvere il nome NETBIOS, aggiungere il nome NETBIOS di SQL Server al file `/etc/hosts` sul computer del servizio di gestione.

## Host SQL Server di IaaS

Un server Windows che ospita il database SQL di IaaS deve soddisfare determinati requisiti.

SQL Server può risiedere in uno dei server IaaS Windows o in un host separato. Se ospitato insieme ai componenti di IaaS, questi requisiti si aggiungono a quelli che riguardano tutti i server IaaS Windows.

- Questa versione di vRealize Automation non supporta la modalità di compatibilità 130 di SQL Server 2016. Se si crea separatamente un database di SQL Server 2016 vuoto da utilizzare con IaaS, utilizzare la modalità di compatibilità 100 o 120.

Se si crea il database mediante un programma di installazione di vRealize Automation, la compatibilità è già configurata.

- AAG (AlwaysOn Availability Group) è supportato solo con SQL Server 2016 Enterprise. Quando si utilizza AAG, specificare il nome di dominio completo del listener AAG come host dell'istanza SQL Server.
- Se ospitato insieme ai componenti di IaaS, è necessario configurare Java.
  - Installare l'aggiornamento 161 di Java 1.8 a 64 bit o versione successiva. Non utilizzare l'edizione a 32 bit.  
JRE è sufficiente. Non è necessario JDK completo.
  - Impostare la variabile di ambiente `JAVA_HOME` sulla cartella di installazione Java.
  - Verificare che `%JAVA_HOME%\bin\java.exe` sia disponibile.
- Utilizzare una versione supportata di SQL Server da [Matrice di supporto di vRealize Automation](#).
- Abilitare il protocollo TCP/IP per SQL Server.
- SQL Server include un database modello per tutti i database creati nell'istanza SQL. Per garantire una corretta installazione di IaaS, non modificare le dimensioni del database modello.
- Generalmente il server necessita di caratteristiche hardware ulteriori rispetto alle caratteristiche minime descritte in [Server Windows IaaS](#).  
Per ulteriori informazioni, vedere [Specifiche hardware e massima capacità di vRealize Automation](#).
- Prima di eseguire il programma di installazione di vRealize Automation, è necessario identificare gli account e aggiungere autorizzazioni in SQL. Vedere [Account e password](#).

## Host Distributed Execution Manager di IaaS

Un server Windows che ospita il componente DEM (Distributed Execution Manager) Orchestrator o Worker deve soddisfare requisiti aggiuntivi rispetto a quelli richiesti per tutti i server Windows IaaS.

Non possono esserci firewall tra un host del DEM e l'host del servizio di gestione. Per informazioni sulla porta, vedere [Porte dei server IaaS Windows](#).

I DEM Worker possono avere requisiti aggiuntivi in base alle risorse di provisioning con cui interagiscono.

### **DEM Worker con Amazon Web Services**

Un DEM Worker IaaS di vRealize Automation che comunica con Amazon Web Services (AWS) deve soddisfare requisiti aggiuntivi rispetto a quelli richiesti per tutti i server Windows IaaS e i DEM in generale.

Un DEM Worker può comunicare con AWS per il provisioning. Il DEM Worker comunica con un account Amazon EC2 e raccoglie dati tramite esso.

- Il DEM Worker deve avere accesso a Internet.
- Se il DEM Worker si trova dietro un firewall, è necessario consentire il traffico dell'HTTPS a e da `aws.amazon.com` nonché gli URL per le regioni EC2 a cui i propri account AWS hanno accesso, come `ec2.us-east-1.amazonaws.com` per la regione Costa orientale degli Stati Uniti.

Ogni URL viene risolto in una gamma di indirizzi IP, pertanto per elencare e configurare questi indirizzi IP può essere necessario ricorrere a uno strumento, come ad esempio quello disponibile sul sito Web di Network Solutions.

- Se il DEM Worker accede a Internet attraverso un server proxy, il servizio DEM deve essere eseguito con credenziali in grado di autenticare il server proxy.

### **DEM Worker con Openstack o PowerVC**

Un DEM Worker vRealize Automation IaaS che comunica con Openstack o PowerVC per raccogliere dati deve soddisfare altri requisiti, oltre a quelli relativi a tutti i server IaaS Windows e ai DEM in generale.

**Tabella 1-17. Requisiti dei DEM Worker Openstack e PowerVC**

Installazione	Requisiti
Tutto	<p>Nel registro di Windows, abilitare il supporto TLS v1.2 per il framework .NET. Ad esempio:</p> <pre>[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319] "SchUseStrongCrypto"=dword:00000001</pre> <pre>[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319] "SchUseStrongCrypto"=dword:00000001</pre>
Host DEM Windows 2008	<p>Nel registro di Windows, abilitare il protocollo TLS v1.2. Ad esempio:</p> <pre>[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2] [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client] "DisabledByDefault"=dword:00000000 "Enabled"=dword:00000001</pre> <pre>[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server] "DisabledByDefault"=dword:00000000 "Enabled"=dword:00000001</pre>
Certificati autofirmati nell'host dell'endpoint dell'infrastruttura	<p>Se l'istanza di PowerVC o di Openstack non utilizza certificati attendibili, importare il certificato SSL dall'istanza di PowerVC o di Openstack nell'archivio delle autorità dei certificati con radice attendibile su ogni server Windows di IaaS in cui si intende installare un DEM di vRealize Automation.</p>

### DEM Worker con Red Hat Enterprise Virtualization

Un DEM Worker vRealize Automation IaaS che comunica con Red Hat Enterprise Virtualization (RHEV) per raccogliere dati deve soddisfare altri requisiti, oltre a quelli relativi a tutti i server Windows IaaS e ai DEM in generale.

- È necessario unire ciascun ambiente RHEV al dominio contenente il server DEM Worker.
- Le credenziali utilizzate per gestire l'endpoint che rappresenta un ambiente RHEV devono disporre di privilegi di amministratore per l'ambiente RHEV. Quando si utilizza RHEV per il provisioning, DEM Worker comunica con quell'account per raccogliere dati.
- Le credenziali devono inoltre disporre di privilegi sufficienti per creare oggetti sugli host contenuti all'interno dell'ambiente.

### DEM Worker con SCVMM

Un DEM Worker vRealize Automation IaaS che gestisce le macchine virtuali mediante SCVMM (System Center Virtual Machine Manager) deve soddisfare altri requisiti, oltre a quelli relativi a tutti i server Windows IaaS e ai DEM in generale.

- Installare il DEM Worker nella stessa macchina in cui si trova la console SCVMM.  
Una procedura consigliata consiste nell'installare una console SCVMM in un DEM Worker separato.
- Il DEM Worker deve avere accesso al modulo SCVMM PowerShell installato con la console.

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

Per verificare i criteri di esecuzione di PowerShell, inserire uno dei seguenti comandi al prompt dei comandi della PowerShell.

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

- Se tutti i DEM Worker di quella istanza non sono su macchine che soddisfano tali requisiti, utilizzare i comandi Skill per indirizzare i workflow in relazione con SCVMM ai DEM Worker che lo sono.

vRealize Automation non supporta un ambiente di distribuzione che utilizza una configurazione di cloud privati SCVMM. Al momento vRealize Automation non può raccogliere da, allocare a o eseguire il provisioning in base ai cloud privati SCVMM.

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

- vRealize Automation supporta SCVMM 2012 R2, che richiede PowerShell 3 o versione successiva.
- Installare la console di SCVMM prima di installare i DEM Worker vRealize Automation che utilizzano elementi di lavoro di SCVMM.

Se si installano i DEM Worker prima della console di SCVMM, verranno generati errori di registro simili all'esempio 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. Controllare l'ortografia del nome oppure, se era presente un percorso, verificare che sia corretto e riprovare.

Per correggere il 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.  
Le credenziali devono anche avere privilegi amministrativi sui server Hyper-V all'interno dell'istanza.
- Per eseguire il provisioning delle macchine in una risorsa SCVMM, l'utente di vRealize Automation che richiede l'elemento del catalogo deve disporre del ruolo di amministratore nell'istanza di SCVMM.
- 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 4.5.2 o successiva deve essere installata e Windows Management Instrumentation (WMI) deve essere abilitato.

- Per eseguire il provisioning di una macchina di seconda generazione su una risorsa SCVMM 2012 R2, è necessario aggiungere le proprietà seguenti nel blueprint.

```
Scvmm.Generation2 = true
Hyperv.Network.Type = synthetic
```

I blueprint di seconda generazione devono disporre di un virtualHardDisk (vHDX) con i dati raccolti esistente nella pagina di informazioni della build del blueprint. Se è vuoto, il provisioning di seconda generazione ha esito negativo.

Per ulteriori informazioni sulla preparazione per il provisioning delle macchine, vedere [Preparazione dell'ambiente SCVMM](#).

## Certificati

vRealize Automation utilizza certificati SSL per garantire la sicurezza delle comunicazioni tra componenti IaaS e istanze dell'appliance vRealize Automation. 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 dei certificati, vedere [Articolo della Knowledge Base VMware 2106583](#).

**Nota** vRealize Automation supporta certificati SHA2. I certificati autofirmati generati dal sistema utilizzano il protocollo SHA-256 con crittografia RSA. I requisiti di sistema operativo o browser possono richiedere l'aggiornamento a certificati SHA2.

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.

**Tabella 1-18. 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 di 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.

## La personalizzazione dell'URL di login di vRealize Automation comporta la modifica del certificato

Se si desidera che gli utenti accedano a un URL diverso da quello di un'appliance o di un servizio di bilanciamento del carico di vRealize Automation, consultare i passaggi relativi a CNAME precedenti e successivi all'installazione in [Impostazione dell'URL di login di vRealize Automation su un nome personalizzato](#).

## Requisiti dei certificati di vRealize Automation

Se si utilizzano i propri certificati con vRealize Automation, è necessario che i certificati soddisfino determinati requisiti.

## Tipi di certificati supportati

In molte organizzazioni, i certificati vengono emessi o richiesti da autorità esterne in base alle esigenze dell'azienda.

I seguenti requisiti riguardano i tipi di certificati e i formati di identità più comuni utilizzati nelle distribuzioni tipiche di vRealize Automation.

Proprietà del certificato	Requisiti
Algoritmo Hash	SHA1, SHA2, (256, 584, 512)
Algoritmo della firma	RSASSA-PKCS1_V1_5
Lunghezza della chiave	2084, 4096

**Nota** La firma RSASSA-PSS non è supportata nelle distribuzioni di vRealize Automation. Questa firma è quella predefinita per una CA di Microsoft in Windows 2012 R2. La firma è un parametro configurabile, quindi è necessario assicurarsi che sia impostata correttamente quando si utilizza una CA di Microsoft.

## Matrice di supporto del certificato di vRealize Automation



Algoritmo Hash	SHA1				SHA2-256			
Algoritmo della firma	RSASSA-PKCS1_V1_5		RSASSA-PSS		RSASSA-PKCS1_V1_5		RSASSA-PSS	
Dimensioni della chiave	2048	4096	2048	4096	2048	4096	2048	4096
vRealize Automation supportato	Supporto verificato	Supporto verificato	Non supportato	Non supportato	Supporto verificato	Supporto verificato	Non supportato	Non supportato

Algoritmo Hash	SHA2-384				SHA2-512			
Algoritmo della firma	RSASSA-PKCS1_V1_5		RSASSA-PSS		RSASSA-PKCS1_V1_5		RSASSA-PSS	
Dimensioni della chiave	2048	4096	2048	4096	2048	4096	2048	4096
vRealize Automation supportato	Supporto verificato	Supporto verificato	Non supportato	Non supportato	Supporto verificato	Supporto verificato	Non supportato	Non supportato

## 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.

**Tabella 1-19. 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</i> -nocerts -out key.pem</code>	<b>Chiave privata RSA</b>
File PEM	<code>openssl pkcs12 -in <i>path_to_.pfx</i> -clcerts -nokeys -out cert.pem</code>	<b>Catena di certificati</b>
(Facoltativa) Passphrase	n/a	<b>Passphrase</b>

## Distribuzione dell'appliance vRealize Automation

L'appliance vRealize Automation viene fornita come file di virtualizzazione aperto da distribuire in un'infrastruttura virtualizzata esistente.

## Informazioni sulla distribuzione dell'appliance vRealize Automation

Per tutte le installazioni è necessario che venga distribuita un'appliance vRealize Automation senza configurazione prima di procedere con una delle opzioni di installazione effettive di vRealize Automation.

- Installazione guidata consolidata basata sul Web
- Configurazione di un'appliance basata sul Web separata, seguita da installazioni di Windows separate per server IaaS
- Programma di installazione invisibile all'utente basato sulla riga di comando, che accetta input da un file di proprietà di risposta
- API REST di installazione che accetta input in formato JSON

## Distribuzione di vRealize Automation appliance

Prima che sia possibile accedere a uno dei percorsi di installazione, vRealize Automation richiede la distribuzione di almeno un'appliance vRealize Automation.

Per creare l'appliance, utilizzare il client vSphere per scaricare e distribuire una macchina virtuale parzialmente configurata da un modello. Potrebbe essere necessario eseguire la procedura più volte, se si prevede di creare una distribuzione enterprise per l'alta disponibilità e il failover. Una distribuzione di questo tipo include in genere più appliance vRealize Automation dietro un servizio di bilanciamento del carico.

### Prerequisiti

- Accedere al client vSphere con un account che disponga delle autorizzazioni per la distribuzione di modelli OVF nell'inventario.
- Scaricare il file .ovf o .ova dell'appliance vRealize Automation in una posizione accessibile per il client vSphere.

### Procedura

- 1 Selezionare l'opzione vSphere **Distribuisci modello OVF**.
- 2 Immettere il percorso del file .ovf o .ova dell'appliance vRealize Automation.
- 3 Esaminare i dettagli del modello.
- 4 Leggere e accettare l'accordo di licenza con l'utente finale.
- 5 Immettere un nome di appliance e una posizione di inventario.

Quando si distribuiscono le appliance, utilizzare un nome diverso per ciascuna di esse ed evitare di includere nei nomi caratteri non alfanumerici come il carattere di sottolineatura (\_).

- 6 Selezionare l'host e il cluster in cui si troverà l'appliance.
- 7 Selezionare il pool di risorse in cui si troverà l'appliance.
- 8 Selezionare lo storage che ospiterà l'appliance.

**9** Selezionare un formato di disco.

I formati thick migliorano le prestazioni, mentre i formati thin consentono di risparmiare spazio di storage.

Il formato non influisce sulle dimensioni del disco dell'appliance. Se un'appliance richiede maggiore spazio per i dati, aggiungere un disco utilizzando vSphere dopo la distribuzione.

**10** Selezionare una rete di destinazione dal menu a discesa.

**11** Completare le proprietà dell'appliance.

**a** Immettere e confermare una password root.

Le credenziali dell'account root consentono di accedere all'interfaccia di amministrazione basata sul browser ospitata dall'appliance o alla console della riga di comando del sistema operativo dell'appliance.

**b** Scegliere se consentire o meno le connessioni SSH remote alla console della riga di comando.

La disabilitazione di SSH garantisce una maggiore sicurezza ma richiede l'accesso alla console direttamente in vSphere anziché tramite un client terminale separato.

- c In **Nome host** immettere il nome di dominio completo dell'appliance.

Per ottenere risultati ottimali, immettere il nome dominio completo anche se si utilizza DHCP.

**Nota** vRealize Automation supporta DHCP, ma per le distribuzioni di produzione è consigliabile utilizzare indirizzi IP statici.

- d Quando vengono utilizzati indirizzi IP statici, nelle proprietà della rete immettere i valori di gateway, maschera di rete e server DNS. È inoltre necessario immettere indirizzo IP, nome di dominio completo e dominio per l'appliance stessa, come illustrato nell'esempio seguente.

**Figura 1-13. Proprietà di esempio dell'appliance virtuale**

▼ Application	3 settings
Enable SSH service in the appliance	<p>This will be used as an initial status of the SSH service in the appliance. You can change the status of the SSH service from the appliance Web console.</p> <input checked="" type="checkbox"/>
Hostname	<p>The host name for this virtual machine. Provide the fully qualified domain name if you use static IP. Leave blank to try to reverse look up the IP address if you use DHCP.</p> <input type="text" value="va1.mycompany.com"/>
Initial root password	<p>This will be used as an initial password for the root user account. You can change the password after installation using the passwd command or from the appliance Web console).</p> <p>Enter password <input type="password" value="*****"/></p> <p>Confirm password <input type="password" value="*****"/></p>
▼ Networking Properties	6 settings
Default Gateway	<p>The default gateway address for this VM. Leave blank if DHCP is desired.</p> <input type="text" value="12.34.56.79"/>
Domain Name	<p>The domain name of this VM. Leave blank if DHCP is desired.</p> <input type="text" value="mycompany.com"/>
Domain Name Servers	<p>The domain name server IP Addresses for this VM (comma separated). Leave blank if DHCP is desired.</p> <input type="text" value="12.34.56.80, 12.34.56.81"/>
Domain Search Path	<p>The domain search path (comma or space separated domain names) for this VM. Leave blank if DHCP is desired.</p> <input type="text" value="mycompany.com"/>
Network 1 IP Address	<p>The IP address for this interface. Leave blank if DHCP is desired.</p> <input type="text" value="12.34.56.78"/>
Network 1 Netmask	<p>The netmask or prefix for this interface. Leave blank if DHCP is desired.</p> <input type="text" value="255.255.254.0"/>

**12** A seconda della distribuzione, di vCenter Server e della configurazione del DNS, selezionare uno dei seguenti modi per terminare la distribuzione e accendere l'appliance.

- Se la distribuzione è avvenuta in vSphere e l'opzione **Accendi dopo la distribuzione** è disponibile nella pagina Completamento, procedere nel modo seguente.
  - a Selezionare **Accendi dopo la distribuzione** e fare clic su **Fine**.
  - b Al termine della distribuzione del file in vCenter Server, fare clic su **Chiudi**.
  - c Attendere l'avvio della macchina virtuale, un'operazione che può richiedere fino a 5 minuti.
- Se la distribuzione è avvenuta in vSphere e l'opzione **Accendi dopo la distribuzione** non è disponibile nella pagina Completamento, procedere nel modo seguente.
  - a Al termine della distribuzione del file in vCenter Server, fare clic su **Chiudi**.
  - b Accendere l'appliance vRealize Automation.
  - c Attendere l'avvio della macchina virtuale, un'operazione che può richiedere fino a 5 minuti.
  - d Verificare che l'appliance vRealize Automation venga distribuita eseguendo il ping del nome di dominio completo corrispondente. Se non è possibile eseguire il ping dell'appliance, riavviare la macchina virtuale.
  - e Attendere l'avvio della macchina virtuale, un'operazione che può richiedere fino a 5 minuti.
- Se l'appliance vRealize Automation è stata distribuita in vCloud utilizzando vCloud Director, vCloud potrebbe sovrascrivere la password immessa durante la distribuzione di OVA. Per impedire la sovrascrittura, procedere nel modo seguente.
  - a Dopo la distribuzione in vCloud Director, fare clic su vApp per visualizzare l'appliance vRealize Automation.
  - b Fare clic con il pulsante destro del mouse sull'appliance vRealize Automation e scegliere **Proprietà**.
  - c Fare clic sulla scheda **Personalizzazione sistema operativo guest**.
  - d In **Reimposta password**, deselezionare l'opzione **Consenti password amministratore locale** e fare clic su **OK**.
  - e Accendere l'appliance vRealize Automation.
  - f Attendere l'avvio della macchina virtuale, un'operazione che può richiedere fino a 5 minuti.

**13** Verificare che l'appliance vRealize Automation venga distribuita eseguendo il ping del nome di dominio completo corrispondente.

#### Operazioni successive

- (Facoltativo) Aggiungere schede NIC. Vedere [Aggiunta di controller NIC prima di eseguire il programma di installazione](#).
- Accedere all'interfaccia di amministrazione basata sul browser per eseguire l'installazione guidata consolidata o per configurare manualmente l'appliance.

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

- In alternativa, è possibile ignorare la registrazione in modo da sfruttare l'installazione di vRealize Automation invisibile all'utente o basata su API.

## Aggiunta di controller NIC prima di eseguire il programma di installazione

vRealize Automation supporta più controller NIC (Network Interface Controller). Prima di eseguire il programma di installazione, è possibile aggiungere controller NIC all'appliance vRealize Automation o al server Windows IaaS.

Se è necessario disporre di più NIC prima di eseguire l'installazione guidata di vRealize Automation, aggiungerli dopo la distribuzione in vCenter, ma prima di avviare la procedura guidata. Alcuni dei motivi per cui è opportuno avere NIC aggiuntivi in anticipo sono i seguenti:

- Si desidera che la rete degli utenti e la rete dell'infrastruttura siano separate.
- È necessario un ulteriore NIC in modo che i server IaaS possano essere aggiunti a un dominio di Active Directory.

Per ulteriori informazioni sugli scenari che prevedono la presenza di più NIC, vedere il [post del blog VMware Cloud Management](#).

Per tre o più NIC, tenere presenti le seguenti limitazioni.

- VIDM richiede l'accesso al database Postgres e ad Active Directory.
- In un cluster HA, VIDM deve poter accedere all'URL del servizio di bilanciamento del carico.
- Le connessioni VIDM precedenti devono passare attraverso i primi due NIC.
- I NIC che seguono il secondo NIC non devono essere utilizzati o riconosciuti da VIDM.
- I NIC che seguono il secondo NIC non devono essere utilizzati per la connessione ad Active Directory.

Quando si configura una directory in vRealize Automation, utilizzare il primo o il secondo NIC.

### Prerequisiti

Distribuire le macchine virtuali OVF e Windows dell'appliance vRealize Automation ma non eseguire il login né avviare l'installazione guidata.

### Procedura

- 1 In vCenter, aggiungere NIC a ogni appliance vRealize Automation.
  - a Fare clic con il pulsante destro del mouse sull'appliance appena distribuita e selezionare **Modifica impostazioni**.
  - b Aggiungere NIC VMXNETn.
  - c Se è accesa, riavviare l'appliance.
- 2 Accedere come root alla riga di comando dell'appliance vRealize Automation.

### 3 Configurare i NIC eseguendo il comando seguente per ogni NIC.

Assicurarsi di includere l'indirizzo del gateway predefinito. Dopo aver completato questa procedura, è possibile configurare route statiche.

```
/opt/vmware/share/vami/vami_set_network network-interface (STATICV4|
STATICV4+DHCPV6|STATICV4+AUTOV6) IPv4-address netmask gateway-v4-address
```

Ad esempio:

```
/opt/vmware/share/vami/vami_set_network eth1 STATICV4 192.168.100.20
255.255.255.0 192.168.100.1
```

- 4 Verificare che tutti i nodi di vRealize Automation possano risolversi a vicenda in base al nome DNS.
- 5 Verificare che tutti i nodi di vRealize Automation possano accedere a qualsiasi nome di dominio completo con carico bilanciato per i componenti di vRealize Automation.
- 6 Se si utilizza Split-Brain DNS, verificare che tutti i nodi e i VIP di vRealize Automation abbiano lo stesso nome di dominio completo in DNS per ogni IP e VIP dei nodi.
- 7 In vCenter, aggiungere i NIC ai server Windows IaaS.
  - a Fare clic con il pulsante destro del mouse sul server IaaS e selezionare **Modifica impostazioni**.
  - b Aggiungere i NIC alla macchina virtuale del server IaaS.
- 8 In Windows, configurare i NIC del server IaaS aggiunti e i relativi indirizzi IP. Se necessario, consultare la documentazione Microsoft.

#### Operazioni successive

- (Facoltativo) Se sono necessarie route statiche, seguire le linee guida in [Configurazione di route statiche](#) prima di continuare con l'installazione.
- Accedere all'interfaccia di amministrazione basata sul browser per eseguire l'installazione guidata consolidata o per configurare manualmente l'appliance.

```
https://vrealize-automation-appliance-FQDN:5480
```
- In alternativa, è possibile ignorare la registrazione in modo da sfruttare l'installazione di vRealize Automation invisibile all'utente o basata su API.

## Installazione di vRealize Automation utilizzando l'installazione guidata

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

Prima di avviare la procedura guidata, distribuire un'appliance vRealize Automation e configurare i server Windows IaaS in modo che soddisfino i prerequisiti. L'installazione guidata viene visualizzata la prima volta che si accede all'appliance vRealize Automation appena distribuita.

- Per arrestare la procedura guidata e riprenderla più tardi, fare clic su **Disconnetti**.

- Per disattivare la procedura guidata, fare clic su **Annulla** oppure disconnettersi e avviare l'installazione manuale tramite le interfacce standard.

La procedura guidata è lo strumento principale per le nuove installazioni di vRealize Automation. Se si desidera espandere una distribuzione esistente di vRealize Automation dopo aver eseguito la procedura guidata, vedere le procedure in [Le interfacce di installazione standard di vRealize Automation](#).

## Utilizzo dell'installazione guidata per le distribuzioni minime

Le distribuzioni minime dimostrano come funziona vRealize Automation ma in genere non hanno capacità sufficiente per supportare ambienti di produzione aziendali.

Installare una distribuzione minima per il lavoro di prototipazione o per acquisire familiarità con vRealize Automation.

### Avvio dell'installazione guidata per una distribuzione minima

Le distribuzioni minime in genere comprendono un'appliance vRealize Automation, un server Windows IaaS e l'agente vSphere per gli endpoint. L'installazione minima colloca tutti i componenti IaaS su un solo server Windows.

#### Prerequisiti

- Soddisfare i prerequisiti in [Preparazione per l'installazione di vRealize Automation](#).
- Creare un'appliance non configurata. Vedere [Distribuzione di vRealize Automation appliance](#).

#### Procedura

- 1 Accedere come utente root all'interfaccia di gestione dell'appliance vRealize Automation.  
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Quando compare l'installazione guidata, fare clic su **Avanti**.
- 3 Accettare il contratto di licenza e fare clic su **Avanti**.
- 4 Nella pagina Tipo di distribuzione, selezionare **Distribuzione minima e Installa infrastruttura come servizio**, quindi fare clic su **Avanti**.
- 5 Nella pagina Prerequisiti d'installazione, interrompere la procedura per eseguire l'accesso al server Windows IaaS e installare l'agente di gestione. L'agente di gestione consente all'appliance vRealize Automation di individuare il server IaaS e di connettersi ad esso.

#### Operazioni successive

Installare l'agente di gestione sul server IaaS Windows. Vedere [Installazione dell'agente di gestione di vRealize Automation](#).

### Installazione dell'agente di gestione di vRealize Automation

Tutti i server Windows IaaS richiedono l'installazione dell'agente di gestione, che li collega alla propria appliance vRealize Automation specifica.



Se il database SQL Server di vRealize Automation è ospitato in una macchina Windows separata che non ospita componenti IaaS, la macchina SQL Server non necessita dell'agente di gestione.

L'agente di gestione registra il server Windows IaaS nell'appliance vRealize Automationspecifica, 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 Windows in un account di dominio con diritti di amministratore nei server Windows IaaS.

## Prerequisiti

Creare un'appliance vRealize Automation e avviare l'installazione guidata.

Vedere [Distribuzione di vRealize Automation appliance](#) e [Avvio dell'installazione guidata per una distribuzione minima](#).

## Procedura

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

```
openssl x509 -in /opt/vmware/etc/lighttpd/server.pem -fingerprint -noout -sha1
```
- 3 Copiare l'impronta digitale per poterla verificare successivamente. Ad esempio:  

```
71:84:47:72:03:57:C8:C2:68:65:00:06:BC:D8:23:98:92:54:BF:89
```
- 4 Accedere al server Windows IaaS utilizzando un account che disponga di diritti di amministratore.
- 5 Aprire un browser Web nell'URL del programma di installazione dell'appliance vRealize Automation.  

```
https://vrealize-automation-appliance-FQDN:5480/installer
```
- 6 Fare clic sul **programma di installazione dell'agente di gestione** e salvare ed eseguire il file .msi.
- 7 Leggere la pagina di benvenuto.
- 8 Accettare il contratto di licenza con l'utente finale.
- 9 Accettare o modificare la cartella di installazione.  

```
Program Files (x86)\VMware\VCAC\Management Agent
```

**10** Immettere i dettagli dell'appliance vRealize Automation:

- a Immettere l'indirizzo HTTPS dell'appliance, includendo il nome di dominio completo e il numero di porta :5480.
- b Immettere le credenziali dell'account root dell'appliance.
- c Fare clic su **Carica** e verificare che l'impronta digitale corrisponda a quella copiata in precedenza. Ignorare i due punti.

Se le impronte digitali non corrispondono, verificare che l'indirizzo dell'appliance sia corretto.

**Figura 1-14. Agente di gestione - Dettagli dell'appliance vRealize Automation**

**11** Immettere il nome utente e la password di dominio per l'account del servizio.

Quest'ultimo deve essere un account di dominio con diritti di amministratore nei server Windows IaaS. Utilizzare sempre lo stesso account del servizio.

**12** Seguire i prompt visualizzati per completare l'installazione dell'agente di gestione.

**Nota** Poiché sono collegati, è necessario reinstallare l'agente di gestione se si sostituisce l'appliance vRealize Automation.

La disinstallazione di IaaS da un server Windows non comporta la rimozione dell'agente di gestione. Per disinstallare un agente di gestione, utilizzare separatamente l'opzione Installazione applicazioni in Windows.

### Operazioni successive

Tornare all'installazione guidata basata sul browser. I server Windows IaaS con l'agente di gestione installato verranno visualizzati nella sezione degli host rilevati.

### Completamento dell'installazione guidata

Dopo aver installato l'agente di gestione, tornare alla procedura guidata e seguire le richieste visualizzate. Se occorrono istruzioni aggiuntive sulle impostazioni, fare clic sul collegamento della Guida in alto a destra nella procedura guidata.

- Terminata la procedura guidata, l'ultima pagina visualizza il percorso e il nome di un file di proprietà. È possibile modificare il file e utilizzarlo per eseguire un'installazione di vRealize Automation invisibile all'utente con impostazioni identiche o simili a quelle utilizzate nella sessione di installazione guidata. Vedere [Installazione di vRealize Automation invisibile all'utente](#).
- Se è stato creato il contenuto iniziale, è possibile accedere al tenant predefinito come utente configurationadmin e richiedere gli elementi di catalogo. Per un esempio di come richiedere l'elemento e completare l'azione utente manuale, vedere [Scenario: Richiesta contenuto iniziale per una distribuzione modello di verifica Rainpole](#).
- Per configurare l'accesso al tenant predefinito per altri utenti, vedere [Configurazione dell'accesso per il tenant predefinito](#).

## Utilizzo dell'installazione guidata per le distribuzioni enterprise

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 dei componenti di IaaS è facoltativa in entrambi i tipi di distribuzione.

Per le distribuzioni con bilanciamento del carico, la presenza di più istanze server Web e appliance vRealize Automation attive determina l'esito negativo dell'installazione. Durante l'installazione, devono essere presenti una sola istanza Web e una sola appliance vRealize Automation attive.

### Avvio dell'installazione guidata per una distribuzione enterprise

Le distribuzioni enterprise sono sufficientemente grandi da accogliere 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 distribuisce un'installazione distribuita con bilanciamenti del carico, 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.

#### Prerequisiti

- Verificare i prerequisiti in [Preparazione per l'installazione di vRealize Automation](#).
- Creare un'appliance non configurata. Vedere [Distribuzione di vRealize Automation appliance](#).

#### Procedura

- 1 Accedere come utente root all'interfaccia di gestione dell'appliance vRealize Automation.  
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Quando compare l'installazione guidata, fare clic su **Avanti**.
- 3 Accettare l'accordo di licenza con l'utente finale e fare clic su **Avanti**.

- 4 Nella pagina Tipo di distribuzione, selezionare **Distribuzione enterprise e Installa infrastruttura come servizio**.
- 5 Nella pagina Prerequisiti d'installazione, interrompere la procedura per eseguire l'accesso ai server Windows IaaS e installare l'agente di gestione. L'agente di gestione consente all'appliance vRealize Automation di individuare i server IaaS e di connettersi agli stessi.

#### Operazioni successive

Installare l'Agente di gestione sui server Windows di IaaS. Vedere [Installazione dell'agente di gestione di vRealize Automation](#).

#### Installazione dell'agente di gestione di vRealize Automation

Tutti i server Windows IaaS richiedono l'installazione dell'agente di gestione, che li collega alla propria appliance vRealize Automation specifica.

Se il database SQL Server di vRealize Automation è ospitato in una macchina Windows separata che non ospita componenti IaaS, la macchina SQL Server non necessita dell'agente di gestione.

L'agente di gestione registra il server Windows IaaS nell'appliance vRealize Automationspecifica, 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 Windows in un account di dominio con diritti di amministratore nei server Windows IaaS.

#### Prerequisiti

Creare un'appliance vRealize Automation e avviare l'installazione guidata.

Vedere [Distribuzione di vRealize Automation appliance](#) e [Avvio dell'installazione guidata per una distribuzione enterprise](#).

#### Procedura

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

```
openssl x509 -in /opt/vmware/etc/lighttpd/server.pem -fingerprint -noout -sha1
```
- 3 Copiare l'impronta digitale per poterla verificare successivamente. Ad esempio:  

```
71:84:47:72:03:57:C8:C2:68:65:00:06:BC:D8:23:98:92:54:BF:89
```
- 4 Accedere al server Windows IaaS utilizzando un account che disponga di diritti di amministratore.
- 5 Aprire un browser Web nell'URL del programma di installazione dell'appliance vRealize Automation.  

```
https://vrealize-automation-appliance-FQDN:5480/installer
```
- 6 Fare clic sul **programma di installazione dell'agente di gestione** e salvare ed eseguire il file .msi.
- 7 Leggere la pagina di benvenuto.
- 8 Accettare il contratto di licenza con l'utente finale.

**9** Accettare o modificare la cartella di installazione.

Program Files (x86)\VMware\VCAC\Management Agent

**10** Immettere i dettagli dell'appliance vRealize Automation:

- a Immettere l'indirizzo HTTPS dell'appliance, includendo il nome di dominio completo e il numero di porta :5480.
- b Immettere le credenziali dell'account root dell'appliance.
- c Fare clic su **Carica** e verificare che l'impronta digitale corrisponda a quella copiata in precedenza. Ignorare i due punti.

Se le impronte digitali non corrispondono, verificare che l'indirizzo dell'appliance sia corretto.

**Figura 1-15. Agente di gestione - Dettagli dell'appliance vRealize Automation**

**11** Immettere il nome utente e la password di dominio per l'account del servizio.

Quest'ultimo deve essere un account di dominio con diritti di amministratore nei server Windows IaaS. Utilizzare sempre lo stesso account del servizio.

**12** Seguire i prompt visualizzati per completare l'installazione dell'agente di gestione.

Ripetere la procedura per tutti i server Windows che ospiteranno i componenti IaaS.

**Nota** Poiché sono collegati, è necessario reinstallare l'agente di gestione se si sostituisce l'appliance vRealize Automation.

La disinstallazione di IaaS da un server Windows non comporta la rimozione dell'agente di gestione. Per disinstallare un agente di gestione, utilizzare separatamente l'opzione Installazione applicazioni in Windows.

### Operazioni successive

Tornare all'installazione guidata basata sul browser. I server Windows IaaS con l'agente di gestione installato verranno visualizzati nella sezione degli host rilevati.

## Completamento dell'installazione guidata

Dopo aver installato l'agente di gestione, tornare alla procedura guidata e seguire le richieste visualizzate. Se occorrono istruzioni aggiuntive sulle impostazioni, fare clic sul collegamento della Guida in alto a destra nella procedura guidata.

- Terminata la procedura guidata, l'ultima pagina visualizza il percorso e il nome di un file di proprietà. È possibile modificare il file e utilizzarlo per eseguire un'installazione di vRealize Automation invisibile all'utente con impostazioni identiche o simili a quelle utilizzate nella sessione di installazione guidata. Vedere [Installazione di vRealize Automation invisibile all'utente](#).
- Se è stato creato il contenuto iniziale, è possibile accedere al tenant predefinito come utente configurationadmin e richiedere gli elementi di catalogo. Per un esempio di come richiedere l'elemento e completare l'azione utente manuale, vedere [Scenario: Richiesta contenuto iniziale per una distribuzione modello di verifica Rainpole](#).
- Per configurare l'accesso al tenant predefinito per altri utenti, vedere [Configurazione dell'accesso per il tenant predefinito](#).

## Procedura di installazione guidata di vRealize Automation

L'installazione guidata di vRealize Automation offre all'utente pagine intuitive dove è possibile verificare i prerequisiti, immettere impostazioni, convalidare impostazioni e installare componenti di vRealize Automation.

---

**Nota** La procedura guidata include dei passaggi in cui questa viene interrotta per accedere ad altri sistemi, ad esempio i bilanciamenti del carico o i server Windows IaaS.

---

### Prerequisiti

- Creare una o più appliance non configurate. Vedere [Distribuzione di vRealize Automation appliance](#).  
Le distribuzioni minime utilizzano una sola appliance vRealize Automation. Le distribuzioni enterprise possono avere più appliance dietro un bilanciamento del carico.
- Tenere a disposizione uno o più sistemi Windows su cui ospitare i componenti IaaS.
- Avviare la procedura guidata accedendo come root all'interfaccia di amministrazione dell'appliance vRealize Automation.

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

### Procedura

#### 1 Tipo di distribuzione

Nella pagina del tipo di distribuzione, è possibile decidere quali e quanti componenti di vRealize Automation si desidera installare.

#### 2 Prerequisiti di installazione

Nella pagina dei prerequisiti di installazione, la procedura viene interrotta per stabilire una connessione alle macchine Windows che ospiteranno l'IaaS di vRealize Automation. È possibile selezionare inoltre un'origine di sincronizzazione dell'ora.

### 3 [Appliance vRealize](#)

(Solo distribuzioni enterprise) Nella pagina delle appliance vRealize, si ha la possibilità di creare una distribuzione ad alta disponibilità con più appliance vRealize Automation.

### 4 [Ruoli server](#)

(Solo distribuzioni enterprise) Nella pagina Ruoli server, assegnare i ruoli del componente IaaS di vRealize Automation alle macchine Windows in cui è stato precedentemente installato l'agente di gestione.

### 5 [Controllo prerequisiti](#)

Nella pagina Controllo prerequisiti, controllare e correggere i server Windows di vRealize Automation per supportare l'installazione di IaaS.

### 6 [Host vRealize Automation](#)

Nella pagina dell'host di vRealize Automation, viene impostato l'indirizzo URL di base per vRealize Automation. L'indirizzo è di solito l'appliance vRealize Automation o, in distribuzioni ad alta disponibilità, un bilanciamento del carico.

### 7 [Single Sign-On](#)

Nella pagina di Single Sign-On, viene impostato l'accesso dell'amministratore di sistema del tenant predefinito di vRealize Automation sotto forma di credenziali.

### 8 [Host IaaS](#)

Nella pagina Host di IaaS, impostare gli indirizzi URL di base per determinati componenti di IaaS. Viene inoltre creata una passphrase di sicurezza per il database SQL IaaS di vRealize Automation.

### 9 [Microsoft SQL Server](#)

Nella pagina di Microsoft SQL Server, è possibile configurare il database SQL dell'IaaS di vRealize Automation. Il database dell'IaaS registra le macchine con provisioning effettuato, gli elementi associati e i criteri.

### 10 [Ruolo Web](#)

(Solo distribuzioni enterprise) Nella pagina del ruolo Web, è possibile configurare separatamente il sito Web dell'IaaS di vRealize Automation in IIS.

### 11 [Ruolo del servizio di gestione](#)

(Solo distribuzioni enterprise) Nella pagina del ruolo del servizio di gestione, è possibile configurare la macchina Windows vRealize Automation separata che ospita il servizio di gestione IaaS.

### 12 [Distributed Execution Manager](#)

Nella pagina dei Distributed Execution Manager, è possibile configurare le macchine Windows vRealize Automation che ospitano i DEM IaaS. Vengono supportati più host DEM.

### 13 [Agenti](#)

Nella pagina degli agenti, è possibile creare il collegamento tra l'IaaS di vRealize Automation e le risorse di virtualizzazione sulle quali è distribuita l'infrastruttura. Si seleziona un tipo di agente e si completano i dettagli dell'endpoint corrispondente.

#### 14 [Certificato di vRealize Appliance](#)

Nella pagina del certificato di vRealize Appliance, è possibile creare o selezionare il certificato di autenticazione utilizzato dall'appliance vRealize Automation. Quando il certificato viene autofirmato, gli utenti finali lo vedono e lo confermano accedendo a vRealize Automation in un browser.

#### 15 [Certificato Web](#)

Nella pagina del certificato Web, è possibile creare o selezionare il certificato di autenticazione utilizzato dal server Web IaaS. L'appliance vRealize Automation si connette al server Web e ha bisogno di autenticarlo e considerarlo attendibile.

#### 16 [Certificato del servizio di gestione](#)

(Solo distribuzioni enterprise) Nella pagina del certificato del servizio di gestione, è possibile creare o selezionare il certificato di autenticazione che utilizza l'host del servizio di gestione IaaS di vRealize Automation. Gli altri server Windows IaaS si connettono all'host del servizio di gestione e hanno bisogno di autenticarlo e considerarlo attendibile.

#### 17 [Bilanciamento del carico](#)

(Solo distribuzioni enterprise) Nella pagina Bilanciamenti del carico, è possibile attivare una pausa per configurare i bilanciamenti del carico per il pool di sistemi membro di vRealize Automation corretto.

#### 18 [Convalida](#)

Nella pagina Convalida, verificare che l'installazione di vRealize Automation possa procedere.

#### 19 [Creazione di snapshot](#)

Nella pagina di creazione degli snapshot, la procedura viene interrotta per poter acquisire snapshot delle macchine virtuali di tutti i componenti di vRealize Automation prima di procedere con l'installazione.

#### 20 [Dettagli di installazione](#)

Nella pagina dei dettagli di installazione, è possibile avviare l'installazione di vRealize Automation o riprovarla nel caso in cui si siano verificati problemi.

#### 21 [Gestione licenze](#)

Nella pagina di gestione delle licenze, immettere una chiave per attivare il prodotto vRealize Automation installato.

#### 22 [Telemetria](#)

Nella pagina della telemetria, è possibile decidere se vRealize Automation invia statistiche sull'utilizzo a VMware come parte del programma CEIP (Customer Experience Improvement Program).

#### 23 [Opzioni di post-installazione](#)

Nella pagina delle opzioni di post-installazione, sono disponibili delle opzioni per creare nuovi dati di vRealize Automation oppure effettuare la migrazione di dati di distribuzioni precedenti a una nuova installazione.



## 24 Configurazione del contenuto iniziale

Nella pagina di configurazione del contenuto iniziale, è possibile creare un nuovo utente del tenant predefinito locale di vRealize Automation, in grado di iniziare un workflow di contenuti per un endpoint vSphere.

## 25 Configurazione della migrazione

Nella pagina di configurazione della migrazione, è possibile avviare il trasferimento di un'altra distribuzione di vRealize Automation, precedente a quella appena installata.

### Tipo di distribuzione

Nella pagina del tipo di distribuzione, è possibile decidere quali e quanti componenti di vRealize Automation si desidera installare.

#### Minima

Le distribuzioni minime utilizzano solo un'appliance vRealize Automation e un server Windows che ospita i componenti IaaS. Nelle distribuzioni minime, è possibile ospitare il database IaaS in un sistema SQL Server separato oppure installare SQL nel server Windows IaaS.

Non è possibile convertire una distribuzione minima in una distribuzione enterprise. Per ampliare una distribuzione, iniziare con una distribuzione enterprise di piccole dimensioni e aggiungervi componenti. Non è possibile iniziare con una distribuzione minima.

#### Enterprise

Le distribuzioni enterprise implicano più appliance separate e host Windows, in genere con bilanciamento del carico. Le distribuzioni enterprise consentono inoltre di ospitare il database IaaS in un sistema SQL Server separato o in uno dei server Windows IaaS.

Quando si seleziona una distribuzione enterprise, vengono visualizzate ulteriori pagine dell'installazione guidata nell'elenco di riepilogo a sinistra della procedura guidata.

#### Infrastructure as a Service (IaaS)

L'opzione Infrastructure as a Service (IaaS) determina se configurare le macchine Windows esistenti con le funzionalità di modellazione e provisioning di vRealize Automation.

Quando si seleziona IaaS, vengono visualizzate ulteriori pagine dell'installazione guidata nell'elenco di riepilogo a sinistra della procedura guidata.

#### Prerequisiti di installazione

Nella pagina dei prerequisiti di installazione, la procedura viene interrotta per stabilire una connessione alle macchine Windows che ospiteranno l'IaaS di vRealize Automation. È possibile selezionare inoltre un'origine di sincronizzazione dell'ora.

#### Server Windows IaaS

Per utilizzare una macchina Windows come host di un componente IaaS, è necessario scaricare e installare vCAC-IaaSManagementAgent-Setup.msi nella macchina Windows.

L'installazione dell'agente di gestione richiede la comunicazione con un'appliance vRealize Automation in esecuzione. Ogni volta che si installa l'agente di gestione su Windows, il sistema si lega in modo univoco all'appliance e alla distribuzione specifiche.

I potenziali server Windows IaaS che hanno installato l'agente di gestione corretto vengono visualizzati in **Host scoperti**.

Per fare in modo che l'host scoperto ignori l'installazione guidata, fare clic su **Elimina**. Eliminando un host Windows non si rimuove l'agente di gestione. Per disinstallare l'agente, utilizzare direttamente la funzionalità Installazione applicazioni di Windows.

### Origine di riferimento dell'ora

È necessario sincronizzare ogni appliance vRealize Automation e server Windows IaaS con la stessa origine di riferimento dell'ora. Sono consentite le seguenti origini:

- Utilizzo dell'ora dell'host: viene effettuata la sincronizzazione con l'host ESXi dell'appliance vRealize Automation.
- Utilizzo del server di riferimento dell'ora: viene effettuata la sincronizzazione con un server Network Time Protocol (NTP) esterno. Immettere il nome di dominio completo o l'indirizzo IP del server NTP.

Non combinare origini di riferimento dell'ora all'interno di una distribuzione vRealize Automation.

### Appliance vRealize

(Solo distribuzioni enterprise) Nella pagina delle appliance vRealize, si ha la possibilità di creare una distribuzione ad alta disponibilità con più appliance vRealize Automation.

Più appliance devono trovarsi dietro un servizio di bilanciamento del carico installato separatamente. In una pagina successiva della procedura guidata è possibile verificare e completare la configurazione delle appliance e del servizio di bilanciamento del carico. Per ciascuna appliance vRealize Automation aggiunta, immetterne il nome di dominio completo e le credenziali root.

### Ruoli server

(Solo distribuzioni enterprise) Nella pagina Ruoli server, assegnare i ruoli del componente IaaS di vRealize Automation alle macchine Windows in cui è stato precedentemente installato l'agente di gestione.

Le macchine Windows di IaaS possono operare come server Web primari e aggiuntivi, host del servizio di gestione, host DEM e host dell'agente. Per informazioni sui ruoli del componente IaaS, vedere [Infrastructure as a Service \(IaaS\)](#).

La separazione dei ruoli server di IaaS è possibile solo nelle distribuzioni enterprise. Nelle distribuzioni minime, un'unica macchina Windows esegue tutti i ruoli.

### Controllo prerequisiti

Nella pagina Controllo prerequisiti, controllare e correggere i server Windows di vRealize Automation per supportare l'installazione di IaaS.

Il controllo prerequisiti ispeziona le macchine Windows su cui è stato installato l'agente di gestione e che ospiteranno componenti IaaS. I prerequisiti includono Java, impostazioni di Internet Information Services (IIS), il servizio Microsoft Distributed Transaction Coordinator (DTC) e altri aspetti. Per l'elenco dettagliato dei prerequisiti, fare clic su **Mostra dettagli**.

L'installazione guidata permette di procedere senza controllare i prerequisiti, ma l'installazione potrebbe non riuscire.

- Per controllare i prerequisiti, fare clic su **Esegui**.
- Se viene rilevata l'assenza di prerequisiti, fare clic su **Mostra dettagli** per saperne di più, quindi fare clic su **Risolvi**.

L'installazione guidata può risolvere la maggior parte dei prerequisiti basati su software o impostazioni. Dopo aver apportato le modifiche, l'installazione guidata riavvia gli host di IaaS.

La procedura guidata non è in grado di correggere i problemi di memoria insufficiente o CPU. È necessario correggere questi problemi in vSphere o nell'hardware, se si verificano.

## Host vRealize Automation

Nella pagina dell'host di vRealize Automation, viene impostato l'indirizzo URL di base per vRealize Automation. L'indirizzo è di solito l'appliance vRealize Automation o, in distribuzioni ad alta disponibilità, un bilanciamento del carico.

- Quando si distribuisce un'appliance vRealize Automation senza bilanciamento del carico, immettere il nome di dominio completo dell'appliance vRealize Automation. È possibile fare clic per consentire all'installazione guidata di popolare il nome di dominio completo per conto dell'utente.
- Quando si distribuisce una configurazione enterprise che include una o più appliance vRealize Automation dietro un bilanciamento del carico, immettere invece il nome di dominio completo di quest'ultimo.

Una singola appliance vRealize Automation può ancora essere distribuita dietro un bilanciamento del carico. Questo approccio consente più facilmente all'utente di aggiungere appliance in un secondo momento, in modo da espandere la distribuzione.

## Single Sign-On

Nella pagina di Single Sign-On, viene impostato l'accesso dell'amministratore di sistema del tenant predefinito di vRealize Automation sotto forma di credenziali.

L'amministratore di sistema del tenant predefinito dispone del maggior numero di autorizzazioni rispetto a qualsiasi altro utente, compresa quella relativa alla creazione di ulteriori tenant. Le credenziali dell'amministratore di sistema del tenant predefinito sono separate dalle credenziali root dell'appliance vRealize Automation.

## Host IaaS

Nella pagina Host di IaaS, impostare gli indirizzi URL di base per determinati componenti di IaaS. Viene inoltre creata una passphrase di sicurezza per il database SQL IaaS di vRealize Automation.

## Distribuzioni minime

Impostazione	Descrizione
Indirizzo Web di IaaS	Immettere il nome di dominio completo del server Windows di IaaS.
Installa componenti di IaaS in	Selezionare o specificare il nome di dominio completo del server Windows di IaaS.
Username	Immettere l'account del servizio nel formato DOMINIO\nomeutente. L'account deve essere un account di dominio con privilegi di amministratore locale sul server Windows di IaaS.
Password	Immettere la password dell'account.
Passphrase di sicurezza	<p>Creare una passphrase per la crittografia dei dati nel database SQL di IaaS.</p> <ul style="list-style-type: none"> <li>Conservare la passphrase con cura poiché sarà necessaria per ripristinare il database in caso di errore e per aggiungere componenti dopo l'installazione iniziale.</li> <li>La passphrase non può contenere il carattere virgolette doppie ( " ).</li> </ul>
Conferma passphrase	Reimmettere la passphrase.

## Distribuzioni enterprise

Impostazione	Descrizione
Indirizzo Web di IaaS	Immettere il nome di dominio completo del server Web di IaaS primario. Se invece si distribuisce una configurazione enterprise che include server Web di IaaS multipli con bilanciamento del carico, specificare il nome di dominio completo del bilanciamento del carico.
Indirizzo del servizio di gestione	Immettere il nome di dominio completo dell'host del servizio di gestione primario. Se invece si distribuisce una configurazione enterprise che include host del servizio di gestione multipli con bilanciamento del carico, specificare il nome di dominio completo del bilanciamento del carico.
Passphrase di sicurezza	<p>Creare una passphrase per la crittografia dei dati nel database SQL di IaaS.</p> <ul style="list-style-type: none"> <li>Conservare la passphrase con cura poiché sarà necessaria per ripristinare il database in caso di errore e per aggiungere componenti dopo l'installazione iniziale.</li> <li>La passphrase non può contenere il carattere virgolette doppie ( " ).</li> </ul>
Conferma passphrase	Reimmettere la passphrase.

## Microsoft SQL Server

Nella pagina di Microsoft SQL Server, è possibile configurare il database SQL dell'IaaS di vRealize Automation. Il database dell'IaaS registra le macchine con provisioning effettuato, gli elementi associati e i criteri.

Impostazione	Descrizione
Nome server	<p>Immettere il nome di dominio completo dell'host di SQL Server, che potrebbe essere un server Windows IaaS o un server separato.</p> <p>Se è necessario specificare un numero di porta o un'istanza denominata, utilizzare il formato FQDN,Port\Instance.</p> <p>Quando si utilizza AAG (AlwaysOn Availability Group) SQL, specificare il nome di dominio completo del listener AAG.</p>
Nome database	Accettare il valore predefinito, <b>vra</b> , oppure immettere un altro nome per il database IaaS.
Crea nuovo database	<p>Consente all'installazione guidata di creare il database.</p> <p>Per fare in modo che questa opzione funzioni, l'account che esegue l'agente di gestione nel server Web IaaS primario deve disporre del ruolo sysadmin in SQL.</p>
Utilizza database vuoto esistente	<p>Non consente all'installazione guidata di creare il database.</p> <p>Quando si crea il database separatamente, le credenziali dell'utente Windows o SQL fornite hanno bisogno dell'autorizzazione dbo nel database.</p>
Impostazioni predefinite	<p>(Solo nuovo database) Deselezionare questa opzione se si desidera utilizzare una posizione di storage alternativa per i dati e i file di registro dell'IaaS.</p> <p>Una volta deselezionata, immettere le directory per i dati (MDF) e i registri. L'account del servizio SQL Server deve disporre dell'autorizzazione di scrittura nelle directory.</p>
Usa SSL per la connessione al database	Codificare le connessioni al database. Per utilizzare questa opzione, è necessario configurare separatamente l'host di SQL Server per SSL. Inoltre, il server Web e l'host del servizio di gestione IaaS devono considerare attendibile il certificato SSL dall'host di SQL Server.
Autenticazione Windows	<p>Deselezionare questa opzione solo se si desidera utilizzare l'autenticazione SQL anziché Windows.</p> <p>Una volta deselezionata, immettere le credenziali di autenticazione SQL.</p>
Percorso di installazione	<p>Lasciare deselezionata questa opzione per accettare il percorso predefinito, %ProgramFiles(x86)%\VMware, oppure immettere una posizione alternativa.</p> <ul style="list-style-type: none"> <li>■ I file di vRealize Automation non sono installati nell'host di SQL Server. Si trovano nel server Web dell'IaaS primario.</li> <li>■ Se si installano più componenti IaaS nella stessa macchina Windows, installarli tutti nello stesso percorso d'installazione.</li> </ul>

## Ruolo Web

(Solo distribuzioni enterprise) Nella pagina del ruolo Web, è possibile configurare separatamente il sito Web dell'IaaS di vRealize Automation in IIS.

In una distribuzione enterprise, è possibile specificare separatamente la macchina Windows IaaS che ospita il componente Web. Per l'alta disponibilità, sono supportati più host.

Impostazione		Descrizione
Nome del sito Web		Personalizzare il nome o lasciare quello del sito Web predefinito IIS.  Evitare di ospitare ulteriori siti Web in IIS. vRealize Automation imposta il binding sulla sua porta di comunicazione a tutti gli indirizzi IP non assegnati, evitando ulteriori binding possibili.
Porta		Personalizzare la porta o accettare il valore predefinito 443.
Server Web IaaS	Nome host IaaS	Immettere il nome di dominio completo di ciascuna macchina Windows IaaS che ospita il componente Web IaaS.
	Username	Immettere l'account del servizio nel formato DOMINIO\nomeutente. L'account deve essere un account di dominio con privilegi di amministratore locale sul server Windows di IaaS.
	Password	Immettere la password dell'account.
	Percorso di installazione	Lasciare deselezionata questa opzione per accettare il percorso predefinito, %ProgramFiles(x86)%\VMware, oppure immettere una posizione alternativa.  Se si installano più componenti IaaS nella stessa macchina Windows, installarli tutti nello stesso percorso d'installazione.

## Ruolo del servizio di gestione

(Solo distribuzioni enterprise) Nella pagina del ruolo del servizio di gestione, è possibile configurare la macchina Windows vRealize Automation separata che ospita il servizio di gestione IaaS.

In una distribuzione enterprise, è possibile specificare separatamente l'host del servizio di gestione, che è un servizio Windows. Per l'alta disponibilità, sono supportati più host.

Impostazione	Descrizione
Active	Selezionare l'host del servizio di gestione primario. Eventuali host aggiuntivi fungono da backup per quello primario.  Quando si procede con l'installazione guidata, in caso di problema il failover del servizio si verifica in modo trasparente e viene utilizzato un backup. Vedere <a href="#">Informazioni sul failover automatico del servizio di gestione</a> .
Nome host IaaS	Immettere il nome di dominio completo di ciascuna macchina Windows IaaS che ospita il servizio di gestione.
Username	Immettere l'account del servizio nel formato DOMINIO\nomeutente. L'account deve essere un account di dominio con privilegi di amministratore locale sul server Windows di IaaS.
Password	Immettere la password dell'account.
Percorso di installazione	Lasciare deselezionata questa opzione per accettare il percorso predefinito, %ProgramFiles(x86)%\VMware, oppure immettere una posizione alternativa.  Se si installano più componenti IaaS nella stessa macchina Windows, installarli tutti nello stesso percorso d'installazione.

## Distributed Execution Manager

Nella pagina dei Distributed Execution Manager, è possibile configurare le macchine Windows vRealize Automation che ospitano i DEM IaaS. Vengono supportati più host DEM.

Impostazione	Descrizione
Nome host IaaS	Immettere il nome di dominio completo di ciascuna macchina Windows IaaS che ospita un DEM.
Nome istanza	Immettere un identificatore univoco per ciascun DEM. Tutti i nomi dei DEM devono essere univoci indipendentemente dal fatto che si trovino sullo stesso host o su host diversi.
Username	Immettere l'account del servizio nel formato DOMINIO\nomeutente. L'account deve essere un account di dominio con privilegi di amministratore locale sul server Windows di IaaS.
Password	Immettere la password dell'account.
Descrizione dell'istanza	Se necessario, immettere una spiegazione dei workflow associati a ciascun DEM.
Percorso di installazione	Lasciare deselezionata questa opzione per accettare il percorso predefinito, %ProgramFiles(x86)%\VMware, oppure immettere una posizione alternativa. Se si installano più componenti IaaS nella stessa macchina Windows, installarli tutti nello stesso percorso d'installazione.

## Agenti

Nella pagina degli agenti, è possibile creare il collegamento tra l'IaaS di vRealize Automation e le risorse di virtualizzazione sulle quali è distribuita l'infrastruttura. Si seleziona un tipo di agente e si completano i dettagli dell'endpoint corrispondente.

- Sono supportati più agenti dello stesso tipo o di tipo diverso.
- È possibile installare gli agenti sullo stesso server o su server distinti.
- Sullo stesso server, sono supportati fino a 25 agenti di qualsiasi tipo.
- Se sullo stesso server si trovano più agenti dello stesso tipo, è necessario che ciascuno di essi disponga di un nome univoco e un endpoint diverso.
- Per garantire una disponibilità elevata, è possibile installare un agente dello stesso tipo, con lo stesso nome o lo stesso su server distinti.
- vSphere normalmente è uno dei tipi di agente.
- È possibile aggiungere gli agenti dopo l'installazione.

## Tipi di agente

**Tabella 1-20. vSphere**

Impostazione	Descrizione
Tipo di agente	Nel menu a discesa, selezionare vSphere.
Nome host IaaS	Nel menu a discesa, selezionare il nome di dominio completo della macchina Windows IaaS che ospita l'agente.

**Tabella 1-20. vSphere (Continua)**

Impostazione	Descrizione
Nome agente	Immettere un identificatore univoco, a meno che non si stia aggiungendo il nome e l'endpoint dello stesso agente su vari server per l'alta disponibilità.
Endpoint	Immettere un nome per l'endpoint vSphere.
Percorso di installazione	Lasciare deselezionata questa opzione per accettare il percorso predefinito, %ProgramFiles(x86)%\VMware, oppure immettere una posizione alternativa. Se si installano più componenti IaaS nella stessa macchina Windows, installarli tutti nello stesso percorso d'installazione.
Username	Immettere l'account del servizio nel formato DOMINIO\nomeutente. L'account deve essere un account di dominio con privilegi di amministratore locale sul server Windows di IaaS.
Password	Immettere la password dell'account.

**Tabella 1-21. EPI PowerShell**

Impostazione	Descrizione
Tipo di agente	Nel menu a discesa, selezionare EpiPowerShell.
Nome host IaaS	Nel menu a discesa, selezionare il nome di dominio completo della macchina Windows IaaS che ospita l'agente.
Nome agente	Immettere un identificatore univoco, a meno che non si stia aggiungendo il nome e l'endpoint dello stesso agente su vari server per l'alta disponibilità.
Tipo	Nel menu a discesa, selezionare il brand del provisioning ospitato dall'endpoint EPIServer.
Server	Immettere il nome di dominio completo dell'EPIServer.
Percorso di installazione	Lasciare deselezionata questa opzione per accettare il percorso predefinito, %ProgramFiles(x86)%\VMware, oppure immettere una posizione alternativa. Se si installano più componenti IaaS nella stessa macchina Windows, installarli tutti nello stesso percorso d'installazione.
Username	Immettere l'account del servizio nel formato DOMINIO\nomeutente. L'account deve essere un account di dominio con privilegi di amministratore locale sul server Windows di IaaS.
Password	Immettere la password dell'account.

**Tabella 1-22. HyperV**

Impostazione	Descrizione
Tipo di agente	Nel menu a discesa, selezionare HyperV.
Nome host IaaS	Nel menu a discesa, selezionare il nome di dominio completo della macchina Windows IaaS che ospita l'agente.
Nome agente	Immettere un identificatore univoco, a meno che non si stia aggiungendo il nome e l'endpoint dello stesso agente su vari server per l'alta disponibilità.
Username	Immettere l'account di accesso all'istanza dell'endpoint HyperV.
Password	Immettere la password dell'account.



**Tabella 1-22. HyperV (Continua)**

Impostazione	Descrizione
Percorso di installazione	Lasciare deselezionata questa opzione per accettare il percorso predefinito, %ProgramFiles(x86)%\VMware, oppure immettere una posizione alternativa.  Se si installano più componenti IaaS nella stessa macchina Windows, installarli tutti nello stesso percorso d'installazione.
Username	Immettere l'account del servizio nel formato DOMINIO\nomeutente. L'account deve essere un account di dominio con privilegi di amministratore locale sul server Windows di IaaS.
Password	Immettere la password dell'account.

**Tabella 1-23. PowerShell di VDI**

Impostazione	Descrizione
Tipo di agente	Nel menu a discesa, selezionare VdiPowerShell.
Nome host IaaS	Nel menu a discesa, selezionare il nome di dominio completo della macchina Windows IaaS che ospita l'agente.
Nome agente	Immettere un identificatore univoco, a meno che non si stia aggiungendo il nome e l'endpoint dello stesso agente su vari server per l'alta disponibilità.
Tipo	Il tipo di endpoint viene automaticamente impostato su XenDesktop e non può essere modificato.
Server	Immettere il nome di dominio completo dell'endpoint XenDesktop.
Versione di XenDesktop	Nel menu a discesa, selezionare la versione.
Percorso di installazione	Lasciare deselezionata questa opzione per accettare il percorso predefinito, %ProgramFiles(x86)%\VMware, oppure immettere una posizione alternativa.  Se si installano più componenti IaaS nella stessa macchina Windows, installarli tutti nello stesso percorso d'installazione.
Username	Immettere l'account del servizio nel formato DOMINIO\nomeutente. L'account deve essere un account di dominio con privilegi di amministratore locale sul server Windows di IaaS.
Password	Immettere la password dell'account.

**Tabella 1-24. Xen**

Impostazione	Descrizione
Tipo di agente	Nel menu a discesa, selezionare Xen.
Nome host IaaS	Nel menu a discesa, selezionare il nome di dominio completo della macchina Windows IaaS che ospita l'agente.
Nome agente	Immettere un identificatore univoco, a meno che non si stia aggiungendo il nome e l'endpoint dello stesso agente su vari server per l'alta disponibilità.
Username	Immettere l'account di accesso all'istanza dell'endpoint Xen.
Password	Immettere la password dell'account.

**Tabella 1-24. Xen (Continua)**

Impostazione	Descrizione
Percorso di installazione	Lasciare deselezionata questa opzione per accettare il percorso predefinito, %ProgramFiles(x86)%\VMware, oppure immettere una posizione alternativa.  Se si installano più componenti IaaS nella stessa macchina Windows, installarli tutti nello stesso percorso d'installazione.
Username	Immettere l'account del servizio nel formato DOMINIO\nomeutente. L'account deve essere un account di dominio con privilegi di amministratore locale sul server Windows di IaaS.
Password	Immettere la password dell'account.

**Tabella 1-25. WMI**

Impostazione	Descrizione
Tipo di agente	Nel menu a discesa, selezionare WMI.
Nome host IaaS	Nel menu a discesa, selezionare il nome di dominio completo della macchina Windows IaaS che ospita l'agente.
Nome agente	Immettere un identificatore univoco, a meno che non si stia aggiungendo il nome e l'endpoint dello stesso agente su vari server per l'alta disponibilità.
Percorso di installazione	Lasciare deselezionata questa opzione per accettare il percorso predefinito, %ProgramFiles(x86)%\VMware, oppure immettere una posizione alternativa.  Se si installano più componenti IaaS nella stessa macchina Windows, installarli tutti nello stesso percorso d'installazione.
Username	Immettere l'account del servizio nel formato DOMINIO\nomeutente. L'account deve essere un account di dominio con privilegi di amministratore locale sul server Windows di IaaS.
Password	Immettere la password dell'account.

**Tabella 1-26. Prova**

Impostazione	Descrizione
Tipo di agente	Nel menu a discesa, selezionare Prova.
Nome host IaaS	Nel menu a discesa, selezionare il nome di dominio completo della macchina Windows IaaS che ospita l'agente.
Nome agente	Immettere un identificatore univoco, a meno che non si stia aggiungendo il nome e l'endpoint dello stesso agente su vari server per l'alta disponibilità.
Percorso di installazione	Lasciare deselezionata questa opzione per accettare il percorso predefinito, %ProgramFiles(x86)%\VMware, oppure immettere una posizione alternativa.  Se si installano più componenti IaaS nella stessa macchina Windows, installarli tutti nello stesso percorso d'installazione.
Username	Immettere l'account del servizio nel formato DOMINIO\nomeutente. L'account deve essere un account di dominio con privilegi di amministratore locale sul server Windows di IaaS.
Password	Immettere la password dell'account.

## Certificato di vRealize Appliance

Nella pagina del certificato di vRealize Appliance, è possibile creare o selezionare il certificato di autenticazione utilizzato dall'appliance vRealize Automation. Quando il certificato viene autofirmato, gli utenti finali lo vedono e lo confermano accedendo a vRealize Automation in un browser.

Impostazione		Descrizione
Azione certificato	Mantieni esistente	Utilizzare il certificato già presente nell'appliance vRealize Automation. Verificare i dettagli delle seguenti voci, come il numero di serie e l'impronta digitale.
	Genera certificato	Utilizzare la procedura guidata per generare un certificato autofirmato dell'appliance vRealize Automation.
	Genera richiesta di firma	<p>Creare un file di richiesta di firma del certificato per l'autorità di certificazione. La richiesta CSR consente alla propria autorità di certificazione di creare un certificato con i valori corretti da importare.</p> <ol style="list-style-type: none"> <li>1 Immettere l'organizzazione, l'unità organizzativa e il prefisso internazionale (vedere sotto).</li> <li>2 Fare clic su <b>Genera richiesta di firma</b>.</li> <li>3 Per scaricare il file di richiesta di firma del certificato per l'autorità di certificazione, fare clic sul collegamento visualizzato.</li> </ol>
	Importazione	<p>Identificare un file del certificato in formato PEM, aggiungerlo all'archivio corretto attraverso la procedura guidata, quindi caricarlo per utilizzarlo tramite vRealize Automation.</p> <p>A meno che non si stia importando un certificato creato dalla richiesta di firma del certificato, questa opzione richiede di immettere la chiave privata del certificato, l'eventuale passphrase della chiave privata e la catena di certificati.</p> <p>Quando si importa un file PEM fornito dall'autorità di certificazione creato a partire dalla propria richiesta di firma del certificato, lasciare la chiave privata e la passphrase vuote.</p>
Nome comune		<p>Il nome di dominio completo dell'appliance vRealize Automation.</p> <p>Nelle distribuzioni enterprise ad alta disponibilità con un bilanciamento del carico di fronte a più appliance, questa voce è invece il nome di dominio completo del bilanciamento del carico.</p>
Organizzazione		Immettere il testo che rappresenta il dipartimento o la business unit più grande.
Unità organizzativa		Immettere il testo che rappresenta il dipartimento o il gruppo di lavoro più piccolo.
Prefisso internazionale		Immettere un'abbreviazione del paese dell'operazione.
Seriale		Identificatore alfanumerico univoco
Impronta digitale		Stringa alfanumerica univoca utilizzata per identificare un certificato o per confrontare certificati tra di loro

Impostazione	Descrizione
Valido da	Timestamp a partire dal quale può essere utilizzato il certificato
Valido fino a	Timestamp a partire dal quale non può più essere utilizzato il certificato

## Certificato Web

Nella pagina del certificato Web, è possibile creare o selezionare il certificato di autenticazione utilizzato dal server Web IaaS. L'appliance vRealize Automation si connette al server Web e ha bisogno di autenticarlo e considerarlo attendibile.

Impostazione	Descrizione
Azione certificato	Mantieni esistente
	Utilizzare il certificato già presente nel server Web IaaS. Verificare i dettagli delle seguenti voci, come il numero di serie e l'impronta digitale.
	Genera certificato
	Utilizzare la procedura guidata per generare un certificato autofirmato del server Web IaaS.
	Genera richiesta di firma
	Creare un file di richiesta di firma del certificato per l'autorità di certificazione. La richiesta CSR consente alla propria autorità di certificazione di creare un certificato con i valori corretti da importare.
	<ol style="list-style-type: none"> <li>1 Immettere l'organizzazione, l'unità organizzativa e il prefisso internazionale (vedere sotto).</li> <li>2 Fare clic su <b>Genera richiesta di firma</b>.</li> <li>3 Per scaricare il file di richiesta di firma del certificato per l'autorità di certificazione, fare clic sul collegamento visualizzato.</li> </ol>
	Importazione
	Identificare un file del certificato in formato PEM, aggiungerlo all'archivio corretto attraverso la procedura guidata, quindi caricarlo per utilizzarlo tramite vRealize Automation.
	A meno che non si stia importando un certificato creato dalla richiesta di firma del certificato, questa opzione richiede di immettere la chiave privata del certificato, l'eventuale passphrase della chiave privata e la catena di certificati.
	Quando si importa un file PEM fornito dall'autorità di certificazione creato a partire dalla propria richiesta di firma del certificato, lasciare la chiave privata e la passphrase vuote.
	Fornisci identificazione personale certificato
	Caricare un certificato già aggiunto all'archivio corretto.
	Nome comune
	Il nome di dominio completo del server Web IaaS.
	Nelle distribuzioni enterprise ad alta disponibilità con un bilanciamento del carico di fronte a più server Web, questa voce è invece il nome di dominio completo del bilanciamento del carico.
	Organizzazione
	Immettere il testo che rappresenta il dipartimento o la business unit più grande.
	Unità organizzativa
	Immettere il testo che rappresenta il dipartimento o il gruppo di lavoro più piccolo.

Impostazione	Descrizione
Prefisso internazionale	Immettere un'abbreviazione del paese dell'operazione.
Seriale	Identificatore alfanumerico univoco
Impronta digitale	Stringa alfanumerica univoca utilizzata per identificare un certificato o per confrontare certificati tra di loro
Valido da	Timestamp a partire dal quale può essere utilizzato il certificato
Valido fino a	Timestamp a partire dal quale non può più essere utilizzato il certificato

## Certificato del servizio di gestione

(Solo distribuzioni enterprise) Nella pagina del certificato del servizio di gestione, è possibile creare o selezionare il certificato di autenticazione che utilizza l'host del servizio di gestione IaaS di vRealize Automation. Gli altri server Windows IaaS si connettono all'host del servizio di gestione e hanno bisogno di autenticarlo e considerarlo attendibile.

Questa pagina viene visualizzata solo quando si ospita il servizio di gestione su una macchina separata dal server Web IaaS. Quando vengono ospitati nella stessa macchina, il certificato Web fornisce l'autenticazione per entrambi i ruoli.

Impostazione	Descrizione
Azione certificato	Mantieni esistente
	Utilizzare il certificato già presente nell'host del servizio di gestione IaaS. Verificare i dettagli delle seguenti voci, come il numero di serie e l'impronta digitale.
	Genera certificato
	Utilizzare la procedura guidata per generare un certificato autofirmato dell'host del servizio di gestione IaaS.
	Genera richiesta di firma
	<p>Creare un file di richiesta di firma del certificato per l'autorità di certificazione. La richiesta CSR consente alla propria autorità di certificazione di creare un certificato con i valori corretti da importare.</p> <ol style="list-style-type: none"> <li>1 Immettere l'organizzazione, l'unità organizzativa e il prefisso internazionale (vedere sotto).</li> <li>2 Fare clic su <b>Genera richiesta di firma</b>.</li> <li>3 Per scaricare il file di richiesta di firma del certificato per l'autorità di certificazione, fare clic sul collegamento visualizzato.</li> </ol>
	Importazione
	<p>Identificare un file del certificato in formato PEM, aggiungerlo all'archivio corretto attraverso la procedura guidata, quindi caricarlo per utilizzarlo tramite vRealize Automation.</p> <p>A meno che non si stia importando un certificato creato dalla richiesta di firma del certificato, questa opzione richiede di immettere la chiave privata del certificato, l'eventuale passphrase della chiave privata e la catena di certificati.</p> <p>Quando si importa un file PEM fornito dall'autorità di certificazione creato a partire dalla propria richiesta di firma del certificato, lasciare la chiave privata e la passphrase vuote.</p>

Impostazione	Descrizione
Fornisci identificazione personale certificato	Caricare un certificato già aggiunto all'archivio corretto.
Nome comune	Il nome di dominio completo dell'host del servizio di gestione IaaS. Nelle distribuzioni enterprise ad alta disponibilità con un bilanciamento del carico di fronte a più host del servizio di gestione, questa voce è invece il nome di dominio completo del bilanciamento del carico.
Organizzazione	Immettere il testo che rappresenta il dipartimento o la business unit più grande.
Unità organizzativa	Immettere il testo che rappresenta il dipartimento o il gruppo di lavoro più piccolo.
Prefisso internazionale	Immettere un'abbreviazione del paese dell'operazione.
Seriale	Identificatore alfanumerico univoco
Impronta digitale	Stringa alfanumerica univoca utilizzata per identificare un certificato o per confrontare certificati tra di loro
Valido da	Timestamp a partire dal quale può essere utilizzato il certificato
Valido fino a	Timestamp a partire dal quale non può più essere utilizzato il certificato

## Bilanciamento del carico

(Solo distribuzioni enterprise) Nella pagina Bilanciamenti del carico, è possibile attivare una pausa per configurare i bilanciamenti del carico per il pool di sistemi membro di vRealize Automation corretto.

L'elenco dei bilanciamenti del carico ha scopo unicamente informativo. In base alle immissioni precedenti nella procedura guidata, esso presenta ciascun bilanciamento del carico della distribuzione insieme a membri, rispettivo ruolo del componente, nome di dominio completo e numero di porta.

Attivare la pausa a questo punto e fare riferimento all'elenco mentre si accede ai bilanciamenti del carico per aggiungere membri di vRealize Automation e aprire porte.

## Convalida

Nella pagina Convalida, verificare che l'installazione di vRealize Automation possa procedere.

Per verificare che tutti i componenti di vRealize Automation, i ruoli e gli account siano corretti e che i sistemi possano autenticarsi tra loro, fare clic su **Convalida**. Il processo può impiegare fino a mezz'ora o più in base all'ambiente.

Se si verificano errori, espandere la voce di riga non riuscita e apportare le correzioni in base allo stato e ai messaggi presentati. Non è possibile procedere con l'installazione di vRealize Automation finché la convalida non ha esito positivo.

## Creazione di snapshot

Nella pagina di creazione degli snapshot, la procedura viene interrotta per poter acquisire snapshot delle macchine virtuali di tutti i componenti di vRealize Automation prima di procedere con l'installazione.

Anche se la procedura è stata convalidata, è consigliabile prepararsi a eventuali problemi imprevisti relativi all'installazione. Prima di avviare l'installazione, utilizzare vSphere Client per acquisire uno snapshot di ciascuna appliance vRealize Automation e di ciascun server Windows IaaS. Altrimenti, sarà necessario installare di nuovo tutte le impostazioni della procedura guidata per tornare a questo punto.

Se le risorse sono sufficienti, è possibile acquisire snapshot di macchine virtuali in esecuzione, nonostante sia una pratica ottimale arrestarle all'inizio.

- 1 Nell'angolo in alto a destra dell'installazione guidata, fare clic su **Disconnetti**.

---

**Importante** Se si chiude la procedura guidata con un metodo diverso da **Disconnetti**, non sarà possibile riaprire la procedura guidata.

---

- 2 In vSphere, arrestare il sistema operativo guest di ciascuna appliance vRealize Automation e di ciascun server Windows IaaS.
- 3 Fare clic con il pulsante destro del mouse sulle macchine virtuali e selezionare **Acquisisci snapshot**.
- 4 Assegnare un nome allo snapshot.
- 5 Per includere la memoria della macchina nello snapshot, selezionare **Snapshot della memoria della macchina virtuale**.
- 6 Fare clic su **OK**.  
Attendere che gli snapshot vengano creati.
- 7 Accendere il sistema operativo guest di ciascuna appliance vRealize Automation e di ciascun server Windows IaaS.
- 8 Tornare alla pagina degli snapshot dell'installazione guidata effettuando di nuovo l'accesso come root.

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

## Dettagli di installazione

Nella pagina dei dettagli di installazione, è possibile avviare l'installazione di vRealize Automation o riprovarla nel caso in cui si siano verificati problemi.

Per avviare l'installazione, fare clic su **Installa**. A seconda dell'ambiente, l'installazione può impiegare fino a un'ora o più.

Durante o dopo l'installazione, è possibile fare clic sul pulsante **Raccogli registri**.

- Quando si raccolgono registri, sopra la tabella di stato viene visualizzato un collegamento per il download del file ZIP.
- Quando si raccolgono registri più di una volta, ogni raccolta sovrascrive quella precedente.

Se si desiderano i registri correnti, scaricarli prima di fare nuovamente clic su **Raccogli registri**.

In caso di problemi, la procedura guidata arresta l'installazione e mostra messaggi per aiutare l'utente ad apportare modifiche. Dopo la valutazione dei messaggi e l'annotazione delle correzioni necessarie, è possibile che l'utente abbia bisogno degli snapshot creati.

## Non effettuare il ripristino agli snapshot

Se la procedura guidata attiva l'opzione **Nuovo tentativo procedura non riuscita**, è possibile apportare le modifiche e riprovare l'installazione senza ripristinare le macchine agli snapshot.

Una volta apportate le modifiche, fare clic su **Nuovo tentativo procedura non riuscita**.

## Ripristino dei server Windows IaaS agli snapshot

Se la procedura guidata attiva l'opzione **Nuovo tentativo per tutti i server IaaS**, seguire questa procedura.

- 1 In vSphere, ripristinare tutte le macchine Windows IaaS agli snapshot acquisiti nella pagina precedente della procedura guidata.
- 2 Se gli snapshot sono stati acquisiti dopo un arresto, accendere i sistemi operativi guest.
- 3 Se è stato utilizzato un SQL Server esterno, eliminare il database SQL di vRealize Automation.
- 4 Apportare le modifiche.
- 5 Fare clic su **Nuovo tentativo per tutti i server IaaS**.

## Ripristino delle appliance e dei server Windows IaaS agli snapshot

Se durante la procedura guidata vengono visualizzati messaggi relativi all'appliance vRealize Automation, seguire questa procedura.

- 1 In vSphere, ripristinare tutte le appliance vRealize Automation e le macchine Windows IaaS agli snapshot acquisiti nella pagina precedente della procedura guidata.
- 2 Se gli snapshot sono stati acquisiti dopo un arresto, accendere i sistemi operativi guest.
- 3 Se è stato utilizzato un SQL Server esterno, eliminare il database SQL di vRealize Automation.
- 4 Apportare le modifiche.
- 5 Tornare all'installazione guidata effettuando di nuovo l'accesso come root.  
<https://vrealize-automation-appliance-FQDN:5480>
- 6 Tornare alla pagina dei dettagli di installazione e fare clic su **Installa**.

## Gestione licenze

Nella pagina di gestione delle licenze, immettere una chiave per attivare il prodotto vRealize Automation installato.

In **Nuova chiave di licenza**, immettere la chiave e fare clic su **Invia chiave**. È possibile inviare separatamente più chiavi, comprese quelle per istanze autonome di vRealize Automation, vRealize Suite, vRealize Business for Cloud e vRealize Code Stream.

In questa pagina è possibile inoltre selezionare se attivare vRealize Code Stream. vRealize Code Stream non è supportato per l'alta disponibilità o per distribuzioni di vRealize Automation di produzione e richiede vRealize Code Stream Management Pack. Per ulteriori informazioni, vedere [Gestione della licenza vRealize Code Stream](#).



## Telemetria

Nella pagina della telemetria, è possibile decidere se vRealize Automation invia statistiche sull'utilizzo a VMware come parte del programma CEIP (Customer Experience Improvement Program).

Selezionare o deselezionare l'opzione per partecipare al programma CEIP (Customer Experience Improvement Program).

Per ulteriori informazioni, vedere [il programma CEIP](#).

## Opzioni di post-installazione

Nella pagina delle opzioni di post-installazione, sono disponibili delle opzioni per creare nuovi dati di vRealize Automation oppure effettuare la migrazione di dati di distribuzioni precedenti a una nuova installazione.

- **Configura contenuto iniziale** crea un nuovo utente locale del tenant predefinito. Questo utente locale può avviare il processo di configurazione nel tenant predefinito.

Per la prima opzione, è necessario prima avere aggiunto almeno un endpoint vSphere nella pagina degli agenti dell'installazione guidata.

- **Migrazione di una distribuzione** trasferisce i dati precedenti di vRealize Automation nella distribuzione appena installata. La migrazione conserva gli elementi essenziali come gruppi, blueprint ed endpoint.
- **Continua** fa passare l'utente al termine dell'installazione guidata.

## Configurazione del contenuto iniziale

Nella pagina di configurazione del contenuto iniziale, è possibile creare un nuovo utente del tenant predefinito locale di vRealize Automation, in grado di iniziare un workflow di contenuti per un endpoint vSphere.

---

**Nota** Questa opzione è disponibile solo se prima, nella pagina degli agenti, era stato aggiunto almeno un endpoint vSphere.

---

Il nuovo nome utente locale è configurationadmin. vRealize Automation conferisce a configurationadmin i seguenti privilegi.

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

Immettere e confermare una password di accesso per configurationadmin. Per generare un elemento del catalogo in modo che configurationadmin possa avviare il processo di configurazione dopo aver effettuato l'accesso al tenant predefinito, fare clic su **Crea contenuto iniziale**.

## Configurazione della migrazione

Nella pagina di configurazione della migrazione, è possibile avviare il trasferimento di un'altra distribuzione di vRealize Automation, precedente a quella appena installata.

Prima della migrazione di una distribuzione precedente, considerare le seguenti linee guida.

- Rivedere in modo approfondito la guida alla migrazione di vRealize Automation associata alla versione della distribuzione precedente. I prerequisiti e altri dettagli potrebbero essere diversi.
- Effettuare la migrazione dei tenant e degli archivi identità precedenti a VMware Identity Manager nella nuova distribuzione.
- Clonare il database IaaS di SQL Server precedente e ripristinarlo nel database IaaS della nuova distribuzione. Annotare il nome del database clonato.
- Ottenere e annotare la chiave di crittografia del database IaaS di SQL Server precedente.
- Creare e annotare la nuova passphrase per crittografare di nuovo i dati migrati.
- Annotare il nome di dominio completo e le credenziali di accesso root del bilanciamento del carico o dell'appliance vRealize Automation precedente.
- Annotare le credenziali di accesso root della nuova distribuzione.

## Le interfacce di installazione standard di vRealize Automation

Dopo aver eseguito l'installazione guidata, può essere necessario o utile eseguire alcune attività d'installazione manualmente, attraverso le interfacce standard.

L'installazione guidata descritta in [Installazione di vRealize Automation utilizzando l'installazione guidata](#) è lo strumento principale per le nuove installazioni di vRealize Automation. Tuttavia dopo aver eseguito la procedura guidata, alcune operazioni dovranno essere ancora eseguite con il vecchio processo d'installazione manuale.

È necessario eseguire i passaggi manuali per espandere una distribuzione vRealize Automation o se la procedura guidata si è arrestata per qualsiasi motivo. Situazioni in cui può essere necessario fare riferimento alle procedure illustrate in questa sezione includono i seguenti esempi.

- Si sceglie di annullare la procedura guidata prima della conclusione dell'installazione.
- L'installazione tramite procedura guidata non è riuscita.
- Si desidera aggiungere un'altra appliance vRealize Automation per l'alta disponibilità.
- Si desidera aggiungere un altro server Web IaaS per l'alta disponibilità.
- È necessario un altro agente proxy.

- È necessario un altro DEM Worker o Orchestrator.

È possibile utilizzare tutti i processi manuali o solo alcuni. Esaminare le informazioni fornite in questa sezione e seguire le procedure che si applicano alla propria situazione.

## Utilizzo delle interfacce standard per le distribuzioni minime

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

L'installazione di vRealize Automation in una configurazione minima è finalizzata a un modello di verifica o a lavoro di sviluppo. Le distribuzioni minime richiedono una quantità inferiore di passaggi per l'installazione, ma non hanno la capacità di produzione di una distribuzione enterprise.

Completare le attività di alto livello rispettando il seguente ordine.

**Tabella 1-27. Elenco di controllo di una distribuzione minima**

Attività	Dettagli
<input type="checkbox"/> Pianificare i prerequisiti d'installazione di ambiente e indirizzo.	<a href="#">Preparazione per l'installazione di vRealize Automation</a>
<input type="checkbox"/> Creare un'appliance vRealize Automation non configurata.	<a href="#">Distribuzione di vRealize Automation appliance</a>
<input type="checkbox"/> Configurare manualmente l'appliance vRealize Automation.	<a href="#">Configurazione dell'appliance vRealize Automation</a>
<input type="checkbox"/> Installare i componenti IaaS su un singolo server Windows.	<a href="#">Installazione dei componenti IaaS</a>
<input type="checkbox"/> Installare agenti aggiuntivi, se necessario.	<a href="#">Installazione degli agenti di vRealize Automation</a>
<input type="checkbox"/> Eseguire le attività post-installazione, come la configurazione del tenant predefinito.	<a href="#">Configurazione dell'accesso per il tenant predefinito</a>

### Configurazione dell'appliance vRealize Automation

L'appliance vRealize Automation è una macchina virtuale parzialmente configurata che ospita il server e il portale Web per gli utenti di vRealize Automation. È necessario scaricare e distribuire il modello OVF (Open Virtualization Format) dell'appliance nell'inventario di vCenter Server o ESX/ESXi.

#### Prerequisiti

- Creare un'appliance non configurata. Vedere [Distribuzione di vRealize Automation appliance](#).
- Richiedere un certificato di autenticazione per l'appliance vRealize Automation.

#### Procedura

- 1 Accedere come root all'interfaccia di gestione dell'appliance vRealize Automation non configurata.  
<https://vrealize-automation-appliance-FQDN:5480>  
Continuare indipendentemente dall'eventuale visualizzazione di avvisi sui certificati.
- 2 Se viene visualizzata l'installazione guidata, annullarla per passare all'interfaccia di gestione.

### 3 Selezionare **Admin > Impostazioni ora** e impostare l'origine di sincronizzazione dell'ora.

Opzione	Descrizione
<b>Ora host</b>	Sincronizza l'ora con quella dell'host ESXi dell'appliance vRealize Automation.
<b>Server di riferimento ora</b>	Sincronizza l'ora con quella di un server NTP (Network Time Protocol) esterno. Immettere il nome di dominio completo o l'indirizzo IP del server NTP.

È necessario sincronizzare le appliance vRealize Automation e i server IaaS Windows con la stessa origine di riferimento dell'ora. Non combinare origini di riferimento dell'ora all'interno di una distribuzione vRealize Automation.

### 4 Selezionare **Impostazioni vRA > Impostazioni host**.

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

**Nota** configurare le impostazioni SSO come descritto più avanti in questa procedura ogni volta che si utilizza **Aggiorna host** per impostare 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 dell'appliance vRealize Automation e a qualsiasi bilanciamento del carico mediante l'uso di certificati SAN (Subject Alternative Name).

Se si desidera generare una richiesta CSR per un nuovo certificato da inviare a un'autorità di certificazione, selezionare **Genera richiesta di firma**. La richiesta CSR consente alla propria autorità di certificazione di creare un certificato con i valori corretti da importare.

**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
<b>Mantieni esistente</b>	Lasciare invariata la configurazione SSL corrente. Selezionare questa opzione per annullare le modifiche.
<b>Genera certificato</b>	<ul style="list-style-type: none"> <li>a Il valore visualizzato nella casella di testo <b>Nome comune</b> è il nome host visualizzato nella parte superiore della pagina. Se sono disponibili istanze aggiuntive dell'appliance vRealize Automation, i rispettivi nomi di dominio completi vengono inclusi nell'attributo SAN del certificato.</li> <li>b Immettere il nome dell'organizzazione, come ad esempio quello della propria azienda, nella casella di testo <b>Organizzazione</b>.</li> <li>c Immettere l'unità organizzativa, ad esempio il nome o la posizione del proprio reparto, nella casella di testo <b>Unità organizzativa</b>.</li> <li>d Immettere il codice di paese ISO 3166 a due lettere, ad esempio <b>IT</b>, nella casella di testo <b>Paese</b>.</li> </ul>
<b>Genera richiesta di firma</b>	<ul style="list-style-type: none"> <li>a Selezionare <b>Genera richiesta di firma</b>.</li> <li>b Verificare le voci nelle caselle di testo <b>Organizzazione</b>, <b>Unità organizzativa</b>, <b>Prefisso internazionale</b> e <b>Nome comune</b>. Queste voci vengono popolate dal certificato esistente. Se necessario, è possibile modificare queste voci.</li> <li>c Fare clic su <b>Genera CSR</b> per generare una richiesta di firma del certificato, quindi fare clic sul collegamento <b>Scarica qui la richiesta CSR generata</b> per aprire una finestra di dialogo che consente di salvare la richiesta CSR in un percorso da cui è possibile inviarla a un'autorità di certificazione.</li> <li>d Una volta ricevuto il certificato preparato, fare clic su <b>Importa</b> e seguire le istruzioni per importare un certificato in vRealize Automation.</li> </ul>
<b>Importazione</b>	<ul style="list-style-type: none"> <li>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 <b>Chiave privata RSA</b>.</li> <li>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 <b>Catena di certificati</b>. Per valori di certificati multipli, includere un'intestazione BEGIN CERTIFICATE e un piè di pagina END CERTIFICATE per ciascun certificato.</li> </ul> <p><b>Nota</b> In caso di certificati concatenati, possono essere disponibili attributi aggiuntivi.</p> <ul style="list-style-type: none"> <li>c (Facoltativo) Se il certificato utilizza una passphrase per crittografare la chiave del certificato, copiare la passphrase e incollarla nella casella di testo <b>Passphrase</b>.</li> </ul>

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

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

- 10 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.

---

- 11 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.

---

- 12 Selezionare se abilitare vRealize Code Stream e immettere una licenza di vRealize Code Stream.

vRealize Code Stream non è supportato per le distribuzioni ad alta disponibilità o di produzione di vRealize Automation.

- 13 Assicurarsi che sia possibile accedere a vRealize Automation.

- a Aprire un browser Web e visitare l'URL dell'interfaccia del prodotto vRealize Automation.  
`https://vrealize-automation-appliance-FQDN/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.

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

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

### Operazioni successive

Vedere [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

L'amministratore di sistema accede alla macchina Windows e utilizza l'installazione guidata per installare i servizi IaaS nella macchina Windows fisica o virtuale.

### Prerequisiti

- Verificare che il server soddisfi i requisiti in [Server Windows IaaS](#).
- [Attivazione della sincronizzazione di data e ora su Windows Server](#).
- Assicurarsi di aver distribuito e configurato completamente l'appliance vRealize Automation e che i servizi necessari siano in esecuzione (plugin-service, catalog-service, iaas-proxy-provider).

### Procedura

#### 1 [Scaricare il programma di installazione di vRealize Automation IaaS](#)

Per installare IaaS in un server Windows fisico o virtuale minimo, scaricare una copia del programma di installazione di IaaS dall'appliance vRealize Automation.

#### 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.

## Scaricare il programma di installazione di vRealize Automation IaaS

Per installare IaaS in un server Windows fisico o virtuale minimo, scaricare una copia del programma di installazione di IaaS dall'appliance vRealize Automation.

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



## Prerequisiti

- Esaminare i requisiti del server Windows di IaaS. Vedere [Server Windows IaaS](#).
- Se si utilizza Internet Explorer per il download, verificare che non sia abilitata la configurazione di sicurezza avanzata. Passare a `res://iesetup.dll/SoftAdmin.htm` nel server Windows.

## Procedura

- 1 Accedere al server IaaS Windows utilizzando un account che dispone di privilegi di amministratore.
- 2 Aprire un browser Web direttamente con l'URL del programma di installazione dell'appliance vRealize Automation.

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

- 3 Fare clic sul **programma d'installazione di IaaS**.
- 4 Salvare `setup__vrealize-automation-appliance-FQDN@5480` nel server Windows.  
Non modificare il nome del file del programma d'installazione, poiché viene utilizzato per collegare l'installazione all'appliance vRealize Automation.

## Selezione del tipo di installazione

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

## Prerequisiti

[Scaricare il programma di installazione di vRealize Automation IaaS](#).

## Procedura

- 1 Fare clic con il pulsante destro del mouse sul file d'installazione `setup__vrealize-automation-appliance-FQDN@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 dell'appliance vRealize Automation e verificare il certificato SSL.
  - a Specificare il nome utente, ovvero **root**, e la password.  
Questa è la password che è stata immessa durante la distribuzione dell'appliance vRealize Automation.
  - b Selezionare **Accetta certificato**.
  - c Fare clic su **Visualizza certificato**.

Confrontare l'identificazione personale del certificato con quella impostata per l'appliance vRealize Automation. È possibile visualizzare il certificato dell'appliance vRealize Automation nel browser client quando si accede alla console di gestione tramite la 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 <b>Avanti</b> .
Errori non critici	Fare clic su <b>Bypass</b> .
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 <b>Controlla di nuovo</b> 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** o nella pagina **Impostazioni rilevate** immettere il nome utente e la password per l'account del servizio Windows. L'account del servizio deve essere un account amministratore locale che abbia anche privilegi amministrativi per SQL.

**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** Per installare un'istanza di database sullo stesso server con i componenti di IaaS, accettare il server predefinito nella casella di testo **Server** nella sezione di informazioni sull'installazione del database Microsoft SQL Server.

Se il database si trova su una macchina diversa, immettere il server nel seguente formato.

*FQDN-macchina, numero-porta\istanza-database-denominata*

**4** Accettare il valore predefinito della casella di testo **Database name** o immettere il 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.

È consigliata l'autenticazione Windows. Quando si seleziona l'autenticazione SQL, in alcuni file di configurazione viene visualizzata la password del database senza crittografia.

**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 ulteriori informazioni sulla configurazione di SSL in SQL Server, vedere [Articolo di Microsoft Technet 189067](#).

**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

[Scaricare il programma di installazione di vRealize Automation IaaS.](#)

### Procedura

- 1 Accettare il valore predefinito del campo **Server**, in cui è inserito il nome di dominio completo del server dell'appliance vRealize Automation da cui è stato scaricato il programma di 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 recuperare il certificato dall'appliance vRealize Automation.  
  
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 Fare 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 in cui si sta eseguendo l'installazione sia connessa alla rete e sia in grado di connettersi all'appliance vRealize Automation da cui è possibile scaricare il programma di 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.

### Operazioni successive

[Verifica dei servizi di IaaS.](#)

## Utilizzo delle interfacce standard per le distribuzioni distribuite

Le distribuzioni enterprise sono progettate per garantire una capacità di vRealize Automation maggiore nella produzione e richiedono la distribuzione di componenti su più macchine. Tali distribuzioni potrebbero anche includere sistemi ridondanti dietro i bilanciamenti del carico.

### 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.

**Tabella 1-28. 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.	<a href="#">Preparazione per l'installazione di vRealize Automation</a>
<input type="checkbox"/> Pianificare e ottenere i certificati SSL.	<a href="#">Requisiti di attendibilità dei certificati in una distribuzione distribuita</a>

**Tabella 1-28. Elenco di controllo di una distribuzione distribuita (Continua)**

Attività	Dettagli
<input type="checkbox"/> Distribuire il server dell'appliance vRealize Automation principale e tutte le appliance aggiuntive a scopo di ridondanza e alta disponibilità.	<a href="#">Distribuzione di vRealize Automation appliance</a>
<input type="checkbox"/> Configurare il bilanciamento del carico per gestire il traffico dell'appliance vRealize Automation.	<a href="#">Configurazione del bilanciamento del carico</a>
<input type="checkbox"/> Configurare il server dell'appliance vRealize Automation principale e tutte le appliance aggiuntive distribuite a scopo di ridondanza e alta disponibilità.	<a href="#">Configurazione di appliance per vRealize Automation</a>
<input type="checkbox"/> Configurare il bilanciamento del carico per gestire il traffico del componente IaaS vRealize Automation e installare i componenti IaaS vRealize Automation.	<a href="#">Installazione dei componenti di IaaS in una configurazione distribuita</a>
<input type="checkbox"/> Se richiesto, installare gli agenti per l'integrazione con i sistemi esterni.	<a href="#">Installazione degli agenti di vRealize Automation</a>
<input type="checkbox"/> Configurare il tenant predefinito e fornire la licenza di IaaS.	<a href="#">Configurazione dell'accesso per il tenant predefinito</a>

## vRealize Orchestrator

L'appliance vRealize Automation include una versione integrata di vRealize Orchestrator consigliata per l'utilizzo con le nuove installazioni. Nelle distribuzioni precedenti o in casi particolari, tuttavia, gli utenti possono collegare vRealize Automation a un vRealize Orchestrator esterno separato. Vedere <https://www.vmware.com/products/vrealize-orchestrator.html>.

Per informazioni sulla connessione di vRealize Automation e vRealize Orchestrator, vedere [Plug-in di VMware vRealize Orchestrator per vRealize Automation](#).

## 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.

## Disattivazione dei controlli di integrità del bilanciamento del carico

I controlli di integrità assicurano che un bilanciamento del carico invii il traffico solo a nodi che sono operativi. Il bilanciamento del carico invia un controllo d'integrità a una frequenza specificata a ogni nodo. I nodi che hanno superato la soglia di esito negativo diventano inidonei per il nuovo traffico.

Per la distribuzione del carico di lavoro e il failover, è possibile posizionare più appliance vRealize Automation dopo un bilanciamento del carico. È inoltre possibile posizionare più server Web IaaS e più server del servizio di gestione IaaS dopo i rispettivi bilanciamenti del carico.

Quando si utilizzano i bilanciamenti del carico, evitare che inviino i controlli di integrità in qualsiasi momento durante l'installazione. I controlli di integrità possono interferire con l'installazione o indurre l'installazione a funzionare in modo imprevedibile.

- Quando si distribuiscono i componenti dell'appliance vRealize Automation o IaaS dopo i bilanciamenti del carico esistenti, disabilitare i controlli di integrità in tutti i bilanciamenti del carico della configurazione proposta prima di installare qualsiasi componente.
- Dopo aver installato e configurato tutti i componenti di vRealize Automation, inclusi quelli dell'appliance vRealize Automation e IaaS, è possibile riabilitare i controlli di integrità.

### **Requisiti di attendibilità dei certificati in una distribuzione distribuita**

vRealize Automation utilizza certificati per gestire le relazioni basate sulla fiducia e fornire una comunicazione sicura tra i componenti in distribuzioni distribuite.

In una distribuzione distribuita, o in cluster, l'organizzazione di certificazione di vRealize Automation si conforma ampiamente alla struttura architettonica in tre livelli di vRealize Automation. Questi tre livelli corrispondono a Appliance vRealize Automation, componenti del sito Web IaaS e componenti del servizio di gestione. In un ambiente distribuito, ciascuna macchina hardware in un livello particolare condivide un certificato. In altre parole, ciascuna istanza di Appliance vRealize Automation condivide un certificato comune e ciascuna macchina del servizio di gestione condivide il certificato comune applicabile a quel livello.

È possibile utilizzare certificati autofirmati del sistema o generati dall'utente, oppure certificati forniti da un'autorità di certificazione con distribuzioni di vRealize Automation distribuite. A partire da vRealize Automation 7.0 e versioni successive, se non vengono forniti certificati dall'utente, il programma di installazione genera automaticamente certificati autofirmati per tutti i nodi applicabili, posizionandoli negli archivi attendibili appropriati.

È possibile utilizzare i bilanciamenti del carico con componenti di vRealize Automation distribuiti per fornire alta disponibilità e supporto di failover. VMware consiglia di utilizzare una configurazione di passaggio per le distribuzioni di vRealize Automation che utilizzano i bilanciamenti del carico. In una configurazione di passaggio, i bilanciamenti del carico passano le richieste ai componenti appropriati anziché decrittografarle. I server Web di Appliance vRealize Automation e IaaS dovranno quindi procedere alla necessaria decrittografia.

Per ulteriori informazioni sull'uso e la configurazione dei bilanciamenti del carico, vedere *Bilanciamento del carico di vRealize Automation*.

Se vengono forniti e generati i propri certificati utilizzando Openssl o un altro strumento, è possibile utilizzare certificati wildcard o SAN (Subject Alternative Name, nome alternativo del soggetto). Tenere presente che i certificati IaaS devono essere certificati multiuso.

Se vengono forniti certificati, è necessario ottenere un certificato multiuso che includa il componente IaaS nel cluster, quindi copiare il certificato nell'archivio attendibile per ciascun componente. Se si utilizzano i bilanciamenti del carico, nell'indirizzo attendibile del certificato multiuso del cluster è necessario includere il nome di dominio completo (FQDN) del bilanciamento del carico.

Se è necessario aggiornare certificati autofirmati generati dal sistema con certificati forniti dall'utente o dall'autorità di certificazione, vedere [Aggiornamento di certificati di vRealize Automation](#).

La tabella Requisiti di attendibilità dei certificati riepiloga i requisiti di registrazione attendibile per i diversi certificati importati.

**Tabella 1-29. Requisiti di attendibilità dei certificati**

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

### Configurazione del componente Web, del servizio di gestione e di attendibilità dei certificati dell'host DEM

I clienti che utilizzano un'identificazione personale con file PFX preinstallati per supportare l'autenticazione degli utenti devono configurare l'attendibilità dell'identificazione personale, il servizio di gestione e le macchine dell'host del DEM Orchestrator e Worker.

I clienti che importano i file PEM o utilizzano certificati autofirmati possono ignorare questa procedura.

#### Prerequisiti

File `web.pfx` e `ms.pfx` validi disponibili per l'autenticazione dell'identificazione personale.

#### Procedura

- 1 Importare i file `web.pfx` e `ms.pfx` nelle seguenti posizioni delle macchine host del componente Web e del servizio di gestione:
  - *Host Computer/Certificates/Personal certificate store*
  - *Host Computer/Certificates/Trusted People certificate store*
- 2 Importare i file `web.pfx` e `ms.pfx` nelle seguenti posizioni delle macchine host del DEM Orchestrator e Worker:
 

*Host Computer/Certificates/Trusted People certificate store*
- 3 In ognuna delle macchine host applicabili aprire una finestra di Microsoft Management Console.

**Nota** Gli effettivi percorsi e opzioni di Management Console possono variare leggermente a seconda delle versioni e delle configurazioni dei sistemi Windows.

- a Selezionare **Aggiungi/Rimuovi snap-in**.
- b Selezionare **Certificati**.



- c Selezionare **Computer locale**.
- d Aprire i file di certificato che sono stati importati in precedenza e copiare l'identificazione personale.

### Operazioni successive

Inserire l'identificazione personale nella pagina Certificato della procedura guidata di vRealize Automation per il servizio di gestione, i componenti Web e i componenti di DEM.

### Fogli di lavoro per l'installazione

I fogli di lavoro registrano informazioni importanti a cui occorre fare riferimento durante l'installazione.

Per le impostazioni viene fatta distinzione tra lettere maiuscole e minuscole. Tenere presente che sono predisposti spazi aggiuntivi per altri componenti qualora si stia effettuando un'implementazione distribuita. Non è necessario usare tutti gli spazi dei fogli di lavoro. Inoltre una macchina potrebbe ospitare più di un componente IaaS. Ad esempio, il server Web primario e DEM Orchestrator potrebbero trovarsi sullo stesso FQDN.

**Tabella 1-30. Appliance vRealize Automation**

Variabile	Valore personale	Esempio
Nome di dominio completo dell'appliance vRealize Automation primaria		automation.nomesocietà.com
Indirizzo IP dell'appliance vRealize Automation primaria Solo per riferimento; non inserire indirizzi IP		123.234.1.105
Nome di dominio completo dell'appliance vRealize Automation aggiuntiva		automation2.nomesocietà.com
Indirizzo IP dell'appliance vRealize Automation aggiuntiva Solo per riferimento; non inserire indirizzi IP		123.234.1.106
Nome di dominio completo del bilanciamento del carico dell'appliance vRealize Automation		automation-balance.nomesocietà.com
Indirizzo IP del bilanciamento del carico dell'appliance vRealize Automation Solo per riferimento; non inserire indirizzi IP		123.234.1.201
Nome utente interfaccia di gestione ( <a href="https://appliance-FQDN:5480">https://appliance-FQDN:5480</a> )	root (predefinito)	root
Password interfaccia di gestione		admin123
Tenant predefinito	vsphere.local (predefinito)	vsphere.local

**Tabella 1-30. Appliance vRealize Automation (Continua)**

Variabile	Valore personale	Esempio
Nome utente tenant predefinito	administrator@vsphere.local (predefinito)	administrator@vsphere.local
Password tenant predefinita		login123

**Tabella 1-31. Server Windows IaaS**

Variabile	Valore personale	Esempio
Server Web IaaS primario con FQDN di Model Manager Data		web.nomesocietà.com
Server Web IaaS primario con indirizzo IP di Model Manager Data Solo per riferimento; non inserire indirizzi IP		123.234.1.107
FQDN del server Web IaaS aggiuntivo		web2.nomesocietà.com
Indirizzo IP del server Web IaaS aggiuntivo Solo per riferimento; non inserire indirizzi IP		123.234.1.108
FQDN del bilanciamento del carico del server Web IaaS		web-balance.nomesocietà.com
Indirizzo IP del bilanciamento del carico del server Web IaaS Solo per riferimento; non inserire indirizzi IP		123.234.1.202
FQDN dell'host del servizio di gestione IaaS attivo		mgr-svc.nomesocietà.com
Indirizzo IP dell'host del servizio di gestione IaaS attivo Solo per riferimento; non inserire indirizzi IP		123.234.1.109
FQDN dell'host del servizio di gestione IaaS passivo		mgr-svc2.nomesocietà.com
Indirizzo IP dell'host del servizio di gestione IaaS passivo Solo per riferimento; non inserire indirizzi IP		123.234.1.110
FQDN del bilanciamento del carico dell'host del servizio di gestione IaaS		mgr-svc-balance.nomesocietà.com
Indirizzo IP del bilanciamento del carico dell'host del servizio di gestione IaaS Solo per riferimento; non inserire indirizzi IP		123.234.203

**Tabella 1-31. Server Windows IaaS (Continua)**

Variabile	Valore personale	Esempio
Per i servizi IaaS, account di dominio con diritti di amministratore sugli host		SUPPORT\provisioner
Password account		login123

**Tabella 1-32. Database di SQL Server IaaS**

Variabile	Valore personale	Esempio
Istanza database		IAASSQL
Nome database	vcac (predefinito)	vcac
Passphrase (usata per l'installazione, l'aggiornamento e la migrazione)		login123

**Tabella 1-33. Distributed Execution Manager IaaS**

Variabile	Valore personale	Esempio
FQDN dell'host DEM		dem.nomesocietà.com
Indirizzo IP dell'host DEM Solo per riferimento; non inserire indirizzi IP		123.234.1.111
FQDN dell'host DEM		dem2.nomesocietà.com
Indirizzo IP dell'host DEM Solo per riferimento; non inserire indirizzi IP		123.234.1.112
Nome univoco di DEM Orchestrator		Orchestrator-1
Nome univoco di DEM Orchestrator		Orchestrator-2
Nome univoco di DEM Worker		Worker-1
Nome univoco di DEM Worker		Worker-2
Nome univoco di DEM Worker		Worker-3
Nome univoco di DEM Worker		Worker-4

### 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 Appliance vRealize Automation.

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 Appliance vRealize Automation.
- 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 ulteriori informazioni sui bilanciamenti del carico, vedere [Bilanciamento del carico di vRealize Automation](#).

Per informazioni sulla scalabilità e sull'alta disponibilità, vedere la guida *Architettura di riferimento di vRealize Automation*.

## 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 della prima appliance vRealize Automation in un cluster

L'appliance vRealize Automation è una macchina virtuale parzialmente configurata che ospita il server e il portale Web per gli utenti di vRealize Automation. È necessario scaricare e distribuire il modello OVF (Open Virtualization Format) dell'appliance nell'inventario di vCenter Server o ESX/ESXi.

#### Prerequisiti

- Creare un'appliance non configurata. Vedere [Distribuzione di vRealize Automation appliance](#).
- Richiedere un certificato di autenticazione per l'appliance vRealize Automation.

Se la rete o il bilanciamento del carico lo richiede, le procedure seguenti consentono di copiare il certificato nel servizio di bilanciamento del carico e nelle appliance aggiuntive.

#### Procedura

- 1 Accedere come root all'interfaccia di gestione dell'appliance vRealize Automation non configurata.  
<https://vrealize-automation-appliance-FQDN:5480>  
 Continuare indipendentemente dall'eventuale visualizzazione di avvisi sui certificati.
- 2 Se viene visualizzata l'installazione guidata, annullarla per passare all'interfaccia di gestione.

### 3 Selezionare **Admin > Impostazioni ora** e impostare l'origine di sincronizzazione dell'ora.

Opzione	Descrizione
<b>Ora host</b>	Sincronizza l'ora con quella dell'host ESXi dell'appliance vRealize Automation.
<b>Server di riferimento ora</b>	Sincronizza l'ora con quella di un server NTP (Network Time Protocol) esterno. Immettere il nome di dominio completo o l'indirizzo IP del server NTP.

È necessario sincronizzare tutte le appliance vRealize Automation e i server IaaS Windows con la stessa origine di riferimento dell'ora. Non combinare origini di riferimento dell'ora diverse all'interno di una distribuzione di vRealize Automation.

### 4 Selezionare **Impostazioni vRA > Impostazioni host**.

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

**Nota** configurare le impostazioni SSO come descritto più avanti in questa procedura ogni volta che si utilizza **Aggiorna host** per impostare 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 dell'appliance vRealize Automation e a qualsiasi bilanciamento del carico mediante l'uso di certificati SAN (Subject Alternative Name).

Se si desidera generare una richiesta CSR per un nuovo certificato da inviare a un'autorità di certificazione, selezionare **Genera richiesta di firma**. La richiesta CSR consente alla propria autorità di certificazione di creare un certificato con i valori corretti da importare.

**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
<b>Mantieni esistente</b>	Lasciare invariata la configurazione SSL corrente. Selezionare questa opzione per annullare le modifiche.
<b>Genera certificato</b>	<ul style="list-style-type: none"> <li>a Il valore visualizzato nella casella di testo <b>Nome comune</b> è il nome host visualizzato nella parte superiore della pagina. Se sono disponibili istanze aggiuntive dell'appliance vRealize Automation, i rispettivi nomi di dominio completi vengono inclusi nell'attributo SAN del certificato.</li> <li>b Immettere il nome dell'organizzazione, come ad esempio quello della propria azienda, nella casella di testo <b>Organizzazione</b>.</li> <li>c Immettere l'unità organizzativa, ad esempio il nome o la posizione del proprio reparto, nella casella di testo <b>Unità organizzativa</b>.</li> <li>d Immettere il codice di paese ISO 3166 a due lettere, ad esempio <b>IT</b>, nella casella di testo <b>Paese</b>.</li> </ul>
<b>Genera richiesta di firma</b>	<ul style="list-style-type: none"> <li>a Selezionare <b>Genera richiesta di firma</b>.</li> <li>b Verificare le voci nelle caselle di testo <b>Organizzazione</b>, <b>Unità organizzativa</b>, <b>Prefisso internazionale</b> e <b>Nome comune</b>. Queste voci vengono popolate dal certificato esistente. Se necessario, è possibile modificare queste voci.</li> <li>c Fare clic su <b>Genera CSR</b> per generare una richiesta di firma del certificato, quindi fare clic sul collegamento <b>Scarica qui la richiesta CSR generata</b> per aprire una finestra di dialogo che consente di salvare la richiesta CSR in un percorso da cui è possibile inviarla a un'autorità di certificazione.</li> <li>d Una volta ricevuto il certificato preparato, fare clic su <b>Importa</b> e seguire le istruzioni per importare un certificato in vRealize Automation.</li> </ul>
<b>Importazione</b>	<ul style="list-style-type: none"> <li>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 <b>Chiave privata RSA</b>.</li> <li>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 <b>Catena di certificati</b>. Per valori di certificati multipli, includere un'intestazione BEGIN CERTIFICATE e un piè di pagina END CERTIFICATE per ciascun certificato.</li> </ul> <p><b>Nota</b> In caso di certificati concatenati, possono essere disponibili attributi aggiuntivi.</p> <ul style="list-style-type: none"> <li>c (Facoltativo) Se il certificato utilizza una passphrase per crittografare la chiave del certificato, copiare la passphrase e incollarla nella casella di testo <b>Passphrase</b>.</li> </ul>

- 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 SSH.

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

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

- 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 Selezionare se abilitare vRealize Code Stream e immettere una licenza di vRealize Code Stream.

vRealize Code Stream non è supportato per le distribuzioni ad alta disponibilità o di produzione di vRealize Automation.

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

- 13** 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.

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

- 15** Assicurarsi che sia possibile accedere a vRealize Automation.

- a Aprire un browser Web e visitare l'URL dell'interfaccia del prodotto vRealize Automation.  
`https://vrealize-automation-appliance-FQDN/vcac`
- 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.

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

## Configurazione di istanze aggiuntive di vRealize Automation Appliance

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

Per ogni appliance vRealize Automation, è necessario abilitare 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 dell'appliance vRealize Automation 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.

## Aggiunta di un'altra appliance vRealize Automation al cluster

Per garantire l'alta disponibilità, le installazioni distribuite possono utilizzare un bilanciamento del carico davanti a un cluster di nodi dell'appliance vRealize Automation.

Utilizzare l'interfaccia di gestione nella nuova appliance vRealize Automation per aggiungerla a un cluster esistente di una o più appliance. L'operazione di unione copia le informazioni di configurazione nella nuova appliance che si sta aggiungendo, inclusi certificato, SSO, gestione licenze, database e informazioni sulla messaggistica.

È necessario aggiungere appliance a un cluster uno alla volta e non in parallelo.



## Prerequisiti

- È necessario che nel cluster siano già presenti una o più appliance vRealize Automation e che una rappresenti il nodo primario. Vedere [Configurazione della prima appliance vRealize Automation in un cluster](#).

È possibile impostare una nuova appliance come nodo primario solo dopo averla aggiunta al cluster.

- Creare il nuovo nodo dell'appliance. Vedere [Distribuzione di vRealize Automation appliance](#).
- Verificare che il bilanciamento del carico sia configurato per essere utilizzato con la nuova appliance.
- Verificare che il traffico possa passare attraverso il bilanciamento del carico per raggiungere tutti i nodi correnti e il nuovo nodo che si sta aggiungendo.
- Verificare che tutti i servizi di vRealize Automation siano avviati nei nodi correnti.

## Procedura

- 1 Accedere all'interfaccia di gestione della nuova appliance vRealize Automation come root.  
<https://vrealize-automation-appliance-FQDN:5480>  
 Continuare indipendentemente dall'eventuale visualizzazione di avvisi sui certificati.
- 2 Se viene visualizzata l'installazione guidata, annullarla per passare all'interfaccia di gestione.
- 3 Selezionare **Admin > Impostazioni ora** e impostare la stessa origine di riferimento dell'ora utilizzata dal resto delle appliance incluse nel cluster.
- 4 Selezionare **Impostazioni vRA > Cluster**.
- 5 Immettere il nome di dominio completo di un'appliance vRealize Automation configurata in precedenza nella casella di testo **Nodo di cluster iniziale**.  
 È possibile utilizzare il nome di dominio completo dell'appliance vRealize Automation primaria o di qualsiasi appliance vRealize Automation 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

Per conservare le risorse interne quando si utilizza un'istanza esterna di vRealize Orchestrator, è possibile disabilitare il servizio vRealize Orchestrator incorporato.

## Prerequisiti

### [Aggiunta di un'altra appliance vRealize Automation al cluster](#)

#### Procedura

- 1 Accedere alla console dell'appliance vRealize Automation.
- 2 Interrompere il servizio vRealize Orchestrator.

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

#### Convalida della distribuzione distribuita

Dopo aver distribuito istanze aggiuntive dell'appliance vRealize Automation, è necessario verificare di poter 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 Confermare che sia possibile accedere a vRealize Automation tramite l'indirizzo di bilanciamento del carico:

<https://vrealize-automation-appliance-load-balancer-FQDN/vcac>

- 3 Dopo avere verificato di poter accedere alla nuova appliance vRealize Automation tramite il bilanciamento del carico, riabilitare 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 dal medesimo utente con account di servizio, che deve essere un account di dominio con privilegi su ciascun server IaaS distribuito. Non utilizzare account del sistema locale.

## Prerequisiti

- [Configurazione della prima appliance vRealize Automation in un cluster.](#)
- Se il sito include più appliance vRealize Automation, [Aggiunta di un'altra appliance vRealize Automation al cluster.](#)
- Verificare che il server soddisfi i requisiti in [Server Windows IaaS.](#)
- 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 [Scaricare il programma di installazione di vRealize Automation IaaS](#)

Per installare IaaS nei server Windows fisici o virtuali distribuiti, scaricare una copia del programma di installazione di IaaS dall'appliance vRealize Automation.

### 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 del server Web IaaS aggiuntivi](#)

Il server Web fornisce l'accesso alle funzionalità dell'infrastruttura in vRealize Automation. Dopo aver installato il primo server Web è possibile aumentare le prestazioni installando server Web IaaS aggiuntivi.

### 6 [Installazione del servizio di gestione attivo](#)

Il servizio di gestione attivo è un servizio Windows che coordina la comunicazione tra Distributed Execution Manager di IaaS, il database, gli agenti, gli agenti proxy e SMTP.

### 7 [Installazione di un componente servizio di gestione di backup](#)

Il servizio di gestione di backup fornisce ridondanza e alta disponibilità e può essere avviato manualmente se il servizio attivo si arresta.

### 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.

### Operazioni successive

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

Sulle macchine Windows 2012 è necessario disattivare TLS1.2 per i certificati che utilizzano SHA512. Per ulteriori informazioni sulla disabilitazione di TLS 1.2, vedere [Articolo della Knowledge Base Microsoft 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`.

### Operazioni successive

[Scaricare il programma di installazione di vRealize Automation IaaS.](#)

### Scaricare il programma di installazione di vRealize Automation IaaS

Per installare IaaS nei server Windows fisici o virtuali distribuiti, scaricare una copia del programma di installazione di IaaS dall'appliance vRealize Automation.

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

### Prerequisiti

- [Configurazione della prima appliance vRealize Automation in un cluster](#) e facoltativamente [Aggiunta di un'altra appliance vRealize Automation al cluster](#).
- Verificare che il server soddisfi i requisiti in [Server Windows IaaS](#).
- 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 al server IaaS Windows utilizzando un account che dispone di privilegi di amministratore.
- 3 Aprire un browser Web direttamente con l'URL del programma di installazione dell'appliance vRealize Automation. Non utilizzare l'indirizzo di un bilanciamento del carico.  
`https://vrealize-automation-appliance-FQDN:5480/installer`
- 4 Fare clic sul **programma d'installazione di IaaS**.

## 5 Salvare `setup__vrealize-automation-appliance-FQDN@5480` nel server Windows.

Non modificare il nome del file del programma d'installazione. poiché viene utilizzato per collegare l'installazione all'appliance vRealize Automation.

## 6 Scaricare il file del programma d'installazione per ogni server Windows IaaS su cui si stanno installando i componenti.

### Operazioni successive

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 nel server SQL, vedere [Articolo di Microsoft Technet 189067](#).

**Tabella 1-34. 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.	<a href="#">Creazione manuale del database IaaS</a> .
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 database con privilegi di <b>dbo</b> per popolare il database.	<a href="#">Preparazione di un database vuoto</a> .
Utilizzare il programma d'installazione per creare il database. Questa è l'opzione più semplice, ma richiede l'uso dei privilegi di <b>sysadmin</b> nel programma d'installazione.	<a href="#">Creazione del database IaaS utilizzando l'installazione guidata</a> .

### Creazione manuale del database IaaS

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

### Prerequisiti

- Installare Microsoft .NET Framework 4.5.2 o versioni successive nell'host SQL Server.

- Per connettersi al database, utilizzare l'autenticazione Windows e non l'autenticazione SQL.
- Verificare i prerequisiti d'installazione del database. Vedere [Host SQL Server di IaaS](#).
- Aprire in un browser Web l'URL del programma di installazione dell'appliance vRealize Automation, quindi scaricare gli script di installazione del database IaaS.

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

**Tabella 1-35. 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.

**Tabella 1-35. Valori del database (Continua)**

Variabile	Valore
<i>Web_user</i>	Nome utente utilizzato per l'esecuzione dei servizi Web.
<i>version_string</i>	Versione di vRealize Automation, trovata accedendo all'appliance vRealize Automation e facendo clic sulla scheda Aggiorna. Ad esempio, la stringa della versione 6.1 di vRealize Automation è 6.1.0.1200.

Il database è stato creato.

### Operazioni successive

[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 IaaS in un database vuoto. Questo metodo d'installazione fornisce il massimo controllo sulla sicurezza del database.

### Prerequisiti

- Verificare i prerequisiti d'installazione del database. Vedere [Host SQL Server di IaaS](#).
- Aprire in un browser Web l'URL del programma di installazione dell'appliance vRealize Automation, quindi scaricare gli script di installazione del database IaaS.

<https://vrealize-automation-appliance-FQDN: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 Aprire in modifica i seguenti file e sostituire tutte le istanze delle variabili elencate nella tabella con i valori correlati al proprio ambiente.

```
CreateDatabase.sql
SetDatabaseSettings.sql
```



**Tabella 1-36. 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 SetDatabaseSettings.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 In coda al contenuto di CreateDatabase.sql, incollare l'intero contenuto modificato di SetDatabaseSettings.sql.
- 11 Fare clic su **Esegui**.

Viene eseguito lo script e creato il database.

#### Operazioni successive

[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.
- [Scaricare il programma di installazione di vRealize Automation IaaS.](#)

## Procedura

- 1 Fare clic con il pulsante destro del mouse sul file d'installazione `setup__vrealize-automation-appliance-FQDN@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 dell'appliance vRealize Automation e verificare il certificato SSL.

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

Questa è la password che è stata immessa durante la distribuzione dell'appliance vRealize Automation.

- b Selezionare **Accetta certificato**.

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

Confrontare l'identificazione personale del certificato con quella impostata per l'appliance vRealize Automation. È possibile visualizzare il certificato dell'appliance vRealize Automation nel browser client quando si accede alla console di gestione tramite la 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.

Anche in una distribuzione distribuita, in alcuni casi è possibile installare più componenti di IaaS nello stesso server Windows.

Se si installano più componenti di IaaS, installarli sempre nello stesso percorso.

- 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 prima configurare il protocollo SSL sul server SQL per supportare l'opzione. Per ulteriori informazioni sulla configurazione di SSL in SQL Server, vedere [Articolo di Microsoft Technet 189067](#).

**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 **User 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.

È consigliata l'autenticazione Windows. Quando si seleziona l'autenticazione SQL, in alcuni file di configurazione viene visualizzata la password del database senza crittografia.

**16** Fare clic su **Avanti**.**17** Completare il Controllo prerequisiti.

Opzione	Descrizione
Nessun errore	Fare clic su <b>Avanti</b> .
Errori non critici	Fare clic su <b>Bypass</b> .
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 <b>Controlla di nuovo</b> 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 sono stati già installati altri componenti IaaS, procurarsi la passphrase creata per il database.
- Se nell'ambiente si utilizzano bilanciamenti del carico, verificare che questi soddisfino i requisiti di configurazione.

## Procedura

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

Il server Web IaaS si installa per fornire l'accesso alle funzionalità dell'infrastruttura in vRealize Automation.

### 2 [Configurazione di Model Manager Data](#)

Il componente Model Manager viene installato sulla stessa macchina che ospita il primo componente del server 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 del server Web IaaS aggiuntivi](#) o [Installazione del servizio di gestione attivo](#).

## Installazione del primo componente del server Web di IaaS

Il server Web IaaS si installa per fornire l'accesso alle funzionalità dell'infrastruttura in vRealize Automation.

È possibile installare più server Web IaaS, ma solo il primo include Model Manager Data.

## Prerequisiti

- [Creazione del database IaaS utilizzando l'installazione guidata](#).
- Verificare che il server soddisfi i requisiti in [Server Windows IaaS](#).
- Se sono stati già installati altri componenti IaaS, assicurarsi di essere a conoscenza della passphrase del database creata.
- Se nell'ambiente si utilizzano bilanciamenti del carico, verificare che questi soddisfino i requisiti di configurazione.

## Procedura

- 1 Se si utilizza un bilanciamento del carico, disabilitare gli altri nodi sotto al bilanciamento del carico e verificare che il traffico sia indirizzato al nodo desiderato.

Disabilitare inoltre i controlli di integrità del bilanciamento del carico fino a quando tutti i componenti di vRealize Automation non sono installati e configurati.

- 2 Fare clic con il pulsante destro del mouse sul file d'installazione `setup__vrealize-automation-appliance-FQDN@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 dell'appliance vRealize Automation e verificare il certificato SSL.

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

Questa è la password che è stata immessa durante la distribuzione dell'appliance vRealize Automation.

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

Confrontare l'identificazione personale del certificato con quella impostata per l'appliance vRealize Automation. È possibile visualizzare il certificato dell'appliance vRealize Automation nel browser client quando si accede alla console di gestione tramite la 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.

Anche in una distribuzione distribuita, in alcuni casi è possibile installare più componenti di IaaS nello stesso server Windows.

Se si installano più componenti di IaaS, installarli sempre nello stesso percorso.

- 10 Fare clic su **Avanti**.

- 11 Selezionare **Sito Web** e **ModelManagerData** 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.

## Configurazione di Model Manager Data

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

### Prerequisiti

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

### Procedura

**1** Fare clic sulla scheda **Model Manager Data**.

**2** Nella casella di testo **Server**, immettere il nome di dominio completo dell'appliance vRealize Automation.

*vrealize-automation-appliance.società.com*

Non immettere l'indirizzo IP.

**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 Digitare **administrator@vsphere.local** nella casella di testo **Nome utente** e nelle caselle di testo **Password** e **Conferma** immettere la password creata durante la configurazione di SSO.
- 8 (Facoltativo) Fare clic su **Prova** per verificare le credenziali.
- 9 Nella casella di testo **Server IaaS**, individuare il componente del server Web IaaS.

Opzione	Descrizione
<b>Senza bilanciamento del carico</b>	Specificare il nome di dominio completo e il numero di porta del bilanciamento del carico del componente del server Web IaaS, <i>web-load-balancer.società.com:443</i> . Non immettere indirizzi IP.
<b>Con bilanciamento del carico</b>	Specificare il nome di dominio completo e il numero di porta della macchina su cui è stato installato il componente del server Web IaaS, <i>web.società.com:443</i> . Non immettere indirizzi IP.

La porta predefinita è 443.

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

Opzione	Descrizione
<b>Nessun errore</b>	Fare clic su <b>Avanti</b> .
<b>Errori non critici</b>	Fare clic su <b>Bypass</b> .
<b>Errori critici</b>	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 <b>Controlla di nuovo</b> per verificare.

- 13 Nella pagina Impostazioni server e account, nelle caselle di testo **Informazioni sull'installazione del server**, inserire il nome utente e la password dell'utente dell'account del servizio con privilegi amministrativi per il server d'installazione corrente.

L'utente dell'account del servizio deve essere un account di dominio con privilegi in ciascun server IaaS distribuito. Non utilizzare account del sistema locale.

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

Opzione	Descrizione
<b>Se sono già stati installati componenti in questo ambiente</b>	Immettere la passphrase precedentemente creata nelle caselle di testo <b>Passphrase</b> e <b>Conferma</b> .
<b>Se questa è la prima installazione</b>	Immettere una passphrase nelle caselle di testo <b>Passphrase</b> e <b>Conferma</b> . 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**.

#### Operazioni successive

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

#### Installazione di componenti del server Web IaaS aggiuntivi

Il server Web fornisce l'accesso alle funzionalità dell'infrastruttura in vRealize Automation. Dopo aver installato il primo server Web è possibile aumentare le prestazioni installando server Web IaaS aggiuntivi.

Non installare Model Manager Data con un componente del server Web aggiuntivo. Solo il primo componente del server Web ospita Model Manager Data.

#### Prerequisiti

- [Installazione di un componente sito Web di IaaS e di Model Manager Data](#).
- Verificare che il nuovo server soddisfi i requisiti in [Server Windows IaaS](#).
- Utilizzare l'interfaccia di gestione dell'appliance vRealize Automation per sostituire il certificato per includere il nome di dominio completo del nuovo nodo. Vedere [Replace Certificates in the vRealize Automation Appliance](#).
- Se sono stati già installati altri componenti IaaS, procurarsi la passphrase creata per il database.
- Se nell'ambiente si utilizzano bilanciamenti del carico, verificare che questi soddisfino i requisiti di configurazione.

#### Procedura

- 1 Se si utilizza un bilanciamento del carico, disabilitare gli altri nodi sotto al bilanciamento del carico e verificare che il traffico sia indirizzato al nodo desiderato.  
  
Disabilitare inoltre i controlli di integrità del bilanciamento del carico fino a quando tutti i componenti di vRealize Automation non sono installati e configurati.
- 2 Fare clic con il pulsante destro del mouse sul file d'installazione `setup__vrealize-automation-appliance-FQDN@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 dell'appliance vRealize Automation e verificare il certificato SSL.

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

Questa è la password che è stata immessa durante la distribuzione dell'appliance vRealize Automation.

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

Confrontare l'identificazione personale del certificato con quella impostata per l'appliance vRealize Automation. È possibile visualizzare il certificato dell'appliance vRealize Automation nel browser client quando si accede alla console di gestione tramite la 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.

Anche in una distribuzione distribuita, in alcuni casi è possibile installare più componenti di IaaS nello stesso server Windows.

Se si installano più componenti di IaaS, installarli sempre nello stesso percorso.

- 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** Nella casella di testo **Server IaaS**, identificare il primo componente del server Web IaaS.

Opzione	Descrizione
<b>Senza bilanciamento del carico</b>	Specificare il nome di dominio completo e il numero di porta del bilanciamento del carico del componente del server Web IaaS, <i>web-load-balancer.società.com:443</i> . Non immettere indirizzi IP.
<b>Con bilanciamento del carico</b>	Specificare il nome di dominio completo e il numero di porta della macchina su cui è stato installato il primo componente del server Web IaaS, <i>web.società.com:443</i> . Non immettere indirizzi IP.

La porta predefinita è 443.

- 19** Fare clic su **Prova** per verificare la connessione con il server.
- 20** Fare clic su **Avanti**.
- 21** Completare il Controllo prerequisiti.

Opzione	Descrizione
<b>Nessun errore</b>	Fare clic su <b>Avanti</b> .
<b>Errori non critici</b>	Fare clic su <b>Bypass</b> .
<b>Errori critici</b>	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 <b>Controlla di nuovo</b> per verificare.

- 22** Nella pagina Impostazioni server e account, nelle caselle di testo **Informazioni sull'installazione del server**, inserire il nome utente e la password dell'utente dell'account del servizio con privilegi amministrativi per il server d'installazione corrente.

L'utente dell'account del servizio deve essere un account di dominio con privilegi in ciascun server IaaS distribuito. Non utilizzare account del sistema locale.

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

Opzione	Descrizione
<b>Se sono già stati installati componenti in questo ambiente</b>	Immettere la passphrase precedentemente creata nelle caselle di testo <b>Passphrase</b> e <b>Conferma</b> .
<b>Se questa è la prima installazione</b>	Immettere una passphrase nelle caselle di testo <b>Passphrase</b> e <b>Conferma</b> . 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**.

#### Operazioni successive

[Installazione del servizio di gestione attivo.](#)

#### Installazione del servizio di gestione attivo

Il servizio di gestione attivo è un servizio Windows che coordina la comunicazione tra Distributed Execution Manager di IaaS, il database, gli agenti, gli agenti proxy e SMTP.

A meno che non si abiliti il failover automatico del servizio di gestione, la distribuzione IaaS richiede che tale servizio venga eseguito attivamente su una sola macchina Windows per volta. Sulle macchine di backup il servizio deve essere interrotto e configurato per l'avvio manuale.

Vedere [Informazioni sul failover automatico del servizio di gestione](#).

#### Prerequisiti

- Se sono stati già installati altri componenti IaaS, procurarsi la passphrase creata per il database.
- (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.
- 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 Se si utilizza un bilanciamento del carico, disabilitare gli altri nodi sotto al bilanciamento del carico e verificare che il traffico sia indirizzato al nodo desiderato.

Disabilitare inoltre i controlli di integrità del bilanciamento del carico fino a quando tutti i componenti di vRealize Automation non sono installati e configurati.

- 2 Fare clic con il pulsante destro del mouse sul file d'installazione `setup__vrealize-automation-appliance-FQDN@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 dell'appliance vRealize Automation e verificare il certificato SSL.
  - a Specificare il nome utente, ovvero **root**, e la password.  
Questa è la password che è stata immessa durante la distribuzione dell'appliance vRealize Automation.
  - b Selezionare **Accetta certificato**.
  - c Fare clic su **Visualizza certificato**.

Confrontare l'identificazione personale del certificato con quella impostata per l'appliance vRealize Automation. È possibile visualizzare il certificato dell'appliance vRealize Automation nel browser client quando si accede alla console di gestione tramite la 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.

Anche in una distribuzione distribuita, in alcuni casi è possibile installare più componenti di IaaS nello stesso server Windows.

Se si installano più componenti di IaaS, installarli sempre nello stesso percorso.

- 9 Fare clic su **Avanti**.
- 10 Selezionare **Servizio di gestione** nella pagina **Installazione personalizzata server IaaS**.

- 11 Nella casella di testo **Server IaaS**, individuare il componente del server Web IaaS.

Opzione	Descrizione
<b>Senza bilanciamento del carico</b>	Specificare il nome di dominio completo e il numero di porta del bilanciamento del carico del componente del server Web IaaS, <i>web-load-balancer.società.com:443</i> . Non immettere indirizzi IP.
<b>Con bilanciamento del carico</b>	Specificare il nome di dominio completo e il numero di porta della macchina su cui è stato installato il componente del server Web IaaS, <i>web.società.com:443</i> . Non immettere indirizzi IP.

La porta predefinita è 443.

- 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 Nella pagina Impostazioni server e account, nelle caselle di testo **Informazioni sull'installazione del server**, inserire il nome utente e la password dell'utente dell'account del servizio con privilegi amministrativi per il server d'installazione corrente.

L'utente dell'account del servizio deve essere un account di dominio con privilegi in ciascun server IaaS distribuito. Non utilizzare account del sistema locale.

- 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 <b>Passphrase</b> e <b>Conferma</b> .
Se questa è la prima installazione	Immettere una passphrase nelle caselle di testo <b>Passphrase</b> e <b>Conferma</b> . 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**.

#### Operazioni successive

- 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

Il servizio di gestione di backup fornisce ridondanza e alta disponibilità e può essere avviato manualmente se il servizio attivo si arresta.

A meno che non si abiliti il failover automatico del servizio di gestione, la distribuzione IaaS richiede che tale servizio venga eseguito attivamente su una sola macchina Windows per volta. Sulle macchine di backup il servizio deve essere interrotto e configurato per l'avvio manuale.

Vedere [Informazioni sul failover automatico del servizio di gestione](#).

#### Prerequisiti

- Se sono stati già installati altri componenti IaaS, procurarsi la passphrase creata per il database.
- (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.

- Utilizzare l'interfaccia di gestione dell'appliance vRealize Automation per sostituire il certificato per includere il nome di dominio completo del nuovo nodo. Vedere [Replace Certificates in the vRealize Automation Appliance](#).
- 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 Se si utilizza un bilanciamento del carico, disabilitare gli altri nodi sotto al bilanciamento del carico e verificare che il traffico sia indirizzato al nodo desiderato.

Disabilitare inoltre i controlli di integrità del bilanciamento del carico fino a quando tutti i componenti di vRealize Automation non sono installati e configurati.

- 2 Fare clic con il pulsante destro del mouse sul file d'installazione `setup__vrealize-automation-appliance-FQDN@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 dell'appliance vRealize Automation e verificare il certificato SSL.
  - a Specificare il nome utente, ovvero **root**, e la password.  
Questa è la password che è stata immessa durante la distribuzione dell'appliance vRealize Automation.
  - b Selezionare **Accetta certificato**.
  - c Fare clic su **Visualizza certificato**.  
Confrontare l'identificazione personale del certificato con quella impostata per l'appliance vRealize Automation. È possibile visualizzare il certificato dell'appliance vRealize Automation nel browser client quando si accede alla console di gestione tramite la 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.

Anche in una distribuzione distribuita, in alcuni casi è possibile installare più componenti di IaaS nello stesso server Windows.

Se si installano più componenti di IaaS, installarli sempre nello stesso percorso.

- 10 Fare clic su **Avanti**.
- 11 Selezionare **Servizio di gestione** nella pagina **Installazione personalizzata server IaaS**.
- 12 Nella casella di testo **Server IaaS**, individuare il componente del server Web IaaS.

Opzione	Descrizione
<b>Senza bilanciamento del carico</b>	Specificare il nome di dominio completo e il numero di porta del bilanciamento del carico del componente del server Web IaaS, <i>web-load-balancer.società.com:443</i> . Non immettere indirizzi IP.
<b>Con bilanciamento del carico</b>	Specificare il nome di dominio completo e il numero di porta della macchina su cui è stato installato il componente del server Web IaaS, <i>web.società.com:443</i> . Non immettere indirizzi IP.

La porta predefinita è 443.

- 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 Nella pagina Impostazioni server e account, nelle caselle di testo **Informazioni sull'installazione del server**, inserire il nome utente e la password dell'utente dell'account del servizio con privilegi amministrativi per il server d'installazione corrente.

L'utente dell'account del servizio deve essere un account di dominio con privilegi in ciascun server IaaS distribuito. Non utilizzare account del sistema locale.



- 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 <b>Passphrase</b> e <b>Conferma</b> .
Se questa è la prima installazione	Immettere una passphrase nelle caselle di testo <b>Passphrase</b> e <b>Conferma</b> . 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**.

#### Operazioni successive

- 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 [Host Distributed Execution Manager di IaaS](#).

### Installazione dei Distributed Execution Manager

È necessario installare 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

[Scaricare il programma di installazione di vRealize Automation IaaS](#).

### Procedura

- 1 Fare clic con il pulsante destro del mouse sul file d'installazione `setup__vrealize-automation-appliance-FQDN@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 dell'appliance vRealize Automation e verificare il certificato SSL.
  - a Specificare il nome utente, ovvero **root**, e la password.

Questa è la password che è stata immessa durante la distribuzione dell'appliance vRealize Automation.
  - b Selezionare **Accetta certificato**.
  - c Fare clic su **Visualizza certificato**.

Confrontare l'identificazione personale del certificato con quella impostata per l'appliance vRealize Automation. È possibile visualizzare il certificato dell'appliance vRealize Automation nel browser client quando si accede alla console di gestione tramite la 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.

Anche in una distribuzione distribuita, in alcuni casi è possibile installare più componenti di IaaS nello stesso server Windows.

Se si installano più componenti di IaaS, installarli sempre nello stesso percorso.

- 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.

L'account del servizio deve avere privilegi di amministratore locale e deve essere l'account di dominio utilizzato durante l'installazione di IaaS. L'account del servizio ha privilegi su ciascun server IaaS distribuito e non deve essere un account di sistema locale.

- 12 Fare clic su **Avanti**.
- 13 Selezionare il tipo di installazione dal menu a discesa **Ruolo DEM**.

Opzione	Descrizione
<b>Worker</b>	Il Worker si occupa di eseguire i workflow.
<b>Orchestrator</b>	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**.
- 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
<b>Senza bilanciamento del carico</b>	Inserire il nome di dominio completo e il numero di porta dell'unità di bilanciamento del carico del componente del servizio di gestione e il server Web che ospita Model Manager, <i>mgr-svc-load-balancer.mycompany.com:443</i> e <i>web-load-balancer.mycompany.com:443</i> . Non immettere indirizzi IP.
<b>Con bilanciamento del carico</b>	Inserire il nome di dominio completo e il numero di porta della macchina su cui è stato installato il componente del servizio di gestione e il server Web che ospita Model Manager, <i>mgr-svc.mycompany.com:443</i> e <i>web.mycompany.com:443</i> . Non immettere indirizzi IP.

La porta predefinita è 443.

- 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**.

#### Operazioni successive

- 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 diverso

Per impostazione predefinita, il file di configurazione di DEM Worker utilizza il percorso di installazione predefinito della console di Microsoft System Center Virtual Machine Manager (SCVMM). Se si installa la console di SCVMM in una posizione non predefinita, è necessario aggiornare il file.

Questa procedura è necessaria soltanto se si dispone di endpoint e agenti SCVMM.

#### Prerequisiti

- Conoscere il percorso non predefinito in cui è installata la console di SCVMM.  
Quello seguente è il percorso predefinito che è necessario sostituire nel file di configurazione.  
`path="{ProgramFiles}\Microsoft System Center 2012 R2\Virtual Machine Manager\bin"`

#### Procedura

- 1 Arrestare servizio il DEM Worker.
- 2 Aprire il seguente file in un editor di testo.  
`Programmi (x86)\VMware\vCAC\Distributed Execution Manager\instance-name\DynamicOps.DEM.exe.config`
- 3 Individuare la sezione `<assemblyLoadConfiguration>`.
- 4 Aggiornare ciascun percorso, utilizzando i seguenti esempi come linee guida.

```
<assemblyLoadConfiguration>
  <assemblies>
    <!-- List of required assemblies for Scvmm -->
    <add name="Errors" path="D:\Microsoft System Center 2012 R2\Virtual Machine Manager\bin"/>
    <add name="Microsoft.SystemCenter.VirtualMachineManager" path="D:\Microsoft System Center 2012 R2\Virtual Machine Manager\bin"/>
    <add name="Remoting" path="D:\Microsoft System Center 2012 R2\Virtual Machine Manager\bin"/>
```

```
<add name="TraceWrapper" path="D:\Microsoft System Center 2012 R2\Virtual Machine Manager\bin"/>
<add name="Utils" path="D:\Microsoft System Center 2012 R2\Virtual Machine Manager\bin"/>
</assemblies>
</assemblyLoadConfiguration>
```

5 Salvare e chiudere `DynamicOps.DEM.exe.config`.

6 Riavviare il servizio DEM Worker.

Per ulteriori informazioni, vedere [DEM Worker con SCVMM](#).

Informazioni aggiuntive sulla preparazione dell'ambiente SCVMM e la creazione di un endpoint di SCVMM sono disponibili in [Preparazione dell'ambiente SCVMM](#) e [Creazione di un endpoint di Hyper-V \(SCVMM\)](#).

### 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 del servizio Windows che accede al database, anche se quest'ultimo è stato creato utilizzando l'autenticazione SQL. È possibile cambiare l'autenticazione runtime da Windows a SQL.

Un motivo per cambiare l'autenticazione runtime, ad esempio, può essere il fatto che il database si trovi un dominio non attendibile.

#### Prerequisiti

Verificare che esista il database SQL Server vRealize Automation. Iniziare con [Scelta di uno scenario di database IaaS](#).

#### Procedura

- 1 Utilizzare un account con privilegi di amministratore per accedere al server IaaS Windows che ospita il servizio di gestione.
- 2 In **Strumenti amministrativi > Servizi**, arrestare il servizio **VMware vCloud Automation Center**.
- 3 Aprire i seguenti file in un editor di testo.

```
C:\Program Files (x86)\VMware\VCAC\Server\ManagerService.exe.config
C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Web\Web.config
```

- 4 Individuare la sezione <connectionStrings> in ciascun file.

- 5 Sostituire

Integrated Security=True;

con

User Id=database-nomeutente;Password=database-password;

- 6 Salvare e chiudere i file.

```
ManagerService.exe.config
Web.config
```

- 7 Avviare il servizio **VMware vCloud Automation Center**.

- 8 Utilizzare il comando `iisreset` per riavviare IIS.

## 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 di vRealize Automation

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.

Per ulteriori informazioni sui criteri di esecuzione di PowerShell, vedere [Articolo di Microsoft PowerShell sui criteri di esecuzione](#). Se i criteri di esecuzione di PowerShell sono gestiti a livello di criteri di gruppo, contattare l'assistenza IT per chiedere informazioni sulle limitazioni relative alle modifiche dei criteri e vedere [Articolo di Microsoft PowerShell sulle impostazioni di Criteri di gruppo](#).

### Prerequisiti

- 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 Utilizzando un account amministratore, accedere alla macchina host IaaS in cui è installato l'agente.
- 2 Scegliere **Start > Tutti i programmi > Windows PowerShell versione > Windows PowerShell**.
- 3 Per RemoteSigned, eseguire `Set-ExecutionPolicy RemoteSigned`.
- 4 Per Unrestricted, eseguire `Set-ExecutionPolicy Unrestricted`.
- 5 Verificare che il comando non restituisca errori.
- 6 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.

**Tabella 1-37. 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.	<a href="#">Installazione e configurazione dell'agente proxy per vSphere</a>
Provisioning di macchine virtuali tramite l'integrazione con un ambiente Microsoft Hyper-V Server.	<a href="#">Installazione dell'agente proxy per Hyper-V o XenServer</a>
Provisioning di macchine virtuali tramite l'integrazione con un ambiente XenServer.	<ul style="list-style-type: none"> <li>■ <a href="#">Installazione dell'agente proxy per Hyper-V o XenServer</a></li> <li>■ <a href="#">Installazione dell'agente EPI per Citrix</a></li> </ul>
Provisioning di macchine virtuali tramite l'integrazione con un ambiente XenDesktop.	<ul style="list-style-type: none"> <li>■ <a href="#">Installazione dell'agente VDI per XenDesktop</a></li> <li>■ <a href="#">Installazione dell'agente EPI per Citrix</a></li> </ul>



**Tabella 1-37. Scelta dello scenario per un agente (Continua)**

Scenario di integrazione	Requisiti dell'agente e procedura
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.	<a href="#">Installazione dell'agente EPI per Visual Basic Scripting</a>
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.	<a href="#">Installazione dell'agente WMI per le richieste WMI remote</a>
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.

Nella seguente tabella sono elencate le autorizzazioni che le credenziali dell'endpoint vSphere devono possedere per gestire un'istanza di vCenter Server. Le autorizzazioni devono essere abilitate per tutti i cluster in vCenter Server, non solo per quelli che fungeranno da host per gli endpoint.

**Tabella 1-38. Autorizzazioni richieste per consentire all'agente di vSphere di gestire l'istanza di vCenter Server**

Valore attributo		Autorizzazione
Datastore		Spazio allocato
		Sfoggia datastore
Datastore cluster		Configurazione di un datastore cluster
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
		Sposta
		Rimuovi
	Interazione	Configura supporto CD
		Interazione console
		Connessione dispositivo
		Spegni
		Accendi
		Reimposta
		Sospendi
		Installazione strumenti
	Configurazione	Aggiungi disco esistente
		Aggiungi nuovo disco
		Aggiungi o rimuovi dispositivo
		Rimuovi disco
		Avanzate
		Cambia numero CPU
		Cambia risorsa
		Estendi disco virtuale
		Traccia cambiamenti disco

**Tabella 1-38. Autorizzazioni richieste per consentire all'agente di vSphere di gestire l'istanza di vCenter Server (Continua)**

Valore attributo	Autorizzazione
Provisioning	Memoria
	Modifica impostazioni dispositivo
	Rinomina
	Imposta annotazione (versione 5.0 e successive)
	Impostazioni
	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

- Installare IaaS, compreso il server Web e l'host del servizio di gestione.
- Verificare che il computer in cui si installa l'agente si trovi in un dominio attendibile per il dominio in cui sono installati i componenti IaaS.
- Verificare che i requisiti in [Requisiti dell'agente di vSphere](#) siano soddisfatti.
- Se è già stato creato un endpoint di vSphere da utilizzare con questo agente, prendere nota del nome dell'endpoint.
- [Scaricare il programma di installazione di vRealize Automation IaaS.](#)

## Procedura

- 1 Fare clic con il pulsante destro del mouse sul file d'installazione `setup__vrealize-automation-appliance-FQDN@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 dell'appliance vRealize Automation e verificare il certificato SSL.
  - a Specificare il nome utente, ovvero **root**, e la password.

Questa è la password che è stata immessa durante la distribuzione dell'appliance vRealize Automation.
  - b Selezionare **Accetta certificato**.
  - c Fare clic su **Visualizza certificato**.

Confrontare l'identificazione personale del certificato con quella impostata per l'appliance vRealize Automation. È possibile visualizzare il certificato dell'appliance vRealize Automation nel browser client quando si accede alla console di gestione tramite la porta 5480.
- 5 Selezionare **Installazione personalizzata** nella pagina Tipo di installazione.
- 6 Nell'area Selezione componenti, selezionare **Agenti proxy**.
- 7 Accettare la posizione d'installazione radice o fare clic su **Cambia** e selezionare un percorso d'installazione diverso.

Anche in una distribuzione distribuita, in alcuni casi è possibile installare più componenti di IaaS nello stesso server Windows.

Se si installano più componenti di IaaS, installarli sempre nello stesso percorso.
- 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** Per l'alta disponibilità, è possibile aggiungere agenti ridondanti e configurarli in modo identico. Altrimenti, mantenere gli agenti univoci.

Opzione	Descrizione
<b>Agente ridondante</b>	Installare gli agenti ridondanti su server diversi. Denominare e configurare gli agenti ridondanti in modo identico.
<b>Agente autonomo</b>	Assegnare un nome univoco all'agente.

**13** Configurare una connessione all'host del servizio di gestione di IaaS.

Opzione	Descrizione
<b>Senza bilanciamento del carico</b>	Specificare il nome di dominio completo e il numero di porta del bilanciamento del carico relativo al componente servizio di gestione, <i>mgr-svc-load-balancer.società.com:443</i> . Non immettere indirizzi IP.
<b>Con bilanciamento del carico</b>	Specificare il nome di dominio completo e il numero di porta della macchina su cui è stato installato il componente servizio di gestione, <i>mgr-svc.società.com:443</i> . Non immettere indirizzi IP.

La porta predefinita è 443.

**14** Configurare una connessione al server Web IaaS.

Opzione	Descrizione
<b>Senza bilanciamento del carico</b>	Specificare il nome di dominio completo e il numero di porta del bilanciamento del carico del componente del server Web, <i>web-load-balancer.società.com:443</i> . Non immettere indirizzi IP.
<b>Con bilanciamento del carico</b>	Specificare il nome di dominio completo e il numero di porta della macchina su cui è stato installato il componente del server Web, <i>web.società.com:443</i> . Non immettere indirizzi IP.

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 agenti multipli con configurazioni differenti e un endpoint sullo stesso sistema.

## Operazioni successive

### Configurazione dell'agente di vSphere.

#### Configurazione dell'agente di vSphere

Configurare l'agente di vSphere nell'ambito della preparazione per la creazione e l'utilizzo di endpoint vSphere nei blueprint vRealize Automation.

Utilizzare l'utilità agente proxy per modificare le porzioni crittografate del file di configurazione dell'agente o per cambiare il criterio di eliminazione delle macchine per le piattaforme di virtualizzazione. Il file di configurazione dell'agente `VRMAgent.exe.config` è solo parzialmente crittografato. Ad esempio, la sezione `serviceConfiguration` non è crittografata.

#### Prerequisiti

Utilizzare un account con privilegi di amministratore per accedere al server IaaS Windows in cui si è installato l'agente di vSphere.

#### Procedura

**1** Aprire un prompt dei comandi di Windows come amministratore.

**2** Passare alla cartella di installazione dell'agente, dove la cartella *nome-agente* è quella contenente l'agente vSphere.

```
cd %SystemDrive%\Program Files (x86)\VMware\VCAC\Agents\nome-agente
```

**3** (Facoltativo) Per visualizzare le impostazioni di configurazione correnti, immettere il comando seguente.

```
DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config get
```

L'esempio seguente mostra un output del comando.

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

**4** (Facoltativo) Per cambiare il nome dell'endpoint configurato durante l'installazione, utilizzare il comando seguente

```
set managementEndpointName
```

Ad esempio: `DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set managementEndpointName mio-endpoint`

Utilizzando questa proprietà è possibile rinominare l'endpoint all'interno di vRealize Automation invece di cambiare gli endpoint.

- 5 (Facoltativo) Per configurare il criterio di eliminazione della macchina virtuale, utilizzare il comando seguente.

`set doDeletes`

Ad esempio: `DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set doDeletes false`

Opzione	Descrizione
<b>true</b>	(Predefinito) Le macchine virtuali eliminate in vRealize Automation da vCenter Server vengono cancellate.
<b>false</b>	Le macchine virtuali eliminate in vRealize Automation vengono spostate nella directory VRMDeleted in vCenter Server.

- 6 Aprire **Strumenti di amministrazione > Servizi** e riavviare il servizio vRealize Automation Agente – *nome-agente*.

#### Operazioni successive

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

- Installare IaaS, compreso il server Web e l'host del servizio di gestione.
- [Scaricare il programma di installazione di vRealize Automation 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__vrealize-automation-appliance-FQDN@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 dell'appliance vRealize Automation e verificare il certificato SSL.

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

Questa è la password che è stata immessa durante la distribuzione dell'appliance vRealize Automation.

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

Confrontare l'identificazione personale del certificato con quella impostata per l'appliance vRealize Automation. È possibile visualizzare il certificato dell'appliance vRealize Automation nel browser client quando si accede alla console di gestione tramite la 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.

Anche in una distribuzione distribuita, in alcuni casi è possibile installare più componenti di IaaS nello stesso server Windows.

Se si installano più componenti di IaaS, installarli sempre nello stesso percorso.

- 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** Per l'alta disponibilità, è possibile aggiungere agenti ridondanti e configurarli in modo identico. Altrimenti, mantenere gli agenti univoci.

---

Opzione	Descrizione
<b>Agente ridondante</b>	Installare gli agenti ridondanti su server diversi. Denominare e configurare gli agenti ridondanti in modo identico.
<b>Agente autonomo</b>	Assegnare un nome univoco all'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 all'host del servizio di gestione di IaaS.

Opzione	Descrizione
<b>Senza bilanciamento del carico</b>	Specificare il nome di dominio completo e il numero di porta del bilanciamento del carico relativo al componente servizio di gestione, <i>mgr-svc-load-balancer.società.com:443</i> . Non immettere indirizzi IP.
<b>Con bilanciamento del carico</b>	Specificare il nome di dominio completo e il numero di porta della macchina su cui è stato installato il componente servizio di gestione, <i>mgr-svc.società.com:443</i> . Non immettere indirizzi IP.

La porta predefinita è 443.

- 15 Configurare una connessione al server Web IaaS.

Opzione	Descrizione
<b>Senza bilanciamento del carico</b>	Specificare il nome di dominio completo e il numero di porta del bilanciamento del carico del componente del server Web, <i>web-load-balancer.società.com:443</i> . Non immettere indirizzi IP.
<b>Con bilanciamento del carico</b>	Specificare il nome di dominio completo e il numero di porta della macchina su cui è stato installato il componente del server Web, <i>web.società.com:443</i> . Non immettere indirizzi IP.

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.

## Operazioni successive

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
```

### Operazioni successive

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

- Installare IaaS, compreso il server Web e l'host del servizio di gestione.
- Verificare che i requisiti in [Requisiti di XenDesktop](#) siano soddisfatti.
- [Scaricare il programma di installazione di vRealize Automation IaaS](#).

## Procedura

- 1 Fare clic con il pulsante destro del mouse sul file d'installazione `setup__vrealize-automation-appliance-FQDN@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 dell'appliance vRealize Automation e verificare il certificato SSL.
  - a Specificare il nome utente, ovvero **root**, e la password.

Questa è la password che è stata immessa durante la distribuzione dell'appliance vRealize Automation.
  - b Selezionare **Accetta certificato**.
  - c Fare clic su **Visualizza certificato**.

Confrontare l'identificazione personale del certificato con quella impostata per l'appliance vRealize Automation. È possibile visualizzare il certificato dell'appliance vRealize Automation nel browser client quando si accede alla console di gestione tramite la 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.

Anche in una distribuzione distribuita, in alcuni casi è possibile installare più componenti di IaaS nello stesso server Windows.

Se si installano più componenti di IaaS, installarli sempre nello stesso percorso.
- 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** Per l'alta disponibilità, è possibile aggiungere agenti ridondanti e configurarli in modo identico. Altrimenti, mantenere gli agenti univoci.

Opzione	Descrizione
<b>Agente ridondante</b>	Installare gli agenti ridondanti su server diversi. Denominare e configurare gli agenti ridondanti in modo identico.
<b>Agente autonomo</b>	Assegnare un nome univoco all'agente.

**14** Configurare una connessione all'host del servizio di gestione di IaaS.

Opzione	Descrizione
<b>Senza bilanciamento del carico</b>	Specificare il nome di dominio completo e il numero di porta del bilanciamento del carico relativo al componente servizio di gestione, <i>mgr-svc-load-balancer.società.com:443</i> . Non immettere indirizzi IP.
<b>Con bilanciamento del carico</b>	Specificare il nome di dominio completo e il numero di porta della macchina su cui è stato installato il componente servizio di gestione, <i>mgr-svc.società.com:443</i> . Non immettere indirizzi IP.

La porta predefinita è 443.

**15** Configurare una connessione al server Web IaaS.

Opzione	Descrizione
<b>Senza bilanciamento del carico</b>	Specificare il nome di dominio completo e il numero di porta del bilanciamento del carico del componente del server Web, <i>web-load-balancer.società.com:443</i> . Non immettere indirizzi IP.
<b>Con bilanciamento del carico</b>	Specificare il nome di dominio completo e il numero di porta della macchina su cui è stato installato il componente del server Web, <i>web.società.com:443</i> . Non immettere indirizzi IP.

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 agenti multipli con configurazioni differenti e un endpoint sullo stesso sistema.

### Operazioni successive

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

- Installare IaaS, compreso il server Web e l'host del servizio di gestione.
- Verificare che i requisiti in [Requisiti di Citrix Provisioning Server](#) siano soddisfatti.
- [Scaricare il programma di installazione di vRealize Automation IaaS](#).

### Procedura

- 1 Fare clic con il pulsante destro del mouse sul file d'installazione `setup__vrealize-automation-appliance-FQDN@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 dell'appliance vRealize Automation e verificare il certificato SSL.
  - a Specificare il nome utente, ovvero **root**, e la password.  
 Questa è la password che è stata immessa durante la distribuzione dell'appliance vRealize Automation.
  - b Selezionare **Accetta certificato**.
  - c Fare clic su **Visualizza certificato**.  
 Confrontare l'identificazione personale del certificato con quella impostata per l'appliance vRealize Automation. È possibile visualizzare il certificato dell'appliance vRealize Automation nel browser client quando si accede alla console di gestione tramite la 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.

Anche in una distribuzione distribuita, in alcuni casi è possibile installare più componenti di IaaS nello stesso server Windows.

Se si installano più componenti di IaaS, installarli sempre nello stesso percorso.

- 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** Per l'alta disponibilità, è possibile aggiungere agenti ridondanti e configurarli in modo identico. Altrimenti, mantenere gli agenti univoci.

Opzione	Descrizione
<b>Agente ridondante</b>	Installare gli agenti ridondanti su server diversi. Denominare e configurare gli agenti ridondanti in modo identico.
<b>Agente autonomo</b>	Assegnare un nome univoco all'agente.

- 13 Configurare una connessione all'host del servizio di gestione di IaaS.

Opzione	Descrizione
<b>Senza bilanciamento del carico</b>	Specificare il nome di dominio completo e il numero di porta del bilanciamento del carico relativo al componente servizio di gestione, <i>mgr-svc-load-balancer.società.com:443</i> . Non immettere indirizzi IP.
<b>Con bilanciamento del carico</b>	Specificare il nome di dominio completo e il numero di porta della macchina su cui è stato installato il componente servizio di gestione, <i>mgr-svc.società.com:443</i> . Non immettere indirizzi IP.

La porta predefinita è 443.

**14 Configurare una connessione al server Web IaaS.**

Opzione	Descrizione
<b>Senza bilanciamento del carico</b>	Specificare il nome di dominio completo e il numero di porta del bilanciamento del carico del componente del server Web, <i>web-load-balancer.società.com:443</i> . Non immettere indirizzi IP.
<b>Con bilanciamento del carico</b>	Specificare il nome di dominio completo e il numero di porta della macchina su cui è stato installato il componente del server Web, <i>web.società.com:443</i> . Non immettere indirizzi IP.

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 agenti multipli con configurazioni differenti e un endpoint sullo stesso sistema.

**Operazioni successive**

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.

**Tabella 1-39. 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 <a href="http://support.microsoft.com">http://support.microsoft.com</a> .
Criteri di esecuzione di MS PowerShell	<p>I criteri di esecuzione di MS PowerShell devono essere impostati su <b>RemoteSigned</b> o <b>Unrestricted</b>.</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

- Installare IaaS, compreso il server Web e l'host del servizio di gestione.
- Verificare che i requisiti in [Requisiti di Visual Basic Scripting](#) siano soddisfatti.

- [Scaricare il programma di installazione di vRealize Automation IaaS.](#)

## Procedura

- 1 Fare clic con il pulsante destro del mouse sul file d'installazione `setup__vrealize-automation-appliance-FQDN@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 dell'appliance vRealize Automation e verificare il certificato SSL.
  - a Specificare il nome utente, ovvero **root**, e la password.

Questa è la password che è stata immessa durante la distribuzione dell'appliance vRealize Automation.
  - b Selezionare **Accetta certificato**.
  - c Fare clic su **Visualizza certificato**.

Confrontare l'identificazione personale del certificato con quella impostata per l'appliance vRealize Automation. È possibile visualizzare il certificato dell'appliance vRealize Automation nel browser client quando si accede alla console di gestione tramite la 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.

Anche in una distribuzione distribuita, in alcuni casi è possibile installare più componenti di IaaS nello stesso server Windows.

Se si installano più componenti di IaaS, installarli sempre nello stesso percorso.
- 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** Per l'alta disponibilità, è possibile aggiungere agenti ridondanti e configurarli in modo identico. Altrimenti, mantenere gli agenti univoci.

Opzione	Descrizione
<b>Agente ridondante</b>	Installare gli agenti ridondanti su server diversi. Denominare e configurare gli agenti ridondanti in modo identico.
<b>Agente autonomo</b>	Assegnare un nome univoco all'agente.

**13** Configurare una connessione all'host del servizio di gestione di IaaS.

Opzione	Descrizione
<b>Senza bilanciamento del carico</b>	Specificare il nome di dominio completo e il numero di porta del bilanciamento del carico relativo al componente servizio di gestione, <i>mgr-svc-load-balancer.società.com:443</i> . Non immettere indirizzi IP.
<b>Con bilanciamento del carico</b>	Specificare il nome di dominio completo e il numero di porta della macchina su cui è stato installato il componente servizio di gestione, <i>mgr-svc.società.com:443</i> . Non immettere indirizzi IP.

La porta predefinita è 443.

**14** Configurare una connessione al server Web IaaS.

Opzione	Descrizione
<b>Senza bilanciamento del carico</b>	Specificare il nome di dominio completo e il numero di porta del bilanciamento del carico del componente del server Web, <i>web-load-balancer.società.com:443</i> . Non immettere indirizzi IP.
<b>Con bilanciamento del carico</b>	Specificare il nome di dominio completo e il numero di porta della macchina su cui è stato installato il componente del server Web, <i>web.società.com:443</i> . Non immettere indirizzi IP.

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 agenti multipli 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

- Installare IaaS, compreso il server Web e l'host del servizio di gestione.
- Verificare che i requisiti in [Abilitazione delle richieste WMI remote su macchine Windows](#) siano soddisfatti.
- [Scaricare il programma di installazione di vRealize Automation IaaS](#).

#### Procedura

- 1 Fare clic con il pulsante destro del mouse sul file d'installazione `setup__vrealize-automation-appliance-FQDN@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 dell'appliance vRealize Automation e verificare il certificato SSL.

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

Questa è la password che è stata immessa durante la distribuzione dell'appliance vRealize Automation.

- b Selezionare **Accetta certificato**.

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

Confrontare l'identificazione personale del certificato con quella impostata per l'appliance vRealize Automation. È possibile visualizzare il certificato dell'appliance vRealize Automation nel browser client quando si accede alla console di gestione tramite la 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.

Anche in una distribuzione distribuita, in alcuni casi è possibile installare più componenti di IaaS nello stesso server Windows.

Se si installano più componenti di IaaS, installarli sempre nello stesso percorso.

- 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** Per l'alta disponibilità, è possibile aggiungere agenti ridondanti e configurarli in modo identico. Altrimenti, mantenere gli agenti univoci.

---

Opzione	Descrizione
<b>Agente ridondante</b>	Installare gli agenti ridondanti su server diversi. Denominare e configurare gli agenti ridondanti in modo identico.
<b>Agente autonomo</b>	Assegnare un nome univoco all'agente.



**13** Configurare una connessione all'host del servizio di gestione di IaaS.

Opzione	Descrizione
<b>Senza bilanciamento del carico</b>	Specificare il nome di dominio completo e il numero di porta del bilanciamento del carico relativo al componente servizio di gestione, <i>mgr-svc-load-balancer.società.com:443</i> . Non immettere indirizzi IP.
<b>Con bilanciamento del carico</b>	Specificare il nome di dominio completo e il numero di porta della macchina su cui è stato installato il componente servizio di gestione, <i>mgr-svc.società.com:443</i> . Non immettere indirizzi IP.

La porta predefinita è 443.

**14** Configurare una connessione al server Web IaaS.

Opzione	Descrizione
<b>Senza bilanciamento del carico</b>	Specificare il nome di dominio completo e il numero di porta del bilanciamento del carico del componente del server Web, <i>web-load-balancer.società.com:443</i> . Non immettere indirizzi IP.
<b>Con bilanciamento del carico</b>	Specificare il nome di dominio completo e il numero di porta della macchina su cui è stato installato il componente del server Web, <i>web.società.com:443</i> . Non immettere indirizzi IP.

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 agenti multipli con configurazioni differenti e un endpoint sullo stesso sistema.

## Installazione di vRealize Automation invisibile all'utente

vRealize Automation include opzioni per l'installazione invisibile all'utente con script dalla riga di comando e l'installazione invisibile all'utente basata sull'API. Entrambi gli approcci richiedono la definizione preliminare dei valori che in genere vengono immessi manualmente durante un'installazione convenzionale

## Informazioni sull'installazione di vRealize Automation invisibile all'utente

L'installazione di vRealize Automation invisibile all'utente utilizza un eseguibile che fa riferimento a un file di risposte basato su testo.

Nel file di risposte vengono preconfigurati i nomi di dominio completi del sistema, le credenziali degli account e altre impostazioni che vengono in genere aggiunte nel corso di un'installazione convenzionale basata su procedura guidata o manuale. L'installazione invisibile all'utente è utile nei seguenti tipi di distribuzione.

- Distribuzione di più ambienti quasi identici.
- Redistribuzione ripetuta dello stesso ambiente
- Esecuzione di installazioni automatiche
- Esecuzione di installazioni controllate da script

## Esecuzione di un'installazione di vRealize Automation invisibile all'utente

È possibile eseguire un'installazione di vRealize Automation automatica, invisibile all'utente, dalla console di un'appliance vRealize Automation appena distribuita.

### Prerequisiti

- Creare un'appliance non configurata. Vedere [Distribuzione di vRealize Automation appliance](#).
- Creare o identificare i server Windows di IaaS e configurarne i relativi prerequisiti.
- Installare l'Agente di gestione sui server Windows di IaaS.

È possibile installare l'Agente di gestione scaricando il file `.msi` come sempre o mediante il processo invisibile all'utente descritto in [Esecuzione di un'installazione dell'agente di gestione di vRealize Automation invisibile all'utente](#).

### Procedura

- 1 Accedere alla console dell'appliance vRealize Automation come utente root.
- 2 Passare alla seguente directory.  
`/usr/lib/vcac/tools/install`
- 3 Aprire il file di risposte `ha.properties` in un editor di testo.
- 4 Aggiungere le voci specifiche per la distribuzione in `ha.properties`, quindi salvare e chiudere il file.

In alternativa, per risparmiare tempo, è possibile copiare e modificare un file `ha.properties` da un'altra distribuzione invece di modificare tutto il file predefinito.

- 5 Dalla stessa directory, eseguire il comando seguente per avviare l'installazione.

```
vra-ha-config.sh
```

Il completamento dell'installazione può impiegare un'ora o più, a seconda dell'ambiente e delle dimensioni della distribuzione.

- 6 (Facoltativo) Al termine dell'installazione, esaminare il file registro.

`/var/log/vcac/vra-ha-config.log`

Il programma di installazione invisibile all'utente non salva nel registro i dati proprietari, quali password, licenze o certificati.

## Esecuzione di un'installazione dell'agente di gestione di vRealize Automation invisibile all'utente

È possibile eseguire un'installazione dell'agente di gestione di vRealize Automation dalla riga di comando su qualsiasi server Windows di IaaS.

L'installazione invisibile all'utente dell'agente di gestione consiste in uno script di Windows PowerShell in cui personalizzare alcune impostazioni. Dopo aver aggiunto le impostazioni specifiche per la distribuzione, è possibile installare in modo invisibile all'utente l'agente di gestione su tutti i server Windows di IaaS eseguendo copie dello stesso script su ognuno di essi.

### Prerequisiti

- Creare un'appliance non configurata. Vedere [Distribuzione di vRealize Automation appliance](#).
- Creare o identificare i server Windows di IaaS e configurarne i relativi prerequisiti.

### Procedura

- 1 Accedere al server IaaS Windows utilizzando un account che dispone di privilegi di amministratore.
- 2 Aprire un browser Web nell'URL del programma di installazione dell'appliance vRealize Automation.  
`https://vrealize-automation-appliance-FQDN:5480/installer`
- 3 Fare clic con il pulsante destro sul collegamento del file di script di PowerShell `InstallManagementAgent.ps1` e salvarlo sul desktop o in una cartella del server Windows di IaaS.
- 4 Aprire `InstallManagementAgent.ps1` in un editor di testo.
- 5 Accanto alla parte superiore del file di script, aggiungere le impostazioni specifiche per la distribuzione.
  - URL dell'appliance vRealize Automation  
`https://vrealize-automation-appliance-FQDN:5480`
  - Credenziali dell'account utente root dell'appliance vRealize Automation
  - Credenziali dell'utente del servizio vRealize Automation, un account di dominio con privilegi di amministratore sui server Windows di IaaS
  - La cartella in cui si desidera installare l'agente di gestione, per impostazione predefinita `Programmi (x86)`
  - (Facoltativo) L'identificatore digitale del certificato in formato PEM utilizzato per l'autenticazione
- 6 Salvare e chiudere `InstallManagementAgent.ps1`.

- 7 Per installare in modo invisibile all'utente l'agente di gestione, fare doppio clic su `InstallManagementAgent.ps1`.
- 8 (Facoltativo) Per verificare il completamento dell'installazione individuare l'**agente di gestione di VMware vCloud Automation Center** nell'elenco Programmi e funzionalità del Pannello di controllo di Windows e nell'elenco dei servizi Windows in esecuzione.

## File di risposte dell'installazione di vRealize Automation invisibile all'utente

Per le installazioni di vRealize Automation invisibili all'utente è necessario predisporre un file di risposte basato su testo.

Tutte le nuove Appliance vRealize Automation distribuite contengono un file di risposte predefinito.

`/usr/lib/vcac/tools/install/ha.properties`

Per eseguire un'installazione invisibile all'utente, è necessario utilizzare un editor di testo per personalizzare le impostazioni in `ha.properties` in base alla distribuzione che si desidera installare. Gli esempi forniti di seguito sono alcune delle impostazioni e informazioni da aggiungere.

- Chiave di licenza di vRealize Automation o della suite
- Nomi FQDN del nodo dell'Appliance vRealize Automation
- Credenziali dell'account root dell'Appliance vRealize Automation
- Nomi FQDN del server Windows di IaaS che fungeranno da nodi Web, nodi del servizio di gestione e così via
- Credenziali dell'utente del servizio vRealize Automation, un account di dominio con privilegi di amministratore sui server Windows di IaaS
- Nomi FQDN del bilanciamento del carico
- Parametri del database di SQL Server
- Parametri dell'agente proxy per il collegamento alle risorse di virtualizzazione
- Se il programma di installazione invisibile all'utente deve tentare di correggere i prerequisiti mancanti del server Windows di IaaS

Il programma di installazione invisibile all'utente può correggere molti prerequisiti Windows mancanti. Tuttavia, alcuni problemi di configurazione, come CPU insufficiente, tuttavia, non possono essere corretti dal programma di installazione invisibile all'utente.

Per risparmiare tempo, è possibile riutilizzare e modificare un file `ha.properties` con impostazioni simili già configurato per un'altra distribuzione. Inoltre, quando si installa vRealize Automation in modo non invisibile all'utente, tramite l'installazione guidata, la procedura guidata crea e salva le impostazioni nel file `ha.properties`. Questo file può essere riutilizzato come base da modificare per l'installazione invisibile all'utente di una distribuzione simile.

La procedura guidata non salva nel file `ha.properties` impostazioni proprietarie quali password, licenze o certificati.

## La riga di comando di installazione di vRealize Automation

vRealize Automation include un'interfaccia della riga di comando basata su console per eseguire regolazioni dell'installazione eventualmente necessarie dopo l'installazione iniziale.

L'interfaccia della riga di comando (CLI) può eseguire attività di installazione e configurazione che non sono più disponibili attraverso l'interfaccia basata su browser dopo l'installazione iniziale. Le caratteristiche della CLI includono il ricontrollo dei prerequisiti, l'installazione dei componenti di IaaS, l'installazione dei certificati e l'impostazione del nome host di vRealize Automation a cui gli utenti puntano il loro browser Web.

La CLI è inoltre utile per gli utenti avanzati che desiderano inserire alcune operazioni in uno script. Alcune funzioni della CLI vengono usate dall'installazione invisibile all'utente per cui la familiarità di entrambe le caratteristiche consolida la conoscenza dello scripting dell'installazione di vRealize Automation.

### Informazioni di base sulla riga di comando dell'installazione di vRealize Automation

L'interfaccia della riga di comando dell'installazione di vRealize Automation comprende operazioni di base di primo livello.

Le operazioni di base mostrano gli ID dei nodi vRealize Automation, eseguono comandi, segnalano lo stato dei comandi o visualizzano le informazioni della Guida. Per visualizzare queste operazioni e le relative opzioni nella schermata della console, immettere il seguente comando senza alcuna opzione o qualificatore.

```
vra-command
```

### Visualizzazione degli ID dei nodi

Sono necessari gli ID dei nodi di vRealize Automation in modo da poter eseguire i comandi per i sistemi target corretti. Per visualizzare gli ID dei nodi, immettere il seguente comando.

```
vra-command list-nodes
```

Prendere nota degli ID dei nodi prima di eseguire comandi su macchine specifiche.

### Esecuzione dei comandi

La maggior parte delle funzioni della riga di comando comporta l'esecuzione di un comando per un nodo nel cluster di vRealize Automation. Per eseguire un comando, utilizzare la seguente sintassi.

```
vra-command execute --node ID-nodo nome-comando --nome-parametro valore-parametro
```

Come mostrato nella precedente sintassi, molti comandi richiedono parametri e valori di parametro scelti dall'utente.

### Visualizzazione dello stato dei comandi

Il completamento di alcuni comandi può richiedere alcuni minuti o addirittura più tempo. Per controllare l'avanzamento di un comando immesso, digitare il seguente comando.

```
vra-command status
```

Il comando relativo allo stato è particolarmente utile per monitorare le installazioni invisibili all'utente, che possono richiedere tempi lunghi per le distribuzioni di grandi dimensioni.

### Visualizzazione della Guida

Per visualizzare le informazioni della Guida per tutti i comandi disponibili, immettere il seguente comando.

```
vra-command help
```

Per visualizzare la Guida per un singolo comando, immettere il seguente comando.

```
vra-command help nome-comando
```

### vRealize Automation Installazione dei nomi di comando

I comandi consentono di accedere alla console per molte attività di installazione e configurazione di vRealize Automation che si intende eseguire dopo l'installazione iniziale.

Esempi di comandi disponibili comprendono le seguenti funzioni.

- Aggiunta di un'altra appliance vRealize Automation a un'installazione esistente
- Impostazione del nome host a cui gli utenti puntano con il browser Web quando accedono a vRealize Automation
- Creazione del database dell'SQL Server IaaS
- Esecuzione del Controllo prerequisiti per un server Windows IaaS
- Importazione certificati

Per un elenco completo dei comandi disponibili in vRealize Automation, accedere alla console dell'appliance vRealize Automation e immettere il seguente comando.

```
vra-command help
```

L'elenco completo di nomi e parametri di comando non è riprodotto nella documentazione separata. Per utilizzare l'elenco in modo efficace, identificare un comando di interesse e limitare la focalizzazione immettendo il seguente comando.

```
vra-command help nome-comando
```

## L'API di installazione di vRealize Automation

L'API REST di vRealize Automation per l'installazione offre la capacità di creare installazioni puramente controllate dal software per vRealize Automation.

L'API di installazione richiede una versione in formato JSON delle stesse voci che l'installazione basata su CLI riceve dal file di risposta `ha.properties`. Le seguenti linee guida aiutano ad acquisire familiarità con il funzionamento dell'API. Da qui l'utente dovrebbe essere in grado di progettare chiamate programmatiche all'API per installare vRealize Automation.

- Per accedere alla documentazione dell'API, aprire la seguente pagina dell'appliance vRealize Automation con un browser Web.

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

È necessaria un'appliance vRealize Automation non configurata. Vedere [Distribuzione di vRealize Automation appliance](#).

- Per sperimentare con l'installazione basata su API, individuare ed espandere il seguente comando PUT.

`PUT /vra-install`

- Copiare il JSON non compilato dalla casella **install\_json** a un editor di testo. Inserire i valori delle risposte come si farebbe per `ha.properties`. Quando le risposte in formato JSON sono pronte, copiare il codice in **install\_json** e sovrascrivere il JSON non compilato.

In alternativa, è possibile modificare il seguente modello JSON e copiare i risultati in **install\_json**.

`/usr/lib/vcac/tools/install/installationProperties.json`

È anche possibile convertire un file `ha.properties` compilato in formato JSON o viceversa.

- Nella casella delle azione, selezionare **validate** (convalida) fare clic su **Try It Out** (Prova).

L'azione di convalida esegue il programma di controllo e correzione dei prerequisiti di vRealize Automation.

- La risposta convalidata include un ID di comando alfanumerico che è possibile inserire nel seguente comando GET.

`GET /commands/command-id/aggregated-status`

La risposta al GET include lo stato di avanzamento dell'operazione di convalida.

- Quando la convalida riesce, è possibile eseguire l'installazione effettiva ripetendo il processo. Nella casella delle azioni selezionare **install** (installa) invece di **validate** (convalida).

L'installazione può impiegare molto tempo a seconda delle dimensioni di distribuzione. Anche in questo caso, individuare l'ID comando e utilizzare il comando di stato aggregato GET per conoscere lo stato di avanzamento dell'installazione. La risposta di GET potrebbe essere simile al seguente esempio.

```
"progress": "78%", "counts": {"failed": 0, "completed": 14, "total": 18,
"queued": 3, "processing": 1}, "failed-commands": 0
```

- Se qualcosa non funziona nell'installazione, è possibile attivare la raccolta dei registri di tutti i nodi con il seguente comando.

`PUT /commands/log-bundle`

Analogamente all'installazione, l'ID di comando alfanumerico consente di monitorare lo stato di raccolta dei registri.

## Conversione tra proprietà invisibili all'utente di vRealize Automation e JSON

Per le installazioni di vRealize Automation invisibili all'utente basate su CLI o API, è possibile convertire nel formato JSON un file di risposta compilato con le proprietà o viceversa. L'installazione invisibile all'utente basata su CLI richiede il file delle proprietà mentre l'API richiede il formato JSON.

### Prerequisiti

Un file di risposta compilato con le proprietà o un file JSON compilato

```
/usr/lib/vcac/tools/install/ha.properties
```

oppure

```
/usr/lib/vcac/tools/install/installationProperties.json
```

### Procedura

- 1 Accedere a una sessione della console dell'appliance vRealize Automation come utente root.
- 2 Eseguire lo script di conversione appropriato.

- Convertire da JSON a Proprietà

```
/usr/lib/vcac/tools/install/convert-properties --from-json  
installationProperties.json
```

Lo script crea un nuovo file di proprietà con indicazione data/ora nel nome, ad esempio:

```
ha.2016-10-17_13.02.15.properties
```

- Convertire da Proprietà a JSON

```
/usr/lib/vcac/tools/install/convert-properties --to-json ha.properties
```

Lo script crea un nuovo file `installationProperties.json` con l'indicazione data/ora nel nome, ad esempio:

```
installationProperties.2016-10-17_13.36.13.json
```

È anche possibile visualizzare la guida relativa allo script.

```
/usr/lib/vcac/tools/install/convert-properties --help
```

## Attività post-installazione di vRealize Automation

Dopo aver installato vRealize Automation, è necessario prestare attenzione ad alcune attività post-installazione.

### Configurazione della crittografia conforme al Federal Information Processing Standard

È possibile abilitare o disabilitare la crittografia conforme a FIPS (Federal Information Processing Standard) 140-2 per il traffico di rete dell'appliance vRealize Automation in entrata e in uscita.



La modifica delle impostazioni relative al FIPS richiede il riavvio di vRealize Automation. FIPS è disattivato per impostazione predefinita.

### Procedura

- 1 Accedere come root all'interfaccia di gestione dell'appliance vRealize Automation.  
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Fare clic su **Impostazioni vRA > Impostazioni host**.
- 3 Nella parte superiore destra della schermata, fare clic sul pulsante per abilitare o disabilitare lo standard FIPS.

Se FIPS è abilitato, il traffico di rete dell'appliance vRealize Automation in entrata e in uscita sulla porta 443 utilizza la crittografia conforme a FIPS 140-2. Indipendentemente dall'impostazione dello standard FIPS, vRealize Automation utilizza algoritmi conformi a AES-256 per tutelare i dati protetti dell'appliance vRealize Automation.

**Nota** Questa versione di vRealize Automation abilita solo in parte la conformità a FIPS, poiché alcuni componenti non utilizzano ancora i moduli di crittografia certificati. Nei casi in cui non siano ancora stati implementati i moduli certificati, vengono utilizzati gli algoritmi conformi ad AES-256.

- 4 Fare clic su **Sì** per riavviare vRealize Automation.

È inoltre possibile configurare FIPS da una sessione della console dell'appliance vRealize Automation come root utilizzando i comandi seguenti.

```
vcac-vami fips enable
vcac-vami fips disable
vcac-vami fips status
```

## Attivazione del failover automatico del servizio di gestione

Il failover automatico del servizio di gestione è disattivato per impostazione predefinita se si installa o si aggiorna il servizio di gestione con il programma d'installazione per Windows standard di vRealize Automation.

Per attivare il failover automatico del servizio di gestione dopo aver avviato il programma d'installazione per Windows standard, attenersi alla procedura seguente.

### Procedura

- 1 Accedere come root a una sessione della console sull'appliance vRealize Automation.
- 2 Passare alla seguente directory.  
`/usr/lib/vcac/tools/vami/commands`
- 3 Immettere il seguente comando.

```
python ./manager-service-automatic-failover ENABLE
```

Per disattivare il failover automatico in un'intera distribuzione di IaaS, immettere invece il seguente comando.

```
python ./manager-service-automatic-failover DISABLE
```

### Informazioni sul failover automatico del servizio di gestione

È possibile configurare il servizio di gestione IaaS di vRealize Automation per il failover in un backup in caso di arresto del servizio di gestione primario.

A partire da vRealize Automation 7.3, non è più necessario avviare o arrestare manualmente il servizio di gestione su ciascun server Windows per scegliere quale utilizzare come servizio primario o di backup. Il failover automatico del servizio di gestione è attivato per impostazione predefinita nei casi seguenti.

- Quando si installa vRealize Automation in modalità invisibile all'utente o con l'installazione guidata.
- Quando si aggiorna IaaS mediante l'interfaccia di amministrazione o con lo script di aggiornamento automatico.

Il failover non è abilitato quando si utilizza il programma di installazione standard basato su Windows per aggiungere un host del servizio di gestione o aggiornare IaaS. Per abilitarlo, vedere [Attivazione del failover automatico del servizio di gestione](#).

Quando è attivato il failover automatico, il servizio di gestione viene avviato automaticamente in tutti gli host del servizio di gestione, inclusi i backup. La funzionalità di failover automatico consente agli host di effettuare il monitoraggio reciproco in modo trasparente ed effettuare il failover quando necessario. La funzionalità richiede che il servizio di Windows sia in esecuzione su tutti gli host.

---

**Nota** Non è richiesto l'uso del failover automatico. È infatti possibile disattivarlo e continuare ad avviare e arrestare manualmente il servizio Windows per scegliere quale host utilizzare come primario o di backup. Se si segue l'approccio del failover manuale, è necessario avviare il servizio su un solo host alla volta. Con la disattivazione del failover automatico, l'esecuzione simultanea del servizio in più server IaaS non consente di utilizzare vRealize Automation.

---

Evitare di attivare o disattivare il failover in modo selettivo. È necessario che il failover automatico venga sempre sincronizzato come attivo o disattivo attraverso ogni host del servizio di gestione in una distribuzione IaaS.

Se il failover automatico non funziona, consultare i suggerimenti della sezione di risoluzione dei problemi [Il failover del servizio di gestione automatico non si attiva](#).

### Failover automatico del database PostgreSQL di vRealize Automation

In una distribuzione di vRealize Automation ad alta disponibilità, alcune configurazioni consentono il failover automatico del database PostgreSQL di vRealize Automation incorporato.

Il failover automatico viene attivato in modalità invisibile all'utente nelle condizioni seguenti.

- La distribuzione ad elevata disponibilità include tre appliance vRealize Automation.

Il failover automatico non è supportato con due sole appliance.

- La replica del database è impostata sulla modalità sincrona in Impostazioni vRA > Database nell'interfaccia di amministrazione di vRealize Automation.

In genere, è consigliabile evitare di eseguire un failover manuale mentre è attivato il failover automatico. Tuttavia, per alcuni problemi dei nodi, il failover automatico potrebbe non essere eseguito anche se è attivato. In questo caso, controllare se è necessario eseguire un failover manuale.

- 1 Dal momento in cui si verifica l'errore nel nodo del database PostgreSQL primario, attendere fino a 5 minuti per consentire la stabilizzazione del resto del cluster.
- 2 Su un nodo dell'appliance vRealize Automation funzionante, aprire un browser al seguente URL.  
`https://vrealize-automation-appliance-FQDN:5434/api/status`
- 3 Cercare `manualFailoverNeeded`.
- 4 Se `manualFailoverNeeded` è `true`, eseguire un failover manuale.

Per ulteriori informazioni, vedere [Esecuzione del failover manuale del database dell'appliance vRealize Automation](#).

## Sostituzione di certificati autofirmati con certificati forniti da un'autorità

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 [Aggiornamento dei certificati di vRealize Automation](#).

## Modifica di nomi host e indirizzi IP

In generale, si consiglia di mantenere i nomi host, i nomi di dominio completo (FQDN) e gli indirizzi IP pianificati per i sistemi vRealize Automation. Sono sempre possibili alcune modifiche successive all'installazione, ma possono essere complicate.

- Se viene modificato il nome host della macchina Windows che ospita il database SQL Server IaaS, vedere [Configurare il database SQL per un nuovo nome host](#).
- Quando vengono ripristinati i componenti IaaS, la ridenominazione di un host può influire sull'host Web IaaS, sull'host del servizio di gestione o sui rispettivi bilanciamenti del carico. Ripristinare questi host o bilanciamenti del carico seguendo le istruzioni di backup e ripristino di *vRealize Suite*.

Per modificare l'indirizzo IP o il nome host di un'appliance vRealize Automation, vedere le sezioni seguenti.

### Modifica del nome host dell'appliance vRealize Automation

Quando si gestisce un ambiente o una rete può essere necessario assegnare un nome host diverso a un'appliance vRealize Automation.

---

**Importante** L'operazione di ridenominazione porta vRealize Automation offline per alcuni minuti.

---

La stessa procedura è applicabile alle appliance vRealize Automation autonome, master e replica.

**Procedura**

- 1 In DNS, creare un record aggiuntivo con il nuovo nome host del nodo.

Non rimuovere ancora il record DNS esistente contenente il nome host precedente.

- 2 Attendere che abbiano luogo la replica del DNS e la distribuzione per zone.
- 3 Accedere come utente root alla riga di comando dell'appliance vRealize Automation.
- 4 Eseguire il comando seguente.

```
vcac-config hostname-change --host new-hostname --certificate certificate-file-name
```

Un file del certificato è facoltativo, a meno che il vecchio nome host dell'appliance non sia stato utilizzato in un certificato. In tal caso, fornire un certificato aggiornato con il nuovo nome host.

Quando si specifica un file del certificato, il comando di ridenominazione importa anche il certificato e restituisce l'ID del certificato.

Un file del certificato deve avere lo stesso formato dell'output di testo del comando API /config/ssl/generate-certificate e contenere il nuovo nome DNS nel campo SAN.

- 5 Attendere per almeno 15 minuti il completamento del processo di ridenominazione. Dopo le azioni del comando che richiedono qualche minuto, sono necessari diversi altri minuti per la ri-registrazione del servizio.
- 6 Se il vecchio nome host dell'appliance è stato utilizzato con un bilanciamento del carico in un ambiente HA, controllare e riconfigurare il bilanciamento del carico con il nuovo nome.
- 7 In DNS, rimuovere il record DNS esistente contenente il nome host precedente.

Se si verificano problemi durante la modifica di un nome host, provare le procedure distinte riportate nella documentazione di vRealize Automation 7.3.

**Modifica dell'indirizzo IP dell'appliance vRealize Automation**

Quando si gestisce un ambiente o una rete, può essere necessario assegnare un indirizzo IP diverso a un'appliance vRealize Automation esistente.

**Prerequisiti**

- Come precauzione, creare snapshot delle appliance vRealize Automation e dei server IaaS.
- Da una sessione della console come root nell'appliance vRealize Automation, ispezionare le voci del file /etc/hosts.

Cercare le assegnazioni di indirizzi che potrebbero essere in conflitto con il piano del nuovo indirizzo IP e apportare le eventuali modifiche necessarie.

In tutti i server IaaS, ripetere il processo per il file Windows\system32\drivers\etc\hosts.

- Arrestare tutte le appliance vRealize Automation.
- Arrestare tutti i servizi vRealize Automation nei server IaaS.

## Procedura

- 1 In vSphere, individuare l'appliance vRealize Automation che si desidera modificare e selezionare **Azioni > Modifica impostazioni**.
- 2 Fare clic su **Opzioni vApp**.
- 3 Espandere **Allocazione IP** e abilitare l'opzione **Ambiente OVF**.
- 4 Espandere **Impostazioni OVF** e abilitare l'opzione **Immagine ISO**.

**Figura 1-16. Opzioni Ambiente OVF e Immagine ISO**

Virtual Hardware	VM Options	SDRS Rules	vApp Options
<div>▼ IP allocation</div> <div>IP allocation scheme</div> <p>A vApp can obtain its network configuration through the OVF environment or a DHCP server. Specify the network configuration schemes supported by this vApp:</p> <p><input type="checkbox"/> DHCP</p> <p><input checked="" type="checkbox"/> OVF environment</p> <p>The IP allocation schemes determine what IP allocation policy options are enabled.</p> <div>IP protocol</div> <p>Specify the IP protocols supported by this vApp:</p> <p>Both ▼</p>			
<div>▼ OVF settings</div> <div>OVF environment</div> <p><a href="#">View...</a></p> <p>The OVF environment is only available when the VM is powered on.</p> <div>OVF environment transport</div> <p><input checked="" type="checkbox"/> ISO image</p> <p>An ISO image, containing the OVF environment document, is mounted on the first available CD-ROM drive.</p> <p><input checked="" type="checkbox"/> VMware Tools</p> <p>The VMware tools guestInfo.ovfEnv variable is initialized with the OVF environment document.</p> <div>Installation boot</div> <p><input type="checkbox"/> Enable</p> <p>The installation boot automatically gets reset upon first power-on of the virtual machine.</p> <p>0 ▼</p> <p>Specify the delay in seconds to wait for the VM to power off. A value of zero means wait until the VM is powered off</p>			

- 5 Fare clic su **OK**.
- 6 Avviare l'appliance vRealize Automation che si sta modificando.
- 7 Accedere come root all'interfaccia di gestione dell'appliance vRealize Automation.  
<https://vrealize-automation-appliance-FQDN:5480>
- 8 Fare clic sulla scheda **Rete**.

**9** Sotto le schede, fare clic su **Indirizzo**.

**10** Aggiornare l'indirizzo IP.

**11** Fare clic su **Salva impostazioni** in alto a destra.

**12** Arrestare l'appliance vRealize Automation che si sta modificando.

**13** In DNS, aggiornare le voci per i nuovi indirizzi IP.

Aggiornare solo i record di tipo A esistenti. Non modificare i nomi di dominio completi.

Se si utilizza il bilanciamento del carico, aggiornare anche le impostazioni IP del bilanciamento del carico per i nodi back-end, i pool di servizi e i server virtuali in base alle esigenze.

**14** Attendere che abbiano luogo la replica del DNS e la distribuzione per zone.

**15** Avviare tutte le appliance vRealize Automation.

**16** Avviare i servizi vRealize Automation nei server IaaS.

**17** Accedere come root all'interfaccia di gestione dell'appliance vRealize Automation.

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

**18** Verificare lo stato dell'appliance vRealize Automation nelle seguenti aree.

- Lo stato della connessione al database in **Impostazioni vRA > Database**
- Lo stato di RabbitMQ in **Impostazioni vRA > Messaggistica**
- Lo stato di Xenon in **Impostazioni vRA > Xenon**
- Tutti i servizi come sono REGISTRATI in **Servizi**

### Regolazione del database SQL per un nome host modificato

Se si sposta il database SQL IaaS vRealize Automation in un nome host diverso, è necessario rivedere le impostazioni di configurazione.

Nello stesso nome host, è possibile ripristinare un database SQL da un backup senza la necessità di ulteriori passaggi. Se esegue il ripristino in un altro nome host, è necessario modificare il file di configurazione per apportare ulteriori modifiche.

Per informazioni sulle modifiche necessarie quando si sposta il database SQL in un nome host diverso, vedere [Articolo della Knowledge Base VMware 2074607](#).

### Modifica dell'indirizzo IP di un server IaaS

Quando si gestisce un ambiente o una rete, può essere necessario assegnare un indirizzo IP diverso a un server Windows IaaS di vRealize Automation esistente.

#### Prerequisiti

- Se è necessario modificare l'indirizzo IP dell'appliance vRealize Automation, eseguire innanzitutto questa operazione. Vedere [Modifica dell'indirizzo IP dell'appliance vRealize Automation](#).
- Come precauzione, creare snapshot delle appliance vRealize Automation e dei server IaaS.

- Da una sessione della console come root nell'appliance vRealize Automation, ispezionare le voci del file `/etc/hosts`.

Cercare le assegnazioni di indirizzi che potrebbero essere in conflitto con il piano del nuovo indirizzo IP e apportare le eventuali modifiche necessarie.

In tutti i server IaaS, ripetere il processo per il file `Windows\system32\drivers\etc\hosts`.

- Arrestare l'appliance vRealize Automation.
- Arrestare tutti i servizi vRealize Automation nei server IaaS.

## Procedura

- 1 Accedere al server IaaS utilizzando un account che disponga di privilegi di amministratore.
- 2 In Windows, modificare l'indirizzo IP.

Cercare l'indirizzo IP nelle impostazioni della scheda di rete di Windows nelle proprietà Protocollo Internet.

- 3 Aggiornare il DNS locale con le modifiche.

L'aggiornamento del DNS consente il rilevamento reciproco dei server Windows IaaS e la riconnessione a un server Windows se si è disconnessi.

- 4 Nell'host del servizio di gestione, ispezionare il file seguente in un editor di testo.

`install-folder\vCAC\Server\ManagerService.exe.config`

La cartella di installazione predefinita è `C:\Program Files (x86)\VMware`.

Verificare gli indirizzi IP o i nomi di dominio completi delle appliance vRealize Automation e dei server Windows IaaS.

- 5 In tutti i server Windows IaaS, ispezionare il file seguente in un editor di testo.

`install-folder\vCAC\Management Agent\VMware.IaaS.Management.Agent.exe.Config`

Verificare l'indirizzo IP o il nome di dominio completo dell'appliance vRealize Automation.

- 6 Accedere all'host SQL Server.
- 7 Verificare che l'indirizzo del repository sia stato configurato correttamente per l'utilizzo del nome di dominio completo nella colonna `ConnectionString`.

Ad esempio, aprire SQL Management Studio ed eseguire la query seguente.

```
"SELECT Name, ConnectionString FROM [database-name].[DynamicOps.RepositoryModel].
[Models]"
```

- 8 Avviare l'appliance vRealize Automation.
- 9 Avviare i servizi vRealize Automation nei server IaaS.
- 10 Ispezionare i file di registro per verificare che Agent, DEM Worker, il servizio di gestione e i servizi host Web siano stati avviati correttamente.
- 11 Accedere a vRealize Automation come utente con ruolo di amministratore dell'infrastruttura.

- 12 Passare a **Infrastruttura > Monitoraggio > Stato di Distributed Execution** e verificare che tutti i servizi siano in esecuzione.
- 13 Verificare il funzionamento corretto controllando i servizi dell'appliance, eseguendo il test del provisioning o utilizzando lo strumento vRealize Production Test.

### Modifica del nome host di un server IaaS

Quando si gestisce un ambiente o una rete, può essere necessario assegnare un nome host diverso a un server Windows IaaS di vRealize Automation esistente.

#### Procedura

- 1 Creare uno snapshot del server IaaS.
- 2 Nel server IaaS, utilizzare Gestione IIS per arrestare i pool di applicazioni di vRealize Automation: Repository, VMware vRealize Automation e Wapi.
- 3 Nel server IaaS, utilizzare Strumenti di amministrazione > Servizi per arrestare tutti i servizi, gli agenti e i DEM di vRealize Automation.
- 4 In DNS, creare un record aggiuntivo con il nuovo nome host.

Non rimuovere ancora il record DNS esistente contenente il nome host precedente.

- 5 Attendere che abbiano luogo la replica del DNS e la distribuzione per zone.
- 6 Nel server IaaS, modificare il nome host, ma non riavviare quando richiesto.

Cercare il nome host nelle proprietà di sistema di Windows, in Impostazioni relative a nome computer, dominio e gruppo di lavoro.

Quando viene chiesto di riavviare, fare clic sull'opzione per riavviare in un secondo momento.

- 7 Se è stato utilizzato il nome host precedente per generare i certificati, aggiornare i certificati.

Per ulteriori informazioni, vedere [Aggiornamento dei certificati di vRealize Automation](#).

- 8 Utilizzare un editor di testo per individuare e aggiornare il nome host nei file di configurazione.

Effettuare gli aggiornamenti in base al nome host del server IaaS che è stato modificato. In una distribuzione HA potrebbe essere necessario accedere a più server. Se si modifica il nome host di un'istanza di DEM Orchestrator o DEM Worker, non sarà necessario apportare aggiornamenti.

**Nota** Aggiornare solo il nome host del server Windows precedente. Se invece si trova il nome di un programma di bilanciamento del carico, mantenere tale nome.

**Tabella 1-40. File da aggiornare quando si modifica il nome host di un nodo Web**

Server di IaaS	Percorso	File
Nodi Web	<i>install-folder</i> \Server\Website	Web.config
	<i>install-folder</i> \Server\Website\Cafe	Vcac-Config.exe.config
	<i>install-folder</i> \Web API	Web.config
	<i>install-folder</i> \Web API\ConfigTool	Vcac-Config.exe.config



**Tabella 1-40. File da aggiornare quando si modifica il nome host di un nodo Web (Continua)**

Server di IaaS	Percorso	File
Nodo con componente Model Manager installato	<i>install-folder\Server\Model Manager Data</i>	Repoutil.exe.config
	<i>install-folder\Server\Model Manager Data\Cafe</i>	Vcac-Config.exe.config
Nodi del servizio di gestione	<i>install-folder\Server</i>	ManagerService.exe.config
Nodi di DEM Orchestrator	<i>install-folder\Distributed Execution Manager\dem</i>	DynamicOps.DEM.exe.config
Nodi di DEM Worker	<i>install-folder\Distributed Execution Manager\DEM-name</i>	DynamicOps.DEM.exe.config
Nodi dell'agente	<i>install-folder\Agents\agent-name</i>	RepoUtil.exe.config
	<i>install-folder\Agents\agent-name</i>	VRMAgent.exe.config

**Tabella 1-41. File da aggiornare quando si modifica il nome host di un nodo del servizio di gestione**

Server di IaaS	Percorso	File
Nodi di DEM Orchestrator	<i>install-folder\Distributed Execution Manager\DEM-name</i>	DynamicOps.DEM.exe.config
Nodi di DEM Worker	<i>install-folder\Distributed Execution Manager\dem</i>	DynamicOps.DEM.exe.config
Nodi dell'agente	<i>install-folder\Agents\agent-name</i>	VRMAgent.exe.config

**Tabella 1-42. File da aggiornare quando si modifica il nome host di un nodo dell'agente**

Server di IaaS	Percorso	File
Nodo dell'agente	<i>install-folder\Agents\agent-name</i>	VRMAgent.exe.config

- 9 Riavviare il server IaaS in cui è stato modificato il nome host.
- 10 Avviare i pool di applicazioni vRealize Automation arrestati in precedenza.
- 11 Avviare i servizi, gli agenti e i DEM vRealize Automation arrestati in precedenza.
- 12 Se il vecchio nome host del server IaaS è stato utilizzato con un bilanciamento del carico in un ambiente HA, controllare e riconfigurare il bilanciamento del carico con il nuovo nome.
- 13 In DNS, rimuovere il record DNS esistente contenente il nome host precedente.
- 14 Attendere che abbiano luogo la replica del DNS e la distribuzione per zone.
- 15 Se si modifica il nome host di un host del servizio di gestione, effettuare i seguenti passaggi aggiuntivi.
  - a Aggiornare gli agenti software nelle macchine virtuali esistenti.
  - b Ricreare eventuali ISO o modelli che contengono un agente guest.

## Operazioni successive

Verificare che vRealize Automation sia pronto per l'uso. Vedere la documentazione relativa a [backup e ripristino di vRealize Suite](#).

## Impostazione dell'URL di login di vRealize Automation su un nome personalizzato

Se si desidera che gli utenti di vRealize Automation effettuino il login a un URL con un nome diverso da quello dell'appliance o del servizio di bilanciamento del carico di vRealize Automation, eseguire le procedure di personalizzazione prima e dopo l'installazione.

### Procedura

- 1 Prima di procedere all'installazione, preparare un certificato che includa il CNAME desiderato, nonché i nomi dell'appliance e del servizio di bilanciamento del carico di vRealize Automation.
- 2 Installare vRealize Automation, immettendo il nome dell'appliance o del servizio di bilanciamento del carico come di consueto. Durante l'installazione, importare il certificato personalizzato.
- 3 Dopo l'installazione, in DNS creare un alias CNAME del nome comune, quindi impostarlo in modo che punti all'indirizzo VIP dell'appliance o del servizio di bilanciamento del carico.
- 4 Accedere come root all'interfaccia di amministrazione dell'appliance vRealize Automation.  
`https://vrealize-automation-appliance-FQDN:5480`
- 5 In **Impostazioni vRA > Impostazioni host**, modificare **Nome host** impostando il CNAME desiderato.

## Gestione della licenza vRealize Code Stream

È possibile abilitare vRealize Code Stream inserendo una licenza di vRealize Code Stream in vRealize Automation.

È possibile immettere la licenza di vRealize Code Stream in una di queste posizioni:

- Nella pagina di gestione delle licenze dell'installazione guidata di vRealize Automation. Per ulteriori informazioni, vedere [Installazione di vRealize Code Stream](#).
- Nella scheda Gestione licenze dell'interfaccia di gestione dell'appliance vRealize Automation. Per ulteriori informazioni, vedere [Applicazione di una licenza vRealize Code Stream a un'appliance](#).

## Installazione dell'agente di vRealize Log Insight su server IaaS

Per impostazione predefinita i server Windows in una configurazione vRealize Automation IaaS non comprendono l'agente di vRealize Log Insight.

vRealize Log Insight fornisce l'indicizzazione e l'aggregazione di registri ed è in grado di raccogliere, importare e analizzare i registri per esporre i problemi del sistema. Se si desidera catturare e analizzare i registri da server IaaS utilizzando vRealize Log Insight, è necessario installare separatamente l'agente di vRealize Log Insight per Windows.

Per ulteriori informazioni, vedere la [documentazione di VMware vRealize Log Insight](#).

Per impostazione predefinita le Appliance vRealize Automation includono l'agente di vRealize Log Insight.

## Modifica della porta del proxy di VMware Remote Console

Se il sito blocca o riserva la porta 8444, è possibile modificare la porta del proxy predefinita utilizzata da VMware Remote Console.

### Procedura

- 1 Accedere al prompt dei comandi dell'appliance vRealize Automation come utente root.
- 2 Aprire il seguente file in un editor di testo.  
`/etc/vcac/security.properties`
- 3 Modificare il valore predefinito 8444 di `consoleproxy.service.port` sostituendolo con quello di una porta non utilizzata.
- 4 Salvare e chiudere `security.properties`.
- 5 Riavviare l'appliance vRealize Automation.

In un ambiente HA, apportare la stessa modifica a tutte le appliance vRealize Automation.

## Ripristino del nome di dominio completo originale di un appliance vRealize Automation

È possibile che in alcuni casi il nome di dominio completo di un'appliance vRealize Automation venga modificato anche se non lo si desidera. Ad esempio, il nome di dominio completo viene modificato se si crea una directory di autenticazione integrata di Windows (IWA) per un dominio diverso dal dominio in cui si trova l'appliance.

Se si crea una directory IWA per un altro dominio, eseguire i passaggi seguenti per ripristinare il nome di dominio completo originale dell'appliance.

### Procedura

- 1 Accedere a vRealize Automation e creare la directory IWA nel modo consueto.  
Vedere [Configurazione di un collegamento Active Directory su LDAP/IWA](#).
- 2 Se si tratta di un ambiente HA, eseguire anche i passaggi in [Configurazione di Gestione directory per l'alta disponibilità](#).
- 3 La creazione di una directory IWA per un dominio diverso da quello in cui si trova l'appliance comporta la modifica del nome di dominio completo dell'appliance in modalità invisibile all'utente.  
Ad esempio, `va1.domain1.local` diventa `va1.domain2.local` quando si crea una directory IWA per `domain2.local`.  
Per annullare la modifica, è sufficiente rinominare ciascuna appliance utilizzando il nome di dominio completo originale. Vedere la procedura associata in [Modifica di nomi host e indirizzi IP](#).

- 4 Dopo aver ripristinato il nome di dominio completo originale per le appliance, accedere a ciascun nodo IaaS ed eseguire i passaggi seguenti.

- a Aprire il seguente file in un editor di testo.

C:\Program Files (x86)\VMware\VCAC\Management Agent\VMware.IaaS.Management.Agent.exe.Config

- b Modificare il nome di dominio completo di ciascuna appliance endpoint address= ripristinando quello originale.

Ad esempio, da:

```
<endpoint address="https://va1.domain2.local:5480/"
thumbprint="90C55BAEC53E31609EE1614CE4A8336848A8D4CF" />
<endpoint address="https://va2.domain2.local:5480/"
thumbprint="0468BF6EDBC6F2209BE01D0D7FD1094197E324ED" />
```

A:

```
<endpoint address="https://va1.domain1.local:5480/"
thumbprint="90C55BAEC53E31609EE1614CE4A8336848A8D4CF" />
<endpoint address="https://va2.domain1.local:5480/"
thumbprint="0468BF6EDBC6F2209BE01D0D7FD1094197E324ED" />
```

- c Salvare e chiudere VMware.IaaS.Management.Agent.exe.Config.

- 5 Accedere come root all'interfaccia di gestione dell'appliance vRealize Automation.

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

- 6 Passare a **Impostazioni vRA > Messaggistica** e fare clic su **Reimposta cluster RabbitMQ**.

- 7 Dopo aver completato la reimpostazione, accedere all'interfaccia di gestione di ciascuna appliance.

- 8 Passare a **Impostazioni vRA > Cluster** e verificare che tutti i nodi siano connessi al cluster.

## Configurazione di AAG (AlwaysOn Availability Group) SQL

Se si imposta AAG (AlwaysOn Availability Group) SQL dopo l'installazione di vRealize Automation, è necessario apportare modifiche alla configurazione.

Se si imposta AAG (AlwaysOn Availability Group) SQL dopo l'installazione, eseguire i passaggi in [Articolo della Knowledge Base VMware 2074607](#) per configurare vRealize Automation con il nome di dominio completo del listener AAG come host di SQL Server.

## Aggiunta di controller NIC dopo l'installazione di vRealize Automation

vRealize Automation supporta più controller NIC (Network Interface Controller). Dopo l'installazione, è possibile aggiungere NIC all'appliance vRealize Automation o al server Windows IaaS.

Per alcune distribuzioni di vRealize Automation, potrebbero essere necessari più NIC, ad esempio:

- Si desidera che la rete degli utenti e la rete dell'infrastruttura siano separate.

- È necessario un ulteriore NIC in modo che i server IaaS possano essere aggiunti a un dominio di Active Directory.

Per ulteriori informazioni sugli scenari che prevedono la presenza di più NIC, vedere il [post del blog VMware Cloud Management](#).

Per tre o più NIC, tenere presenti le seguenti limitazioni.

- VIDM richiede l'accesso al database Postgres e ad Active Directory.
- In un cluster HA, VIDM deve poter accedere all'URL del servizio di bilanciamento del carico.
- Le connessioni VIDM precedenti devono passare attraverso i primi due NIC.
- I NIC che seguono il secondo NIC non devono essere utilizzati o riconosciuti da VIDM.
- I NIC che seguono il secondo NIC non devono essere utilizzati per la connessione ad Active Directory.

Quando si configura una directory in vRealize Automation, utilizzare il primo o il secondo NIC.

### Prerequisiti

Installare completamente vRealize Automation nell'ambiente vCenter.

### Procedura

- 1 In vCenter, aggiungere NIC a ogni appliance vRealize Automation.
  - a Fare clic con il pulsante destro del mouse sull'appliance e selezionare **Modifica impostazioni**.
  - b Aggiungere NIC VMXNETn.
  - c Se è accesa, riavviare l'appliance.
- 2 Accedere come root all'interfaccia di gestione dell'appliance vRealize Automation.  
`https://vrealize-automation-appliance-FQDN:5480`
- 3 Selezionare **Rete** e verificare che siano disponibili più NIC.
- 4 Selezionare **Indirizzo** e configurare l'indirizzo IP per i NIC.

**Tabella 1-43. Esempio di configurazione di NIC**

Impostazione	Valore
Tipo di indirizzo IPv4	Static
Indirizzo IPv4	172.22.0.2
Maschera di rete	255.255.255.0

- 5 Verificare che tutti i nodi di vRealize Automation possano risolversi a vicenda in base al nome DNS.
- 6 Verificare che tutti i nodi di vRealize Automation possano accedere a qualsiasi nome di dominio completo con carico bilanciato per i componenti di vRealize Automation.
- 7 Se si utilizza Split-Brain DNS, verificare che tutti i nodi e i VIP di vRealize Automation abbiano lo stesso nome di dominio completo in DNS per ogni IP e VIP dei nodi.

- 8 In vCenter, aggiungere i NIC ai server Windows IaaS.
  - a Fare clic con il pulsante destro del mouse sul server IaaS e selezionare **Modifica impostazioni**.
  - b Aggiungere i NIC alla macchina virtuale del server IaaS.
- 9 In Windows, configurare i NIC del server IaaS aggiunti e i relativi indirizzi IP. Se necessario, consultare la documentazione Microsoft.

#### Operazioni successive

(Facoltativo) Se sono necessarie route statiche, vedere [Configurazione di route statiche](#).

## Configurazione di route statiche

Quando si aggiungono NIC a un'installazione di vRealize Automation, se sono necessarie route statiche, aprire una sessione del prompt dei comandi per configurarle.

#### Prerequisiti

Aggiungere più NIC ad appliance di vRealize Automation o a server Windows IaaS.

#### Procedura

- 1 Accedere come root alla riga di comando dell'appliance vRealize Automation.
- 2 Aprire il file di route in un editor di testo.  
`/etc/sysconfig/network/routes`
- 3 Individuare la riga `default` per il gateway predefinito ma non modificarla.

---

**Nota** Nei casi in cui il gateway predefinito deve essere modificato, usare invece l'interfaccia di gestione di vRealize Automation.

---

- 4 Sotto la riga `default`, aggiungere nuove righe per le route statiche. Ad esempio:

```
default 10.10.10.1 - -  
172.30.30.0 192.168.100.1 255.255.255.0 eth0  
192.168.210.0 192.168.230.1 255.255.255.0 eth2
```

- 5 Salvare e chiudere il file di route.
- 6 Riavviare l'appliance.
- 7 Nei cluster HA, ripetere la procedura per ogni appliance.
- 8 Accedere al server Windows di IaaS come amministratore.
- 9 Aprire un prompt dei comandi come amministratore.

- 10** Per configurare una route statica, immettere il comando `route -p add`, dove `-p` conserva la route statica a ogni riavvio. Ad esempio:

```
C:\Windows\system32> route -p add 172.30.30.0 mask 255.255.255.0 192.168.100.1 metric 1
OK!
```

Per ulteriori informazioni sulla configurazione di route statiche in Windows, vedere la documentazione Microsoft.

## Gestione delle patch di accesso

Il supporto tecnico per l'installazione di vRealize Automation potrebbe richiedere una patch software che si installa o si elimina utilizzando l'interfaccia di gestione dell'appliance vRealize Automation.

L'interfaccia di patch non può applicare la patch ai seguenti componenti vRealize Automation.

- Agente di gestione
- Agenti non vSphere come XenServer, VDI o Hyper-V

### Prerequisiti

- Creare snapshot di tutti i nodi di vRealize Automation durante l'installazione.
- Verificare che tutti i nodi nell'installazione di vRealize Automation siano attivi e in esecuzione.

Se si tenta di installare o rimuovere una patch senza che tutti i nodi siano in esecuzione, l'interfaccia di gestione dell'appliance vRealize Automation potrebbe smettere di rispondere. In tal caso, contattare il supporto tecnico. Non tentare di gestire le patch con altri metodi o utilizzare vRealize Automation finché non viene risolto il problema.

- Se l'ambiente utilizza servizi di bilanciamento del carico per l'alta disponibilità, disabilitare il traffico verso i nodi secondari solo dopo l'installazione o l'eliminazione delle patch.
- Se si installa una nuova patch, ottenere il file della patch e copiarlo nel file system disponibile per il browser che si utilizza per l'interfaccia di gestione dell'appliance vRealize Automation.
- Controllare [Knowledge Base di VMware](#) per informazioni aggiornate sulle patch.

Aprire la Knowledge Base e immettere *Patch di vRealize Automation* nella casella di ricerca. Ad esempio, l'[articolo 51708 di VMware Knowledge Base](#) viene monitorato e aggiornato con le informazioni più recenti sulla patch per vRealize Automation 7.4.

### Procedura

- 1 Accedere come root all'interfaccia di gestione dell'appliance vRealize Automation.  
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Fare clic su **Impostazioni vRA > Patch**.

- 3 In Gestione patch, fare clic sull'opzione desiderata e seguire le istruzioni visualizzate.

Opzione	Descrizione
<b>Nuova patch</b>	Installare una nuova patch scaricata.
<b>Patch installate</b>	Aggiungere le patch installate più di recente ai nodi del cluster appena aggiunti.
<b>Rollback</b>	Rimuovere le patch installate più di recente ed eseguire il rollback di vRealize Automation al livello di patch precedente.
<b>Cronologia</b>	Esaminare l'elenco delle patch installate e rimosse.

Per abilitare o disabilitare Gestione patch, eseguire il login al prompt dei comandi dell'appliance vRealize Automation come utente root e immettere uno dei seguenti comandi.

```
/opt/vmware/share/htdocs/service/hotfix/scripts/hotfix.sh enable
/opt/vmware/share/htdocs/service/hotfix/scripts/hotfix.sh disable
```

### Installazione di una nuova patch

È possibile installare nuove patch di vRealize Automation tramite l'interfaccia di gestione dell'appliance vRealize Automation.

#### Prerequisiti

Controllare i prerequisiti e passare all'interfaccia di gestione delle patch. Vedere [Gestione delle patch di accesso](#).

#### Procedura

- 1 Fare clic su **Nuova patch**.
- 2 Fare clic su **Carica patch**.
- 3 Individuare e selezionare il file della patch.
- 4 Una volta caricata la patch, esaminare i dettagli.
- 5 Se la patch non è corretta, annullare l'operazione facendo clic su **Rimuovi**. In caso contrario, fare clic su **Installa**.
- 6 Verificare che i prerequisiti siano soddisfatti e fare clic su **Installa**.  
L'installazione della patch potrebbe richiedere diversi minuti.
- 7 Fare clic su **Fine**.

Se l'installazione della patch non riesce, è possibile fare clic su **Riprova** per riprovare o su **Rimuovi** per annullare l'operazione. L'annullamento comporta il rollback di vRealize Automation allo stato in cui si trovava prima dell'inizio dell'installazione della patch.

### Installazione della patch corrente in nuovi nodi

È possibile aggiungere la patch di vRealize Automation installata più di recente ai nodi del cluster appena aggiunti.



## Prerequisiti

Controllare i prerequisiti e passare all'interfaccia di gestione delle patch. Vedere [Gestione delle patch di accesso](#).

## Procedura

- 1 Fare clic su **Patch installate**.
- 2 Selezionare la patch più recente.
- 3 Fare clic su **Installa**.
- 4 Seguire le istruzioni visualizzate.

## Rimozione della patch corrente

È possibile rimuovere la patch di vRealize Automation installata più di recente ed eseguire il rollback alla patch precedente.

## Prerequisiti

Passare all'interfaccia di gestione delle patch. Vedere [Gestione delle patch di accesso](#).

## Procedura

- 1 Fare clic su **Rollback**.
- 2 Selezionare la patch più recente.
- 3 Fare clic su **Rollback**.
- 4 Seguire le istruzioni visualizzate.

## Configurazione dell'accesso per il tenant predefinito

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 a vRealize Automation come amministratore di sistema del tenant predefinito.
  - a Passare all'interfaccia del prodotto vRealize Automation.  
`https://vrealize-automation-FQDN/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 su **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**.**

**Operazioni successive**

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 delle impostazioni del tenant](#).
- Gli amministratori IaaS preparano le risorse esterne per il provisioning. Vedere [Preparazioni esterne per il provisioning](#).
- 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 su come richiedere l'elemento e completare l'azione dell'utente manuale, vedere [Scenario: richiesta di contenuto iniziale per una distribuzione di prototipazione Rainpole](#).

## **Risoluzione dei problemi d'installazione di vRealize Automation**

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.

## Posizioni predefinite dei registri

Consultare i file dei registri di sistema e prodotti per avere maggiori informazioni su un'installazione non riuscita.

**Nota** Per la raccolta dei registri, si consiglia di sfruttare i pacchetti di contenuti di vRealize Automation e vRealize Orchestrator per vRealize Log Insight. I pacchetti di contenuti e Log Insight offrono un riepilogo consolidato dei componenti degli eventi di registro in vRealize Suite. Per ulteriori informazioni, visitare [VMware Solution Exchange](#).

Per l'elenco delle posizioni dei registri più recenti, vedere [Articolo della Knowledge Base VMware 2141175](#).

### 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	<b>Start &gt; Pannello di controllo &gt; Strumenti di amministrazione &gt; Visualizzatore eventi</b>

### 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

- 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.

**Tabella 1-44. 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 di vRealize Automation

È possibile creare un bundle di supporto di vRealize Automation tramite l'interfaccia di gestione dell'appliance vRealize Automation. I bundle di supporto raccolgono registri e consentono all'utente o al supporto tecnico di VMware di risolvere i problemi di vRealize Automation.

### Procedura

- 1 Aprire un browser Web e passare all'URL dell'interfaccia di gestione dell'appliance vRealize Automation.

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

- 2 Accedere come root, quindi fare clic su **Impostazioni vRA > Cluster**.

- 3 Fare clic su **Crea bundle di supporto**.

- 4 Fare clic su **Download** e salvare il file del bundle di supporto nel sistema.

I bundle di supporto includono informazioni dai server Windows IaaS e dall'appliance vRealize Automation. Se la connessione tra l'appliance vRealize Automation e i componenti di IaaS si interrompe, è possibile che nel bundle di supporto manchino i registri dei componenti di IaaS.

Per visualizzare i file di registro raccolti, decomprimere il bundle di supporto e aprire il file `Environment.html` in un browser Web. Senza connessione, i componenti di IaaS potrebbero essere visualizzati in rosso nella tabella Nodi. Un altro motivo per cui i registri di IaaS potrebbero mancare è dovuto al fatto che il servizio dell'agente di gestione di vRealize Automation è stato interrotto nei server Windows IaaS visualizzati in rosso.

## 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.
- 2 Eseguire nuovamente l'installazione o l'aggiornamento.

**Gli orari dei server non sono sincronizzati**

Se gli orari dei server IaaS non sono sincronizzati con l'appliance vRealize Automation, è possibile che l'installazione non riesca.

**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**

Sincronizzare tutte le appliance vRealize Automation e tutti i server IaaS Windows con la stessa origine di riferimento dell'ora. Non combinare origini di riferimento dell'ora diverse all'interno di una distribuzione di vRealize Automation.

- Impostare un'origine di riferimento dell'ora dell'appliance vRealize Automation:
  - a Accedere come root all'interfaccia di gestione dell'appliance vRealize Automation.  
`https://vrealize-automation-appliance-FQDN:5480`
  - b Selezionare **Admin > Impostazioni ora** e impostare l'origine di sincronizzazione dell'ora.

Opzione	Descrizione
Ora host	Sincronizza l'ora con quella dell'host ESXi dell'appliance vRealize Automation.
Server di riferimento ora	Sincronizza l'ora con quella di un server NTP (Network Time Protocol) esterno. Immettere il nome di dominio completo o l'indirizzo IP del server NTP.

- Per i server IaaS Windows, vedere [Attivazione della sincronizzazione di data e ora su Windows Server](#).

## 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 `vcac-config.exe.config` in un editor di testo e individuare l'indirizzo del repository:  
`<add key="repositoryAddress" value="https://IaaS-address:443/repository/" />`
- 2 Aprire Internet Explorer e passare all'indirizzo.
- 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 Aprire un browser Web e passare all'URL dell'interfaccia di gestione dell'appliance vRealize Automation.  
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Accedere come root e fare clic su **Rete**.
- 3 Immettere l'indirizzo FQDN o IP del server proxy del sito e il numero di porta.
- 4 Se il server proxy richiede credenziali, immettere nome utente e password.
- 5 Fare clic su **Salva impostazioni**.

## Operazioni successive

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 agli utenti di VMware Identity Manager](#)

## Passaggi di console per la configurazione del contenuto iniziale

Esiste un'alternativa all'uso dell'interfaccia d'installazione di vRealize Automation per creare l'account dell'amministratore della configurazione e il contenuto iniziale.

### Problema

Come ultima parte dell'installazione di vRealize Automation, si segue il processo per immettere una nuova password, creare l'account dell'utente locale configurationadmin e creare il contenuto iniziale. Se si verifica un errore, l'interfaccia passa a uno stato non ripristinabile.

### Soluzione

Anziché utilizzare l'interfaccia, immettere i comandi di console per creare l'utente configurationadmin e il contenuto iniziale. Si noti che l'interfaccia potrebbe non essere caricata dopo aver completato correttamente parte del processo, per cui potrebbero essere necessari solo alcuni comandi.

Ad esempio si potrebbero ispezionare i file di registro e l'esecuzione del workflow di vRealize Orchestrator e stabilire che la configurazione basata sull'interfaccia ha creato l'utente configurationadmin ma non il contenuto iniziale. In tal caso è possibile immettere solo gli ultimi due comandi di console per completare il processo.

### Procedura

- 1 Accedere alla console dell'appliance vRealize Automation come utente root.
- 2 Importare il workflow di vRealize Orchestrator immettendo il seguente comando:

```
/usr/sbin/vcac-config -e content-import --
workflow /usr/lib/vcac/tools/initial-config/vra-initial-config-bundle-
workflow.package --user $SSO_ADMIN_USERNAME --password $SSO_ADMIN_PASSWORD --
tenant $TENANT
```

- 3 Eseguire il workflow per creare l'utente configurationadmin:

```
/usr/bin/python /opt/vmware/share/htdocs/service/wizard/initialcontent/workfl
owexecutor.py --host $CURRENT_VA_HOSTNAME --username $SSO_ADMIN_USERNAME --
password $SSO_ADMIN_PASSWORD --workflowid f2b3064a-75ca-4199-
a824-1958d9c1efed --configurationAdminPassword $CONFIGURATIONADMIN_PASSWORD
--tenant $TENANT
```

- 4 Importare il blueprint ASD immettendo il seguente comando:

```
/usr/sbin/vcac-config -e content-import --
blueprint /usr/lib/vcac/tools/initial-config/vra-initial-config-bundle-
asd.zip --user $CONFIGURATIONADMIN_USERNAME --password
$CONFIGURATIONADMIN_PASSWORD --tenant $TENANT
```

**5** Eseguire il workflow per configurare il contenuto iniziale:

```
/usr/bin/python /opt/vmware/share/htdocs/service/wizard/initialcontent/workflowexecutor.py --host $CURRENT_VA_HOSTNAME --username $SSO_ADMIN_USERNAME --password $SSO_ADMIN_PASSWORD --workflowid ef00fce2-80ef-4b48-96b5-fdee36981770 --configurationAdminPassword $CONFIGURATIONADMIN_PASSWORD
```

**Impossibile eseguire il downgrade delle licenze di vRealize Automation**

Quando si invia la chiave di licenza di una versione precedente del prodotto, si verifica un errore.

**Problema**

Il seguente messaggio viene visualizzato quando si utilizza la pagina Gestione licenze dell'interfaccia di amministrazione di vRealize Automation per inviare la chiave a una versione del prodotto precedente a quella corrente. Ad esempio, nel caso in cui si inizi con una licenza Enterprise e si tenti di passare a una licenza Advanced.

```
Unable to downgrade existing license edition
```

**Causa**

Questa versione di vRealize Automation non supporta il downgrade delle licenze. È possibile aggiungere solo licenze di una versione uguale o successiva.

**Soluzione**

Per passare a una versione precedente, reinstallare vRealize Automation.

**Risoluzione dei problemi dell'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 dei programmi di installazione dall'appliance vRealize Automation non è riuscito.

**Problema**

I programmi di installazione non si scaricano quando viene eseguito `setup__vrealize-automation-appliance-FQDN@5480.exe`.

**Causa**

- Problemi di connettività di rete durante la connessione alla macchina dell'appliance vRealize Automation.
- Impossibilità di connettersi alla macchina dell'appliance vRealize Automation perché non è possibile raggiungere la macchina o la stessa non risponde prima del timeout della connessione.

**Soluzione**

- 1 Verificare che sia possibile connettersi all'URL di vRealize Automation in un browser Web.  
`https://vrealize-automation-appliance-FQDN`
- 2 Consultare gli altri argomenti relativi alla risoluzione dei problemi dell'appliance vRealize Automation.
- 3 Scaricare il file di installazione e riconnettersi all'appliance vRealize Automation.

**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 Appliance vRealize Automation 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.

**Operazioni successive**

Accedere alla pagina Tenant per accertarsi di poter accedere senza l'errore.

## Identity Manager di Gestione directory non si avvia dopo il riavvio di Horizon Workspace

In un ambiente vRealize Automation ad alta disponibilità, Identity Manager di Gestione directory 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
```

### Causa

Identity Manager potrebbe non avviarsi in un ambiente ad alta disponibilità a causa di problemi con l'utilità di gestione dei dati liquibase utilizzata da vRealize Automation.

### Soluzione

1 Accedere come utente root a una sessione della console nell'appliance vRealize Automation.

2 Arrestare il servizio Horizon Workspace immettendo il seguente comando.

```
#service horizon-workspace stop
```

3 Aprire la shell di Postgres come super user.

```
su postgres
```

4 Passare alla directory bin corretta.

```
cd /opt/vmware/vpostgres/current/bin
```

5 Stabilire la connessione al database.

```
psql vcac
```

6 Da `saas.databasechangelock`, eseguire la seguente query SQL.

```
select * from databasechangelock;
```

Se l'output mostra il valore "t" di true, il blocco dev'essere rilasciato manualmente.

7 Per rilasciare manualmente il blocco, eseguire la query SQL seguente.

```
update saas.databasechangelock set locked=FALSE, lockgranted=NULL,
lockedby=NULL where id=1;
```

8 Da `saas.databasechangelock`, eseguire la seguente query SQL.

```
select * from databasechangelock;
```

L'output dovrebbe mostrare il valore "f" di false, a indicare che il blocco non è attivo.

**9** Uscire dal database vcac Postgres.

```
vcac=# \q
```

**10** Chiudere la shell di Postgres.

```
exit
```

**11** Avviare il servizio Horizon Workspace.

```
#service horizon-workspace start
```

## Errate assegnazioni del ruolo dell'appliance dopo failover

In seguito a un failover, l'assegnazione dei ruoli nei nodi master e replica dell'appliance vRealize Automation potrebbe non essere corretta. Ciò influisce su tutti i servizi che richiedono l'accesso in scrittura al database.

### Problema

In un cluster di appliance vRealize Automation ad alta disponibilità, si arresta o si rende inaccessibile il nodo master del database. Si utilizza la console di gestione su un altro nodo per promuovere tale nodo come il nuovo master, che ripristina l'accesso in scrittura al database vRealize Automation.

In seguito si riporta il vecchio nodo master online, ma la scheda Database nella sua console di gestione elenca ancora il nodo come nodo master anche se non lo è. Eventuali tentativi di utilizzare qualsiasi console di gestione dei nodi per eliminare il problema promuovendo ufficialmente il vecchio nodo a master falliranno.

### Soluzione

Quando si verifica un failover, attenersi a queste linee guida quando si configurano nodi master vecchi anziché nuovi.

- Prima di promuovere un altro nodo a master, rimuovere il precedente nodo master dal pool del bilanciamento del carico dei nodi dell'appliance vRealize Automation.
- Per fare in modo che vRealize Automation ripristini un vecchio nodo master nel cluster, consentire alla vecchia macchina di connettersi online. Quindi aprire la nuova console di gestione dei master. Cercare il vecchio nodo elencato come `invalid` nella scheda Database e fare clic sul suo pulsante **Reimposta**.

Dopo una corretta reimpostazione, è possibile ripristinare il vecchio nodo nel pool del bilanciamento del carico dei nodi dell'appliance vRealize Automation.

- Per ripristinare un vecchio nodo master nel cluster, collegare la macchina online e unirla al cluster come se fosse un nuovo nodo. Durante l'unione, specificare il nodo appena promosso come nodo primario.

Dopo una corretta unione, è possibile ripristinare il vecchio nodo nel pool del bilanciamento del carico dei nodi dell'appliance vRealize Automation.

- Finché non si reimposta o unisce di nuovo correttamente un vecchio nodo master al cluster, non utilizzarne la console di gestione per operazioni di gestione del cluster anche se il nodo torna online.

- Dopo aver eseguire correttamente la reimpostazione o la nuova unione, è possibile promuovere un vecchio nodo nel master.

### **Errori dopo la promozione di nodi di replica e master**

I problemi relativi allo spazio su disco, così come la promozione di nodi di database di appliance vRealize Automation di replica e master, possono causare problemi di provisioning.

#### **Problema**

Il nodo master esaurisce lo spazio su disco. L'utente accede all'interfaccia di gestione della pagina Database del nodo master e promuove al ruolo di nuovo master un nodo di replica dotato di spazio sufficiente. Quando l'utente aggiorna la pagina dell'interfaccia di gestione, le promozioni sembrano essere andate a buon fine anche se viene visualizzato un messaggio di errore.

In un secondo momento, l'utente libera spazio su disco sul nodo che era del vecchio master. Dopo aver di nuovo promosso il nodo a master, tuttavia, le operazioni di provisioning non riescono perché si bloccano nello stato IN\_PROGRESS.

#### **Causa**

vRealize Automation non può aggiornare correttamente la configurazione di un vecchio nodo master quando il problema è dovuto all'insufficienza di spazio.

#### **Soluzione**

Se l'interfaccia di gestione restituisce errori durante la promozione, escludere temporaneamente il nodo dal bilanciamento del carico. Correggere il problema del nodo, ad esempio aggiungendo un disco, prima di includerlo di nuovo nel bilanciamento del carico. Quindi, aggiornare la pagina Database dell'interfaccia di gestione e verificare che i nodi master e replica siano corretti.

### **Registrazioni dei servizi componenti di vRealize Automation non corrette**

L'interfaccia di gestione dell'appliance vRealize Automation consente di risolvere i problemi di registrazione relativi ai servizi componenti di vRealize Automation.

#### **Problema**

Durante il normale funzionamento, tutti i servizi componenti di vRealize Automation devono essere univoci e trovarsi nello stato REGISTRATI. Qualsiasi altro set di condizioni può causare comportamenti non prevedibili da parte di vRealize Automation.

#### **Causa**

Di seguito sono forniti alcuni esempi di problemi che possono verificarsi con i servizi componenti di vRealize Automation.

- Un servizio è diventato inattivo.
- A causa delle impostazioni del server, un servizio si trova in uno stato diverso da REGISTRATO.
- A causa di una dipendenza da un altro servizio, un servizio si trova in uno stato diverso da REGISTRATO.

## Soluzione

Registrare nuovamente i servizi componenti in cui si verificano problemi.

- 1 Creare uno snapshot dell'appliance vRealize Automation.

Potrebbe essere necessario tornare allo snapshot se si provano modifiche differenti del servizio che portano l'appliance a uno stato imprevisto.

- 2 Accedere come root all'interfaccia di gestione dell'appliance vRealize Automation.

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

- 3 Fare clic su **Servizi**.

- 4 Nell'elenco dei servizi, cercare un servizio il cui stato non è corretto o in cui si verificano altri problemi.

- 5 Se il servizio difettoso è `iaas-service`, andare al passaggio successivo.

Altrimenti, per fare in modo che vRealize Automation registri di nuovo il servizio, accedere come root a una sessione della console nell'appliance vRealize Automation e riavviare vRealize Automation immettendo il comando seguente.

```
service vcac-server restart
```

Se all'istanza vRealize Orchestrator incorporata sono associati servizi, immettere il seguente comando aggiuntivo.

```
service vco-restart restart
```

- 6 Se il servizio con problemi è `iaas-service`, eseguire i passaggi seguenti per registrarlo nuovamente.

- a Non annullare la registrazione del servizio.
- b Sul server Web IaaS primario, accedere con un account dotato di diritti amministrativi.
- c Aprire un prompt dei comandi come amministratore.
- d Eseguire il comando seguente.

```
"C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe" RegisterSolutionUser -url https://appliance-or-load-balancer-IP-or-FQDN/ -t vsphere.local -cu administrator -cp password -f "C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.data" -v
```

La password è quella dell'utente `administrator@vsphere.local`.

- e Eseguire un comando per aggiornare le informazioni di registrazione nel database di IaaS.

SQL Server con autenticazione Windows:

```
"C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe" MoveRegistrationDataToDb -s IaaS-SQL-server-IP-or-FQDN -d SQL-database-name -f "C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.data" -v
```



SQL Server con autenticazione SQL nativa:

```
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe" MoveRegistrationDataToDb -s SQL-server-IP-or-FQDN -d SQL-database-name -su SQL-user -sp SQL-user-password -f "C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.data" -v
```

Per trovare il nome del server o del database, analizzare il file seguente in un editor di testo e cercare repository. I valori di Data Source e Initial Catalog rappresentano rispettivamente l'indirizzo del server e il nome del database.

```
C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Web\Web.config
```

L'utente SQL deve avere i privilegi DBO per il database.

- f Registrare gli endpoint eseguendo i comandi seguenti:

```
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe" RegisterEndpoint --EndpointAddress https://IaaS-Web-server-or-load-balancer-IP-or-FQDN /vcac --Endpoint ui -v
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe" RegisterEndpoint --EndpointAddress https://IaaS-Web-server-or-load-balancer-IP-or-FQDN /WAPI --Endpoint wapi -v
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe" RegisterEndpoint --EndpointAddress https://IaaS-Web-server-or-load-balancer-IP-or-FQDN /repository --Endpoint repo -v
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe" RegisterEndpoint --EndpointAddress https://IaaS-Web-server-or-load-balancer-IP-or-FQDN /WAPI/api/status --Endpoint status -v
```

- g Registrare gli elementi del catalogo eseguendo il comando seguente:

```
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe" RegisterCatalogTypesAsync -v
```

- h Riavviare IIS.

```
iisreset
```

- i Accedere all'host del servizio di gestione di IaaS primario.

- j Riavviare il servizio di Windows di vRealize Automation.

```
VMware vCloud Automation Center Service
```

- 7 Per ripetere la registrazione di qualsiasi servizio associato a un sistema esterno, ad esempio un'istanza vRealize Orchestrator esterna, accedere al sistema esterno per riavviare i servizi.

### L'aggiunta di una NIC causa errori nell'interfaccia di gestione

Dopo aver aggiunto una seconda scheda dell'interfaccia di rete (NIC) a un'appliance vRealize Automation, il caricamento di alcune pagine dell'interfaccia di gestione di vRealize Automation non viene eseguito correttamente.

## Problema

Dopo aver completato correttamente l'aggiunta di una seconda NIC tramite vCenter, le seguenti pagine dell'interfaccia di gestione di vRealize Automation visualizzano errori e non vengono caricate.

- La pagina **Rete > Stato** visualizza un errore relativo a uno script che non risponde.
- La pagina **Rete > Indirizzo** visualizza un errore relativo alla lettura non riuscita delle informazioni dell'interfaccia di rete.

## Causa

A partire dalla versione 7.3, l'appliance vRealize Automation supporta la coesistenza di due NIC. Tuttavia, il modello di engineering su cui è basata l'appliance impedisce il funzionamento corretto dell'interfaccia di gestione finché non viene applicata la soluzione.

## Soluzione

Dopo aver aggiunto una seconda NIC, riavviare l'appliance vRealize Automation.

## Impossibile promuovere un'appliance virtuale secondaria al livello master

In vRealize Automation, una quantità di memoria insufficiente nell'appliance virtuale potrebbe impedire le promozioni dell'appliance virtuale nel cluster.

## Problema

La memoria del nodo master è insufficiente. Si accede quindi alla pagina Database dell'interfaccia di gestione di tale nodo e si tenta di promuovere un nodo secondario al ruolo di nuovo master. Si verifica il seguente errore.

```
Fail to execute on Node node-name, host is master-FQDN
because of: Could not read remote lock command result for node: node-name
on address: master-FQDN, reason is: 500 Internal Server Error
```

## Causa

La promozione riesce solo quando tutti i nodi possono confermare la riconfigurazione in un master appena promosso. La memoria insufficiente impedisce al vecchio master di confermare, anche se tutti i nodi sono raggiungibili.

## Soluzione

Spegnere il nodo master la cui memoria è insufficiente. Accedere alla pagina Database dell'interfaccia di gestione del nodo secondario e promuovere il nodo secondario.

## Il tempo di conservazione del registro della sincronizzazione di Active Directory è troppo breve

In vRealize Automation, i registri della sincronizzazione di Active Directory vengono conservati solo per un paio di giorni.

**Problema**

Dopo due giorni, i registri della sincronizzazione di Active Directory non sono più disponibili nell'interfaccia di gestione. Anche le cartelle dei registri non sono più disponibili nella seguente directory dell'appliance vRealize Automation.

```
/db/elasticsearch/horizon/nodes/0/indices
```

**Causa**

Per risparmiare spazio, vRealize Automation imposta su tre giorni il tempo di conservazione massimo dei registri della sincronizzazione di Active Directory.

**Soluzione**

- 1 Accedere a una sessione della console nell'appliance vRealize Automation come utente root.
- 2 Aprire il seguente file in un editor di testo.  
`/usr/local/horizon/conf/runtime-config.properties`
- 3 Aumentare il valore della proprietà `analytics.maxQueryDays`.
- 4 Salvare e chiudere `runtime-config.properties`.
- 5 Riavviare Identity Manager e i servizi di ricerca flessibili.

```
service horizon-workspace restart
service elasticsearch restart
```

**RabbitMQ non è in grado di risolvere i nomi host**

Per impostazione definita, RabbitMQ utilizza nomi host brevi per le appliance vRealize Automation. Ciò potrebbe impedire la risoluzione reciproca dei nodi.

**Problema**

Si tenta di aggiungere un'altra appliance vRealize Automation al cluster e si verifica un errore simile al seguente.

```
Clustering node 'rabbit@sc2-rdops-vm01-dhcp-62-2' with rabbit@company ...
Error: unable to connect to nodes [rabbit@company]: nodedown

DIAGNOSTICS
=====

attempted to contact: [rabbit@company]

rabbit@company:
  * unable to connect to epmd (port 4369) on company: nxdomain (non-existing domain)

current node details:
- node name: 'rabbitmq-cli-11@sc2-rdops-vm01-dhcp-62-2'
- home dir: /var/lib/rabbitmq
```

```
- cookie hash: 4+kP1tKnxGYaGjrPL2C8bQ==
```

```
[2017-09-01 14:58:04] [root] [INFO] RabbitMQ join failed with exit code: 69, see RabbitMQ logs for details.
```

### Causa

La configurazione di rete non consente la risoluzione reciproca delle appliance vRealize Automation in base al nome host breve.

### Soluzione

- 1 Per tutte le appliance vRealize Automation nella distribuzione, accedere come root a una sessione della console.

- 2 Arrestare il servizio RabbitMQ.

```
service rabbitmq-server stop
```

- 3 Aprire il seguente file in un editor di testo.

```
/etc/rabbitmq/rabbitmq-env.conf
```

- 4 Impostare la proprietà seguente su true.

```
USE_LONGNAME=true
```

- 5 Salvare e chiudere rabbitmq-env.conf.

- 6 Reimpostare RabbitMQ.

```
vcac-vami rabbitmq-cluster-config reset-rabbitmq-node
```

- 7 In un solo nodo dell'appliance vRealize Automation, eseguire il seguente script.

```
vcac-config cluster-config-ping-nodes --services rabbitmq-server
```

- 8 In tutti i nodi, verificare che il servizio RabbitMQ sia avviato.

```
vcac-vami rabbitmq-cluster-config get-rabbitmq-status
```

## Risoluzione dei problemi relativi ai componenti IaaS

Negli argomenti relativi alla risoluzione dei problemi dei componenti IaaS di vRealize Automation vengono fornite soluzioni per i potenziali problemi di installazione che potrebbero verificarsi quando si utilizza vRealize Automation.

### Il programma di correzione dei prerequisiti non può installare le funzionalità di .NET

L'opzione **Risolvi** di Controllo prerequisiti di vRealize Automation non riesce e vengono visualizzati messaggi nei quali è indicata l'impossibilità di trovare l'origine di installazione di .NET 3.5.1.

### Problema

Controllo prerequisiti deve verificare che .NET 3.5.1 sia installato per poter soddisfare i requisiti per i sistemi Windows Server 2008 R2 con IIS 7.5 e i sistemi Windows Server 2012 R2 con IIS 8.

## Causa

Per Windows Server 2012 R2, l'impossibilità di connettersi a Internet può impedire l'installazione automatica di .NET. Anche determinati aggiornamenti di Windows 2012 R2 possono impedire l'installazione. Il problema si verifica perché la versione di Windows non dispone di una copia locale dell'origine di installazione di .NET Framework 3.5.

## Soluzione

Fornire manualmente un'origine di installazione di .NET Framework 3.5.

- 1 Sull'host Windows, montare un'immagine ISO del supporto d'installazione di Windows Server 2012 R2.
- 2 In Server Manager, abilitare .NET Framework 3.5 utilizzando Aggiunta guidata ruoli e funzionalità.
- 3 Durante la procedura guidata, selezionare il percorso d'installazione di .NET Framework 3.5 nell'immagine ISO del supporto.
- 4 Dopo aver aggiunto .NET Framework 3.5, eseguire nuovamente Controllo prerequisiti di 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 dell'appliance vRealize Automation e SSO.

## Problema

Quando si utilizzano funzionalità 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 come 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 dell'appliance vRealize Automation non può continuare quando la password dell'account del servizio 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 dell'appliance vRealize Automation non è riuscita a causa di parametri `msiexec` 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

È possibile che l'installazione di vRealize Automation non riesca se il programma di 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 all'appliance vRealize Automation o 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 all'URL di vRealize Automation in un browser Web.

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

- 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.

- Da un browser Web, controllare lo stato del servizio MetaModel e verificare che non vengano visualizzati errori relativi al certificato:

`https://FQDN-or-IP/repository/data/MetaModel.svc`

- 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.

- Da un browser Web, controllare lo stato del servizio MetaModel:

`https://FQDN-or-IP/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.

### I server Windows IaaS non supportano FIPS

Un'installazione non può avere esito positivo se è abilitato lo standard FIPS (Federal Information Processing Standard).

#### Problema

L'installazione non riesce con il seguente errore durante l'installazione del componente Web IaaS.

Questa implementazione non fa parte degli algoritmi crittografici con convalida FIPS della piattaforma Windows.

#### Causa

vRealize Automation IaaS è creato sulla base di Microsoft Windows Communication Foundation (WCF), che non supporta FIPS.

#### Soluzione

Disabilitare i criteri FIPS sul server Windows IaaS.

- 1 Accedere a **Start > Pannello di controllo > Strumenti di amministrazione > Criteri di sicurezza locali**.
- 2 Nella finestra di dialogo Criteri di gruppo, in **Criteri locali**, selezionare **Opzioni di sicurezza**.
- 3 Trovare e disabilitare la voce seguente.

Crittografia di sistema: utilizza algoritmi FIPS compatibili per crittografia, hash e firma.

### 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 [Articolo della Knowledge Base Microsoft 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.

Inoltre, l'host del servizio di gestione di IaaS deve essere in grado di risolvere il nome NETBIOS dell'host del database SQL Server di IaaS. Se non è in grado di risolvere il nome NETBIOS, aggiungere il nome NETBIOS di SQL Server al file `/etc/hosts` della macchina del servizio di gestione e riavviare il servizio di gestione.

---

- 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 all'interfaccia del prodotto di vRealize Automation.  
`https://vrealize-automation-appliance-FQDN/vcac/org/tenant-name`
  - 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 server IaaS clonati da un modello in cui DTC era già installato contengono identificatori duplicati per DTC, che impediscono la comunicazione tra i nodi.

## Problema

Si verifica un errore del servizio di gestione IaaS e nel registro viene visualizzato il messaggio riportato di seguito.

```
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 server IaaS in cui DTC è già installato, il clone contiene lo stesso identificatore univoco per DTC dell'elemento padre. La comunicazione tra le due macchine non riesce.

## Soluzione

- 1 Sul clone aprire un prompt dei comandi come Amministratore.
- 2 Eseguire il comando riportato di seguito.  
`msdtc -uninstall`
- 3 Riavviare il clone.
- 4 Aprire un altro prompt dei comandi ed eseguire il comando riportato di seguito.  
`msdtc -install manager-service-host-FQDN`

## 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 `@tuodominio` 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`.

### Accesso con alta disponibilità non riuscito

Quando sono presenti più appliance vRealize Automation, devono essere in grado identificarsi a vicenda mediante il nome host breve. Altrimenti non è possibile effettuare l'accesso.

**Problema**

Si configura vRealize Automation per l'alta disponibilità installando un'ulteriore appliance vRealize Automation. Quando si tenta di accedere a vRealize Automation, viene visualizzato un messaggio sulla licenza non valida. Tuttavia il messaggio non è corretto perché si è determinato che la licenza è valida.

**Causa**

I nodi dell'appliance vRealize Automation non costituiscono un cluster ad alta disponibilità corretto finché non sono in grado di risolvere i nomi host brevi dei nodi nel cluster.

**Soluzione**

Per consentire a un cluster di appliance vRealize Automation ad alta disponibilità di risolvere nomi host brevi, adottare uno degli approcci seguenti. È necessario modificare tutte le appliance del cluster.

**Procedura**

- Modificare o creare una riga di ricerca in `/etc/resolv.conf`. La riga deve contenere domini che includono appliance vRealize Automation. Per separare più domini, inserire uno spazio tra un dominio e l'altro. Ad esempio:

```
search sales.mycompany.com support.mycompany.com
```

- Modificare o creare le righe di dominio in `/etc/resolv.conf`. Ogni riga deve contenere un dominio che include appliance vRealize Automation. Ad esempio:

```
domain support.mycompany.com
```

- Aggiungere le righe al file `/etc/hosts` affinché ogni nome breve di appliance vRealize Automation sia mappato al nome di dominio completo corrispondente. Ad esempio:

```
node1    node1.support.mycompany.com
node2    node2.support.mycompany.com
```

**Il proxy impedisce l'accesso agli utenti di VMware Identity Manager**

La configurazione per l'utilizzo di un proxy potrebbe impedire l'accesso agli utenti di VMware Identity Manager.

**Problema**

vRealize Automation viene configurato per accedere alla rete tramite un server proxy e quando gli utenti di VMware Identity Manager provano ad accedere, viene visualizzato il seguente messaggio di errore.

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 dell'appliance vRealize Automation come utente root.
- 2 Aprire il seguente file in un editor di testo.  
`/etc/sysconfig/proxy`
- 3 Aggiornare la riga NO\_PROXY in modo che il server proxy venga ignorato per gli accessi a VMware Identity Manager.  
  
`NO_PROXY=vrealize-automation-hostname`  
  
Ad esempio: `NO_PROXY=localhost, 127.0.0.1, automation.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`

## Aggiornamento di vRealize Automation

È possibile aggiornare l'ambiente vRealize Automation all'ultima versione.

In base all'ambiente vRealize Automation corrente è possibile eseguire l'aggiornamento all'ultima versione eseguendo un aggiornamento sul posto o un aggiornamento affiancato. Esaminare le informazioni su questa pagina per determinare il metodo di aggiornamento migliore per il proprio ambiente.

Un aggiornamento sul posto è un processo con passaggi multipli. Le procedure vengono eseguite rispettando un ordine particolare per aggiornare i vari componenti nell'ambiente corrente. È necessario aggiornare tutti i componenti del prodotto alla stessa versione. Per questi percorsi è possibile eseguire solo un aggiornamento sul posto.

- Da vRealize Automation 6.2.5 a 7.4
- Da vRealize Automation 7.1 a 7.4
- Da vRealize Automation 7.2 a 7.4
- Da vRealize Automation 7.3.x alla versione 7.4

Un aggiornamento affiancato trasferisce i dati presenti nell'ambiente vRealize Automation corrente a un ambiente di destinazione distribuito con la versione più recente di vRealize Automation. Per i seguenti percorsi è possibile eseguire un aggiornamento affiancato.

- Da vRealize Automation (dalla versione 6.2.0 alla versione 6.2.5) a 7.4
- Da vRealize Automation 7.0 e 7.0.1 a 7.4
- Da vRealize Automation 7.1, 7.2 e 7.3.x alla versione 7.4

La migrazione non modifica l'ambiente corrente. Se l'ambiente corrente è integrato con vCloud Director, vCloud Air o dispone di endpoint fisici, è necessario utilizzare la migrazione per eseguire un aggiornamento. La migrazione rimuove tutti gli endpoint non supportati e tutti gli elementi associati ad essi nell'ambiente di destinazione.

Individuare la versione corrente di vRealize Automation in questa tabella. Utilizzare i documenti disponibili a destra per eseguire un aggiornamento dell'ambiente vRealize Automation all'ultima versione.

**Tabella 1-45. Percorsi di aggiornamento supportati per vRealize Automation 7.4**

Versione correntemente installata	Documentazione per aggiornamenti incrementali
vRealize Automation 7.1, 7.2 o 7.3.x	Consultare uno dei seguenti argomenti. <ul style="list-style-type: none"> <li>■ <a href="#">Aggiornamento di vRealize Automation 7.1 o versioni successive alla versione 7.4</a></li> <li>■ <a href="#">Migrazione a vRealize Automation 7.4</a></li> </ul>
vRealize Automation 7.0 o 7.0.1	Vedere <a href="#">Migrazione a vRealize Automation 7.4</a> .
vRealize Automation 6.2.5	Consultare uno dei seguenti argomenti. <ul style="list-style-type: none"> <li>■ <a href="#">Aggiornamento di vRealize Automation 6.2.5 alla versione 7.4</a></li> <li>■ <a href="#">Migrazione a vRealize Automation 7.4</a></li> </ul>
vRealize Automation 6.2.0, 6.2.1, 6.2.2, 6.2.3, 6.2.4	Vedere <a href="#">Migrazione a vRealize Automation 7.4</a>

Questa tabella include informazioni relative all'aggiornamento da una versione di vCloud Automation Center precedente. Prima di eseguire l'aggiornamento alla versione più recente di vRealize Automation, è necessario eseguire l'aggiornamento a vRealize Automation 6.2.5. È possibile trovare i collegamenti alla documentazione per le versioni 5.x e 6.x di vCloud Automation Center e vRealize Automation all'indirizzo <https://www.vmware.com/support/pubs/vcac-pubs.html>.

**Tabella 1-46. Percorsi di aggiornamento supportati per vRealize Automation 6.2.5**

Versione correntemente installata	Documentazione per aggiornamenti incrementali
vCloud Automation Center 6.0	Eseguire gli aggiornamenti nell'ordine seguente: <ol style="list-style-type: none"> <li>1 <i>Aggiornamento di vCloud Automation Center 6.0 alla versione 6.0.1</i></li> <li>2 <i>Aggiornamento a vCloud Automation Center 6.1</i></li> <li>3 <i>Aggiornamento a vRealize Automation 6.2.x</i></li> </ol>
vCloud Automation Center 6.0.1	Eseguire gli aggiornamenti nell'ordine seguente: <ol style="list-style-type: none"> <li>1 <i>Aggiornamento a vCloud Automation Center 6.1</i></li> <li>2 <i>Aggiornamento a vRealize Automation 6.2.x</i></li> </ol>
vCloud Automation Center 6.1.x	<i>Aggiornamento a vRealize Automation 6.2.x</i>
vRealize Automation 6.2.x	Aggiornare direttamente alla versione 6.2.5 come descritto in <i>Aggiornamento a vRealize Automation 6.2.x</i> .

**Nota** Cambiato il nome di vCloud Automation Center in vRealize Automation nella 6.2.0. Sono stati modificati solamente i nomi dei servizi e l'interfaccia utente. I nomi delle directory e i nomi dei programmi che contengono vcac non sono interessati da questa modifica.



Se si esegue l'aggiornamento da un ambiente 6.2.x, esaminare questi elementi.

- Lo strumento di assistenza all'aggiornamento di VMware vRealize per i test in ambiente di produzione analizza l'ambiente di vRealize Automation 6.2.x per rilevare eventuali configurazioni di funzionalità che possono provocare problemi di aggiornamento e verifica che l'ambiente sia pronto per l'aggiornamento. Lo strumento può essere scaricato dalla pagina di download del prodotto di [VMware vRealize Production Test Tool](#).
- L'aggiornamento da un ambiente con versione 6.2.x alla versione più recente di vRealize Automation introduce molti cambiamenti funzionali. Per ulteriori informazioni, vedere [Considerazioni sull'aggiornamento a questa versione di vRealize Automation](#).
- Se la distribuzione di vRealize Automation 6.2.x è stata personalizzata, contattare lo staff dell'assistenza CCE per ulteriori informazioni sugli aspetti correlati all'aggiornamento.
- I controlli del dizionario delle proprietà che non sono supportati dopo l'aggiornamento possono essere ripristinati utilizzando le relazioni tra vRealize Orchestrator e il dizionario delle proprietà.
- Se nell'ambiente di origine sono presenti workflow che contengono codice obsoleto, consultare la [guida alla migrazione dell'estensibilità di vRealize Automation](#) per informazioni sulle modifiche al codice necessarie per la conversione in sottoscrizioni del gestore di eventi.

Per evitare un problema noto durante l'aggiornamento da vRealize Automation 6.2.0, eseguire i passaggi seguenti in tutti i nodi dei siti Web di IaaS prima di procedere con l'aggiornamento. Questo problema riguarda solo la versione 6.2.0. Altre versioni 6.2.x non sono interessate.

- 1 Aprire Blocco note con i diritti amministrativi. Dal menu Start, fare clic con il pulsante destro del mouse sull'icona del Blocco note e scegliere **Esegui come amministratore**.
- 2 Aprire il file seguente:  
C:\Programmi (x86)\VMware\VCAC\Server\Model Manager Web\web.config
- 3 Individuare la seguente istruzione nel file:  
<!-- add key="DisableMessageSignatureCheck" value="false"-->
- 4 Rimuovere il commento dell'istruzione e modificare il valore da false a true.  
<add key="DisableMessageSignatureCheck" value="true" />
- 5 Salvare il file.  
Se Blocco note richiede di eseguire l'operazione Salva con nome, non aprire il Blocco note come amministratore e tornare al passaggio 1.
- 6 Aprire una finestra del prompt dei comandi con diritti amministrativi. Dal menu Start, fare clic con il pulsante destro del mouse sull'icona del Prompt dei comandi e scegliere **Esegui come amministratore**.
- 7 Eseguire il reset.
- 8 Ripetere i passaggi da 1 a 7 per tutti i nodi dei siti Web.

## Aggiornamento di vRealize Automation 7.1 o versioni successive alla versione 7.4

Quando si esegue l'aggiornamento dell'ambiente vRealize Automation 7.1 o versione successiva alla versione più recente, si utilizzano le procedure di aggiornamento specifiche per l'ambiente 7.1 o successivo.

Queste informazioni si riferiscono specificamente all'aggiornamento di vRealize Automation 7.1 o versione successiva alla versione 7.4. Per informazioni su altri percorsi di aggiornamento supportati, vedere [Aggiornamento di vRealize Automation](#).

### Aggiornamento di vRealize Automation 7.1, 7.2 o 7.3.x alla versione 7.4

È possibile eseguire l'aggiornamento dell'ambiente vRealize Automation 7.1, 7.2 o 7.3.x corrente alla versione 7.4. Per questa operazione, è necessario utilizzare procedure di aggiornamento specifiche per questa versione.

Un aggiornamento sul posto è un processo in tre passaggi. Aggiornare i componenti dell'ambiente corrente nel seguente ordine.

- 1 Appliance vRealize Automation
- 2 Server Web IaaS
- 3 vRealize Orchestrator

È necessario aggiornare tutti i componenti del prodotto alla stessa versione.

A partire da vRealize Automation 7.2, JFrog Artifactory Pro non è più fornito in dotazione con l'appliance vRealize Automation. Se si esegue l'aggiornamento da una versione precedente di vRealize Automation, il processo di aggiornamento rimuove JFrog Artifactory Pro. Per ulteriori informazioni, vedere [Knowledge Base 2147237](#).

### Prerequisiti per l'aggiornamento di vRealize Automation

Prima di eseguire l'aggiornamento dell'ambiente vRealize Automation 7.1, 7.2 o 7.3.x alla versione 7.4, esaminare i seguenti prerequisiti.

#### Requisiti della configurazione del sistema

Prima di un aggiornamento, verificare che siano soddisfatti i seguenti prerequisiti.

- Verificare che tutte le appliance e i server facenti parte della distribuzione soddisfino i requisiti di sistema relativi alla versione più recente. Vedere la *vRealize Automation Matrice di supporto* nella [documentazione di VMware vRealize Automation](#).
- Consultare il documento *VMware Product Interoperability Matrix* sul sito Web di VMware per informazioni sulla compatibilità con altri prodotti VMware.
- Verificare che la versione di vRealize Automation dalla quale si sta effettuando l'aggiornamento sia in condizioni di funzionamento stabili. Correggere eventuali problemi prima di effettuare l'aggiornamento.

- Assicurarsi di aver modificato le impostazioni di timeout del bilanciamento del carico dal valore predefinito ad almeno 10 minuti.

### Requisiti di configurazione dell'hardware

Verificare che l'hardware nell'ambiente sia adeguato per vRealize Automation 7.4.

Vedere [Specifiche hardware e massima capacità di vRealize Automation](#)

Prima di un aggiornamento, verificare che siano soddisfatti i seguenti prerequisiti.

- Per poter eseguire l'aggiornamento sono necessari almeno 18 GB di RAM, 4 CPU, disco1 = 50 GB, disco3 = 25 GB e disco4=50 GB.

Se la macchina virtuale è presente in vCloud Networking and Security, potrebbe essere necessario allocare più spazio RAM.

Benché il supporto generico per vCloud Networking and Security sia terminato, l'utilizzo delle proprietà personalizzate di VCNS in NSX è ancora valido. Vedere l'[articolo 2144733 della Knowledge Base](#).

- Questi nodi devono avere almeno 5 GB di spazio libero su disco:
  - Sito Web IaaS primario
  - Database Microsoft SQL
  - Model Manager
- Il nodo Web IaaS primario in cui sono installati i dati Model Manager dev'essere installato JAVA SE Runtime Environment 8, a 64 bit, aggiornamento 161 o versione successiva. Dopo aver installato Java, è necessario impostare la variabile di ambiente JAVA\_HOME sulla nuova versione.
- Per scaricare ed eseguire l'aggiornamento, è necessario disporre delle risorse seguenti:
  - Almeno 5 GB sulla partizione root
  - 5 GB sulla partizione /storage/db per il master Appliance vRealize Automation
  - 5 GB sulla partizione root per ogni appliance virtuale di replica
- Verificare la sottocartella /storage/log e rimuovere eventuali file ZIP precedenti archiviati per liberare spazio.

### Prerequisiti generali

Prima di un aggiornamento, verificare che siano soddisfatti i seguenti prerequisiti.

- È necessario installare PowerShell 3.0 o versione successiva nei sistemi Windows IaaS prima dell'aggiornamento. Se PowerShell 3.0 o versione successiva non è installato, l'aggiornamento non riesce.

- Se è installato Microsoft IIS, eseguire IISRESET nelle macchine del servizio Web e di gestione IaaS. Se si esegue IISRESET, viene verificato che non esista un servizio dipendente IIS disabilitato in modalità di avvio.
- Si dispone dell'accesso a tutti i database e a tutti i bilanciamenti del carico interessati o partecipanti all'aggiornamento di vRealize Automation.
- Il sistema viene reso non disponibile per gli utenti durante l'esecuzione dell'aggiornamento.
- Si disabilita ogni applicazione che effettua una query su vRealize Automation.
- Verificare che Microsoft Distributed Transaction Coordinator (MSDTC) sia attivo in tutte le istanze di vRealize Automation e nei server SQL associati. Per le istruzioni, consultare l'[articolo 2089503 della Knowledge Base](#).
- Se si esegue l'aggiornamento di un ambiente distribuito configurato con un database PostgreSQL incorporato, completare la procedura che segue.
  - a Prima di aggiornare gli host di replica, esaminare i file nella directory pgdata sull'host master.
  - b Andare alla cartella di dati PostgreSQL sull'host master nel percorso `/var/vmware/vpostgres/current/pgdata/`.
  - c Chiudere tutti i file aperti nella directory pgdata e rimuovere gli eventuali file con suffisso `.swp`.
  - d Verificare che tutti i file di questa directory abbiano la proprietà corretta: `postgres:users`.

Inoltre, verificare che le proprietà personalizzate non contengano spazi nei nomi. Prima dell'aggiornamento a questa versione di vRealize Automation, rimuovere eventuali spazi da nomi di proprietà personalizzate, ad esempio sostituire lo spazio con un carattere di sottolineatura, per consentire il riconoscimento della proprietà personalizzata nell'installazione vRealize Automation aggiornata. I nomi della proprietà personalizzata vRealize Automation non possono contenere spazi. Questo problema può influire sull'utilizzo di un'installazione di vRealize Orchestrator aggiornata che utilizza proprietà personalizzate che contenevano spazi nelle versioni precedenti di vRealize Automation o vRealize Orchestrator oppure entrambi.

### Elenco di controllo per l'aggiornamento di vRealize Automation

Quando si esegue l'aggiornamento di vRealize Automation 7.1, 7.2 o 7.3.x alla versione 7.4, è necessario aggiornare tutti i componenti di vRealize Automation in un ordine specifico.

L'ordine di aggiornamento varia a seconda che si intenda aggiornare un ambiente minimo o un ambiente distribuito con appliance vRealize Automation multiple.

Utilizzare l'elenco di controllo per tenere traccia del lavoro durante l'aggiornamento. Completare le attività nell'ordine in cui sono riportate.



**Tabella 1-47. Elenco di controllo per l'aggiornamento di un ambiente minimo vRealize Automation**

Attività	Istruzioni
<input type="checkbox"/> Eseguire la raccolta dati di Inventario rete e sicurezza di NSX prima dell'aggiornamento di vRealize Automation 7.1, 7.2 o 7.3.x alla versione 7.4. Questa operazione è necessaria solo quando vRealize Automation è integrato con NSX.	Vedere <a href="#">Esecuzione della raccolta dati di Inventario rete e sicurezza di NSX prima dell'aggiornamento di vRealize Automation</a> .
<input type="checkbox"/> Eseguire il backup dell'installazione corrente. Questo è un passaggio essenziale.	Per ulteriori informazioni su come eseguire il backup e ripristinare il sistema, vedere <a href="#">Backup dell'ambiente vRealize Automation esistente</a> . Per informazioni generali, vedere <i>Configurazione di backup e ripristino utilizzando Symantec Netbackup</i> all'indirizzo <a href="http://www.vmware.com/pdf/vrealize-backup-and-restore-netbackup.pdf">http://www.vmware.com/pdf/vrealize-backup-and-restore-netbackup.pdf</a> .
<input type="checkbox"/> Scaricare l'aggiornamento nell'appliance vRealize Automation.	Vedere <a href="#">Download degli aggiornamenti delle appliance vRealize Automation</a> .
<input type="checkbox"/> Installare l'aggiornamento nell'appliance vRealize Automation e nei componenti IaaS.	Vedere <a href="#">Installazione dell'aggiornamento nell'appliance vRealize Automation e nei componenti IaaS</a>

**Tabella 1-48. Elenco di controllo per l'aggiornamento di un ambiente distribuito vRealize Automation**

Attività	Istruzioni
<input type="checkbox"/> Eseguire la raccolta dati di Inventario rete e sicurezza di NSX prima dell'aggiornamento di vRealize Automation 7.1, 7.2 o 7.3.x alla versione 7.4. Questa operazione è necessaria solo quando vRealize Automation è integrato con NSX.	Vedere <a href="#">Esecuzione della raccolta dati di Inventario rete e sicurezza di NSX prima dell'aggiornamento di vRealize Automation</a> .
<input type="checkbox"/> Eseguire il backup dell'installazione corrente. Questo è un passaggio essenziale.	Per ulteriori informazioni su come eseguire il backup e ripristinare il sistema, vedere <a href="#">Backup dell'ambiente vRealize Automation esistente</a> . Per informazioni dettagliate, vedere <i>Configurazione di backup e ripristino utilizzando Symantec Netbackup</i> all'indirizzo <a href="http://www.vmware.com/pdf/vrealize-backup-and-restore-netbackup.pdf">http://www.vmware.com/pdf/vrealize-backup-and-restore-netbackup.pdf</a>
<input type="checkbox"/> Se si esegue l'aggiornamento da vRealize Automation 7.3.x, disabilitare il failover automatico di PostgreSQL.	Vedere <a href="#">Impostazione della modalità asincrona per la replica PostgreSQL di vRealize Automation</a> .
<input type="checkbox"/> Scaricare gli aggiornamenti nell'appliance vRealize Automation.	Vedere <a href="#">Download degli aggiornamenti delle appliance vRealize Automation</a> .
<input type="checkbox"/> Disattivare il bilanciamento del carico.	Vedere la documentazione del bilanciamento del carico.

**Tabella 1-48. Elenco di controllo per l'aggiornamento di un ambiente distribuito vRealize Automation (Continua)**

Attività	Istruzioni
 Installare l'aggiornamento nell'appliance vRealize Automation master e nei componenti IaaS.	Vedere <a href="#">Installazione dell'aggiornamento nell'appliance vRealize Automation e nei componenti IaaS</a> .
<b>Nota</b> È necessario installare l'aggiornamento nell'appliance master in un ambiente distribuito.	
 Attivare il bilanciamento del carico.	<a href="#">Attivare i bilanciamenti del carico</a>

## Interfacce utente dell'ambiente vRealize Automation

È possibile utilizzare e gestire l'ambiente vRealize Automation con varie interfacce.

### Interfacce utente

Queste tabelle descrivono le interfacce che si utilizzano per gestire l'ambiente vRealize Automation.

**Tabella 1-49. vRealize Automation Console di amministrazione**

Scopo	Accesso	Credenziali necessarie
È possibile utilizzare la console vRealize Automation per queste attività di amministratore di sistema.	1 Avviare un browser e aprire la pagina iniziale dell'appliance vRealize Automation utilizzando il nome di dominio completo dell'appliance virtuale:	È necessario disporre del ruolo di amministratore di sistema.
<ul style="list-style-type: none"> <li>■ Aggiungere i tenant.</li> <li>■ Personalizzare l'interfaccia utente di vRealize Automation.</li> <li>■ Configurare i server email.</li> <li>■ Consente di visualizzare i registri degli eventi.</li> <li>■ Configurare vRealize Orchestrator.</li> </ul>	https://vra-va-hostname.domain.name. 2 Fare clic nella <b>console di vRealize Automation</b> . È inoltre possibile utilizzare questo URL per aprire la console di vRealize Automation: https://vra-va-hostname.domain.name/vcac 3 Accedere.	

**Tabella 1-50. Console tenant vRealize Automation . Questa interfaccia è l'interfaccia utente principale utilizzata per creare e gestire i servizi e le risorse.**

Scopo	Accesso	Credenziali necessarie
<p>È possibile utilizzare vRealize Automation per eseguire le attività seguenti.</p> <ul style="list-style-type: none"> <li>■ Richiedere nuovi blueprint dei servizi IT.</li> <li>■ Creare e gestire le risorse IT e cloud.</li> <li>■ Creare e gestire gruppi personalizzati.</li> <li>■ Consente di creare e gestire gruppi di business.</li> <li>■ Assegnare ruoli agli utenti.</li> </ul>	<p>1 Avviare un browser e immettere l'URL della tenancy utilizzando il nome di dominio completo dell'appliance virtuale e il nome URL del tenant:</p> <p><code>https://vra-va-hostname.domain.name/vcac/org/tenant_URL_name</code></p> <p>2 Accedere.</p>	<p>È necessario disporre di uno o più dei ruoli seguenti:</p> <ul style="list-style-type: none"> <li>■ Architetto dell'applicazione</li> <li>■ Amministratore approvazioni</li> <li>■ Amministratore del catalogo</li> <li>■ Amministratore contenitori</li> <li>■ Architetto di contenitori</li> <li>■ Consumatore di integrità</li> <li>■ Architetto dell'infrastruttura</li> <li>■ Consumatore esportazione sicura</li> <li>■ Architetto del software</li> <li>■ Amministratore tenant</li> <li>■ Architetto XaaS</li> </ul>

**Tabella 1-51. Console di gestione dell'appliance vRealize Automation . Questa interfaccia talvolta viene chiamata VAMI (Virtual Appliance Management Interface).**

Scopo	Accesso	Credenziali necessarie
<p>È possibile utilizzare la console di gestione dell'appliance vRealize Automation per eseguire le attività seguenti.</p> <ul style="list-style-type: none"> <li>■ Visualizzare lo stato dei servizi registrati.</li> <li>■ Visualizzare le informazioni di sistema ed eseguire riavvio o shutdown dell'appliance.</li> <li>■ Gestire la partecipazione al programma Analisi utilizzo software.</li> <li>■ Visualizzare lo stato della rete.</li> <li>■ Visualizzare lo stato dell'aggiornamento e installare gli aggiornamenti.</li> <li>■ Gestire le impostazioni di amministrazione.</li> <li>■ Gestire le impostazioni dell'host vRealize Automation.</li> <li>■ Gestire le impostazioni SSO.</li> <li>■ Gestire le licenze di prodotto.</li> <li>■ Configurare il database Postgres vRealize Automation.</li> <li>■ Configurare la messaggistica di vRealize Automation.</li> <li>■ Configurare la registrazione di vRealize Automation.</li> <li>■ Installare i componenti IaaS.</li> <li>■ Eseguire la migrazione da un'installazione vRealize Automation esistente.</li> <li>■ Gestire i certificati del componente IaaS.</li> <li>■ Configurare il servizio Xenon.</li> </ul>	<ol style="list-style-type: none"> <li>1 Avviare un browser e aprire la pagina iniziale dell'appliance vRealize Automation utilizzando il nome di dominio completo dell'appliance virtuale:  <code>https://vra-va-hostname.domain.name.</code></li> <li>2 Fare clic su <b>gestione dell'appliance vRealize Automation</b>  Per aprire vRealize Automation Appliance Management, è inoltre possibile utilizzare l'URL <code>https://vra-va-hostname.domain.name:5480.</code></li> <li>3 Accedere.</li> </ol>	<ul style="list-style-type: none"> <li>■ Nome utente: root</li> <li>■ Password: la password immessa durante la distribuzione dell'appliance vRealize Automation.</li> </ul>



Tabella 1-52. Client vRealize Orchestrator

Scopo	Accesso	Credenziali necessarie
<p>È possibile utilizzare il client vRealize Orchestrator per eseguire le attività seguenti.</p> <ul style="list-style-type: none"> <li>■ Sviluppare azioni.</li> <li>■ Sviluppare workflow.</li> <li>■ Gestire criteri</li> <li>■ Installare pacchetti.</li> <li>■ Gestire autorizzazioni di utenti e gruppi di utenti.</li> <li>■ Applicare tag a oggetti URI.</li> <li>■ Visualizzare l'inventario.</li> </ul>	<ol style="list-style-type: none"> <li>1 Avviare un browser e aprire la pagina iniziale di vRealize Automation utilizzando il nome di dominio completo dell'appliance virtuale:  <code>https://vra-va-hostname.domain.name.</code></li> <li>2 Per scaricare il file <code>client.jnlp</code> nel computer locale, fare clic su <b>Client di vRealize Orchestrator</b>.</li> <li>3 Fare clic con il pulsante destro del mouse sul file <code>client.jnlp</code> e scegliere <b>Avvia</b>.</li> <li>4 Nella finestra di dialogo in cui viene chiesto se si desidera continuare, fare clic su <b>Continua</b>.</li> <li>5 Accedere.</li> </ol>	<p>È necessario essere un utente con ruolo di amministratore di sistema o far parte del gruppo <code>vcoadmins</code> configurato nelle impostazioni del provider di autenticazione di vRealize Orchestrator Control Center.</p>

Tabella 1-53. vRealize Orchestrator Control Center

Scopo	Accesso	Credenziali necessarie
<p>È possibile utilizzare vRealize Orchestrator Control Center per modificare la configurazione dell'istanza di vRealize Orchestrator predefinita incorporata in vRealize Automation.</p>	<ol style="list-style-type: none"> <li>1 Avviare un browser e aprire la pagina iniziale dell'appliance vRealize Automation utilizzando il nome di dominio completo dell'appliance virtuale:  <code>https://vra-va-hostname.domain.name.</code></li> <li>2 Fare clic su <b>gestione dell'appliance vRealize Automation</b>  Per aprire vRealize Automation Appliance Management, è inoltre possibile utilizzare l'URL <code>https://vra-va-hostname.domain.name:5480.</code></li> <li>3 Accedere.</li> <li>4 Fare clic su <b>Impostazioni vRA &gt; Orchestrator</b>.</li> <li>5 Selezionare <b>Interfaccia utente di Orchestrator</b>.</li> <li>6 Fare clic su <b>Avvia</b>.</li> <li>7 Fare clic sull'URL dell'interfaccia utente di Orchestrator.</li> <li>8 Accedere.</li> </ol>	<p>Nome utente</p> <ul style="list-style-type: none"> <li>■ Se non è configurata l'autenticazione basata sul ruolo, inserire <b>root</b>.</li> <li>■ Immettere il nome utente di vRealize Automation se è configurato per l'autenticazione basata sul ruolo.</li> </ul> <p>Password</p> <ul style="list-style-type: none"> <li>■ Inserire la password immessa durante la distribuzione dell'appliance vRealize Automation se non è configurata l'autenticazione basata sul ruolo.</li> <li>■ Inserire la password relativa al proprio nome utente se è configurato per l'autenticazione basata sul ruolo.</li> </ul>

**Tabella 1-54. Prompt dei comandi di Linux**

Scopo	Accesso	Credenziali necessarie
È possibile utilizzare il prompt dei comandi di Linux in un host, ad esempio nell'host dell'appliance vRealize Automation, per eseguire le attività seguenti.	1 Nell'host dell'appliance vRealize Automation, aprire un prompt dei comandi.  Un modo per aprire il prompt dei comandi nel computer locale consiste nell'avviare una sessione nell'host utilizzando un'applicazione come PuTTY.	<ul style="list-style-type: none"> <li>Nome utente: root</li> <li>Password: la password creata durante la distribuzione dell'appliance vRealize Automation.</li> </ul>
<ul style="list-style-type: none"> <li>Avviare o arrestare servizi</li> <li>Modificare file di configurazione</li> <li>Eseguire comandi</li> <li>Recuperare dati</li> </ul>	2 Accedere.	

**Tabella 1-55. Prompt dei comandi di Windows**

Scopo	Accesso	Credenziali necessarie
È possibile utilizzare il prompt dei comandi di Windows in un host, ad esempio l'host IaaS, per eseguire script.	1 Nell'host IaaS, accedere a Windows.  Un modo per effettuare l'accesso dal computer locale consiste nell'avviare una sessione desktop remota.	<ul style="list-style-type: none"> <li>Nome utente: l'utente con privilegi amministrativi.</li> <li>Password: la password dell'utente.</li> </ul>
	2 Aprire il prompt dei comandi di Windows.  Un modo per aprire il prompt dei comandi consiste nel fare clic con il pulsante destro del mouse sull'icona Start nell'host e selezionare <b>Prompt dei comandi</b> o <b>Prompt dei comandi (amministratore)</b> .	

## Aggiornamento dei prodotti VMware integrati con vRealize Automation

È necessario gestire qualsiasi prodotto VMware integrato con l'ambiente vRealize Automation quando si aggiorna vRealize Automation.

Se l'ambiente vRealize Automation è integrato con uno o più prodotti aggiuntivi, è necessario eseguire l'aggiornamento di vRealize Automation prima di aggiornare i prodotti aggiuntivi. Se vRealize Business for Cloud è integrato con vRealize Automation, è necessario annullare la registrazione di vRealize Business for Cloud prima di procedere con l'aggiornamento di vRealize Automation.

Seguire il workflow suggerito per la gestione dei prodotti integrati quando si esegue l'aggiornamento di vRealize Automation.

- 1 Aggiornare vRealize Automation.
- 2 Aggiornare VMware vRealize Operations Manager.
- 3 Aggiornare VMware vRealize Log Insight.
- 4 Aggiornare VMware vRealize Business for Cloud.

In questa sezione vengono fornite istruzioni aggiuntive per la gestione di vRealize Business for Cloud quando è integrato con l'ambiente vRealize Automation.

## Aggiornamento di vRealize Operations Manager integrato con vRealize Automation

Aggiornare vRealize Operations Manager dopo aver aggiornato vRealize Automation.

### Procedura

- 1 Aggiornare vRealize Automation.
- 2 Aggiornare vRealize Operations Manager. Per informazioni, vedere *Aggiornamento del software* nella [documentazione di VMware vRealize Operations Manager](#).

## Aggiornamento di vRealize Log Insight integrato con vRealize Automation

Aggiornare vRealize Log Insight dopo aver aggiornato vRealize Automation.

### Procedura

- 1 Aggiornare vRealize Automation.
- 2 Aggiornare vRealize Log Insight. Per informazioni, vedere *Aggiornamento di vRealize Log Insight* nella [documentazione di VMware vRealize Log Insight](#).

## Aggiornamento di vRealize Business for Cloud integrato con vRealize Automation

Quando si effettua l'aggiornamento dell'ambiente vRealize Automation, è necessario annullare ed eseguire la registrazione della connessione a vRealize Business for Cloud.

Eseguire questa procedura per garantire la continuità del servizio con vRealize Business for Cloud quando si aggiorna l'ambiente vRealize Automation.

### Procedura

- 1 Annullare la registrazione di vRealize Business for Cloud da vRealize Automation. Vedere l'argomento relativo all'*annullamento della registrazione di vRealize Business for Cloud da vRealize Automation* nella [documentazione di VMware vRealize Business for Cloud](#).
- 2 Aggiornare vRealize Automation.
- 3 Se necessario, aggiornare vRealize Business for Cloud. Vedere l'argomento relativo all'*aggiornamento di vRealize Business for Cloud* nella [documentazione di VMware vRealize Business for Cloud](#).
- 4 Registrare vRealize Business for Cloud in vRealize Automation. Vedere l'argomento relativo alla *registrazione di vRealize Business for Cloud con vRealize Automation* nella [documentazione di VMware vRealize Business for Cloud](#).

## Preparazione per l'aggiornamento di vRealize Automation

Completare le attività seguenti prima di aggiornare vRealize Automation 7.1, 7.2 o 7.3.x alla versione 7.4.

Completare le attività nell'ordine in cui sono disposte nell'elenco di controllo. Vedere [Elenco di controllo per l'aggiornamento di vRealize Automation](#).

## Esecuzione della raccolta dati di Inventario rete e sicurezza di NSX prima dell'aggiornamento di vRealize Automation

Prima di effettuare l'aggiornamento di vRealize Automation 7.1, 7.2 o 7.3 alla versione 7.4, è necessario eseguire la raccolta dati di Inventario rete e sicurezza di NSX nell'ambiente vRealize Automation 7.1, 7.2 o 7.3.x.

La raccolta dati è necessaria per assicurare il funzionamento dell'azione di riconfigurazione del bilanciamento del carico in vRealize Automation 7.4 per le distribuzioni delle versioni 7.1, 7.2 o 7.3.x.

### Procedura

- ◆ Eseguire la raccolta dati di Inventario rete e sicurezza di NSX in vRealize Automation 7.1, 7.2 o 7.3.x prima di effettuare l'aggiornamento alla versione 7.4. Vedere [Avvio manuale della raccolta dati degli endpoint](#).

### Operazioni successive

[Prerequisiti del backup per l'aggiornamento di vRealize Automation 7.1, 7.2 o 7.3 alla versione 7.4.](#)

### Prerequisiti del backup per l'aggiornamento di vRealize Automation 7.1, 7.2 o 7.3 alla versione 7.4

Conformarsi ai prerequisiti del backup prima di avviare l'aggiornamento.

#### Prerequisiti

- Verificare che l'ambiente di origine sia completamente installato e configurato.
- Accedere al client vSphere. Per ciascuna appliance dell'ambiente di origine, eseguire il backup di tutti i file di configurazione dell'appliance vRealize Automation nelle seguenti directory:
  - /etc/vcac/
  - /etc/vco/
  - /etc/apache2/
  - /etc/rabbitmq/
- Eseguire il backup del database Microsoft SQL Server IaaS. Per informazioni, cercare gli articoli disponibili in [Microsoft Developer Network](#) relativi alla creazione di un backup di database SQL Server completo.
- Eseguire il backup di ogni file personalizzato, ad esempio DataCenterLocations.xml.
- Creare uno snapshot di ogni appliance virtuale e server IaaS. Seguire le linee guida comuni per il backup dell'intero sistema nel caso in cui l'aggiornamento di vRealize Automation non vada a buon fine. Vedere [Backup e ripristino per le installazioni di vRealize Automation](#).

### Backup dell'ambiente vRealize Automation esistente

Prima di eseguire l'aggiornamento da vRealize Automation 7.1, 7.2 o 7.3.x alla versione 7.4, arrestare e creare uno snapshot di ogni server IaaS vRealize Automation in ciascun nodo Windows e di ogni appliance vRealize Automation in ciascun nodo Linux. Se un aggiornamento non riesce, utilizzare lo snapshot per tornare all'ultima configurazione corretta nota e tentare un altro aggiornamento.

Per informazioni sull'avvio di vRealize Automation, vedere [Avvio di vRealize Automation](#).

### Prerequisiti

- [Prerequisiti del backup per l'aggiornamento di vRealize Automation 7.1, 7.2 o 7.3 alla versione 7.4](#).
- A partire da vRealize Automation 7.0, il database PostgreSQL è sempre configurato nella modalità ad alta disponibilità. Accedere alla console di gestione dell'appliance vRealize Automation e selezionare **Impostazioni vRA > Database** per individuare il nodo master corrente. Se la configurazione del database è elencata come database esterno, creare un backup manuale di tale database.
- Se il database Microsoft SQL vRealize Automation non è in hosting sul server IaaS, creare un file di backup del database.
- Verificare che i prerequisiti di backup per l'aggiornamento siano stati completati.
- Verificare di aver creato uno snapshot del sistema mentre è spento. Questo è il metodo preferibile per creare lo snapshot. Vedere la *documentazione di vSphere 6.0*.

---

**Nota** Quando si esegue il backup dell'appliance vRealize Automation e dei componenti IaaS, disabilitare gli snapshot in memoria e gli snapshot inattivi.

---

- Se è stato modificato il file `app.config`, eseguirne il backup. Vedere [Ripristino delle modifiche di registrazione nel file app.config](#).
- Creare un backup dei file di configurazione workflow esterni (xmldb). Vedere [Ripristino dei file di timeout del workflow esterno](#).
- Verificare di disporre di una posizione esterna alla cartella corrente in cui è possibile archiviare il file di backup. Vedere [Le copie di backup dei file .xml causano il timeout del sistema](#).

### Procedura

- 1 Accedere al client vSphere.
- 2 Individuare ciascuna macchina Windows IaaS vRealize Automation e ogni nodo dell'appliance vRealize Automation.
- 3 Su ciascuna macchina, fare clic su **Arresta guest** in questo ordine.
  - a Macchine Windows Server IaaS
  - b Appliance vRealize Automation.
- 4 Creare uno snapshot di ciascuna macchina vRealize Automation.
- 5 Utilizzare il metodo di backup preferito per creare un backup completo di ciascun nodo dell'appliance.
- 6 Accensione del sistema. Per ulteriori informazioni, vedere Avvio di vRealize Automation in *Gestione di vRealize Automation*.

Nel caso di un ambiente ad alta disponibilità, procedere come segue per accendere le appliance virtuali.

- a Avviare l'appliance vRealize Automation master.

- b Accedere alla console di gestione dell'appliance vRealize Automation, fare clic su **Servizi** e attendere finché lo stato del servizio di licenza non passa a Registrato.
- c Avviare contemporaneamente le appliance vRealize Automation rimanenti.
- d Avviare il nodo Web primario e attendere il completamento dell'avvio.
- e Avviare la macchina principale del servizio di gestione e attendere da 2 a 5 minuti.

Il tempo effettivo dipende alla configurazione del sito.

---

**Nota** Sulle macchine secondarie, non avviare o eseguire il servizio di Windows, a meno che sia stata implementata la configurazione per il failover automatico del servizio di gestione.

---

- f Avviare i Distributed Execution Manager Orchestrator e Worker e tutti gli agenti proxy di vRealize Automation.

---

**Nota** È possibile avviare questi componenti in qualsiasi ordine. Non è necessario attendere che un componente completi l'operazione prima di avviarne un altro.

---

- 7 Accedere a ciascuna console di gestione delle appliance vRealize Automation e verificare che il sistema funzioni in modo corretto.
  - a Fare clic su **Servizi**.
  - b Verificare che ciascun servizio sia REGISTRATO.

#### Operazioni successive

[Impostazione della modalità asincrona per la replica PostgreSQL di vRealize Automation.](#)

#### Impostazione della modalità asincrona per la replica PostgreSQL di vRealize Automation

Se si esegue l'aggiornamento da un ambiente vRealize Automation distribuito che funziona in modalità di replica PostgreSQL sincrona, prima dell'aggiornamento è necessario modificare la modalità impostando quella asincrona.

#### Prerequisiti

- Si dispone di un ambiente vRealize Automation distribuito che si desidera aggiornare.
- Si è connessi come **root** all'interfaccia di gestione dell'appliance vRealize Automation all'indirizzo `https://vra-va-hostname.domain.name:5480`.

#### Procedura

- 1 Fare clic su **Impostazioni vRA > Database**.
- 2 Fare clic su **Modalità asincrona** e attendere il completamento dell'azione.
- 3 Verificare che per tutti i nodi nella colonna Stato sincronizzazione sia visualizzato lo stato Asincrono.

#### Operazioni successive

[Download degli aggiornamenti delle appliance vRealize Automation](#)

## Download degli aggiornamenti delle appliance vRealize Automation

Nella console di gestione dell'appliance è possibile controllare la disponibilità di aggiornamenti ed eventualmente scaricarli in uno dei seguenti modi.

Per massimizzare le prestazioni dell'aggiornamento, utilizzare il metodo file ISO.

Per evitare la possibilità del verificarsi di problemi o nel caso in cui si verifichino effettivamente problemi durante l'aggiornamento dell'appliance, vedere l'[articolo della Knowledge Base di VMware](#) relativo alla *non riuscita dell'aggiornamento di vRealize Automation a causa di duplicati nel database di vRealize Orchestrator (54987)*.

## Download degli aggiornamenti delle appliance virtuali per l'uso tramite unità CD-ROM

È possibile aggiornare l'appliance virtuale da un file ISO che l'appliance leggerà dall'unità CD-ROM virtuale. Questo è il metodo preferito.

Scaricare il file ISO e configurare l'appliance primaria in modo che utilizzi questo file per aggiornare l'appliance in uso.

### Prerequisiti

- Eseguire il backup dell'ambiente vRealize Automation esistente.
- Verificare che tutte le unità CD-ROM utilizzate nell'aggiornamento siano abilitate prima di eseguire l'aggiornamento di un'appliance vRealize Automation. Fare riferimento alla documentazione di vSphere per informazioni sull'aggiunta di un'unità CD-ROM a una macchina virtuale nel client di vSphere.

### Procedura

- 1 Scaricare il file ISO del repository di aggiornamento.
  - a Avviare un browser e passare alla [pagina del prodotto vRealize Automation](#) sul sito [www.vmware.com](http://www.vmware.com).
  - b Fare clic su **Download di vRealize Automation** per passare alla pagina di download di VMware.
  - c Scaricare il file appropriato.
- 2 Individuare il file scaricato nel sistema per verificare che la dimensione del file corrisponda a quella del file sulla pagina di download di VMware. Utilizzare i checksum forniti nella pagina di download per convalidare l'integrità del file scaricato. Per ulteriori informazioni, vedere i collegamenti disponibili in fondo alla pagina di download di VMware.
- 3 Assicurarsi che l'appliance virtuale primaria sia accesa.
- 4 Collegare l'unità CD-ROM per l'appliance virtuale primaria al file ISO scaricato.
- 5 Nell'appliance vRealize Automation primaria, accedere alla gestione dell'appliance di vRealize Automation come **root** utilizzando la password immessa durante la distribuzione dell'appliance vRealize Automation.
- 6 Fare clic sulla scheda **Aggiorna**.
- 7 Fare clic su **Impostazioni**.

8 In Aggiorna repository, selezionare **Usa aggiornamenti CDROM**.

9 Fare clic su **Salva impostazioni**.

### Download di aggiornamenti di vRealize Automation appliance da un repository VMware

È possibile scaricare l'aggiornamento per l'appliance vRealize Automation da un repository pubblico sul sito Web [vmware.com](http://vmware.com).

#### Prerequisiti

- Backup dell'ambiente vRealize Automation esistente.
- Verificare che l'appliance vRealize Automation sia accesa.

#### Procedura

- 1 Nell'appliance vRealize Automation primaria, accedere alla gestione dell'appliance di vRealize Automation come **root** utilizzando la password immessa durante la distribuzione dell'appliance vRealize Automation.
- 2 Fare clic sulla scheda **Aggiorna**.
- 3 Fare clic su **Impostazioni**.
- 4 (Facoltativo) Impostare la frequenza di controllo aggiornamenti nel pannello Aggiornamenti automatici.
- 5 Selezionare **Usa repository predefinito** nel pannello Aggiorna repository.  
Il repository predefinito è impostato all'URL VMware.com corretto.
- 6 Fare clic su **Salva impostazioni**.

### Aggiornamento dell'appliance vRealize Automation e dei componenti IaaS

Dopo aver soddisfatto i prerequisiti di aggiornamento e aver scaricato l'aggiornamento dell'appliance virtuale, è possibile installare l'aggiornamento nell'appliance vRealize Automation 7.1, 7.2 o 7.3.x per aggiornarla alla versione 7.4.

Per un ambiente minimo, installare l'aggiornamento nell'appliance vRealize Automation. Nel caso di un ambiente distribuito, è necessario installare l'aggiornamento nel nodo master dell'appliance. Il tempo necessario per completare l'aggiornamento varia a seconda dell'ambiente e della rete. Al termine dell'aggiornamento, nella pagina Stato aggiornamento dell'interfaccia di gestione dell'appliance vRealize Automation vengono visualizzate le modifiche apportate. Quando l'aggiornamento dell'appliance termina, riavviare l'appliance. Se l'appliance master viene riavviata in un ambiente distribuito, il sistema riavvia ogni nodo di replica.



Dopo il riavvio, nella pagina Stato aggiornamento viene visualizzato un messaggio simile a In attesa dell'avvio dei servizi VA. L'aggiornamento dei componenti IaaS viene avviato dopo l'inizializzazione completa del sistema e quando tutti i servizi sono in esecuzione. È possibile osservare l'avanzamento dell'aggiornamento dei componenti IaaS nella pagina Stato aggiornamento. Per completare questa operazione per il primo componente server IaaS, potrebbero essere necessari circa 30 minuti. Durante l'aggiornamento, viene visualizzato un messaggio simile al seguente Aggiornamento dei componenti server per il nodo web1-vra.mycompany.com.

Alla fine del processo di aggiornamento di ogni nodo del servizio di gestione, viene visualizzato un messaggio simile al seguente Attivazione della modalità di failover automatico del servizio di gestione per il nodo mgr-vra.mycompany.com. A partire da vRealize Automation 7.3, il nodo del servizio di gestione attivo passa dalla modalità di selezione manuale alla modalità automatica per decidere quale nodo deve assumere il ruolo di server di failover. Il sistema attiva questa funzionalità durante l'aggiornamento. In caso di problemi con questa funzionalità, vedere [L'aggiornamento dell'agente di gestione non riesce](#).

### Installazione dell'aggiornamento nell'appliance vRealize Automation e nei componenti IaaS

L'aggiornamento viene installato nell'appliance virtuale vRealize Automation 7.1, 7.2 o 7.3.x per aggiornare vRealize Automation e i componenti IaaS alla versione 7.4.

Durante l'installazione dell'aggiornamento, non chiudere la console di gestione.

Se si verificano problemi durante il processo di aggiornamento, vedere [Risoluzione dei problemi relativi all'aggiornamento di vRealize Automation](#).

---

**Nota** Durante l'aggiornamento dell'agente di gestione nelle macchine virtuali IaaS, viene installato temporaneamente un certificato pubblico di VMware nell'archivio di certificati degli autori attendibili. Il processo di aggiornamento dell'agente di gestione utilizza uno script PowerShell firmato con questo certificato. Al termine dell'aggiornamento, questo certificato viene rimosso dall'archivio di certificati.

---

#### Prerequisiti

- Verificare di aver selezionato un metodo di download e di aver completato la procedura per tale metodo. Vedere [Download degli aggiornamenti delle appliance vRealize Automation](#).
- Per tutti gli ambienti ad alta disponibilità, vedere [Backup dell'ambiente vRealize Automation esistente](#).
- Per gli ambienti con bilanciamenti dei carichi, verificare di aver disattivato tutti i nodi ridondanti e di aver rimosso i monitor di integrità. Per informazioni, vedere la documentazione relativa al bilanciamento del carico.
  - Appliance vRealize Automation
  - Sito Web IaaS
  - Servizio di gestione IaaS
- Per ambienti con bilanciamenti dei carichi, verificare che il traffico venga diretto solo al nodo primario.

- Verificare che il servizio IaaS ospitato in Microsoft Internet Information Services (IIS) sia in esecuzione eseguendo i passaggi seguenti:
  - a Avviare un browser e immettere l'URL **`https://webhostname/Repository/Data/MetaModel.svc`** per verificare che il repository Web sia in esecuzione. Se l'esito è positivo, non vengono restituiti errori e viene visualizzato un elenco dei modelli in formato XML.
  - b Accedere al sito Web IaaS e controllare che lo stato registrato nel file `Repository.log` sia OK. Il file si trova nella cartella home di VCAC all'indirizzo `/Server/Model Manager Web/Logs/Repository.log`.

---

**Nota** Per un sito Web IaaS distribuito, accedere al sito Web secondario, senza MMD, e arrestare Microsoft IIS temporaneamente. Per assicurarsi che il traffico del bilanciamento del carico passi esclusivamente attraverso il nodo Web primario, controllare la connettività di `MetaModel.svc` e riavviare Microsoft IIS.

---

- Verificare che tutti i nodi IaaS siano in buone condizioni, procedendo come segue:
  - a Nell'appliance virtuale primaria, accedere alla gestione dell'appliance di vRealize Automation come **root** utilizzando la password immessa durante la distribuzione dell'appliance vRealize Automation.
  - b Selezionare **Impostazioni vRA > Cluster**.
  - c In **Ultima connessione** verificare quanto segue.
    - I nodi IaaS nella tabella hanno un tempo di ultima connessione inferiore a 30 secondi.
    - I nodi dell'appliance virtuale hanno un tempo di ultima connessione inferiore a 10 minuti.

Se i nodi IaaS non sono in comunicazione con l'appliance vRealize Automation, l'aggiornamento non riesce.

Per diagnosticare i problemi di connettività tra agente di gestione e appliance virtuale, eseguire la procedura descritta di seguito.

    - 1 Accedere a ogni nodo IaaS non elencato o con un tempo di **Ultima connessione** superiore a 30 secondi.
    - 2 Controllare i registri dell'agente di gestione per verificare se sono stati registrati eventuali errori.
    - 3 Se l'agente di gestione non è in esecuzione, riavviarlo dalla console dei servizi.
  - d Prendere nota degli eventuali nodi orfani elencati nella tabella. Un nodo orfano è un nodo duplicato che viene segnalato nell'host ma non esiste nell'host. Tutti i nodi orfani devono essere eliminati. Per ulteriori informazioni, vedere [Eliminazione di nodi orfani in vRealize Automation](#).
- Se si dispone di un'appliance virtuale di replica che non fa più parte del cluster, è necessario eliminarla dalla tabella del cluster. Se non si elimina questa appliance, il processo di aggiornamento mostra un messaggio di avviso per comunicare che l'aggiornamento della replica non è riuscito.

- Prima di effettuare l'aggiornamento, assicurarsi che tutte le richieste salvate e in corso siano state completate correttamente.
- Se si aggiornano i componenti IaaS manualmente dopo l'aggiornamento dell'appliance vRealize Automation 7.1, 7.2 o 7.3, vedere [Esclusione dell'aggiornamento di IaaS](#). Se si intende aggiornare IaaS manualmente, è anche necessario interrompere tutti i servizi IaaS, tranne l'agente di gestione, su ciascun nodo IaaS.

## Procedura

- 1 Nell'appliance vRealize Automation primaria, accedere alla gestione dell'appliance di vRealize Automation come **root** utilizzando la password immessa durante la distribuzione dell'appliance vRealize Automation.

Per un ambiente distribuito, aprire la console di gestione nell'appliance master.

- 2 Fare clic su **Servizi** e verificare che tutti i servizi siano registrati.
- 3 Selezionare **Impostazioni vRA > Database** e verificare che questa appliance sia l'appliance vRealize Automation master.

L'aggiornamento deve essere installato solo nell'appliance vRealize Automation master. Ogni appliance vRealize Automation di replica viene aggiornata con l'appliance master.

- 4 Selezionare **Aggiorna > Stato**.
- 5 Fare clic su **Controlla aggiornamenti** per verificare l'accessibilità di un aggiornamento.
- 6 (Facoltativo) Per le istanze dell'appliance vRealize Automation, fare clic su **Dettagli** nell'area della versione dell'appliance per visualizzare informazioni sulla posizione delle note di rilascio.
- 7 Fare clic su **Installa aggiornamenti**.
- 8 Fare clic su **OK**.

Viene visualizzato un messaggio che segnala l'aggiornamento in corso. Le modifiche apportate durante un aggiornamento vengono mostrate in una pagina di riepilogo. Il tempo necessario per completare l'aggiornamento varia a seconda dell'ambiente e della rete.

- 9 (Facoltativo) Per monitorare l'aggiornamento in modo più dettagliato, utilizzare un emulatore di terminale con cui accedere all'appliance primaria. Visualizzare il file `updatecli.log` nel percorso `/opt/vmware/var/log/vami/updatecli.log`.

Ulteriori informazioni sull'avanzamento dell'aggiornamento possono essere visualizzate anche in questi file.

- `/opt/vmware/var/log/vami/vami.log`
- `/var/log/vmware/horizon/horizon.log`
- `/var/log/bootstrap/*.log`

Se si esce mentre il processo di aggiornamento è in corso, è possibile continuare a seguirne l'avanzamento nel file di registro. Il file `updatecli.log` potrebbe visualizzare informazioni sulla versione di vRealize Automation dalla quale si sta eseguendo l'aggiornamento. La versione visualizzata passa alla versione corretta più avanti nel corso dell'aggiornamento.

- 10 Al termine dell'aggiornamento dell'appliance vRealize Automation, fare clic su **Sistema > Riavvia** nella console di gestione.

In un ambiente distribuito tutti i nodi dell'appliance di replica aggiornati correttamente vengono riavviati al riavvio dell'appliance master.

L'aggiornamento di IaaS inizia quando il sistema viene inizializzato e tutti i servizi sono in esecuzione. Fare clic su **Aggiorna > Stato** per osservare lo stato di avanzamento dell'aggiornamento dei componenti IaaS.

- 11 Al termine dell'aggiornamento di IaaS, fare clic su **Cluster** nella console di gestione dell'appliance e verificare che il numero di versione sia quello corrente per tutti i nodi e i componenti IaaS.
- 12 Fare clic su **Telemetria** nella console di gestione dell'appliance. Leggere la nota sulla partecipazione al programma CEIP (Customer Experience Improvement Program) e scegliere se partecipare o meno al programma.

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>.

Per ulteriori informazioni sul programma CEIP, vedere [Partecipazione o uscita dal programma CEIP per vRealize Automation](#).

### Operazioni successive

Se la distribuzione utilizza un bilanciamento del carico, eseguire la procedura descritta di seguito.

- 1 Abilitare i controlli di integrità di vRealize Automation del servizio di bilanciamento del carico.
- 2 Riabilitare il traffico del servizio di bilanciamento del carico per tutti i nodi di vRealize Automation.

Se l'aggiornamento dei componenti IaaS non viene eseguito correttamente, vedere [Aggiornamento separato dei componenti server IaaS quando il processo di aggiornamento non riesce](#).

### Aggiornamento separato dei componenti server IaaS quando il processo di aggiornamento non riesce

Se il processo di aggiornamento automatico non riesce, è possibile aggiornare i componenti IaaS separatamente.

Se il sito Web IaaS e il servizio di gestione di vRealize Automation sono stati aggiornati correttamente, è possibile eseguire nuovamente lo script della shell di aggiornamento IaaS senza dover ripristinare gli snapshot acquisiti prima dell'aggiornamento. In alcuni casi, un evento di riavvio in sospeso generato durante l'aggiornamento di più componenti IaaS installati nella stessa macchina virtuale può comportare l'esito negativo dell'aggiornamento. In questo caso, provare a riavviare il nodo IaaS manualmente ed eseguire nuovamente l'aggiornamento per risolvere il problema. Se il problema persiste, contattare il supporto VMware o tentare un aggiornamento manuale eseguendo i passaggi seguenti.

- 1 Ripristinare lo stato precedente all'aggiornamento dell'appliance vRealize Automation.
- 2 Eseguire un comando per escludere i componenti IaaS dal processo di aggiornamento. Vedere [Esclusione dell'aggiornamento di IaaS](#).
- 3 Eseguire il processo di aggiornamento sull'appliance vRealize Automation.
- 4 Aggiornare i componenti IaaS separatamente utilizzando lo script della shell di aggiornamento o il pacchetto MSI del programma di installazione IaaS di vRealize Automation 7.4.

### **Aggiornamento dei componenti IaaS tramite lo script della shell di aggiornamento dopo l'aggiornamento dell'appliance vRealize Automation**

Utilizzare lo script della shell di aggiornamento per aggiornare i componenti IaaS dopo aver aggiornato ciascuna appliance vRealize Automation 7.1, 7.2 o 7.3.x alla versione 7.4.

L'Appliance vRealize Automation aggiornata contiene uno script della shell da utilizzare per aggiornare ciascun nodo e componente IaaS.

È possibile eseguire lo script di aggiornamento utilizzando la console di vSphere per la macchina virtuale oppure una sessione della console SSH. Se si utilizza la console di vSphere, si evitano i problemi di connettività di rete intermittente, che possono interrompere l'esecuzione dello script.

Se si arresta lo script durante l'aggiornamento di un componente, lo script si arresta quando ha finito di aggiornare il componente. Se altri componenti del nodo devono ancora essere aggiornati, è possibile eseguire di nuovo lo script.

Al termine dell'aggiornamento, è possibile esaminare il risultato dell'aggiornamento aprendo il file di registro dell'aggiornamento in `/opt/vmware/var/log/vami/upgrade-iaas.log`.

### **Prerequisiti**

- Rivedere [Risoluzione dei problemi relativi all'aggiornamento di vRealize Automation](#).
- Verificare che tutte le appliance vRealize Automation siano state aggiornate.
- Se si riavvia un server IaaS dopo aver aggiornato tutte le appliance vRealize Automation ma prima di aggiornare i componenti IaaS, arrestare tutti i servizi IaaS in Windows, ad eccezione del servizio dell'agente di gestione.
- Prima di eseguire lo script della shell di aggiornamento nel nodo master delle appliance vRealize Automation, fare clic su **Servizi** nella console di gestione dell'appliance. Verificare che ogni servizio, ad eccezione di `iaas-service`, sia REGISTRATO.

- Per installare manualmente l'agente di gestione IaaS su ogni nodo IaaS, completare la procedura che segue.
    - a Aprire un browser e passare alla pagina di installazione dell'IaaS di VMware vRealize Automation sull'appliance all'indirizzo `https://virtual_appliance_host_FQDN:5480/installer`.
    - b Scaricare il programma di installazione dell'agente di gestione, `VCAC-IaaSManagementAgent-Setup.msi`.
    - c Accedere a ciascuna macchina IaaS di vRealize Automation e aggiornare l'agente di gestione con il programma di installazione dell'agente di gestione. Riavviare il servizio Windows Management Agent.
  - Verificare che nel sito Web IaaS primario e nel nodo Model Manager sia installato JAVA SE Runtime Environment 8, a 64 bit, aggiornamento 161 o versione successiva. Una volta installato Java, è necessario impostare la variabile di ambiente `JAVA_HOME` nella nuova versione su ciascun nodo del server.
  - Accedere a ogni nodo del sito Web IaaS e verificare che la data di creazione sia antecedente alla data di modifica nel file `web.config`. Se la data di creazione del file `web.config` coincide o è successiva alla data di modifica, eseguire la procedura in [Aggiornamento non riuscito per il componente sito Web di IaaS](#).
  - Per verificare che per ogni nodo IaaS sia presente un agente di gestione aggiornato, eseguire questi passaggi su ciascun nodo IaaS:
    - a Accedere alla console di gestione dell'appliance vRealize Automation.
    - b Selezionare **Impostazioni vRA > Cluster**.
    - c Espandere l'elenco di tutti i componenti installati su ciascun nodo IaaS e individuare l'agente di gestione IaaS.
    - d Verificare che la versione dell'agente di gestione sia corrente.
  - [Esclusione dell'aggiornamento di IaaS](#).
  - Verificare che il backup del database Microsoft SQL Server IaaS sia accessibile qualora si rendesse necessario un ripristino dello stato precedente.
  - Verificare che gli snapshot dei server IaaS nella distribuzione siano disponibili.
- Se l'aggiornamento non riesce, tornare allo snapshot e al backup del database e provare a eseguire un altro aggiornamento.

## Procedura

- 1 Aprire una nuova sessione della console sull'host Appliance vRealize Automation. Accedere con l'account root.
- 2 Cambiare le directory in `/usr/lib/vcac/tools/upgrade/`.

Prima di eseguire lo script della shell di `./upgrade`, è importante che tutti gli agenti di gestione di IaaS siano aggiornati e integri. Se un agente di gestione IaaS presenta problemi quando si esegue lo script di shell di aggiornamento, vedere [L'aggiornamento dell'agente di gestione non riesce](#).

### 3 Eseguire lo script di aggiornamento.

- a Al prompt dei comandi, inserire `./upgrade`.
- b Premere Invio.

Per una descrizione del processo di aggiornamento di IaaS, vedere [Aggiornamento dell'appliance vRealize Automation e dei componenti IaaS](#).

Se lo script della shell di aggiornamento non viene eseguito correttamente, esaminare il file `upgrade-iaas.log`.

Dopo aver risolto il problema è possibile eseguire di nuovo lo script di aggiornamento.

#### Operazioni successive

- 1 [Ripristino dell'accesso al Control Center di vRealize Orchestrator integrato](#).
- 2 Se per la distribuzione viene utilizzato un servizio di bilanciamento del carico, riabilitare i controlli di integrità vRealize Automation e il traffico in tutti i nodi.

Per ulteriori informazioni, vedere *Bilanciamento del carico di vRealize Automation*.

#### **Aggiornamento dei componenti IaaS tramite il file eseguibile del programma di installazione IaaS dopo l'aggiornamento dell'appliance vRealize Automation**

È possibile utilizzare il seguente metodo alternativo per aggiornare i componenti IaaS dopo l'aggiornamento dell'appliance vRealize Automation 7.1, 7.2 o 7.3.x alla versione 7.4.

#### **Download del programma di installazione di IaaS per aggiornare i componenti di IaaS dopo l'aggiornamento dell'appliance vRealize Automation**

Dopo aver aggiornato l'appliance vRealize Automation alla versione 7.4, scaricare il programma di installazione di IaaS nella macchina in cui sono installati i componenti di IaaS da aggiornare.

Se durante questa procedura vengono visualizzati avvisi relativi ai certificati, è possibile ignorarli.

---

**Nota** A eccezione di un'istanza di backup passiva del servizio di gestione, il tipo di avvio per tutti i servizi deve essere impostato su Automatico durante il processo di aggiornamento. Se i servizi sono impostati su Manuale, il processo di aggiornamento avrà esito negativo.

---

#### **Prerequisiti**

- Verificare che sulla macchina di installazione di IaaS sia installato Microsoft .NET Framework 4.5.2 o versione successiva. È possibile scaricare il programma di installazione di .NET dalla pagina Web del programma di installazione di vRealize Automation. Se si aggiorna .NET alla versione 4.5.2 dopo aver arrestato i servizi e riavviato la macchina nel corso dell'installazione, è necessario arrestare manualmente tutti i servizi IaaS tranne l'agente di gestione.
- Se si utilizza Internet Explorer per il download, verificare che non sia abilitata la configurazione di sicurezza avanzata. Immettere `res://iesetup.dll/SoftAdmin.htm` nella barra di ricerca e premere Invio.

- Accedere in qualità di amministratore locale al server Windows in cui sono installati uno o più componenti IaaS da aggiornare.

### Procedura

- 1 Aprire un browser Web.
- 2 Immettere l'URL della pagina di download del programma di installazione di Windows.  
  
Ad esempio, **`https://vcac-va-hostname.domain.name:5480/installer`**, dove *vcac-va-hostname.domain.name* è il nome del nodo primario (master) di Appliance vRealize Automation.
- 3 Fare clic sul collegamento **IaaS installer**.
- 4 Quando richiesto, salvare sul desktop il file del programma di installazione `setup__vcac-va-hostname.domain.name@5480.exe`.  
  
Non modificare il nome del file poiché esso è utilizzato per collegare l'installazione alla Appliance vRealize Automation.

### Operazioni successive

[Aggiornamento dei componenti IaaS dopo l'aggiornamento di vRealize Automation 7.1 o 7.2 alla versione 7.3.](#)

### Aggiornamento dei componenti IaaS dopo l'aggiornamento di vRealize Automation 7.1 o 7.2 alla versione 7.3

È necessario aggiornare il database SQL e configurare tutti i sistemi su cui sono installati componenti di IaaS. È possibile utilizzare questi passaggi per installazioni minime e distribuite.

---

**Nota** Il programma di installazione di IaaS deve trovarsi nella macchina che contiene i componenti IaaS dei quali si desidera eseguire l'aggiornamento. Non è possibile eseguire il programma di installazione da una posizione esterna, ad eccezione del database di Microsoft SQL che può essere aggiornato anche da remoto dal nodo Web.

---

Verificare che gli snapshot dei server IaaS nella distribuzione siano disponibili. Se l'aggiornamento non riesce, è possibile tornare allo snapshot e tentare un altro aggiornamento.

Eseguire l'aggiornamento in modo che i servizi siano aggiornati nell'ordine seguente:

#### 1 Siti Web IaaS

Se si utilizza un bilanciamento del carico, disabilitare il traffico su tutti i nodi non primari.

Completare l'aggiornamento su un server prima di aggiornare quello successivo che esegue un servizio sito Web. Iniziare da quello su cui è installato il componente Model Manager Data.

Se si sta eseguendo un aggiornamento manuale del database Microsoft SQL esterno, è necessario aggiornare l'applicazione SQL esterna prima di aggiornare il nodo Web. È possibile eseguire l'aggiornamento del database SQL esterno in remoto da un nodo Web.

#### 2 Servizi di gestione



Aggiornare il servizio di gestione attivo prima di aggiornare il servizio di gestione passivo.

Se la crittografia SSL non è abilitata nell'istanza di SQL, deselezionare la casella di controllo relativa alla crittografia SSL accanto alla definizione SQL nella finestra di dialogo per la configurazione dell'aggiornamento di IaaS.

### 3 DEM Orchestrator e DEM Worker

Aggiornare tutti i DEM Orchestrator e i DEM Worker. Completare l'aggiornamento su un server prima di aggiornare quello successivo.

### 4 Agenti

Completare l'aggiornamento su un server prima di aggiornare quello successivo che esegue un agente.

### 5 Agente di gestione

Aggiornato automaticamente come parte del processo di aggiornamento.

I diversi servizi eventualmente presenti su un unico server vengono aggiornati nell'ordine corretto. Se ad esempio nel sito sono presenti sullo stesso server il sito Web e i servizi di gestione, selezionare entrambi per l'aggiornamento. Il programma di installazione dell'aggiornamento applica gli aggiornamenti nell'ordine corretto. È necessario completare l'aggiornamento su un server prima di iniziare ad aggiornarne un altro.

---

**Nota** Se la distribuzione utilizza un bilanciamento del carico, l'appliance primaria deve essere connessa al bilanciamento del carico. Tutte le altre istanze di Appliance vRealize Automation appliance devono essere disabilitate per il traffico di bilanciamento del carico prima di applicare l'aggiornamento onde evitare errori di cache.

---

## Prerequisiti

- Eseguire il backup dell'ambiente vRealize Automation esistente.
- Se si riavvia un server IaaS dopo aver aggiornato tutte le appliance vRealize Automation ma prima di aggiornare i componenti IaaS, nel server arrestare tutti i servizi Windows di IaaS ad eccezione del servizio dell'agente di gestione.
- [Download del programma di installazione di IaaS per aggiornare i componenti di IaaS dopo l'aggiornamento dell'appliance vRealize Automation.](#)
- Verificare che il sito Web IaaS primario, il database Microsoft SQL e il nodo Model Manager dispongano di JAVA SE Runtime Environment 8, a 64 bit, aggiornamento 111 o successivo installato. Una volta installato Java, è necessario impostare la variabile di ambiente JAVA\_HOME nella nuova versione su ciascun nodo del server.
- Verificare che la data di creazione sia antecedente alla data di modifica nel file `web.config`. Se la data di creazione del file `web.config` coincide o è successiva alla data di modifica, eseguire la procedura in [Aggiornamento non riuscito per il componente sito Web di IaaS](#).

- Completare la procedura che segue per riconfigurare il servizio Microsoft Distributed Transaction Coordinator (DTC).

---

**Nota** Anche quando il servizio Distributed Transaction Coordinator è abilitato, la transazione distribuita potrebbe non riuscire se il firewall è attivato.

---

- a Sull'appliance vRealize Automation selezionare **Avvia > Strumenti di amministrazione > Servizi componenti**.
- b Espandere **Servizi componenti > Computer > Computer locale > Distributed Transaction Coordinator**.
- c Scegliere l'attività appropriata.
  - Per un DTC autonomo locale, fare clic con il pulsante destro del mouse su **DTC locale** e scegliere **Proprietà**
  - Per un DTC cluster, espandere **DTC cluster**, fare clic con il pulsante destro del mouse sul DTC cluster denominato e scegliere **Proprietà**.
- d Fare clic su **Sicurezza**.
- e Selezionare tutte le opzioni seguenti:
  - **Accesso di rete DTC**
  - **Consenti client remoti**
  - **Consenti connessioni in ingresso**
  - **Consenti connessioni in uscita**
  - **Necessaria autenticazione reciproca**
- f Fare clic su **OK**.

#### Procedura

- 1 Se si utilizza il bilanciamento del carico, preparare l'ambiente.
  - a Verificare che il nodo del sito Web IaaS che contiene i dati di Model Manager sia abilitato per il traffico del bilanciamento del carico.  
È possibile identificare questo nodo dalla presenza della *cartella* `vCAC\Server\ConfigTool`.
  - b Disabilitare tutti gli altri siti Web IaaS e i servizi di gestione non primari per il traffico del bilanciamento del carico.
- 2 Fare clic con il pulsante destro del mouse sul file d'installazione `setup__vrealize-automation-appliance-FQDN@5480.exe` e scegliere **Esegui come amministratore**.
- 3 Fare clic su **Avanti**.
- 4 Accettare il contratto di licenza e fare clic su **Avanti**.

- 5 Immettere le credenziali dell'amministratore per la distribuzione corrente nella pagina di accesso.

Il nome utente è **root** e la password corrisponde a quella specificata in fase di distribuzione dell'appliance.

- 6 Selezionare **Accetta certificato**.

- 7 Nella pagina **Tipo di installazione**, verificare che sia selezionato **Aggiorna**.

Se **Aggiorna** non è selezionato, i componenti del sistema sono già aggiornati a questa versione.

- 8 Fare clic su **Avanti**.

- 9 Configurare le impostazioni di aggiornamento.

Opzione	Azione
<b>Se si sta aggiornando Model Manager Data</b>	<p>Selezionare la casella di controllo <b>Model Manager Data</b> nella sezione vCAC Server.</p> <p>La casella di controllo è selezionata per impostazione predefinita. Aggiornare Model Manager Data una sola volta. Se si esegue il file di installazione su più macchine per aggiornare un'installazione distribuita, i server Web smettono di funzionare perché le versioni dei server Web e quella di Model Manager Data non corrispondono. Eseguito l'aggiornamento di Model Manager Data e di tutti i server Web, tutti i server Web dovrebbero essere in funzione.</p>
<b>Se non si sta aggiornando Model Manager Data</b>	<p>Deselezionare la casella di controllo <b>Model Manager Data</b> nella sezione vCAC Server.</p>
<b>Per preservare i workflow personalizzati nell'ultima versione in Model Manager Data</b>	<p>Se si sta aggiornando Model Manager Data, selezionare la casella di controllo <b>Preserva ultime versioni dei workflow</b> nella sezione Workflow di estendibilità.</p> <p>La casella di controllo è selezionata per impostazione predefinita. I workflow personalizzati vengono sempre preservati. La casella di controllo determina solo l'ordine delle versioni. Se è stato utilizzato vRealize Automation Designer per personalizzare i workflow in Model Manager, selezionare questa opzione per conservare la versione più recente di ogni workflow personalizzato prima di aggiornare come versione più recente dopo l'aggiornamento.</p> <p>Se non si seleziona questa opzione, la versione di ogni workflow fornito con vRealize Automation Designer diventa la più recente dopo l'aggiornamento, e la versione più recente prima dell'aggiornamento diventa la seconda più recente.</p> <p>Per informazioni su vRealize Automation Designer, vedere <a href="#">Estensione del ciclo di vita delle macchine utilizzando vRealize Automation Designer</a>.</p>
<b>Se si sta aggiornando un Distributed Execution Manager o un agente proxy</b>	<p>Immettere le credenziali dell'account di amministratore nella sezione Account servizio.</p> <p>Tutti i servizi aggiornati vengono eseguiti con questo account.</p>

Opzione	Azione
<b>Per specificare il database di Microsoft SQL Server</b>	<p>Se si sta aggiornando Model Manager Data, immettere i nomi del server di database e dell'istanza del database nella casella di testo <b>Server</b> della sezione di informazioni sull'installazione del database Microsoft SQL Server. Immettere il nome di dominio completo (FQDN) del nome del server di database nella casella di testo <b>Nome database</b>.</p> <p>Se l'istanza del database si trova su una porta SQL non predefinita, includere il numero della porta nella definizione dell'istanza del server. La porta predefinita di Microsoft SQL è 1433.</p> <p>Quando si aggiornano i nodi di gestione, l'opzione SSL di MSSQL è selezionata per impostazione predefinita. Se il database non utilizza SSL, deselezionare <b>Usa SSL per la connessione al database</b>.</p>

**10** Fare clic su **Avanti**.

**11** Verificare che tutti i servizi da aggiornare appaiano nella pagina Pronto per l'aggiornamento e fare clic su **Aggiorna**.

Viene visualizzata la pagina dell'aggiornamento e un indicatore di avanzamento. Terminato il processo di aggiornamento, il pulsante **Avanti** viene abilitato.

**12** Fare clic su **Avanti**.

**13** Fare clic su **Fine**.

**14** Verificare che tutti i servizi vengano riavviati.

**15** Ripetere la procedura per ogni server IaaS della distribuzione nell'ordine raccomandato.

**16** Dopo aver aggiornato tutti i componenti, accedere alla console di gestione dell'appliance e verificare che tutti i servizi, incluso IaaS, ora siano registrati.

**17** (Facoltativo) Attivare il failover automatico del servizio di gestione. Vedere [Abilitazione del failover automatico del servizio di gestione dopo l'aggiornamento](#).

Tutti i componenti selezionati sono aggiornati alla nuova versione.

#### Operazioni successive

**1** [Ripristino dell'accesso al Control Center di vRealize Orchestrator integrato](#).

**2** Se la distribuzione utilizza un bilanciamento del carico, aggiornare ogni nodo del bilanciamento del carico in modo che utilizzi i controlli di integrità di vRealize Automation e riabilitare il traffico del bilanciamento del carico per tutti i nodi non connessi.

Per ulteriori informazioni, vedere *Bilanciamento del carico di vRealize Automation*.

#### Ripristino dell'accesso al Control Center di vRealize Orchestrator integrato

Una volta aggiornati i componenti del server IaaS, è necessario ripristinare l'accesso a vRealize Orchestrator.

Quando si effettua l'aggiornamento da vRealize Automation 7.3 e versioni precedenti alla versione 7.4, è necessario eseguire la seguente procedura per integrare la nuova funzionalità di controllo dell'accesso in base al ruolo. Questa procedura è stata scritta per un ambiente ad alta disponibilità.

## Prerequisiti

Creare uno snapshot dell'ambiente di vRealize Automation.

## Procedura

- 1 Accedere alla console di gestione di Appliance vRealize Automation come root utilizzando il nome di dominio completo dell'host dell'appliance, `https://va-hostname.domain.name:5480`.
- 2 Selezionare **Impostazioni vRA > Database**.
- 3 Identificare i nodi master e replica.
- 4 Su ogni nodo di replica, aprire una sessione SSH, accedere come amministratore ed eseguire questo comando:
 

```
service vco-server stop && service vco-configurator stop
```
- 5 Nel nodo master, aprire una sessione SSH, accedere come amministratore ed eseguire questo comando:
 

```
rm /etc/vco/app-server/vco-registration-id
```
- 6 Sul nodo master, passare alla directory `/etc/vco/app-server/`.
- 7 Aprire il file `sso.properties`.
- 8 Se il nome della proprietà `com.vmware.o11n.sso.admin.group.name` contiene spazi o qualsiasi altro carattere correlato alla Bash, ovvero accettati come carattere speciale in un comando Bash come ad esempio un apostrofo (') o un segno di dollaro (\$), continuare con questa procedura.
  - a Copiare la riga con la proprietà `com.vmware.o11n.sso.admin.group.name` e immettere `AdminGroup` come valore.
  - b Aggiungere `#` all'inizio della riga originale contenente la proprietà `com.vmware.o11n.sso.admin.group.name` per impostare la riga come commento.
  - c Salvare e chiudere il file `sso.properties`.
- 9 Eseguire il comando seguente:
 

```
vcac-vami vco-service-reconfigure
```
- 10 Aprire il file `sso.properties`. Se il file è cambiato, procedere come segue.
  - a Rimuovere l'asterisco `#` dall'inizio della riga originale contenente la proprietà `com.vmware.o11n.sso.admin.group.name` per rimuovere il commento dalla riga.
  - b Rimuovere la copia della riga con la proprietà `com.vmware.o11n.sso.admin.group.name`.
  - c Salvare e chiudere il file `sso.properties`.
- 11 Per riavviare il servizio `vco-server`, eseguire il comando seguente:
 

```
service vco-server restart
```
- 12 Per riavviare il servizio `vco-configurator`, eseguire il comando seguente:
 

```
service vco-configurator restart
```

- 13 Nella console di gestione di Appliance vRealize Automation, fare clic su **Servizi** e attendere che tutti i servizi nel nodo master siano REGISTRATI.
- 14 Quando tutti i servizi sono registrati, unire i nodi replica di vRealize Automation al cluster vRealize Automation per sincronizzare la configurazione di vRealize Orchestrator. Per informazioni, vedere [Riconfigurazione del vRealize Orchestrator incorporato per il supporto dell'alta disponibilità](#).

#### Operazioni successive

[Aggiornamento di vRealize Orchestrator dopo l'aggiornamento di vRealize Automation.](#)

## Aggiornamento di vRealize Orchestrator dopo l'aggiornamento di vRealize Automation

È necessario aggiornare l'istanza di vRealize Orchestrator quando si esegue l'aggiornamento di vRealize Automation 7.1, 7.2 o 7.3.x alla versione 7.4.

Con il rilascio di vRealize Orchestrator 7.4, sono disponibili due opzioni per aggiornare vRealize Orchestrator quando si esegue l'aggiornamento a vRealize Automation 7.4.

- È possibile eseguire la migrazione del server vRealize Orchestrator esterno esistente all'istanza di vRealize Orchestrator incorporata inclusa in vRealize Automation 7.4.
- È possibile aggiornare il server vRealize Orchestrator autonomo o in cluster per consentirne il funzionamento con vRealize Automation 7.4.

### Migrazione di un server vRealize Orchestrator esterno in vRealize Automation

È possibile migrare il server vRealize Orchestrator esterno esistente in un'istanza di vRealize Orchestrator incorporata in vRealize Automation 7.4.

È possibile distribuire vRealize Orchestrator come istanza esterna del server e configurare vRealize Automation per il funzionamento con tale istanza esterna oppure configurare e utilizzare il server vRealize Orchestrator incluso in Appliance vRealize Automation.

VMware consiglia di effettuare la migrazione del server vRealize Orchestrator esterno nel server Orchestrator integrato in vRealize Automation. La migrazione da un server Orchestrator esterno a uno incorporato offre i seguenti vantaggi:

- Riduce il costo totale di proprietà.
- Semplifica il modello di distribuzione.
- Migliora l'efficienza operativa.

---

**Nota** È consigliabile utilizzare il server vRealize Orchestrator esterno nei casi seguenti:

- Tenant multipli nell'ambiente vRealize Automation
  - Ambiente diffuso geograficamente
  - Gestione del carico di lavoro
  - Uso di plug-in specifici, ad esempio vecchie versioni del plug-in Site Recovery Manager
-

## Differenze di Control Center tra server Orchestrator esterni e incorporati

Alcune delle voci di menu disponibili in Control Center per un server vRealize Orchestrator esterno non sono incluse nella vista di Control Center predefinita di un'istanza di Orchestrator incorporata.

In un server Orchestrator incorporato, alcune opzioni di Control Center sono nascoste per impostazione predefinita.

Voce di menu	Dettagli
<b>Gestione licenze</b>	Il server Orchestrator incorporato è preconfigurato per l'utilizzo di vRealize Automation come provider di licenze.
<b>Esporta/Importa configurazione</b>	La configurazione del server Orchestrator incorporato è inclusa nei componenti di vRealize Automation esportati.
<b>Consente di configurare database</b>	Il server Orchestrator incorporato utilizza il database usato da vRealize Automation.
<b>Programma per il miglioramento dell'esperienza del cliente (CEIP)</b>	È possibile partecipare al programma CEIP dall'interfaccia di gestione dell'appliance vRealize Automation.  Vedere <i>Programma per il miglioramento dell'esperienza del cliente</i> in <i>Gestione di vRealize Automation</i> .

Altre opzioni nascoste dalla vista di Control Center predefinita sono la casella di testo **Indirizzo host** e il pulsante **ANNULLA REGISTRAZIONE** nella pagina **Configura provider di autenticazione**.

**Nota** Per vedere l'intera serie di opzioni di Control Center in vRealize Orchestrator integrato in vRealize Automation, è necessario accedere alla pagina di gestione avanzata di Orchestrator all'indirizzo [https://vra-va-hostname.domain.name\\_or\\_load\\_balancer\\_address:8283/vco-controlcenter/#/?advanced](https://vra-va-hostname.domain.name_or_load_balancer_address:8283/vco-controlcenter/#/?advanced) e premere il pulsante F5 sulla tastiera per aggiornare la pagina.

## Migrazione di un server vRealize Orchestrator 7.x esterno in vRealize Automation 7.4

È possibile esportare la configurazione dall'istanza del server Orchestrator esterno esistente e importarla nel server Orchestrator integrato in vRealize Automation.

**Nota** Se sono presenti più nodi di Appliance vRealize Automation, eseguire la procedura di migrazione solo nel nodo vRealize Automation primario.

### Prerequisiti

- Aggiornare o migrare vRealize Automation alla versione 7.4. Per ulteriori informazioni, vedere *Aggiornamento di vRealize Automation* in *Installazione o Aggiornamento di vRealize Automation*.
- Arrestare il servizio del server Orchestrator esterno.
- Eseguire il backup del database del server Orchestrator esterno, incluso lo schema di database.

## Procedura

- 1 Esportare la configurazione dal server Orchestrator esterno.
  - a Accedere al servizio Control Center del server Orchestrator esterno come **root** o come **amministratore** a seconda della versione di origine.
  - b Arrestare il servizio del server Orchestrator dalla pagina **Opzioni di avvio** per impedire modifiche indesiderate al database.
  - c Passare alla pagina **Esporta/Importa configurazione**.
  - d Nella pagina **Esporta configurazione**, selezionare **Esporta configurazione server, Plug-in bundle** ed **Esporta configurazioni plug-in**.
- 2 Effettuare la migrazione della configurazione esportata nell'istanza del server Orchestrator incorporato.
  - a Caricare il file di configurazione di Orchestrator incorporato nella directory `/usr/lib/vco/tools/configuration-cli/bin` di Appliance vRealize Automation.
  - b Accedere all'Appliance vRealize Automation su SSH come **root**.
  - c Arrestare il servizio del server Orchestrator e il servizio Control Center del server vRealize Orchestrator integrato.

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

- d Importare il file di configurazione del server Orchestrator nel server vRealize Orchestrator integrato eseguendo lo script `vro-configure` con il comando `import`.

```
./vro-configure.sh import --type embedded --path orchestrator-config-export-orchestrator_appliance_ip-date_hour.zip
```

- 3 Se il server Orchestrator esterno da cui si desidera effettuare la migrazione utilizza il database PostgreSQL integrato, modificare i suoi file di configurazione del database.
  - a Nel file `/var/vmware/vpostgres/current/pgdata/postgresql.conf`, rimuovere il commento per la riga `listen_addresses`.
  - b Impostare i valori di `listen_addresses` su un carattere jolly (\*).

```
listen_addresses = '*'
```



- c Aggiungere una riga al file `/var/vmware/vpostgres/current/pgdata/pg_hba.conf`.

```
host all all vra-va-ip-address/32 md5
```

**Nota** Il file `pg_hba.conf` richiede l'uso di un formato di prefisso CIDR al posto di un indirizzo IP e di una subnet mask.

- d Riavviare il servizio del server PostgreSQL.

```
service vpostgres restart
```

- 4 Migrare il database nel database PostgreSQL interno mediante l'esecuzione dello script `vro-configure` con il comando `db-migrate`.

```
./vro-configure.sh db-migrate --sourceJdbcUrl JDBC_connection_URL --sourceDbUsername database_user  
--sourceDbPassword database_user_password
```

**Nota** Racchiudere tra apici le password contenenti caratteri speciali.

Il valore di `JDBC_connection_URL` dipende dal tipo di database utilizzato.

PostgreSQL: `jdbc:postgresql://host:port/database_name`

MSSQL: `jdbc:jtds:sqlserver://host:port/database_name\;` if using SQL authentication and MSSQL:  
`jdbc:jtds:sqlserver://host:port/database_name\;domain=domain\;useNTLMv2=TRUE` if using Windows authentication.

Oracle: `jdbc:oracle:thin:@host:port:database_name`

Le informazioni di accesso del database predefinite sono:

<code>database_name</code>	vmware
<code>database_user</code>	vmware
<code>database_user_password</code>	vmware

- 5 Rimuovere tutti i certificati dal keystore del database.

```
./vro-configuration.sh untrust --reset-db
```

- 6 Reinstallare i plug-in di Orchestrator.

- Accedere a Control Center come **root**.
- Fare clic su **Risoluzione dei problemi**.
- Fare clic su **Forza reinstallazione plug-in**.

- 7 Avviare il servizio del server di Orchestrator.

## 8 Ripristinare la configurazione predefinita dei file `postgresql.conf` e `pg_hba.conf`.

- a Riavviare il servizio del server PostgreSQL.

È stata effettuata correttamente la migrazione di un'istanza del server Orchestrator esterno a un'istanza di vRealize Orchestrator incorporata in vRealize Automation.

### Operazioni successive

Configurare il server vRealize Orchestrator integrato. Vedere [Configurazione del server vRealize Orchestrator integrato](#).

### Configurazione del server vRealize Orchestrator integrato

Dopo aver esportato la configurazione di un server Orchestrator esterno e averla importata in vRealize Automation 7.4, è necessario configurare il server Orchestrator integrato in vRealize Automation.

### Prerequisiti

Migrazione della configurazione dal server vRealize Orchestrator esterno a quello interno.

### Procedura

- 1 Accedere all'Appliance vRealize Automation su SSH come **root**.
- 2 Avviare il servizio Control Center e il servizio del server Orchestrator del server vRealize Orchestrator integrato.

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

- 3 Accedere al servizio Control Center del server Orchestrator integrato come **amministratore**.

---

**Nota** Se si effettua la migrazione da un'istanza di vRealize Orchestrator 7.4 esterna, andare al passaggio 5.

---

- 4 Verificare che Orchestrator sia configurato correttamente nella pagina **Convalida configurazione** in Control Center.
- 5 Se il server Orchestrator esterno è stato configurato per l'utilizzo in modalità cluster, riconfigurare il cluster Orchestrator in vRealize Automation.
  - a Passare alla pagina **Orchestrator Cluster Management** avanzata all'indirizzo `https://vra-va-hostname.domain.name_or_load_balancer_address:8283/vco-controlcenter/#/control-app/ha?remove-nodes`.

---

**Nota** Se non vengono visualizzate le caselle di controllo **Rimuovi** accanto ai nodi esistenti nel cluster, sarà necessario aggiornare la pagina del browser premendo il pulsante F5 sulla tastiera.

---

- b Selezionare le caselle di controllo accanto ai nodi Orchestrator esterni e fare clic su **Rimuovi** per rimuoverli dal cluster.

- c Per uscire dalla pagina di gestione del cluster avanzata, eliminare la stringa `remove-nodes` dall'URL e aggiornare la pagina del browser premendo il pulsante F5 sulla tastiera.
  - d Nella pagina **Convalida configurazione** di Control Center verificare che il server Orchestrator sia configurato correttamente.
- 6 (Facoltativo) Nella scheda **Certificato di firma pacchetto** nella pagina **Certificati**, generare un nuovo certificato di firma del pacchetto.
  - 7 (Facoltativo) Modificare i valori per **Tenant predefinito** e **Gruppo Amministratori** nella pagina **Configura provider di autenticazione**.
  - 8 Verificare che il servizio `vco-server` sia contrassegnato come REGISTRATO nella scheda **Servizi** nella console di gestione dell'appliance Appliance vRealize Automation.
  - 9 Selezionare i servizi `vco` del server Orchestrator esterno e fare clic su **Annulla registrazione**.

#### Operazioni successive

- Importare i certificati considerati attendibili dal server Orchestrator esterno nell'archivio Attendibilità del server Orchestrator integrato.
- Unire i nodi di replica di vRealize Automation al cluster di vRealize Automation per sincronizzare la configurazione del server Orchestrator.

Per ulteriori informazioni, vedere la *sezione relativa alla riconfigurazione del server vRealize Orchestrator integrato di destinazione per il supporto dell'alta disponibilità* in *Installazione o aggiornamento di vRealize Automation*.

---

**Nota** Le istanze di vRealize Orchestrator vengono incluse automaticamente nel cluster e sono disponibili per l'utilizzo.

---

- Riavviare il servizio `vco-configurator` in tutti i nodi del cluster.
- Aggiornare l'endpoint di vRealize Orchestrator in modo che punti al server Orchestrator integrato di cui è stata eseguita la migrazione.
- Aggiungere l'host vRealize Automation e l'host IaaS all'inventario del plug-in vRealize Automation, eseguendo i workflow per l'aggiunta di un host vRA e l'aggiunta dell'host IaaS di un host vRA.

#### Aggiornamento di un'appliance vRealize Orchestrator autonoma per l'utilizzo con vRealize Automation

Se si gestisce un'istanza esterna autonoma di vRealize Orchestrator per l'utilizzo con vRealize Automation, è necessario aggiornare vRealize Orchestrator quando si aggiorna vRealize Automation dalla versione 7.1, 7.2 o 7.3 alla versione 7.4.

Le istanze incorporate di vRealize Orchestrator vengono aggiornate come parte dell'aggiornamento di vRealize Automation appliance. Per un'istanza incorporata non è necessario eseguire altre operazioni.

Se si sta aggiornando un cluster di appliance vRealize Orchestrator, vedere [Aggiornamento di un cluster di appliance vRealize Orchestrator per l'utilizzo con vRealize Automation 7.4](#).

## Prerequisiti

- [Installazione dell'aggiornamento nell'appliance vRealize Automation e nei componenti IaaS.](#)
- Smontare tutti i file system di rete. Vedere *Amministrazione delle macchine virtuali vSphere* nella documentazione di vSphere.
- Aumentare la memoria dell'appliance vSphere Orchestrator fino ad almeno 6 GB. Vedere *Amministrazione delle macchine virtuali vSphere* nella documentazione di vSphere.
- Creare uno snapshot della macchina virtuale vSphere Orchestrator. Vedere *Amministrazione delle macchine virtuali vSphere* nella documentazione di vSphere.
- Se si utilizza un database esterno, eseguirne il backup.
- Se si utilizza il database PostgreSQL preconfigurato in vSphere Orchestrator, eseguire il backup del database utilizzando il menu per l'**esportazione del database** in vSphere Control Center.

## Procedura

- ◆ Utilizzare uno dei metodi descritti nella documentazione per aggiornare l'istanza di vRealize Orchestrator autonoma.
  - [Aggiornamento di Orchestrator Appliance mediante il repository predefinito di VMware.](#)
  - [Aggiornamento di Orchestrator Appliance utilizzando un'immagine ISO.](#)
  - [Aggiornamento di Orchestrator Appliance mediante un repository specificato.](#)

## Aggiornamento di Orchestrator Appliance mediante il repository predefinito di VMware

È possibile configurare Orchestrator in modo che scarichi il pacchetto di aggiornamento del repository predefinito di VMware.

## Prerequisiti

- Smontare tutti i file system di rete. Per ulteriori informazioni, vedere la documentazione *Amministrazione delle macchine virtuali vSphere*.
- Aumentare la memoria di Orchestrator Appliance fino ad almeno 6 GB. Per ulteriori informazioni, vedere la documentazione *Amministrazione delle macchine virtuali vSphere*.
- Aumentare le dimensioni del disco della macchina virtuale di vRealize Orchestrator: disco 1 = 7 GB, disco 2 = 10 GB.
- Accertarsi che la partizione radice di Orchestrator Appliance disponga di almeno 3 GB di spazio libero. Per ulteriori informazioni sull'aumento della dimensione di una partizione del disco, vedere KB 1004071: <http://kb.vmware.com/kb/1004071>.
- Creare uno snapshot della macchina virtuale Orchestrator. Per ulteriori informazioni, vedere la documentazione *Amministrazione delle macchine virtuali vSphere*.
- Se si utilizza un database esterno, eseguirne il backup.
- Se si utilizza il database PostgreSQL preconfigurato in Orchestrator, eseguire il backup del database utilizzando il menu per l'**esportazione del database** in Control Center.

## Procedura

- 1 Passare a VAMI (Virtual Appliance Management Interface) all'indirizzo `https://orchestrator_server:5480` e accedere come **root**.
- 2 Nella scheda **Aggiorna**, fare clic su **Impostazioni**.  
Il pulsante di opzione accanto all'opzione **Usa repository predefinito** è selezionato.
- 3 Nella pagina **Stato**, fare clic su **Verifica aggiornamenti**.
- 4 Se sono disponibili aggiornamenti, fare clic su **Installa aggiornamenti**.
- 5 Accettare l'accordo di licenza con l'utente finale (EULA) di VMware e confermare che si desidera installare l'aggiornamento.
- 6 Per completare l'aggiornamento, riavviare Orchestrator Appliance.
  - a Accedere nuovamente a VAMI come **root**.
- 7 (Facoltativo) Nella scheda **Aggiorna**, verificare che la versione più recente di Orchestrator Appliance sia stata installata correttamente.
- 8 Accedere a Control Center come **root**.
- 9 Se si intende creare un cluster delle istanze di Orchestrator, riconfigurare le impostazioni degli host.
  - a Nella pagina **Impostazioni host** in Control Center fare clic su **MODIFICA**.
  - b Sostituire il nome dell'appliance vRealize Orchestrator con il nome host del server di bilanciamento del carico.
- 10 Riconfigurare l'autenticazione.
  - a Se prima dell'aggiornamento il server Orchestrator è stato configurato per l'utilizzo di **LDAP** o **SSO (legacy)** come metodo di autenticazione, configurare **vSphere** o **vRealize Automation** come provider di autenticazione.
  - b Se l'autenticazione è già impostata su **vSphere** o su **vRealize Automation**, annullare la registrazione delle impostazioni e registrarle nuovamente.

---

**Nota** Se prima dell'aggiornamento, l'Orchestrator ha utilizzato **vSphere** come provider di autenticazione ed è stato configurato per connettersi al nome di dominio completo o all'indirizzo IP di vCenter Server, nel caso in cui si disponga di un Platform Services Controller esterno, dopo l'aggiornamento è necessario configurare Orchestrator per connettersi al nome di dominio completo o all'indirizzo IP dell'istanza di Platform Services Controller che contiene il vCenter Single Sign-On. È inoltre necessario importare manualmente in Orchestrator i certificati di tutti i Platform Services Controller che condividono lo stesso dominio vCenter Single Sign-On.

---

L'aggiornamento di Orchestrator Appliance è stato eseguito correttamente.

## Operazioni successive

Verificare che Orchestrator sia configurato correttamente nella pagina **Convalida configurazione** in Control Center.

## Aggiornamento di Orchestrator Appliance utilizzando un'immagine ISO

È possibile configurare Orchestrator in modo che scarichi il pacchetto di aggiornamento da un file di immagine ISO montata nell'unità CD-ROM dell'appliance.

### Prerequisiti

- Smontare tutti i file system di rete. Per ulteriori informazioni, vedere la documentazione *Amministrazione delle macchine virtuali vSphere*.
- Aumentare la memoria di Orchestrator Appliance fino ad almeno 6 GB. Per ulteriori informazioni, vedere la documentazione *Amministrazione delle macchine virtuali vSphere*.
- Aumentare le dimensioni del disco della macchina virtuale di vRealize Orchestrator: disco 1 = 7 GB, disco 2 = 10 GB.
- Accertarsi che la partizione radice di Orchestrator Appliance disponga di almeno 3 GB di spazio libero. Per ulteriori informazioni sull'aumento della dimensione di una partizione del disco, vedere KB 1004071: <http://kb.vmware.com/kb/1004071>.
- Creare uno snapshot della macchina virtuale Orchestrator. Per ulteriori informazioni, vedere la documentazione *Amministrazione delle macchine virtuali vSphere*.
- Se si utilizza un database esterno, eseguirne il backup.
- Se si utilizza il database PostgreSQL preconfigurato in Orchestrator, eseguire il backup del database utilizzando il menu per l'**esportazione del database** in Control Center.

### Procedura

- 1 Scaricare l'archivio VMware-vRO-Appliance-version-build\_number-updaterepo.iso dal sito di download ufficiale di VMware.
- 2 Connettere l'unità CD-ROM della macchina virtuale Orchestrator Appliance. Per ulteriori informazioni, vedere la documentazione *Amministrazione delle macchine virtuali vSphere*.
- 3 Montare il file di immagine ISO nell'unità CD-ROM dell'appliance. Per ulteriori informazioni, vedere la documentazione *Amministrazione delle macchine virtuali vSphere*.
- 4 Passare a VAMI (Virtual Appliance Management Interface) all'indirizzo [https://orchestrator\\_server:5480](https://orchestrator_server:5480) e accedere come **root**.
- 5 Nella scheda **Aggiorna**, fare clic su **Impostazioni**.
- 6 Selezionare il pulsante di opzione accanto all'opzione **Usa aggiornamenti da CD-ROM**.
- 7 Tornare alla pagina **Stato**.  
Viene visualizzata la versione dell'aggiornamento disponibile.
- 8 Fare clic su **Installa aggiornamenti**.
- 9 Accettare l'accordo di licenza con l'utente finale (EULA) di VMware e confermare che si desidera installare l'aggiornamento.

- 10 Per completare l'aggiornamento, riavviare Orchestrator Appliance.
  - a Accedere nuovamente a VAMI come **root**.
- 11 (Facoltativo) Nella scheda **Aggiorna**, verificare che la versione più recente di Orchestrator Appliance sia stata installata correttamente.
- 12 Accedere a Control Center come **root**.
- 13 Se si intende creare un cluster delle istanze di Orchestrator, riconfigurare le impostazioni degli host.
  - a Nella pagina **Impostazioni host** in Control Center fare clic su **MODIFICA**.
  - b Sostituire il nome dell'appliance vRealize Orchestrator con il nome host del server di bilanciamento del carico.
- 14 Riconfigurare l'autenticazione.
  - a Se prima dell'aggiornamento il server Orchestrator è stato configurato per l'utilizzo di **LDAP** o **SSO (legacy)** come metodo di autenticazione, configurare **vSphere** o **vRealize Automation** come provider di autenticazione.
  - b Se l'autenticazione è già impostata su **vSphere** o su **vRealize Automation**, annullare la registrazione delle impostazioni e registrarle nuovamente.

---

**Nota** Se prima dell'aggiornamento, l'Orchestrator ha utilizzato **vSphere** come provider di autenticazione ed è stato configurato per connettersi al nome di dominio completo o all'indirizzo IP di vCenter Server, nel caso in cui si disponga di un Platform Services Controller esterno, dopo l'aggiornamento è necessario configurare Orchestrator per connettersi al nome di dominio completo o all'indirizzo IP dell'istanza di Platform Services Controller che contiene il vCenter Single Sign-On. È inoltre necessario importare manualmente in Orchestrator i certificati di tutti i Platform Services Controller che condividono lo stesso dominio vCenter Single Sign-On.

---

L'aggiornamento di Orchestrator Appliance è stato eseguito correttamente.

#### Operazioni successive

Verificare che Orchestrator sia configurato correttamente nella pagina **Convalida configurazione** in Control Center.

#### Aggiornamento di Orchestrator Appliance mediante un repository specificato

È possibile configurare Orchestrator in modo che utilizzi un repository locale, in cui è stato caricato l'archivio di aggiornamento.

#### Prerequisiti

- Smontare tutti i file system di rete. Per ulteriori informazioni, vedere la documentazione *Amministrazione delle macchine virtuali vSphere*.
- Aumentare la memoria di Orchestrator Appliance fino ad almeno 6 GB. Per ulteriori informazioni, vedere la documentazione *Amministrazione delle macchine virtuali vSphere*.

- Aumentare le dimensioni del disco della macchina virtuale di vRealize Orchestrator: disco 1 = 7 GB, disco 2 = 10 GB.
- Accertarsi che la partizione radice di Orchestrator Appliance disponga di almeno 3 GB di spazio libero. Per ulteriori informazioni sull'aumento della dimensione di una partizione del disco, vedere KB 1004071: <http://kb.vmware.com/kb/1004071>.
- Creare uno snapshot della macchina virtuale Orchestrator. Per ulteriori informazioni, vedere la documentazione *Amministrazione delle macchine virtuali vSphere*.
- Se si utilizza un database esterno, eseguirne il backup.
- Se si utilizza il database PostgreSQL preconfigurato in Orchestrator, eseguire il backup del database utilizzando il menu per **l'esportazione del database** in Control Center.

### Procedura

- 1 Preparare il repository locale per gli aggiornamenti.
  - a Installare e configurare un server Web locale.
  - b Scaricare l'archivio VMware-vRO-Appliance-version-build\_number-updaterepo.zip dal sito di download ufficiale di VMware.
  - c Estrarre l'archivio .ZIP nel repository locale.
- 2 Passare a VAMI (Virtual Appliance Management Interface) all'indirizzo `https://orchestrator_server:5480` e accedere come **root**.
- 3 Nella scheda **Aggiorna**, fare clic su **Impostazioni**.
- 4 Selezionare il pulsante di opzione accanto all'opzione **Usa repository specificato**.
- 5 Immettere l'indirizzo URL del repository locale puntando alla directory Update\_Repo.  
`http://local_web_server:port/build/mts/release/bora-build_number/publish/exports/Update_Repo`
- 6 Se il repository locale richiede l'autenticazione, immettere nome utente e password.
- 7 Fare clic su **Salva impostazioni**.
- 8 Nella pagina **Stato**, fare clic su **Verifica aggiornamenti**.
- 9 Se sono disponibili aggiornamenti, fare clic su **Installa aggiornamenti**.
- 10 Accettare l'accordo di licenza con l'utente finale (EULA) di VMware e confermare che si desidera installare l'aggiornamento.
- 11 Per completare l'aggiornamento, riavviare Orchestrator Appliance.
  - a Accedere nuovamente a VAMI come **root**.
- 12 (Facoltativo) Nella scheda **Aggiorna**, verificare che la versione più recente di Orchestrator Appliance sia stata installata correttamente.
- 13 Accedere a Control Center come **root**.



- 14 Se si intende creare un cluster delle istanze di Orchestrator, riconfigurare le impostazioni degli host.
  - a Nella pagina **Impostazioni host** in Control Center fare clic su **MODIFICA**.
  - b Sostituire il nome dell'appliance vRealize Orchestrator con il nome host del server di bilanciamento del carico.
- 15 Riconfigurare l'autenticazione.
  - a Se prima dell'aggiornamento il server Orchestrator è stato configurato per l'utilizzo di **LDAP** o **SSO (legacy)** come metodo di autenticazione, configurare **vSphere** o **vRealize Automation** come provider di autenticazione.
  - b Se l'autenticazione è già impostata su **vSphere** o su **vRealize Automation**, annullare la registrazione delle impostazioni e registrarle nuovamente.

---

**Nota** Se prima dell'aggiornamento, l'Orchestrator ha utilizzato **vSphere** come provider di autenticazione ed è stato configurato per connettersi al nome di dominio completo o all'indirizzo IP di vCenter Server, nel caso in cui si disponga di un Platform Services Controller esterno, dopo l'aggiornamento è necessario configurare Orchestrator per connettersi al nome di dominio completo o all'indirizzo IP dell'istanza di Platform Services Controller che contiene il vCenter Single Sign-On. È inoltre necessario importare manualmente in Orchestrator i certificati di tutti i Platform Services Controller che condividono lo stesso dominio vCenter Single Sign-On.

---

L'aggiornamento di Orchestrator Appliance è stato eseguito correttamente.

#### Operazioni successive

Verificare che Orchestrator sia configurato correttamente nella pagina **Convalida configurazione** in Control Center.

#### Aggiornamento di un cluster di appliance vRealize Orchestrator per l'utilizzo con vRealize Automation 7.4

Se si utilizza un cluster di appliance vRealize Orchestrator con vRealize Automation, è necessario aggiornare il cluster di appliance Orchestrator alla versione 7.4 aggiornando una singola istanza e unendo i nodi della versione 7.4 appena installata all'istanza aggiornata.

Per aggiornare una singola istanza di vRealize Orchestrator, vedere [Aggiornamento di un'appliance vRealize Orchestrator autonoma per l'utilizzo con vRealize Automation](#).

#### Prerequisiti

- [Installazione dell'aggiornamento nell'appliance vRealize Automation e nei componenti IaaS](#).
- Configurare un bilanciamento del carico per distribuire il traffico tra più istanze di vRealize Orchestrator. Vedere la [guida alla configurazione del bilanciamento del carico di vRealize Orchestrator](#).
- Creare uno snapshot di tutti i nodi del server vRealize Orchestrator.
- Eseguire il backup del database condiviso di vRealize Orchestrator.

## Procedura

- 1 Arrestare i servizi di Orchestrator `vco-server` e `vco-configurator` in tutti i nodi del cluster.
- 2 Aggiornare una sola istanza del server Orchestrator nel cluster utilizzando una delle procedure documentate.
- 3 Distribuire una nuova appliance Orchestrator nella versione 7.3.
  - a Configurare il nuovo nodo con le impostazioni di rete di un'istanza esistente non aggiornata che fa parte del cluster.
- 4 Accedere a Control Center del secondo nodo per avviare la configurazione guidata.
  - a Passare a `https://your_orchestrator_server_IP_or_DNS_name:8283/vco-controlcenter`.
  - b Accedere come **root** utilizzando la password immessa durante la distribuzione di OVA.
- 5 Selezionare il tipo di distribuzione **Orchestrator in cluster**.  
Selezionando questo tipo, si sceglie di unire il nodo a un cluster Orchestrator esistente.
- 6 Nella casella di testo **Nome host**, immettere il nome host o l'indirizzo IP della prima istanza del server Orchestrator.

---

**Nota** Deve essere l'IP o il nome host locale dell'istanza di Orchestrator a cui unire il secondo nodo. Non utilizzare l'indirizzo del bilanciamento del carico.

---

- 7 Nelle caselle di testo **Nome utente** e **Password**, immettere le credenziali di root della prima istanza del server Orchestrator.
- 8 Fare clic su **Unisci**. L'istanza di Orchestrator clona la configurazione del nodo a cui si unisce.  
Il servizio del server Orchestrator di entrambi i nodi viene riavviato automaticamente.
- 9 Accedere a Control Center del cluster Orchestrator aggiornato mediante l'indirizzo del bilanciamento del carico e accedere come **amministratore**.
- 10 Nella pagina **Gestione cluster Orchestrator** verificare che la stringa dell'**impronta digitale della configurazione attiva** corrisponda a quella dell'**impronta digitale della configurazione in sospeso** in tutti i nodi del cluster.

---

**Nota** Potrebbe essere necessario aggiornare la pagina più volte fino a quando le due stringhe non corrispondono.

---

- 11 Verificare che il cluster vRealize Orchestrator sia configurato in modo appropriato aprendo la pagina **Convalida configurazione** in Control Center.
- 12 (Facoltativo) Ripetere i passaggi da 3 a 8 per ogni nodo aggiuntivo nel cluster.

Il cluster di Orchestrator è stato aggiornato.

## Operazioni successive

[Attivare i bilanciamenti del carico.](#)

## Attivare i bilanciamenti del carico

Se la distribuzione utilizza bilanciamenti del carico, riabilitare i nodi secondari e i controlli di integrità e ripristinare le impostazioni del timeout dei bilanciamenti del carico.

I controlli di integrità per vRealize Automation variano in base alla versione. Per informazioni, consultare *Guida alla configurazione del bilanciamento del carico di vRealize Automation* nella [Documentazione di VMware vRealize Automation](#).

Ripristinare il valore predefinito delle impostazioni del timeout dei bilanciamenti del carico il cui valore è 10 minuti.

## Attività successive all'aggiornamento di vRealize Automation

Dopo aver aggiornato da vRealize Automation 7.3.x, 7.1 o 7.2 alla versione 7.4, è necessario eseguire le attività successive all'aggiornamento richieste.

### Aggiornamento degli agenti software a TLS 1.2

Dopo l'aggiornamento a vRealize Automation 7.4, è necessario eseguire varie attività per aggiornare gli agenti software dell'ambiente vRealize Automation 7.1, 7.2, 7.3 o 7.3.1 alla versione TLS 1.2

A partire da vRealize Automation 7.4, Transport Layer Security (TLS) 1.2 è l'unico protocollo TLS supportato per la comunicazione dati tra vRealize Automation e il browser.

Dopo la migrazione, è necessario aggiornare i modelli di macchina virtuale esistenti dell'ambiente vRealize Automation 7.1, 7.2, 7.3 o 7.3.1, nonché tutte le macchine virtuali esistenti.

### Aggiornamento dei modelli delle macchine virtuali di vRealize Automation

Una volta completato l'aggiornamento a vRealize Automation 7.4, è necessario aggiornare i modelli esistenti in modo che gli agenti software utilizzino il protocollo TLS 1.2.

L'agente guest e il codice bootstrap dell'agente devono essere aggiornati nei modelli di vRealize Automation 7.1, 7.2, 7.3 e 7.3.1. Se si utilizza l'opzione di un clone collegato, potrebbe essere necessario mappare nuovamente i modelli alle nuove macchine virtuali create e ai relativi snapshot.

Per aggiornare i modelli, completare le seguenti attività.

- 1 Accedere a vSphere.
- 2 Convertire ogni modello da vRealize Automation 7.1, 7.2, 7.3 o 7.3.1 a una macchina virtuale e accendere la macchina.
- 3 Importare il programma di installazione del software appropriato ed eseguire il programma di installazione del software in ogni macchina virtuale.
- 4 Convertire nuovamente ogni macchina virtuale in un modello.

Per individuare il programma di installazione del software per Linux o Windows, utilizzare la seguente procedura.

**Prerequisiti**

Aggiornamento a vRealize Automation 7.4 riuscito.

**Procedura**

- 1 Avviare un browser e aprire la pagina iniziale dell'appliance vRealize Automation 7.4 utilizzando il nome di dominio completo dell'appliance virtuale: `https://vra-va-hostname.domain.name`.
- 2 Fare clic sulla **pagina degli agenti guest e software**.
- 3 Seguire le istruzioni per il programma di installazione del software di Linux o Windows.

**Operazioni successive**

[Identificazione delle macchine virtuali che richiedono l'aggiornamento dell'agente software.](#)

**Identificazione delle macchine virtuali che richiedono l'aggiornamento dell'agente software**

È possibile utilizzare il servizio di integrità in vRealize Automation per identificare le macchine virtuali che richiedono un aggiornamento dell'agente software a TLS 1.2.

È possibile utilizzare il servizio di integrità per identificare le macchine virtuali che richiedono un aggiornamento dell'agente software a TLS 1.2. Tutti gli agenti software nell'ambiente di vRealize Automation 7.4 devono essere aggiornati affinché sia possibile eseguire le procedure di post-provisioning, che richiedono una comunicazione sicura tra il browser e vRealize Automation.

**Prerequisiti**

- È stato effettuato l'aggiornamento a vRealize Automation 7.4.
- Si è connessi a vRealize Automation 7.4 nell'appliance virtuale primaria come amministratore tenant.

**Procedura**

- 1 Fare clic su **Amministrazione > Integrità**.
- 2 Fare clic su **Nuova configurazione**.
- 3 Nella pagina dei dettagli della configurazione, fornire le informazioni richieste.

Opzione	Commento
Nome	Immettere <b>SW Agent verification</b> .
Descrizione	Aggiungere una descrizione facoltativa, ad esempio <b>Locate software agents for upgrade to TLS 1.2</b> .
Prodotto	Selezionare vRealize Automation 7.4.0.
Pianificazione	Selezionare <b>Nessuna</b> .

- 4 Fare clic su **Avanti**.
- 5 Nella pagina di selezione delle suite di prove, selezionare **Prove di sistema per vRealize Automation** e **Prove del tenant per vRealize Automation**.
- 6 Fare clic su **Avanti**.

- 7 Nella pagina dei parametri di configurazione, fornire le informazioni richieste.

**Tabella 1-56. Appliance virtuale vRealize Automation**

Opzione	Descrizione
Indirizzo server Web pubblico	<ul style="list-style-type: none"> <li>■ Per una distribuzione minima, l'URL di base per l'host dell'appliance vRealize Automation. Ad esempio, <code>https://va-host.domain/</code>.</li> <li>■ Per una distribuzione ad alta disponibilità, l'URL di base per il servizio di bilanciamento del carico di vRealize Automation. Ad esempio, <code>https://load-balancer-host.domain/</code>.</li> </ul>
Indirizzo console SSH	Nome di dominio completo dell'appliance vRealize Automation. Ad esempio, <code>va-host.domain</code> .
Utente console SSH	<b>root</b>
Password console SSH	Password root.
Tempo di risposta massimo del servizio (ms)	Accettare il valore predefinito: 2000

**Tabella 1-57. Tenant di sistema vRealize Automation**

Opzione	Descrizione
Amministratore tenant di sistema	administrator
Password tenant di sistema	Password per l'amministratore.

**Tabella 1-58. Monitoraggio dello spazio su disco di vRealize Automation**

Opzione	Descrizione
Percentuale soglia di avviso	Accettare il valore predefinito: 75
Percentuale soglia critica	Accettare il valore predefinito: 90

**Tabella 1-59. Tenant vRealize Automation**

Opzione	Descrizione
Tenant in prova	Tenant selezionato per la prova.
Nome utente amministratore della struttura	<p>Nome dell'utente amministratore della struttura Ad esempio, <code>admin@va-host.local</code>.</p> <p><b>Nota</b> L'amministratore della struttura deve anche disporre di un ruolo di amministratore tenant e di amministratore IaaS nell'ordine per tutte le prove da eseguire.</p>
Password amministratore struttura	Password per l'amministratore della struttura.

- 8 Fare clic su **Avanti**.
- 9 Nella pagina Riepilogo, esaminare le informazioni e fare clic su **Fine**.
- La configurazione di verifica dell'agente software è terminata.
- 10 Nella scheda della verifica dell'agente SW, fare clic su **Esegui**.

- 11 Una volta completata la prova, fare clic al centro della scheda di verifica dell'agente SW.
- 12 Nella pagina dei risultati della verifica dell'agente SW, scorrere i risultati delle prove e individuare la prova Check Software Agent Version nella colonna Nome. Se il risultato della prova è Non riuscita, fare clic sul collegamento **Causa** nella colonna Causa per visualizzare le macchine virtuali il cui agente software è obsoleto.

### Operazioni successive

Se sono presenti macchine virtuali con un agente software obsoleto, vedere [Aggiornamento degli agenti software in vSphere](#).

### Aggiornamento degli agenti software in vSphere

È possibile aggiornare gli agenti software obsoleti in vSphere a TLS 1.2 dopo l'aggiornamento utilizzando la console di gestione dell'appliance di vRealize Automation.

Questa procedura aggiorna gli agenti software obsoleti a TLS 1.2 nelle macchine virtuali nell'ambiente aggiornato. È necessaria per l'aggiornamento a vRealize Automation 7.4.

### Prerequisiti

- Aggiornamento a vRealize Automation 7.4 riuscito.
- È stato utilizzato il servizio di integrità per identificare le appliance virtuali con agenti software obsoleti.

### Procedura

- 1 Nell'appliance vRealize Automation primaria, accedere alla gestione dell'appliance di vRealize Automation come **root** utilizzando la password immessa durante la distribuzione dell'appliance vRealize Automation.

Per un ambiente ad alta disponibilità, aprire la console di gestione dell'appliance nell'appliance master.

- 2 Fare clic su **Impostazioni vRA > Agenti SW**.

- 3 Fare clic su **Attiva/Disattiva TLS 1.0, 1.1**.

Lo stato di TLS v1.0, v1.1 è Abilitato.

- 4 Per le credenziali del tenant, immettere le informazioni richieste per l'appliance vRealize Automation 7.4.

Opzione	Descrizione
Nome tenant	Nome del tenant nell'appliance vRealize Automation aggiornata.  <b>Nota</b> All'utente del tenant è necessario assegnare il ruolo Architetto del software.
Username	Nome utente dell'amministratore tenant nell'appliance vRealize Automation.
Password	Password dell'amministratore tenant.

- 5 Fare clic su **Prova connessione**.

Se viene stabilita una connessione, viene visualizzato un messaggio che indica che l'operazione è riuscita.

- 6 Fare clic su **Elenca batch**.

Viene visualizzata una tabella che include i batch.

- 7 Fare clic su **Mostra**.

Viene visualizzata una tabella con l'elenco delle macchine virtuali con agenti software obsoleti.

- 8 Aggiornare l'agente software per le macchine virtuali con stato Aggiornabile.

- Per aggiornare l'agente software in una singola macchina virtuale, fare clic su **Mostra** per un gruppo di macchine virtuali, identificare la macchina virtuale che si desidera aggiornare e fare clic su **Esegui** per avviare il processo di aggiornamento.
- Per aggiornare l'agente software per un batch di macchine virtuali, identificare il gruppo che si desidera aggiornare e fare clic su **Esegui** per avviare il processo di aggiornamento.

Se sono presenti più di 200 macchine virtuali da aggiornare, è possibile controllare la velocità del processo di aggiornamento batch inserendo i valori per questi parametri.

Opzione	Descrizione
Dimensioni batch	Il numero di macchine virtuali selezionato per l'aggiornamento batch. È possibile modificare questo numero per regolare la velocità di aggiornamento.
Profondità coda	Numero di aggiornamenti paralleli eseguiti contemporaneamente. Ad esempio, 20. È possibile modificare questo numero per regolare la velocità di aggiornamento.
Errori batch	Numero di errori REST che causano il rallentamento dell'aggiornamento batch. Se ad esempio si desidera arrestare l'aggiornamento batch corrente dopo 5 errori per migliorare la stabilità dell'aggiornamento, inserire 5 nel campo di testo.

Opzione	Descrizione
Operazioni batch non riuscite	Numero di aggiornamenti dell'agente software non riusciti che causano il rallentamento dell'elaborazione batch. Se ad esempio si desidera arrestare l'aggiornamento batch corrente dopo 5 errori per migliorare la stabilità dell'aggiornamento, inserire 5 nel campo di testo.
Polling batch	Frequenza con cui viene eseguito il polling nel processo di aggiornamento per controllarne l'avanzamento. È possibile modificare questo numero per regolare la velocità di aggiornamento.

Se il processo di aggiornamento è troppo lento o produce troppi aggiornamenti non riusciti, è possibile modificare questi parametri per migliorare le prestazioni dell'aggiornamento.

**Nota** Se si fa clic su **Aggiorna**, l'elenco dei batch viene cancellato. Ciò non influisce sul processo di aggiornamento. L'operazione aggiorna anche le informazioni relative al fatto che TLS 1.2 sia o meno impostato. Se si fa clic su **Aggiorna**, viene inoltre eseguito un controllo dell'integrità dei servizi di vRealize Automation. Se i servizi non sono in esecuzione, il sistema visualizza un messaggio di errore e disattiva tutti gli altri pulsanti di azione.

## 9 Fare clic su **Attiva/Disattiva TLS 1.0, 1.1**.

Lo stato di TLS v1.0, v1.1 è Disabilitato.

## Aggiornamento degli agenti software su Amazon Web Service o Azure

È possibile aggiornare manualmente qualsiasi agente software obsoleto nelle macchine virtuali in Amazon Web Service (AWS) o Azure.

### Prerequisiti

- Aggiornamento a vRealize Automation 7.4 riuscito.
- È presente un tunnel software e l'indirizzo IP della macchina virtuale del tunnel è noto.

### Procedura

#### 1 Creare un file di nodo per ogni nodo da aggiornare.

```
/usr/lib/vcac/server/webapps/ROOT/software/initializeUpdateSoftwareAgents.py -a <
$DestinationVRAServer> -t <$Tenant> -tu <$TenantUser> -S <$SourceVRAServer>
```

**Nota** Per un aggiornamento sul posto, \$DestinationVRAServer corrisponde a \$SourceVRAServer.



## 2 Creare un file di piano per aggiornare l'agente software in una macchina virtuale Windows o Linux.

- Modificare il file params di migrazione in `/var/log/vcac/agentupdate/{tenant}/{subtenant-UUID}` in modo che contenga il valore dell'indirizzo IP privato corrispondente all'endpoint di AWS o Azure.

```
"key": "ipAddress",

    "value": {

        "type": "string",

        "value": "<$PrivateIp:$PrivatePort>"

    }
}
```

- Utilizzare questo comando per aggiornare una macchina Linux.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer>
-t <$Tenant> -S <$SourceVRAServer> -tu <$TenantUser> -CL Software.LinuxAgentUpdate74 --
source_cloud_provider azure
```

- Utilizzare questo comando per aggiornare una macchina Windows.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer>
-t <$Tenant> -S <$SourceVRAServer> -tu <$TenantUser> -CW Software.WindowsAgentUpdate74 --
source_cloud_provider azure
```

- Questo comando esegue il file di piano.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer>
-t <$Tenant> -tu <$TenantUser> --plan_file /usr/lib/vcac/server/webapps/ROOT/software/plan
```

- 3 Utilizzare questo comando per aggiornare l'agente software utilizzando il file di nodo del passaggio 1 e il file di piano del passaggio 2.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer> -t <$tenant> -tu <$TenantUser> --component_windows Software.WindowsAgentUpdate74 --component_linux Software.LinuxAgentUpdate74 --plan_file /usr/lib/vcac/server/webapps/ROOT/software/plan --plan_index 0 --node_file /usr/lib/vcac/server/webapps/ROOT/software/node --source_cloud_provider azure --action plan_batch -S <$SourceVRAServer>
```

In alternativa, è possibile utilizzare questo comando per eseguire un nodo alla volta a partire dal file di nodo, fornendo un indice dei nodi.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer> -t <$tenant> -tu <$TenantUser> --component_windows Software.WindowsAgentUpdate74 --component_linux Software.LinuxAgentUpdate74 --plan_file /usr/lib/vcac/server/webapps/ROOT/software/plan --plan_index 0 --node_file /usr/lib/vcac/server/webapps/ROOT/software/node --source_cloud_provider azure --action execute_node -S <$SourceVRAServer> --node_index <0 through n-1>
```

Quando si esegue questa procedura, è possibile accodare i registri dell'appliance virtuale vRealize Automation e dalla macchina host per vedere il processo di aggiornamento dell'agente server.

Dopo l'aggiornamento, il processo di aggiornamento importa uno script di aggiornamento del software per Windows o Linux nell'appliance virtuale vRealize Automation 7.4. È possibile accedere all'host dell'appliance virtuale vRealize Automation per assicurarsi che il componente software sia stato importato correttamente. Dopo l'importazione del componente, un aggiornamento software viene inviato al servizio EBS (Event Broker Service) precedente per l'inoltro degli script di aggiornamento software alle macchine virtuali identificate. Quando l'aggiornamento viene completato e i nuovi agenti software diventano operativi, effettuano il binding alla nuova appliance virtuale di vRealize Automation inviando una richiesta di ping.

---

**Nota** File di registro utili

---

- Output di Catalina per vRealize Automation di origine: `/var/log/vcac/catalina.out`. In questo file sono contenute le richieste di aggiornamento create all'esecuzione delle migrazioni degli agenti. Questa attività corrisponde all'esecuzione di una richiesta di provisioning del software.
- Output di Catalina per vRealize Automation di destinazione: `/var/log/vcac/catalina.out`. In questo file sono contenute le richieste di ping delle macchine virtuali migrate per includere numeri di versione 7.4.0-SNAPSHOT. È possibile registrarle insieme confrontando i nomi degli argomenti EBS, ad esempio `sw-agent-UUID`.
- Cartella di aggiornamento dell'agente nel file di registro dell'aggiornamento master della macchina vRealize Automation di destinazione: `/var/log/vmware/vcac/agentupdate/updateSoftwareAgents.log`. È possibile accodare questo file per vedere quale operazione di aggiornamento è in corso.
- Registri singoli disponibili nelle cartelle del tenant: `/var/log/vcac/agentupdate/{tenant}/{subtenant-UUID}`. Qui sono elencati i singoli nodi come file LOT con errori ed estensioni in corso.

- Macchine virtuali migrate: /opt/vmware-appdirector/agent/logs/darwin\*.log. È possibile controllare a campione questo percorso in cui vengono elencate le richieste di aggiornamento software ricevute e l'eventuale riavvio di agent\_bootstrap + agente software.

### Impostazione della modalità sincrona per la replica PostgreSQL di vRealize Automation

Se prima di eseguire l'aggiornamento si imposta la replica PostgreSQL sulla modalità asincrona, è possibile impostarla sulla modalità sincrona dopo l'aggiornamento di un ambiente vRealize Automation distribuito.

#### Prerequisiti

- È stato eseguito l'aggiornamento di un ambiente vRealize Automation distribuito.
- Si è connessi come **root** all'interfaccia di gestione dell'appliance vRealize Automation appropriata all'indirizzo <https://vra-vd-hostname.domain.name:5480>.

#### Procedura

- 1 Fare clic su **Impostazioni vRA > Database**.
- 2 Fare clic su **Modalità sincrona** e attendere il completamento dell'azione.
- 3 Verificare che per tutti i nodi nella colonna Stato di sincronizzazione sia visualizzato lo stato Sincrono.

#### Operazioni successive

[Esecuzione di Prova connessione e verifica degli endpoint aggiornati.](#)

### Esecuzione di Prova connessione e verifica degli endpoint aggiornati

L'aggiornamento da vRealize Automation 7.3 o versioni precedenti alla versione 7.4 apporta modifiche agli endpoint nell'ambiente di destinazione.

Dopo aver effettuato l'aggiornamento a vRealize Automation 7.4, è necessario utilizzare l'azione **Prova connessione** per tutti gli endpoint applicabili. Potrebbe anche essere necessario apportare modifiche ad alcuni endpoint aggiornati. Per ulteriori informazioni, vedere [Considerazioni sull'utilizzo degli endpoint aggiornati o migrati](#).

L'impostazione di sicurezza predefinita per gli endpoint aggiornati o migrati prevede che i certificati non attendibili non vengano accettati.

Dopo l'aggiornamento o la migrazione da un'installazione precedente di vRealize Automation, se venivano utilizzati certificati non attendibili, è necessario eseguire la procedura che segue per tutti gli endpoint vSphere e NSX per consentire la convalida dei certificati. In caso contrario, le operazioni sugli endpoint non riusciranno e verranno restituiti errori di certificato. Per ulteriori informazioni, vedere gli

articoli della Knowledge Base di VMware *Endpoint communication is broken after upgrade to vRA 7.3* (2150230) all'indirizzo <http://kb.vmware.com/kb/2150230> e *How to download and install vCenter Server root certificates to avoid Web Browser certificate warnings* (2108294) all'indirizzo <http://kb.vmware.com/kb/2108294>.

- 1 Dopo l'aggiornamento o la migrazione, accedere alla macchina dell'agente vRealize Automation vSphere e riavviare gli agenti vSphere utilizzando la scheda **Servizi**.

La migrazione potrebbe non riavviare tutti gli agenti, pertanto è necessario riavviarli manualmente se richiesto.

- 2 Attendere il completamento di almeno un report di ping. Questa operazione richiede uno o due minuti.
- 3 Dopo che gli agenti vSphere avranno avviato la raccolta dati, accedere a vRealize Automation come amministratore IaaS.
- 4 Fare clic su **Infrastruttura > Endpoint > Endpoint**.
- 5 Modificare un endpoint vSphere e fare clic su **Prova connessione**.
- 6 Se viene visualizzato un prompt sul certificato, fare clic su **OK** per accettare il certificato.  
  
In caso contrario, è possibile che al momento il certificato sia correttamente archiviato presso un'autorità root attendibile del servizio di hosting della macchina Windows per l'endpoint, ad esempio come macchina agente proxy o come macchina DEM.
- 7 Fare clic su **OK** per accettare il certificato e salvare l'endpoint.
- 8 Ripetere questa procedura per ogni endpoint vSphere.
- 9 Ripetere questa procedura per ogni endpoint NSX.

Se l'azione **Prova connessione** riesce ma alcune operazioni di provisioning o di raccolta dati hanno esito negativo, è possibile installare lo stesso certificato in tutte le macchine agente che servono l'endpoint e su tutte le macchine DEM. In alternativa, è possibile disinstallare il certificato dalle macchine esistenti e ripetere la procedura precedente per l'endpoint in cui si verifica l'errore.

### **Esecuzione della raccolta dati di Inventario rete e sicurezza di NSX dopo l'aggiornamento da vRealize Automation**

Dopo avere effettuato l'aggiornamento da vRealize Automation 7.1, 7.2 o 7.3.x alla versione 7.4, è necessario eseguire la raccolta dati di Inventario rete e sicurezza di NSX nell'ambiente di vRealize Automation 7.4.

La raccolta dati è necessaria per assicurare il funzionamento dell'azione di riconfigurazione del bilanciamento del carico in vRealize Automation 7.4 per le distribuzioni delle versioni 7.1, 7.2 o 7.3.x.

#### **Prerequisiti**

- [Esecuzione della raccolta dati di Inventario rete e sicurezza di NSX prima dell'aggiornamento di vRealize Automation](#).
- Aggiornamento a vRealize Automation 7.4 riuscito.

**Procedura**

- ◆ Eseguire la raccolta dati di Inventario rete e sicurezza di NSX in vRealize Automation 7.4 dopo l'aggiornamento. Vedere [Avvio manuale della raccolta dati degli endpoint](#).

**Inserimenti di un'appliance di replica in un cluster**

Dopo aver completato l'aggiornamento dell'appliance vRealize Automation master, ogni nodo di replica aggiornato viene inserito automaticamente nel nodo master. Qualora sia necessario aggiornare separatamente un nodo di replica, seguire questi passaggi per inserire manualmente il nodo di replica nel cluster.

Accedere alla console di gestione dell'appliance del nodo di replica che non è inserito nel cluster ed eseguire questi passaggi.

**Procedura**

- 1 Selezionare **Impostazioni vRA > Cluster**.
- 2 Fare clic su **Unisci cluster**.

**Configurazione della porta per distribuzioni ad alta disponibilità**

Dopo aver completato un aggiornamento in una distribuzione ad alta disponibilità, è necessario configurare il bilanciamento del carico per consentire il passaggio del traffico dalla porta 8444 verso l'appliance vRealize Automation per il supporto delle funzionalità della console remota.

Per ulteriori informazioni, consultare *Guida alla configurazione del bilanciamento del carico di vRealize Automation* nella [Documentazione di vRealize Automation](#).

**Riconfigurazione del vRealize Orchestrator incorporato per il supporto dell'alta disponibilità**

Per una distribuzione ad alta disponibilità, è necessario ricongiungere manualmente ogni appliance vRealize Automation di replica target al cluster per abilitare il supporto dell'alta disponibilità per il componente vRealize Orchestrator incorporato.

**Prerequisiti**

Accedere alla console di gestione dell'appliance vRealize Automation di replica target.

- 1 Avviare un browser e aprire la console di gestione dell'appliance vRealize Automation di replica target utilizzando il nome di dominio completo (FQDN) dell'appliance virtuale di replica target: `https://vra-va-hostname.domain.name:5480`.
- 2 Accedere con il nome utente **root** e la password impostata quando è stata effettuata la distribuzione dell'appliance vRealize Automation di replica target.

**Procedura**

- 1 Selezionare **Impostazioni vRA > Cluster**.
- 2 Nella casella di testo **Nodo di cluster iniziale**, immettere il nome di dominio completo dell'appliance vRealize Automation master target.
- 3 Immettere la password root nella casella di testo **Password**.

#### 4 Fare clic su **Unisci cluster**.

Continuare indipendentemente dall'eventuale visualizzazione di avvisi sui certificati. Il sistema riavvia i servizi per il cluster.

#### 5 Verificare che i servizi siano in esecuzione.

- a Nella barra delle schede in alto fare clic su **Servizi**.
- b Fare clic su **Aggiorna** per monitorare lo stato di avanzamento dell'avvio dei servizi.

### Ripristino dei file di timeout del workflow esterno

È necessario riconfigurare i file di timeout del workflow esterno di vRealize Automation perché il processo di aggiornamento sovrascrive i file xmldb.

#### Procedura

- 1 Aprire i file di configurazione (xmldb) workflow esterni sul sistema dalla directory seguente.  
`\VMware\VCAC\Server\ExternalWorkflows\xmldb\.`
- 2 Sostituire i file xmldb con i file di cui è stato eseguito il backup prima della migrazione. Se non si dispone dei file di backup, riconfigurare le impostazioni di timeout del workflow esterno.
- 3 Salvare le impostazioni.

### Abilitazione dell'azione Connetti a console remota per i clienti

L'azione della console remota per i clienti è supportata per le appliance il cui provisioning viene eseguito da vSphere in vRealize Automation.

Modificare il blueprint dopo aver aggiornato la versione e selezionare l'azione **Connetti a console remota** nella scheda **Azione**.

Per ulteriori informazioni, consultare l'[articolo 2109706 della Knowledge Base](#).

### Ripristino delle modifiche di registrazione nel file app.config

Il processo di aggiornamento sovrascrive le modifiche apportate durante la registrazione nei file di configurazione. Al termine dell'aggiornamento, è necessario ripristinare le eventuali modifiche apportate al file `app.config` prima dell'aggiornamento.

### Abilitazione del failover automatico del servizio di gestione dopo l'aggiornamento

Per impostazione predefinita, il failover automatico del servizio di gestione è disabilitato quando si esegue l'aggiornamento di vRealize Automation.

Per abilitare il servizio di gestione automatico dopo l'aggiornamento, completare la procedura che segue.

#### Procedura

- 1 Aprire un prompt dei comandi come root nell'appliance vRealize Automation.
- 2 Modificare le directory in `/usr/lib/vcac/tools/vami/commands`.

- 3 Per abilitare il failover automatico del servizio di gestione, eseguire il comando che segue.

```
python ./manager-service-automatic-failover ENABLE
```

Per disabilitare il failover automatico all'interno di una distribuzione IaaS, eseguire il comando che segue.

```
python ./manager-service-automatic-failover DISABLE
```

### Informazioni sul failover automatico del servizio di gestione

È possibile configurare il servizio di gestione IaaS di vRealize Automation per il failover automatico in un backup in caso di arresto del servizio di gestione primario.

A partire da vRealize Automation 7.3, non è più necessario avviare o arrestare manualmente il servizio di gestione su ciascun server Windows per scegliere quale utilizzare come servizio primario o di backup. Il failover automatico del servizio di gestione è disattivato per impostazione predefinita quando si aggiorna IaaS utilizzando lo script della shell di aggiornamento o il file eseguibile del programma di installazione di IaaS.

Quando è attivato il failover automatico, il servizio di gestione viene avviato automaticamente in tutti gli host del servizio di gestione, inclusi i backup. La funzionalità di failover automatico consente agli host di monitorarsi a vicenda in modo trasparente e di eseguire il failover quando necessario, ma è necessario che il servizio Windows sia in esecuzione in tutti gli host.

---

**Nota** Non è richiesto l'uso del failover automatico. È infatti possibile disattivarlo e continuare ad avviare e arrestare manualmente il servizio Windows per scegliere quale host utilizzare come primario o di backup. Se si segue l'approccio del failover manuale, è necessario avviare il servizio su un solo host alla volta. Con la disattivazione del failover automatico, l'esecuzione simultanea del servizio in più server IaaS non consente di utilizzare vRealize Automation.

---

Evitare di attivare o disattivare il failover in modo selettivo. È necessario che il failover automatico venga sempre sincronizzato come attivo o disattivo attraverso ogni host del servizio di gestione in una distribuzione IaaS.

## Risoluzione dei problemi relativi all'aggiornamento di vRealize Automation

Gli argomenti di questa sezione forniscono le soluzioni ai problemi che possono verificarsi durante l'aggiornamento di vRealize Automation dalla versione 7.1, 7.2 o 7.3.x alla versione 7.4.

### Il failover del servizio di gestione automatico non si attiva

Suggerimenti per la risoluzione dei problemi del comando di failover automatico del servizio di gestione.

## Soluzione

- Il comando di failover automatico del servizio di gestione non riesce o viene visualizzato il seguente messaggio per più di due minuti: Attivazione modalità failover automatico del servizio di gestione sul nodo: `IAAS_MANAGER_SERVICE_NODEID`.
  - a Accedere alla console di gestione dell'appliance vRealize Automation all'indirizzo `https://va-hostname.domain.name:5480` utilizzando il nome utente **host** e la password immessa durante la distribuzione dell'appliance.
  - b Selezionare **Impostazioni vRA > Cluster**.
  - c Verificare che il servizio dell'agente di gestione sia in esecuzione su tutti gli host del servizio di gestione.
  - d Verificare che la durata dell'ultima connessione per tutti i nodi del servizio di gestione laaS sia inferiore a 30 secondi.

Se si riscontrano problemi di connettività dell'agente di gestione, risolverli manualmente e riprovare il comando per attivare il failover automatico del servizio di gestione.

- Il comando di failover automatico del servizio di gestione non riesce ad attivare il failover su un nodo del servizio di gestione. Per correggere questo problema in modo sicuro, è possibile rieseguire il comando.
- In alcuni host del servizio di gestione nella distribuzione laaS è attivato il failover e in altri no. È necessario che in tutti gli host del servizio di gestione nella distribuzione laaS sia attivato il failover, altrimenti non funziona. Per correggere questo problema, effettuare una delle operazioni seguenti:
  - Disattivare il failover su tutti i nodi del servizio di gestione e utilizzare invece l'approccio di failover manuale. Eseguire il failover su un solo host alla volta.
  - Se dopo vari tentativi non è ancora possibile attivare la funzionalità in un nodo del servizio di gestione, arrestare il servizio VMware vCloud Automation Center di Windows in questo nodo e impostare il tipo di avvio del nodo su Manuale finché non verrà risolto il problema.
- Utilizzare Python per verificare che il failover sia abilitato in ogni nodo del servizio di gestione.
  - a Accedere all'appliance master vRealize Automation come **root** utilizzando SSH.
  - b Avviare `python /usr/lib/vcac/tools/vami/commands/manager-service-automatic-failover ENABLE`.
  - c Verificare che il sistema restituisca il messaggio seguente: Attivazione modalità failover automatico del servizio di gestione sul nodo: `IAAS_MANAGER_SERVICE_NODEID` fatto.
- Convalidare l'attivazione del failover su ciascun nodo del servizio di gestione ispezionando il file di configurazione del servizio di gestione.
  - a Aprire un prompt dei comandi su un nodo del servizio di gestione.
  - b Passare alla cartella di installazione di vRealize Automation e aprire il file di configurazione del servizio di gestione all'indirizzo `VMware\VCAC\Server\ManagerService.exe.config`.



- c Verificare la presenza dei seguenti elementi nella sezione <appSettings>.
  - <add key="FailoverModeEnabled" value="True" />
  - <add key="FailoverPingIntervalMilliseconds" value="30000" />
  - <add key="FailoverNodeState" value="active" />
  - <add key="FailoverMaxFailedDatabasePingAttempts" value="5" />
  - <add key="FailoverMaxFailedRepositoryPingAttempts" value="5" />
- Verificare che lo stato del servizio VMware vCloud Automation Center di Windows sia Avviato e che il tipo di avvio sia Automatico.
- Utilizzare Python per verificare che il failover sia disabilitato in ogni nodo del servizio di gestione.
  - a Accedere all'appliance master vRealize Automation come **root** utilizzando SSH.
  - b Avviare python /usr/lib/vcac/tools/vami/commands/manager-service-automatic-failover DISABLE.
  - c Verificare che il sistema restituisca il messaggio seguente: Disattivazione modalità failover automatico del servizio di gestione sul nodo: *IAAS\_MANAGER\_SERVICE\_NODEID* fatto.
- Convalidare la disattivazione del failover su ciascun nodo del servizio di gestione ispezionando il file di configurazione del servizio di gestione.
  - a Aprire un prompt dei comandi su un nodo del servizio di gestione.
  - b Passare alla cartella di installazione di vRealize Automation e aprire il file di configurazione del servizio di gestione all'indirizzo VMware\VCAC\Server\ManagerService.exe.config.
  - c Verificare la presenza del seguente elemento nella sezione <appSettings>.
    - <add key="FailoverModeEnabled" value="False" />
- Per creare un nodo del servizio di gestione standby a freddo, impostare lo stato del servizio VMware vCloud Automation Center di Windows su Interrotto e il tipo di avvio su Manuale.
- Per un nodo del servizio di gestione attivo, è necessario che lo stato del servizio VMware vCloud Automation Center di Windows sia Avviato e che il tipo di avvio sia Automatico.
- Il comando di failover automatico del servizio di gestione utilizza l'ID interno del nodo del servizio di gestione - *IAAS\_MANAGER\_SERVICE\_NODEID*. Per trovare il nome dell'host corrispondente a questo ID interno, eseguire il comando `vra-command list-nodes` e cercare l'host del servizio di gestione con il seguente ID nodo: *IAAS\_MANAGER\_SERVICE\_NODEID*.
- Per individuare il servizio di gestione che il sistema ha scelto in modo automatico come attualmente attivo, eseguire i passaggi seguenti.
  - a Accedere all'appliance master vRealize Automation come **root** utilizzando SSH.
  - b Avviare `vra-command list-nodes --components`.
    - Se il failover è attivato, trovare il nodo del servizio di gestione con Stato: Attivo.

- Se il failover è disattivato, trovare il nodo del servizio di gestione con Stato: Avviato.

### **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.
- 2 Eseguire nuovamente l'installazione o l'aggiornamento.

### **Aggiornamento non riuscito per il componente sito Web di IaaS**

L'aggiornamento di IaaS non riesce ed è impossibile continuare l'operazione.

#### **Problema**

L'aggiornamento di IaaS non riesce per il componente sito Web. Il file di registro del programma di installazione include i seguenti messaggi di errore.

- System.Data.Services.Client.DataServiceQueryException:  
An error occurred while processing this request. --->  
System.Data.Services.Client.DataServiceClientException: <!DOCTYPE html>
- <b> Description: </b>An application error  
occurred on the server. The current custom error settings for this application  
prevent the details of the application error from being viewed remotely (for  
security reasons). It could, however, be viewed by browsers running on the  
local server machine.
- Warning: Non-zero return code. Command failed.
- Done Building Project "C:\Program Files  
(x86)\VMware\VCAC\Server\Model Manager Data\DeployRepository.xml"  
(InstallRepoModel target(s)) -- FAILED.

Il file di registro del repository include i seguenti messaggi di errore.

- [Error]: [sub-thread-Id="20"  
context="" token=""] Failed to start repository service. Reason:  
System.InvalidOperationException: Configuration section encryptionKey is not  
protected  
at  
DynamicOps.Common.Utils.EncryptionHelpers.ReadKeyFromConfiguration(Configuration  
config)  
at DynamicOps.Common.Utils.EncryptionHelpers.Decrypt(String value)  
at DynamicOps.Repository.Runtime.CoreModel.GlobalPropertyItem.Decrypt(Func`2  
decryptFunc)  
at  
DynamicOps.Common.Entity.ContextHelpers.OnObjectMaterializedCallbackEncryptable(Object  
sender, ObjectMaterializedEventArgs e)  
at  
System.Data.Common.Internal.Materialization.Shaper.RaiseMaterializedEvents()  
at  
System.Data.Common.Internal.Materialization.Shaper`1.SimpleEnumerator.MoveNext()  
at System.Linq.Enumerable.FirstOrDefault[TSource](IEnumerable`1 source)  
at System.Linq.Queryable.FirstOrDefault[TSource](IQueryable`1 source)  
at  
DynamicOps.Repository.Runtime.Common.GlobalPropertyHelper.GetGlobalPropertyItemValue(Core  
ModelEntities  
coreModelContext, String propertyName, Boolean throwIfPropertyNotFound)  
at  
DynamicOps.Repository.Runtime.CafeClientAbstractFactory.LoadSolutionUserCertificate()  
at  
DynamicOps.Repository.Runtime.CafeClientAbstractFactory.InitializeFromDb(String  
coreModelConnectionString)  
at DynamicOps.Repository.Runtime.Common.RepositoryRuntime.Initialize().

## Causa

L'aggiornamento di IaaS non riesce quando la data di creazione del file `web.config` coincide o è successiva alla data di modifica.

## Soluzione

- 1 Nell'host IaaS, accedere a Windows.
- 2 Aprire il prompt dei comandi di Windows.
- 3 Passare alla cartella di installazione di vRealize Automation.
- 4 Avviare l'editor di test preferito con l'opzione **Esegui come amministratore**.
- 5 Individuare e selezionare il file `web.config` e salvarlo per modificare la data dell'ultima modifica.
- 6 Esaminare le proprietà del file `web.config` per verificare che la data di modifica del file sia successiva alla data di creazione.
- 7 Aggiornare IaaS.

## Errore di esecuzione del servizio di gestione a causa di errori di convalida SSL durante il runtime

Si verificano errori nel servizio di gestione a causa di errori di convalida SSL.

## Problema

Nel file registro del servizio di gestione viene visualizzato il messaggio di errore seguente:

```
[Info]: Thread-Id="6" - context="" token="" Connessione non riuscita al database core. Verrà effettuato un nuovo tentativo in 00:00:05. Dettagli dell'errore: è stata correttamente stabilita una connessione con il server, ma si è verificato successivamente un errore durante il processo di accesso. (provider: Provider SSL, errore: 0 - La catena di certificati è stata rilasciata da un'autorità non attendibile.)
```

## Causa

Durante il runtime, si verificano errori nel servizio di gestione a causa di errori di convalida SSL.

## Soluzione

- 1 Aprire il file di configurazione `ManagerService.config`.
- 2 Aggiornare **Encrypt=False** nella riga seguente:
 

```
<add name="vcac-repository" providerName="System.Data.SqlClient"
      connectionString="Data Source=iaas-db.sqa.local;Initial Catalog=vcac;Integrated
      Security=True;Pooling=True;Max Pool
      Size=200;MultipleActiveResultSets=True;Connect Timeout=200, Encrypt=True" />
```

## L'accesso non riesce dopo l'aggiornamento

È necessario chiudere il browser e accedere nuovamente dopo un aggiornamento per sessioni che utilizzano account utente sincronizzati.

### Problema

Dopo aver eseguito l'aggiornamento di vRealize Automation, il sistema nega l'accesso agli account utente non sincronizzati quando eseguono l'accesso.

### Soluzione

Chiudere il browser ed eseguire nuovamente vRealize Automation.

### Eliminazione di nodi orfani in vRealize Automation

Un nodo orfano è un nodo duplicato che viene segnalato nell'host ma non esiste nell'host.

### Problema

Quando si verifica se tutti i nodi IaaS e dell'appliance virtuale sono integri, è possibile scoprire che un host ha uno o più nodi orfani. Tutti i nodi orfani devono essere eliminati.

### Soluzione

- 1 Nell'appliance vRealize Automation primaria, accedere alla gestione dell'appliance di vRealize Automation come **root** utilizzando la password immessa durante la distribuzione dell'appliance vRealize Automation.
- 2 Selezionare **Impostazioni vRA > Cluster**.
- 3 Per ogni nodo orfano nella tabella, fare clic su **Elimina**.

### Il comando Unisci cluster sembra non avere esito positivo dopo aver aggiornato un ambiente ad alta disponibilità

Dopo aver fatto clic su **Unisci cluster** nella console di gestione di un nodo di cluster secondario, scompare l'indicatore di avanzamento.

### Problema

Quando si utilizza la console di gestione dell'appliance vRealize Automation dopo l'aggiornamento per unire un nodo di cluster secondario al nodo primario, l'indicatore di avanzamento scompare e non viene visualizzato alcun messaggio di errore o di corretta esecuzione. Questo problema si verifica in modo intermittente.

### Causa

L'indicatore di avanzamento scompare perché alcuni browser smettono di attendere una risposta dal server. Questo funzionamento non arresta il processo di unione dei cluster. È possibile confermare che il processo di unione dei cluster ha avuto esito positivo visualizzando il file di registro in `/var/log/vmware/vcac/vcac-config.log`.

### L'unione di aggiornamento del database PostgreSQL non viene eseguita

L'unione del database PostgreSQL esterno con il database PostgreSQL incorporato non viene eseguita.

**Problema**

Se l'unione di aggiornamento del database PostgreSQL non ha esito positivo, è possibile eseguire un'unione manuale.

**Soluzione**

- 1 Ripristinare l'appliance virtuale vRealize Automation allo snapshot effettuato prima dell'aggiornamento.
- 2 Accedere all'appliance virtuale vRealize Automation ed eseguire questo comando per consentire il completamento dell'aggiornamento se l'unione del database non ha esito positivo.

```
touch /tmp/allow-external-db
```

Il comando non disattiva l'unione automatica.

- 3 Nell'host di database PostgreSQL remoto, connettersi al database PostgreSQL utilizzando lo strumento psql ed eseguire questi comandi.

```
CREATE EXTENSION IF NOT EXISTS "hstore";
```

```
CREATE EXTENSION IF NOT EXISTS "uuid-ossf";
```

```
CREATE SCHEMA saas AUTHORIZATION vcac;
```

L'utente di questo comando è vcac. Se vRealize Automation si connette al database esterno con un utente diverso, sostituire vcac in questo comando con il nome di tale utente.

```
CREATE EXTENSION IF NOT EXISTS "citext" SCHEMA saas;
```

- 4 Eseguire l'aggiornamento.

Se l'aggiornamento avviene correttamente, il sistema funziona come previsto con il database PostgreSQL esterno. Assicurarsi che il database PostgreSQL esterno venga eseguito correttamente.

- 5 Accedere all'appliance virtuale vRealize Automation ed eseguire questi comandi

```
/etc/bootstrap/postupdate.d/00-20-db-merge-external
```

```
/etc/bootstrap/postupdate.d/11-db-merge-external
```

**L'aggiornamento dell'appliance vRealize Automation di replica non viene eseguito correttamente**

L'aggiornamento dell'appliance vRealize Automation di replica non riesce durante l'aggiornamento dell'appliance master.

## Causa

L'aggiornamento di un'appliance di replica potrebbe non riuscire a causa di problemi di connettività o per altri guasti. Quando ciò si verifica, nella scheda **Aggiorna** dell'appliance vRealize Automation master viene visualizzato un messaggio di avviso in cui viene indicata la replica che non è stata aggiornata correttamente.

## Soluzione

- 1 Ripristinare il backup o lo snapshot dell'appliance virtuale di replica allo stato pre-aggiornamento e avviarla.
- 2 Accedere come utente root all'interfaccia di gestione dell'appliance vRealize Automation di replica.  
`https://vrealize-automation-appliance-FQDN:5480`
- 3 Fare clic su **Aggiorna > Impostazioni**.
- 4 Nella sezione relativa all'aggiornamento del repository, scegliere se scaricare gli aggiornamenti da un repository VMware o da un CD-ROM.
- 5 Fare clic su **Stato**.
- 6 Fare clic su **Controlla aggiornamenti** per verificare l'accessibilità di un aggiornamento.
- 7 Fare clic su **Installa aggiornamenti**.
- 8 Fare clic su **OK**.

Viene visualizzato un messaggio che segnala l'aggiornamento in corso.

- 9 Aprire i file di registro per verificare che l'aggiornamento procede correttamente.

- `/opt/vmware/var/log/vami/vami.log`
- `/var/log/vmware/horizon/horizon.log`

Se ci si disconnette durante il processo di aggiornamento e si accede di nuovo prima che l'aggiornamento sia concluso, è possibile continuare a seguire l'avanzamento dell'aggiornamento nel file registro. Il file `updatecli.log` potrebbe visualizzare informazioni sulla versione di vRealize Automation dalla quale si sta eseguendo l'aggiornamento. La versione visualizzata passa alla versione corretta più avanti nel corso dell'aggiornamento.

Il tempo necessario per completare l'aggiornamento varia a seconda dell'ambiente.

- 10 Al termine dell'aggiornamento, riavviare l'appliance virtuale.
  - a Fare clic su **Sistema**.
  - b Fare clic su **Riavvia** e confermare la selezione.
- 11 Selezionare **Impostazioni vRA > Cluster**.
- 12 Inserire il nome di dominio completo dell'appliance vRealize Automation master e fare clic su **Unisci cluster**.

## Le copie di backup dei file .xml causano il timeout del sistema

vRealize Automation registra qualsiasi file con un'estensione .xml nella directory \VMware\vmCAC\Server\ExternalWorkflows\xml\\*. Se questa directory contiene file di backup con un'estensione .xml, il sistema esegue workflow duplicati che causano il timeout del sistema.

### Soluzione

Soluzione: quando si esegue il backup dei file in questa directory, spostare i backup in un'altra directory oppure modificare l'estensione del file di backup in un'estensione diversa da .xml.

## Esclusione dell'aggiornamento di IaaS

È possibile aggiornare l'appliance vRealize Automation senza aggiornare i componenti IaaS.

Utilizzare questa procedura per aggiornare l'appliance vRealize Automation senza aggiornare i componenti IaaS. Questa procedura

- Non arresta i servizi di IaaS.
- Salta l'aggiornamento degli agenti di gestione.
- Impedisce l'aggiornamento automatico dei componenti di IaaS dopo gli aggiornamenti dell'appliance vRealize Automation.

### Procedura

- 1 Aprire una connessione shell protetta al nodo dell'appliance vRealize Automation primaria.
- 2 Al prompt dei comandi, eseguire questo comando per creare il file di commutazione::  
**touch /tmp/disable-iaas-upgrade**
- 3 Arrestare manualmente i servizi IaaS.
  - a Accedere al server Windows di IaaS.
  - b Selezionare **Start > Strumenti di amministrazione > Servizi**.
  - c Arrestare tali servizi rispettando il seguente ordine.

---

**Nota** Non spegnere il server Windows di IaaS.

---

- 1 Tutti gli agenti proxy di VMware vRealize Automation.
  - 2 Tutte le istanze di DEM Worker VMware.
  - 3 L'istanza di DEM Orchestrator VMware.
  - 4 Il servizio VMware vCloud Automation Center.
- 4 Accedere alla console di gestione dell'appliance vRealize Automation primaria e aggiornare l'appliance vRealize Automation primaria.

## Impossibile creare una nuova directory in vRealize Automation

Il tentativo di aggiungere una nuova directory con il primo connettore di sincronizzazione non riesce.



## Problema

Questo problema si verifica a causa di un `config-state.json` file errato ubicato in `usr/local/horizon/conf/states/VSPHERE.LOCAL/3001/`.

Per ulteriori informazioni sulla risoluzione di questo problema, vedere l'[articolo della Knowledge Base 2145438](#).

## Timeout dell'aggiornamento dell'appliance virtuale di replica vRealize Automation

Quando si aggiorna l'appliance virtuale master, si verifica il timeout dell'aggiornamento dell'appliance virtuale di replica vRealize Automation.

## Problema

Quando si aggiorna l'appliance virtuale master, nella scheda di aggiornamento della console di gestione vRealize Automation master è evidenziata un'appliance virtuale di replica che ha raggiunto il limite del timeout per l'aggiornamento.

## Causa

Il timeout dell'aggiornamento si verifica a causa di un problema relativo alle prestazioni o all'infrastruttura.

## Soluzione

- 1 Verificare lo stato di avanzamento dell'aggiornamento dell'appliance virtuale di replica.
  - a Aprire la console di gestione dell'appliance virtuale di replica utilizzando il rispettivo nome di dominio completo, `https://va-hostname.domain.name:5480`.
  - b Accedere utilizzando il nome utente **root** e la password immessi al momento della distribuzione dell'appliance.
  - c Selezionare **Aggiorna > Stato** e verificare lo stato di avanzamento dell'aggiornamento.  
Eeguire una delle seguenti azioni:
    - Se l'aggiornamento non riesce, eseguire i passaggi descritti nell'argomento relativo alla risoluzione dei problemi [L'aggiornamento dell'appliance vRealize Automation di replica non viene eseguito correttamente](#).
    - Se l'aggiornamento dell'appliance virtuale di replica è in corso, attendere fino al completamento e andare al passaggio 2.
- 2 Riavviare l'appliance virtuale.
  - a Fare clic su **Sistema**.
  - b Fare clic su **Riavvia** e confermare la selezione.
- 3 Selezionare **Impostazioni vRA > Cluster**.
- 4 Inserire il nome di dominio completo dell'appliance virtuale vRealize Automation master e fare clic su **Unisci cluster**.

## Per alcune macchine virtuali non viene creata una distribuzione durante l'aggiornamento

Per le macchine virtuali il cui stato al momento dell'aggiornamento risulta mancante non viene creata una distribuzione corrispondente nell'ambiente target.

### Problema

Se durante l'aggiornamento lo stato di una macchina virtuale risulta mancante nell'ambiente di origine, nell'ambiente target non viene creata una distribuzione corrispondente. Se dopo l'aggiornamento lo stato di una macchina virtuale non risulta più mancante, è possibile importare la macchina nella distribuzione target utilizzando l'importazione di massa.

### Errore di certificato non attendibile

Quando viene visualizzata la pagina Visualizzatore registro dell'infrastruttura nella console Appliance vRealize Automation, è possibile che venga visualizzato un report di errore di connessione dell'endpoint contenente la frase seguente: `Certificate is not trusted`.

### Problema

Nella console Appliance vRealize Automation, selezionare **Infrastruttura > Monitoraggio > Registro**. Nella pagina Visualizzatore registro, è possibile che venga visualizzato un report simile al seguente:

Connessione all'endpoint non riuscita. Per convalidare la possibilità di stabilire una connessione protetta a questo endpoint, andare all'endpoint vSphere nella pagina Endpoint e fare clic sul pulsante Prova connessione.

Inner Exception: Certificate is not trusted (RemoteCertificateChainErrors). Subject: C=US, CN=vc6.mycompany.com Thumbprint: DC5A8816231698F4C9013C42692B0AF93D7E35F1

### Causa

L'aggiornamento da vRealize Automation 7.3 o versioni precedenti alla versione 7.4 comporta modifiche degli endpoint dell'ambiente originale. Per gli ambienti aggiornati di recente a vRealize Automation 7.4, l'amministratore IaaS deve controllare tutti gli endpoint esistenti che utilizzano una connessione https protetta. Se in un endpoint si presenta l'errore `Certificate is not trusted`, significa che l'endpoint non funziona correttamente.

### Soluzione

- 1 Accedere alla console vRealize Automation come amministratore di infrastruttura.
- 2 Selezionare **Infrastruttura > Endpoint > Endpoint**.
- 3 Completare questi passaggi per ciascun endpoint con connessione sicura.
  - a Fare clic su **Modifica**.
  - b Fare clic su **Prova connessione**.
  - c Controllare i dettagli del certificato e fare clic su **OK** se si considera attendibile il certificato.
  - d Riavviare i servizi Windows per tutti gli agenti proxy IaaS utilizzati da questo endpoint.

- 4 Verificare che non vengano più visualizzati errori Certificate is not trusted nella pagina Visualizzatore registro dell'infrastruttura.

### L'installazione o l'aggiornamento a vRealize Automation non riesce

L'installazione o l'aggiornamento di vRealize Automation non riesce e nel file di registro viene visualizzato un messaggio di errore.

#### Problema

Quando si esegue l'installazione o l'aggiornamento di vRealize Automation, la procedura non riesce. Ciò avviene in genere quando una correzione applicata durante l'installazione o l'aggiornamento non va a buon fine. Nel file di registro viene visualizzato un messaggio di errore simile al seguente: Security error. Applying automatic fix for FIREWALL prerequisite failed. RPM Status 1: Pre install script failed, package test and installation skipped.

#### Causa

L'ambiente Windows dispone di criteri di gruppo abilitati per l'esecuzione dello script PowerShell.

#### Soluzione

- 1 Nella macchina host di Windows, eseguire `gpedit.msc` per aprire l'Editor Criteri di gruppo locali.
- 2 Nel riquadro a sinistra sotto **Configurazione computer**, fare clic sul pulsante Espandi per aprire **Modelli amministrativi > Componenti di Windows > Windows PowerShell**.
- 3 In **Attiva l'esecuzione di script**, modificare lo stato da Enabled a Not Configured.

### Impossibile aggiornare i componenti DEO e DEM

Durante l'aggiornamento di vRealize Automation 7.2 alla versione 7.3.x, non è possibile aggiornare i componenti DEO e DEM

#### Problema

Dopo l'aggiornamento di vRealize Automation 7.2 alla versione 7.3.x, i componenti DEM e DEO installati in un percorso personalizzato, ad esempio l'unità D:, non vengono aggiornati.

Vedere l'[articolo 2150517 della Knowledge Base](#).

### L'aggiornamento dell'agente di gestione non riesce

Quando si fa clic su **Installa aggiornamenti** nella pagina dello stato dell'aggiornamento della console di gestione di Appliance vRealize Automation, viene visualizzato un messaggio di errore relativo all'agente di gestione.

#### Problema

Il processo di aggiornamento non va a buon fine. Viene visualizzato il messaggio che informa che è impossibile aggiornare l'agente di gestione nel nodo x. In alcuni casi, il messaggio riporta più nodi.

## Causa

Questo problema può essere causato da diverse condizioni. Il messaggio di errore identifica solo l'ID del nodo della macchina interessata. Ulteriori informazioni sono disponibili nel file `All.log` per l'agente di gestione nella macchina in cui si è verificato l'errore di comando.

Eseguire queste attività sui nodi interessati in base alle proprie circostanze:

## Soluzione

- Se il servizio dell'agente di gestione non è in esecuzione, avviare il servizio e riavviare l'aggiornamento sull'appliance virtuale.
- Se il servizio dell'agente di gestione è in esecuzione e l'agente di gestione viene aggiornato, riavviare l'aggiornamento sull'appliance virtuale.
- Se il servizio dell'agente di gestione è in esecuzione ma l'agente di gestione non viene aggiornato, eseguire un aggiornamento manuale.
  - a Aprire un browser e passare alla pagina d'installazione dell'laaS di vRealize Automation sull'appliance vRealize Automation all'indirizzo `https:// va-hostname.domain.name: 5480/install`.
  - b Scaricare ed eseguire il programma di installazione dell'agente di gestione.
  - c Riavviare la macchina dell'agente di gestione.
  - d Riavviare l'aggiornamento sull'appliance virtuale.

## Aggiornamento dell'agente di gestione non riuscito

L'aggiornamento dell'agente di gestione ha esito negativo se viene eseguito da vRealize Automation alla versione 7.2. - 7.3.x.

## Problema

Se un incidente di failover ha scambiato l'host primario con l'host secondario dell'agente di gestione, l'aggiornamento non riesce perché il processo di aggiornamento automatico non trova l'host previsto. Eseguire questa procedura in ciascun nodo laaS in cui l'agente di gestione non è aggiornato.

## Soluzione

- 1 Aprire il file `All.log` nella cartella dei file di registro dell'agente di gestione, disponibile all'indirizzo `C:\Programmi (x86)\VMware\VCAC\Management Agent\Logs\`.

Il percorso della cartella di installazione potrebbe essere diverso da quello predefinito.

- 2 Cercare nel file di registro un messaggio relativo a un'appliance virtuale obsoleta o spenta.

Ad esempio, `INNER EXCEPTION: System.Net.WebException: Impossibile effettuare la connessione al server remoto ---> System.Net.Sockets.SocketException: Impossibile stabilire la connessione. Risposta non corretta della parte connessa dopo l'intervallo di tempo oppure mancata risposta dall'host collegato IP_Address:5480`

- 3 Modificare il file di configurazione dell'agente di gestione all'indirizzo C:\Programmi Files (x86)\VMware\VCAC\Management Agent\VMware.IaaS.Management.Agent.exe.config per sostituire il valore `alternativeEndpointaddress` esistente con l'URL dell'endpoint primario dell'appliance virtuale.

Il percorso della cartella di installazione potrebbe essere diverso da quello predefinito.

Esempio di `alternativeEndpointaddress` in `VMware.IaaS.Management.Agent.exe.config`.

```
<alternativeEndpoint address="https://FQDN:5480/" thumbprint="numero
thumbprint" />
```

- 4 Riavviare il servizio Agente di gestione di Windows e controllare il file `All.log` per verificare che funzioni.
- 5 Eseguire la procedura di aggiornamento nell'appliance vRealize Automation primaria.

### L'aggiornamento di vRealize Automation ha esito negativo a causa delle impostazioni di timeout predefinite

È possibile aumentare l'impostazione del tempo per l'aggiornamento se l'impostazione predefinita per la sincronizzazione dei database è troppo breve per il proprio ambiente.

#### Problema

L'impostazione del timeout per il comando `Vcac-Config SynchronizeDatabases` non è sufficiente per alcuni ambienti in cui la sincronizzazione dei database richiede più tempo rispetto al valore predefinito di 3600 secondi.

I valori delle proprietà `cafeTimeoutInSeconds` e `cafeRequestPageSize` nel file `Vcac-Config.exe.config` regolano la comunicazione tra l'API e lo strumento di utilità `Vcac-config.exe`. Il file si trova in `IaaS installation location\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe.config`.

È possibile sovrascrivere il valore di timeout predefinito solo per il comando `SynchronizeDatabases` specificando un valore per questi parametri facoltativi.

Parametro	Nome breve	Descrizione
<code>--DatabaseSyncTimeout</code>	<code>-dstm</code>	Imposta il valore di timeout della richiesta http solo per <code>SynchronizeDatabases</code> in secondi.
<code>--DatabaseSyncPageSize</code>	<code>-dsps</code>	Imposta le dimensioni della pagina di richiesta solo per la sincronizzazione di Prenotazione o Criterio di prenotazione. Il valore predefinito è 10.

Se questi parametri non sono impostati nel file `Vcac-Config.exe.config`, il sistema utilizza il valore di timeout predefinito.

## L'aggiornamento di IaaS in un ambiente ad alta disponibilità non riesce

Il processo di aggiornamento di IaaS nel nodo del server Web primario con bilanciamento del carico abilitato non riesce. Potrebbero venire visualizzati i seguenti messaggi di errore:

"System.Net.WebException: timeout dell'operazione" o "401 - Autorizzazione negata: accesso negato a causa di credenziali non valide".

### Problema

L'aggiornamento di IaaS con il bilanciamento del carico abilitato può causare un errore intermittente. In questo caso, è necessario eseguire nuovamente l'aggiornamento di vRealize Automation con il bilanciamento del carico disabilitato.

### Soluzione

- 1 Ripristinare gli snapshot dell'ambiente precedenti all'aggiornamento.
- 2 Aprire una connessione desktop remoto al nodo del server Web IaaS primario.
- 3 Passare al file degli host di Windows in c:\windows\system32\drivers\etc.
- 4 Aprire il file degli host e aggiungere la seguente riga per disabilitare il bilanciamento del carico del server Web.

*IP\_address\_of\_primary\_iaas\_website\_node vrealizeautomation\_iaas\_website\_lb\_fqdn*

Esempio:

10.10.10.5 vra-iaas-web-lb.domain.com

- 5 Salvare il file degli host e riprovare a eseguire l'aggiornamento di vRealize Automation.
- 6 Al termine dell'aggiornamento di vRealize Automation, aprire il file degli host e rimuovere la riga aggiunta al passaggio 4.

## Risoluzione dei problemi di aggiornamento

È possibile modificare il processo di aggiornamento per risolvere problemi di aggiornamento.

### Soluzione

Quando si verificano problemi durante l'aggiornamento dell'ambiente di vRealize Automation, utilizzare questa procedura per modificare il processo di aggiornamento selezionando uno dei flag disponibili.

#### Procedura

- 1 Aprire una connessione shell protetta al nodo dell'appliance vRealize Automation primaria.

- 2 Al prompt dei comandi, eseguire questo comando per creare il file di commutazione::

**touch *available\_flag***

Ad esempio: **touch /tmp/disable-iaas-upgrade**

**Tabella 1-60. Flag disponibili**

Flag	Descrizione
/tmp/disable-iaas-upgrade	<ul style="list-style-type: none"> <li>■ Impedisce il processo di aggiornamento di IaaS dopo il riavvio dell'appliance virtuale.</li> <li>■ Impedisce l'aggiornamento dell'agente di gestione.</li> <li>■ Impedisce il controllo automatico dei prerequisiti e le correzioni.</li> <li>■ Impedisce l'arresto dei servizi di IaaS.</li> </ul>
/tmp/do-not-upgrade-ma	Impedisce l'aggiornamento dell'agente di gestione. Questo flag è utile quando l'agente di gestione viene aggiornato manualmente.
/tmp/skip-prereq-checks	Impedisce il controllo automatico dei prerequisiti e le correzioni. Questo flag è utile quando si verifica un problema con le correzioni automatiche dei prerequisiti e le correzioni vengono applicate manualmente.
/tmp/do-not-stop-services	Impedisce l'arresto dei servizi di IaaS. L'aggiornamento non arresta i servizi Windows di IaaS, ad esempio il servizio di gestione, DEM e gli agenti.
/tmp/do-not-upgrade-servers	<p>Impedisce l'aggiornamento automatico di tutti i componenti IaaS server, ad esempio il database, il sito Web, WAPI, il repository, i dati di Model Mfrontanager e il servizio di gestione.</p> <p><b>Nota</b> Questo flag impedisce inoltre l'abilitazione della modalità di failover automatica del servizio di gestione.</p>
/tmp/do-not-upgrade-dems	Impedisce l'aggiornamento di DEM.
/tmp/do-not-upgrade-agents	Impedisce l'aggiornamento dell'agente proxy di IaaS.

## 3 Completare le attività per il flag scelto.

Tabella 1-61. Attività aggiuntive

Flag	Attività
/tmp/disable-iaas-upgrade	<ul style="list-style-type: none"> <li>■ Aggiornare manualmente l'agente di gestione.</li> <li>■ Applicare manualmente tutti i prerequisiti di IaaS necessari.</li> <li>■ Arrestare manualmente i servizi IaaS.               <ol style="list-style-type: none"> <li>a Accedere al server Windows di IaaS.</li> <li>b Selezionare <b>Start &gt; Strumenti di amministrazione &gt; Servizi</b>.</li> <li>c Arrestare tali servizi rispettando il seguente ordine.</li> </ol> <p><b>Nota</b> Non spegnere il server Windows di IaaS.</p> <ol style="list-style-type: none"> <li>a Tutti gli agenti proxy di VMware vRealize Automation.</li> <li>b Tutte le istanze di DEM Worker VMware.</li> <li>c L'istanza di DEM Orchestrator VMware.</li> <li>d Il servizio VMware vCloud Automation Center.</li> </ol> </li> <li>■ Avviare manualmente l'aggiornamento di IaaS al termine dell'aggiornamento dell'appliance virtuale.</li> </ul>
/tmp/do-not-upgrade-ma	Aggiornare manualmente l'agente di gestione.
/tmp/skip-prereq-checks	Applicare manualmente tutti i prerequisiti di IaaS necessari.
/tmp/do-not-stop-services	<p>Arrestare manualmente i servizi IaaS.</p> <ol style="list-style-type: none"> <li>1 Accedere al server Windows di IaaS.</li> <li>2 Selezionare <b>Start &gt; Strumenti di amministrazione &gt; Servizi</b>.</li> <li>3 Arrestare tali servizi rispettando il seguente ordine.</li> </ol> <p><b>Nota</b> Non spegnere il server Windows di IaaS.</p> <ol style="list-style-type: none"> <li>a Tutti gli agenti proxy di VMware vRealize Automation.</li> <li>b Tutte le istanze di DEM Worker VMware.</li> <li>c L'istanza di DEM Orchestrator VMware.</li> <li>d Il servizio VMware vCloud Automation Center.</li> </ol>
/tmp/do-not-upgrade-servers	
/tmp/do-not-upgrade-dems	
/tmp/do-not-upgrade-agents	



- 4 Accedere alla console di gestione dell'appliance vRealize Automation primaria e aggiornare l'appliance vRealize Automation primaria.

---

**Nota** Poiché ogni flag resta attivo finché non viene rimosso, eseguire questo comando per rimuovere il flag scelto dopo l'aggiornamento: `rm /flag_path/flag_name`. Ad esempio `rm /tmp/disable-iaas-upgrade`.

---

## Aggiornamento di vRealize Automation 6.2.5 alla versione 7.4

Quando si esegue l'aggiornamento dell'ambiente vRealize Automation 6.2.5 all'ultima versione, si utilizzano le procedure di aggiornamento specifiche per l'ambiente 6.2.5.

Queste informazioni si riferiscono specificamente all'aggiornamento di vRealize Automation 6.2.5 alla versione 7.4. Per informazioni su altri percorsi di aggiornamento supportati, vedere [Aggiornamento di vRealize Automation](#).

### Aggiornamento di vRealize Automation 6.2.5 alla versione 7.4

È possibile eseguire un aggiornamento sul posto dell'ambiente vRealize Automation 6.2.5 corrente alla versione 7.4. Per aggiornare l'ambiente, è necessario eseguire le procedure di aggiornamento specifiche per questa versione.

Un aggiornamento sul posto è un processo in tre passaggi. Aggiornare i componenti dell'ambiente corrente nel seguente ordine.

- 1 Appliance vRealize Automation
- 2 Server Web IaaS
- 3 vRealize Orchestrator

È necessario aggiornare tutti i componenti del prodotto alla stessa versione.

Lo strumento di assistenza all'aggiornamento di vRealize per i test in ambiente di produzione analizza l'ambiente di vRealize Automation 6.2.x per rilevare eventuali configurazioni di funzionalità che possono provocare problemi di aggiornamento e verifica che l'ambiente sia pronto per l'aggiornamento. Lo strumento può essere scaricato dalla pagina di download del prodotto di [VMware vRealize Production Test Tool](#).

I controlli del dizionario delle proprietà che non sono supportati dopo l'aggiornamento possono essere ripristinati utilizzando le relazioni tra vRealize Orchestrator e il dizionario delle proprietà.

Se nell'ambiente di origine sono presenti workflow che contengono codice obsoleto, consultare la [guida alla migrazione dell'estensibilità di vRealize Automation](#) per informazioni sulle modifiche al codice necessarie per la conversione in sottoscrizioni del gestore di eventi.

A partire da vRealize Automation 7.2, JFrog Artifactory Pro non è più fornito in dotazione con Appliance vRealize Automation. Se si esegue l'aggiornamento da una versione precedente di vRealize Automation, il processo di aggiornamento rimuove JFrog Artifactory Pro. Per ulteriori informazioni, vedere [Knowledge Base 2147237](#).

---

**Nota** Se l'ambiente vRealize Automation 6.2.5 corrente è stato personalizzato, contattare lo staff dell'assistenza CCE per ulteriori informazioni sull'aggiornamento.

---

## Prerequisiti per l'aggiornamento di vRealize Automation

Prima di eseguire l'aggiornamento da vRealize Automation 6.2.5, esaminare i seguenti prerequisiti.

### Requisiti della configurazione del sistema

Prima di avviare un aggiornamento, verificare che i requisiti di sistema indicati di seguito siano soddisfatti.

- Verificare che tutte le appliance e i server facenti parte della distribuzione soddisfino i requisiti di sistema relativi alla versione più recente. Vedere la *vRealize Automation Matrice di supporto* nella [documentazione di VMware vRealize Automation](#).
- Consultare il documento *VMware Product Interoperability Matrix* sul sito Web di VMware per informazioni sulla compatibilità con altri prodotti VMware.
- Verificare che la versione di vRealize Automation dalla quale si sta effettuando l'aggiornamento sia in condizioni di funzionamento stabili. Correggere eventuali problemi prima di effettuare l'aggiornamento.
- Se si esegue l'aggiornamento da vRealize Automation 6.2.5, registrare la chiave di licenza di vCloud Suite utilizzata per l'ambiente vRealize Automation corrente. In seguito all'aggiornamento, le chiavi di licenza esistenti verranno rimosse dal database.
- Assicurarsi di aver modificato le impostazioni di timeout del bilanciamento del carico dal valore predefinito ad almeno 10 minuti.

### Requisiti di configurazione dell'hardware

Verificare che l'hardware nell'ambiente sia adeguato per vRealize Automation nella versione di destinazione.

Vedere [Specifiche hardware e massima capacità di vRealize Automation](#)

Prima di avviare un aggiornamento, verificare che i requisiti di sistema indicati di seguito siano soddisfatti.

- Prima di scaricare l'aggiornamento è necessario configurare l'hardware esistente. Vedere [Incremento delle risorse hardware di vCenter Server per vRealize Automation 6.2.5](#).
- Per poter eseguire l'aggiornamento sono necessari almeno 18 GB di RAM, 4 CPU, disco1 = 50 GB, disco3 = 25 GB e disco4=50 GB.

Se la macchina virtuale è presente in vCloud Networking and Security, potrebbe essere necessario allocare più spazio RAM.

Benché il supporto generico per vCloud Networking and Security sia terminato, l'utilizzo delle proprietà personalizzate di VCNS in NSX è ancora valido. Vedere l'[articolo 2144733 della Knowledge Base](#).

- Questi nodi devono avere almeno 5 GB di spazio libero su disco:
  - Sito Web IaaS primario
  - Database Microsoft SQL
  - Model Manager
- Il nodo Web IaaS primario in cui sono installati i dati Model Manager dev'essere installato JAVA SE Runtime Environment 8, a 64 bit, aggiornamento 161 o versione successiva. Dopo aver installato Java, è necessario impostare la variabile di ambiente JAVA\_HOME sulla nuova versione.
- Per scaricare ed eseguire l'aggiornamento, è necessario disporre delle risorse seguenti:
  - Almeno 5 GB sulla partizione root
  - 5 GB sulla partizione /storage/db per il master Appliance vRealize Automation
  - 5 GB sulla partizione root per ogni appliance virtuale di replica
- Verificare la sottocartella /storage/log e rimuovere eventuali file ZIP precedenti archiviati per liberare spazio.

## Prerequisiti generali

Prima di avviare un aggiornamento, verificare che i requisiti di sistema indicati di seguito siano soddisfatti.

- Si dispone dell'accesso a un account di Active Directory con formato username@domain e autorizzazioni di binding alla directory.
- Si soddisfano le condizioni seguenti:
  - Si dispone di accesso a un account con il formato SAMaccountName.
  - I privilegi di cui si dispone sono sufficienti per unire il sistema al dominio creando dinamicamente un oggetto computer o per l'unione in un oggetto creato in precedenza.
- Si dispone dell'accesso a tutti i database e a tutti i bilanciamenti del carico interessati o partecipanti all'aggiornamento di vRealize Automation.
- Il sistema viene reso non disponibile per gli utenti durante l'esecuzione dell'aggiornamento.
- Si disabilita ogni applicazione che effettua una query su vRealize Automation.
- Verificare che Microsoft Distributed Transaction Coordinator (MSDTC) sia attivo in tutte le istanze di vRealize Automation e nei server SQL associati. Per le istruzioni, consultare l'[articolo 2089503 della Knowledge Base](#).
- Se l'ambiente include un'appliance vRealize Orchestrator esterna e un'appliance vRealize Orchestrator esterna connessa all'Identity Appliance, eseguire l'aggiornamento di vRealize Orchestrator prima di aggiornare vRealize Automation.

- Prima di eseguire l'aggiornamento, è necessario completare attività aggiuntive per preparare le macchine virtuali vRealize Automation. Prima di eseguire l'aggiornamento, consultare l'[articolo 51531 della Knowledge Base](#).
- Assicurarsi di aver modificato le impostazioni di timeout del bilanciamento del carico dal valore predefinito ad almeno 10 minuti.
- Se si utilizza il plug-in DynamicTypes, è necessario esportare le configurazioni del plug-in DynamicTypes di vRealize Orchestrator come un workflow del pacchetto.  
/Library/Dynamic Types/Configuration/Export Configuration As Package
- Se si esegue l'aggiornamento di un ambiente distribuito configurato con un database PostgreSQL incorporato, completare la procedura che segue.
  - a Prima di aggiornare gli host di replica, esaminare i file nella directory pgdata sull'host master.
  - b Andare alla cartella di dati PostgreSQL sull'host master nel percorso /var/vmware/vpostgres/current/pgdata/.
  - c Chiudere tutti i file aperti nella directory pgdata e rimuovere gli eventuali file con suffisso .swp.
  - d Verificare che tutti i file di questa directory abbiano la proprietà corretta: postgres:users.

### Considerazioni sull'aggiornamento a questa versione di vRealize Automation

vRealize Automation 7 e versione successiva introduce diverse modifiche funzionali durante e dopo il processo di aggiornamento. Prima di aggiornare la distribuzione di vRealize Automation 6.2.5 alla nuova versione, è necessario esaminare le modifiche.

Esaminare queste considerazioni prima dell'aggiornamento.

### Aggiornamento e specifiche di Identity Appliance

Durante il processo di aggiornamento di vRealize Automation, vengono visualizzati alcuni prompt per l'aggiornamento di Identity Appliance.

La distribuzione target utilizza VMware Identity Manager.

### Aggiornamento e licenze

Durante l'aggiornamento vengono rimosse le licenze di vRealize Automation 6.2.5 esistenti e tutte le licenze di vCloud Suite 6.x eventualmente presenti. È necessario immettere di nuovo le licenze nella console di gestione dell'appliance vRealize Automation di vRealize Automation 7.4.

Verrà quindi utilizzata la licenza di vRealize Automation per le appliance virtuali e IaaS immettendo le informazioni sulla chiave di licenza nell'appliance vRealize Automation. Le informazioni sulla licenza non sono più disponibili nell'interfaccia utente di IaaS e IaaS non esegue più i controlli di licenza. Gli endpoint e le quote vengono applicati tramite gli accordi di licenza con l'utente finale.

---

**Nota** Prendere nota della chiave di licenza di vCloud Suite 6.x se la si è utilizzata per vRealize Automation 6.2.5 prima dell'aggiornamento. In seguito all'aggiornamento, le chiavi di licenza esistenti verranno rimosse dal database.

---

Per ulteriori informazioni sul reinserimento delle informazioni sulle licenze durante o dopo l'aggiornamento, vedere [Aggiornamento della chiave di licenza](#).

### Modalità di aggiornamento dei ruoli

Quando si aggiorna vRealize Automation, le assegnazioni dei ruoli esistenti dell'organizzazione vengono mantenute. L'aggiornamento crea anche alcune assegnazioni di ruoli per supportare ruoli di architetto di blueprint aggiuntivi.

Per supportare la definizione del blueprint nella tela di progettazione vengono utilizzati i seguenti ruoli di architetto:

- Architetto dell'applicazione: assembla i componenti e i blueprint esistenti per creare blueprint compositi.
- Architetto dell'infrastruttura. Crea e gestisce i blueprint delle macchine virtuali.
- Architetto XaaS. Crea e gestisce i blueprint di XaaS.
- Architetto del software: crea e gestisce i componenti Software.

In vRealize Automation 7, per impostazione predefinita gli amministratori tenant e i manager dei gruppi di business non possono progettare blueprint. Agli amministratori tenant e ai manager dei gruppi di business aggiornati viene assegnato il ruolo di architetto dell'infrastruttura.

Gli utenti che possono riconfigurare una macchina virtuale nella versione di origine di vRealize Automation 6.2.x possono modificare la proprietà della macchina virtuale dopo l'aggiornamento alla nuova versione.

Durante l'aggiornamento vengono eseguite le seguenti assegnazioni di ruoli. I ruoli non elencati nella tabella vengono aggiornati allo stesso nome di ruolo nella distribuzione di destinazione.

**Tabella 1-62. Ruoli assegnati durante l'aggiornamento**

Ruolo nella distribuzione di origine	Ruolo nella distribuzione di destinazione
Amministratore tenant	Amministratore tenant e architetto dell'infrastruttura
Manager gruppo di business	Manager del gruppo di business e architetto dell'infrastruttura
Service Architect	Architetto XaaS
Architetto dell'applicazione	Architetto del software

Per ulteriori informazioni sui ruoli, vedere [Ruoli e responsabilità del tenant in vRealize Automation](#).

### Modalità di aggiornamento dei blueprint

Come regola, i blueprint pubblicati vengono aggiornati come blueprint pubblicati.

Tuttavia esistono delle eccezioni a tale regola. I blueprint per più macchine sono aggiornati come blueprint compositi contenenti componenti blueprint. I blueprint per più macchine che contengono impostazioni non supportate vengono aggiornati come non pubblicati.

---

**Nota** vRealize Automation 7.x esegue uno snapshot del blueprint in fase di distribuzione. Se si verificano i problemi di riconfigurazione durante l'aggiornamento delle proprietà della macchina quali CPU e memoria RAM in una distribuzione, vedere l'articolo della Knowledge Base [2150829 relativo alla creazione dello snapshot blueprint vRA 7.x](#).

---

Per ulteriori informazioni sull'aggiornamento di un blueprint, vedere [Aggiornamento e blueprint di vApp, endpoint vCloud e prenotazioni vCloud](#) e [Informazioni sulla modalità di aggiornamento dei blueprint di più macchine](#).

### **Aggiornamento e blueprint di vApp, endpoint vCloud e prenotazioni vCloud**

Non è possibile aggiornare una distribuzione che contiene endpoint vApp (vCloud). La presenza di endpoint vApp (vCloud) impedisce l'aggiornamento a questa versione di vRealize Automation.

L'aggiornamento non riesce sull'appliance virtuale master se nella distribuzione di origine è presente un endpoint vApp (vCloud). Nel registro e nell'interfaccia utente viene visualizzato un messaggio. Per stabilire se la distribuzione di origine contiene un endpoint vApp (vCloud), accedere alla console di vRealize Automation come utente amministratore IaaS. Selezionare **Infrastruttura > Endpoint**. Se l'elenco di endpoint contiene endpoint vApp (vCloud), non è possibile eseguire l'aggiornamento a questa versione di vRealize Automation.

Le vApp gestite per le risorse di vCloud Air o vCloud Director non sono supportate nell'ambiente vRealize Automation di destinazione.

---

**Nota** I tipi seguenti di criterio di approvazione sono diventati obsoleti. Se vengono visualizzati nell'elenco dei tipi di criterio di approvazione disponibili al termine dell'aggiornamento, non è possibile utilizzarli.

- Catalogo dei servizi - Richiesta di elemento del catalogo - vApp
  - Catalogo dei servizi - Richiesta di elemento del catalogo - Componente vApp
- 

È possibile creare prenotazioni ed endpoint vCloud Air e vCloud Director nella distribuzione di destinazione. È anche possibile creare blueprint con componenti macchina virtuale vCloud Air o vCloud Director.

### **Informazioni sulla modalità di aggiornamento dei blueprint di più macchine**

È possibile effettuare l'aggiornamento dei blueprint di più macchine di servizi gestiti da una distribuzione vRealize Automation versione 6.2.x supportata.

Quando si effettua l'aggiornamento di un blueprint di più macchine, i blueprint dei componenti vengono aggiornati come blueprint di macchine singole. Il blueprint di più macchine viene aggiornato come blueprint composito in cui i blueprint figlio precedenti sono nidificati come componenti blueprint separati.

L'aggiornamento crea nella distribuzione target un unico blueprint composito che contiene un componente macchina virtuale per ogni blueprint di componente nel blueprint di più macchine di origine. Se un blueprint include un'impostazione non supportata nella nuova versione, viene aggiornato e impostato sullo stato di bozza. Se, ad esempio, il blueprint di più macchine contiene un profilo di rete privata, l'impostazione del profilo di rete privata viene ignorata durante l'aggiornamento e il blueprint viene aggiornato in uno stato di bozza. È possibile modificare il blueprint bozza in modo da immettere informazioni sul profilo di rete supportate e pubblicarlo.

---

**Nota** Se un blueprint pubblicato nella distribuzione di origine viene aggiornato in un blueprint in stato bozza, il blueprint non fa più parte di un servizio o permesso. Dopo aver aggiornato e pubblicato il blueprint nella versione di vRealize Automation aggiornata, è necessario ricreare i rispettivi permessi e criteri di approvazione necessari.

---

Alcune impostazioni dei blueprint di più macchine non sono supportate nella distribuzione vRealize Automation di destinazione, inclusi i profili delle reti private e delle reti instradate con impostazioni edge PLR associate. Se è stata utilizzata una proprietà personalizzata per specificare le impostazioni edge PLR (`VCNS.LoadBalancerEdgePool.Names`), tale proprietà viene aggiornata.

È possibile aggiornare un blueprint di più macchine con endpoint vSphere e impostazioni di rete e sicurezza NSX. Il blueprint aggiornato conterrà componenti rete e sicurezza di NSX nella tela di progettazione.

---

**Nota** Le specifiche dei gateway instradati per i blueprint di più macchine, come definito nelle prenotazioni, vengono aggiornate. Tuttavia, la distribuzione vRealize Automation di destinazione non supporta le prenotazioni per i profili instradati che contengono impostazioni edge PLR associate. Se la prenotazione di origine contiene un valore di gateway instradato per un edge PLR, la prenotazione viene aggiornata ma l'impostazione del gateway instradato viene ignorata. Durante l'aggiornamento viene pertanto generato un messaggio di errore nel file di registro e la prenotazione viene disabilitata.

---

Mentre l'aggiornamento è in corso, spazi e caratteri speciali vengono rimossi dalla rete di riferimento e dai nomi dei componenti di sicurezza.

---

**Nota** vRealize Automation 7.x esegue uno snapshot del blueprint in fase di distribuzione. Se si verificano i problemi di riconfigurazione durante l'aggiornamento delle proprietà della macchina quali CPU e memoria RAM in una distribuzione, vedere l'articolo della Knowledge Base [2150829 relativo alla creazione dello snapshot blueprint vRA 7.x](#).

---

In base al tipo di impostazione, le informazioni di rete e sicurezza vengono acquisite sotto forma di diverse impostazioni nel nuovo blueprint.

- Impostazioni per l'intero blueprint nella rispettiva pagina delle proprietà. Queste informazioni includono isolamento app, zona di trasporto e gateway instradato o informazioni sul criterio di prenotazione di NSX Edge.
- Impostazioni disponibili per i componenti macchina virtuale di vSphere in componenti rete e sicurezza di NSX nella tela di progettazione.

- Impostazioni nelle schede di rete e sicurezza dei singoli componenti macchina virtuale di vSphere nella tela di progettazione.

### Aggiornamento ed endpoint, prenotazioni e blueprint fisici

Non è possibile aggiornare una distribuzione che contiene endpoint fisici. Se sono presenti endpoint fisici, il processo di aggiornamento di vRealize Automation non riesce.

L'aggiornamento non riesce sull'appliance virtuale master quando la distribuzione vRealize Automation 6.2.x include un endpoint fisico. Nel registro e nell'interfaccia di migrazione viene visualizzato un messaggio di errore. Per stabilire se la distribuzione vRealize Automation 6.2.x include un endpoint fisico, accedere a vRealize Automation come utente amministratore IaaS. Selezionare **Infrastruttura > Endpoint** ed esaminare l'elenco di endpoint. Se l'elenco include un endpoint Platform Type Physical, non è possibile eseguire l'aggiornamento a vRealize Automation 7,0 e versione successiva.

vRealize Automation 7,0 e versione successiva non supporta endpoint fisici, prenotazioni e componenti macchina virtuale nei blueprint.

### Aggiornamento e impostazioni dei profili di rete

I profili di rete privata non sono supportati in vRealize Automation 7 e versione successiva e vengono dunque ignorati durante l'aggiornamento. Anche i profili di rete instradata con impostazioni edge PLR associate non sono supportati in vRealize Automation 7 e versione successiva e vengono ignorati durante l'aggiornamento.

Il tipo di profilo di rete privata non è supportato in vRealize Automation 7 e versione successiva. Quando il processo di aggiornamento di vRealize Automation rileva un profilo di rete privata nella distribuzione di origine, ignora il profilo di rete. Anche i bilanciamenti del carico che fanno riferimento quelle reti private vengono ignorati durante l'aggiornamento. Le stesse condizioni di aggiornamento sono vere per un profilo di rete instradata con impostazioni edge PLR associate. Nessuna delle due configurazioni di profili di rete viene aggiornata.

Se una prenotazione contiene un profilo di rete privata, l'impostazione del profilo di rete privata viene ignorata durante l'aggiornamento e la prenotazione viene aggiornata come disabilitata nella distribuzione target.

Se una prenotazione contiene un profilo di rete instradata con impostazioni edge PLR associate, la specifica del profilo di rete instradata viene ignorata durante l'aggiornamento e la prenotazione viene aggiornata come disabilitata nella distribuzione target.

Per informazioni sull'aggiornamento di un blueprint per più macchine contenente impostazioni di rete, vedere [Informazioni sulla modalità di aggiornamento dei blueprint di più macchine](#).

### Aggiornamento e azioni autorizzate

Non è possibile aggiornare le azioni della macchina virtuale.

Le azioni che è possibile eseguire sulle macchine virtuali con provisioning, in base alle specifiche del blueprint, non vengono aggiornate. Per creare nuovamente tali azioni, personalizzare i permessi per i blueprint in modo da consentire solo determinate azioni.

Per le informazioni relative, vedere [Azioni in Permessi](#).



## Aggiornamento e proprietà personalizzate

Tutte le proprietà personalizzate fornite da vRealize Automation sono disponibili nella distribuzione aggiornata. Proprietà personalizzate e gruppi di proprietà vengono aggiornati.

### Terminologia e cambiamenti correlati

Tutti i profili di build creati nella distribuzione di origine vengono aggiornati come gruppi di proprietà. Il termine *profilo di build* è stato ritirato.

Il termine *set di proprietà* è stato ritirato e i file dei set di proprietà CSV non sono più disponibili.

### Distinzione tra maiuscole e minuscole nei nomi delle proprietà personalizzate

Prima di vRealize Automation 7.0, per i nomi delle proprietà personalizzate non veniva fatta distinzione tra maiuscole e minuscole. A partire da vRealize Automation 7.0 e versioni successive, tale distinzione viene applicata. Durante l'aggiornamento, è necessario verificare l'esatta corrispondenza dei nomi delle proprietà personalizzate. Questo consente di evitare la sovrascrittura dei valori delle proprietà e assicura la corrispondenza tra nomi e definizioni del dizionario delle proprietà. Ad esempio, una proprietà personalizzata `hostname` e un'altra proprietà personalizzata `HOSTNAME` vengono considerate proprietà personalizzate differenti da vRealize Automation 7.0 e versioni successive. La proprietà personalizzata `hostname` e la proprietà personalizzata `HOSTNAME` non si sovrascrivono reciprocamente durante l'aggiornamento.

### Spazi nei nomi della proprietà personalizzata

Prima dell'aggiornamento a questa versione di vRealize Automation, rimuovere eventuali spazi da nomi di proprietà personalizzate, ad esempio sostituire lo spazio con un carattere di sottolineatura, per consentire il riconoscimento della proprietà personalizzata nell'installazione vRealize Automation aggiornata. I nomi della proprietà personalizzata vRealize Automation non possono contenere spazi. Questo problema può anche influire sull'utilizzo di un'installazione di vRealize Orchestrator aggiornata che utilizza proprietà personalizzate che contenevano spazi nelle versioni precedenti di vRealize Automation o vRealize Orchestrator oppure entrambi.

### Nomi di proprietà riservati

Alcune parole chiave ora sono riservate e questo potrebbe influire su determinate proprietà aggiornate. Alcune parole chiave utilizzate nel codice dei blueprint possono essere importate, ad esempio utilizzando le funzioni di importazione dei blueprint di vRealize CloudClient. Alcune parole chiave sono considerate riservate e non sono disponibili per proprietà da aggiornare. Tre esempi di parole chiave sono `cpu`, `storage` e `memory`.

### Aggiornamento e Application Services

L'aggiornamento di Application Services è supportato in vRealize Automation 7 e versione successiva.

Dopo aver completato la migrazione a vRealize Automation 7.4, è possibile utilizzare vRealize Automation Application Services Migration Tool per aggiornare i servizi delle applicazioni. Per scaricare lo strumento, procedere come segue.

- 1 Fare clic su [Scarica VMware vRealize Automation](#).

## 2 Selezionare **Driver e strumenti > VMware vRealize Application Services Migration Tool**.

### Aggiornamento e Advanced Service Design

Quando si esegue l'aggiornamento a vRealize Automation 7 e versione successiva, gli elementi di Advanced Service Design vengono aggiornati agli elementi XaaS.

I componenti XaaS sono disponibili per l'uso nella tela di progettazione.

### Aggiornamento e informazioni sui prezzi dei blueprint

A partire dalla versione 7.0, i profili dei prezzi di vRealize Automation non sono più supportati e non vengono migrati nella distribuzione target durante l'aggiornamento. È tuttavia possibile utilizzare l'integrazione avanzata con vRealize Business for Cloud per gestire i costi delle risorse di vRealize Automation.

vRealize Business for Cloud è ora completamente integrato con vRealize Automation e supporta le funzionalità avanzate di gestione dei prezzi riportate di seguito.

- Posizione unificata in vRealize Business for Cloud per una definizione flessibile dei criteri di prezzo per:
  - Blueprint di applicazioni, macchine e risorse delle infrastrutture
  - Macchine virtuali con provisioning in vRealize Automation per gli endpoint supportati come vCenter Server, vCloud Director, Amazon Web Services, Azure e OpenStack.
  - Prezzi operativi, una tantum e sulle proprietà personalizzate delle macchine virtuali con provisioning
  - Distribuzioni, che includono il prezzo delle macchine virtuali nelle distribuzioni
- Report di showback basati su ruoli in vRealize Business for Cloud
- Utilizzo completo delle nuove funzionalità in vRealize Business for Cloud

Prima di eseguire l'aggiornamento, è possibile esportare i report sulle spese esistenti dalla propria istanza di vRealize Automation di origine come riferimento. Al termine dell'aggiornamento, è possibile installare e configurare vRealize Business for Cloud per gestire i prezzi.

---

**Nota** vRealize Automation 7.4 è compatibile solo con vRealize Business for Cloud 7.4 e versioni successive.

---

### Aggiornamento ed elementi del catalogo

Dopo aver aggiornato da vRealize Automation 6.2.x alla versione più recente, alcuni elementi del catalogo vengono visualizzati nel catalogo dei servizi, ma non sono disponibili per la richiesta.

Dopo la migrazione all'ultima versione di vRealize Automation, gli elementi del catalogo che utilizzano le definizioni delle proprietà vengono visualizzati all'interno del catalogo dei servizi, ma non sono disponibili per la richiesta.

- Tipi di controllo: casella di controllo o collegamento.
- Attributi: relazione, espressioni regolari o layout delle proprietà.

In vRealize Automation 7.x, le definizioni delle proprietà non utilizzano più questi elementi. È necessario ricreare la definizione della proprietà o configurarla in modo che utilizzi un'azione di script di vRealize Orchestrator anziché i tipi di controllo o gli attributi incorporati. Per ulteriori informazioni, vedere [Gli elementi del catalogo vengono visualizzati nel catalogo dei servizi dopo l'aggiornamento, ma non sono disponibili per la richiesta](#).

### Elenco di controllo per l'aggiornamento di vRealize Automation

Quando si esegue l'aggiornamento di vRealize Automation dalla versione 6.2.5 alla versione 7.4, è necessario aggiornare tutti i componenti di vRealize Automation in un ordine specifico.

Utilizzare l'elenco di controllo per tenere traccia del lavoro durante l'aggiornamento. Completare le attività nell'ordine in cui sono riportate.

**Nota** È necessario aggiornare tutti i componenti ed esattamente nell'ordine indicato. Se si segue un ordine diverso, l'aggiornamento può dar luogo a comportamenti imprevisti o non riuscire del tutto.

L'ordine di aggiornamento varia a seconda che si intenda aggiornare un ambiente minimo o un ambiente distribuito con appliance vRealize Automation multiple.



**Tabella 1-63. Elenco di controllo per l'aggiornamento di un ambiente vRealize Automation minimo**

Attività	Istruzioni
 Eseguire il backup dell'installazione corrente. L'esecuzione di questo backup è un'attività critica.	Per ulteriori informazioni su come eseguire il backup e ripristinare il sistema, vedere <a href="#">Backup dell'ambiente vRealize Automation 6.2.5 esistente</a> .  Per informazioni generali, vedere <i>Configurazione di backup e ripristino utilizzando Symantec Netbackup</i> all'indirizzo <a href="http://www.vmware.com/pdf/vrealize-backup-and-restore-netbackup.pdf">http://www.vmware.com/pdf/vrealize-backup-and-restore-netbackup.pdf</a>
 Preparare le macchine virtuali vRealize Automation 6.2.x per l'aggiornamento.	È necessario esaminare l' <a href="#">articolo della Knowledge Base 51531</a> ed eseguire eventuali correzioni rilevanti agli ambienti prima dell'aggiornamento.
 Arrestare i servizi Windows di vRealize Automation nel server IaaS.	Vedere <a href="#">Arresto dei servizi di vRealize Automation nel server Windows IaaS</a> .





**Tabella 1-63. Elenco di controllo per l'aggiornamento di un ambiente vRealize Automation minimo (Continua)**

Attività	Istruzioni
<input type="checkbox"/> Se il catalogo dei componenti comuni è installato, è necessario disinstallarlo prima di procedere con l'aggiornamento.	<p>Per informazioni su come disinstallare i componenti del Catalogo dei componenti comuni, vedere la <i>guida all'installazione del catalogo di componenti comuni</i>.</p> <p>Se questa guida non è disponibile, eseguire questi passaggi in ciascun nodo IaaS.</p> <ol style="list-style-type: none"> <li>1 Accedere al nodo IaaS.</li> <li>2 Fare clic su <b>Avvia</b>.</li> <li>3 Immettere <b>services</b> (servizi) nella casella di testo <b>Search programs and files</b> (Cerca programmi e file).</li> <li>4 Fare clic su <b>Servizi</b>.</li> <li>5 Nel riquadro destro della finestra Services, fare clic con il pulsante destro del mouse su ciascun servizio IaaS e selezionare <b>Stop</b> (Interrompi).</li> <li>6 Fare clic su <b>Start &gt; Control Panel &gt; Programs and Features</b> (Programmi e funzionalità).</li> <li>7 Fare clic su ciascun componente Common Components Catalog installato e selezionare <b>Uninstall</b> (Disinstalla).</li> <li>8 Fare clic su <b>Start &gt; Command Prompt</b> (Prompt dei comandi).</li> <li>9 Al prompt dei comandi, eseguire <b>iisreset</b>.</li> </ol>
<input type="checkbox"/> Vedere le considerazioni per l'aggiornamento a questa versione di vRealize Automation per capire cosa può essere aggiornato, cosa non può essere aggiornato e i possibili comportamenti diversi degli elementi aggiornati. Non tutti gli elementi, inclusi blueprint, prenotazioni ed endpoint, possono essere aggiornati. La presenza di alcune configurazioni non supportate non permettono il proseguimento dell'aggiornamento.	<p>Vedere <a href="#">Considerazioni sull'aggiornamento a questa versione di vRealize Automation</a>.</p>
<input type="checkbox"/> Configurare le risorse hardware.	<p>Vedere <a href="#">Incremento delle risorse hardware di vCenter Server per vRealize Automation 6.2.5</a>.</p>
<input type="checkbox"/> Scaricare gli aggiornamenti nell'appliance vRealize Automation.	<p>Vedere <a href="#">Download degli aggiornamenti delle appliance vRealize Automation</a>.</p>
<input type="checkbox"/> Installare l'aggiornamento nell'appliance vRealize Automation.	<p>Vedere <a href="#">Installazione dell'aggiornamento su vRealize Automation Appliance</a>.</p>
<input type="checkbox"/> Aggiornare l'utilità Single-Sign On all'utilità VMware Identity Manager.	<p>Vedere <a href="#">Aggiornamento della password di Single Sign-On per VMware Identity Manager</a>.</p>
<input type="checkbox"/> Aggiornare la chiave di licenza.	<p>Vedere <a href="#">Aggiornamento della chiave di licenza</a>.</p>
<input type="checkbox"/> Effettuare la migrazione dell'archivio identità a VMware Identity Manager.	<p><a href="#">Migrazione degli archivi identità in VMware Identity Manager</a></p>
<input type="checkbox"/> Aggiornare i componenti di IaaS.	<p>Vedere <a href="#">Aggiornamento dei componenti del server IaaS Server dopo l'aggiornamento di vRealize Automation</a>.</p>

**Tabella 1-63. Elenco di controllo per l'aggiornamento di un ambiente vRealize Automation minimo (Continua)**

Attività	Istruzioni
 Aggiornare l'istanza di vRealize Orchestrator esterna.	Vedere <a href="#">Aggiornamento di un'appliance vRealize Orchestrator autonoma per l'utilizzo con vRealize Automation</a> . Vedere <a href="#">Aggiornamento di un cluster di appliance vRealize Orchestrator esterno per l'utilizzo con vRealize Automation</a>
 Aggiungere utenti o gruppi a una connessione Active Directory	Vedere <a href="#">Aggiunta di utenti o gruppi a una connessione Active Directory</a> .

**Tabella 1-64. Elenco di controllo per l'aggiornamento di un ambiente distribuito vRealize Automation**

Attività	Istruzioni
 Eseguire il backup dell'installazione corrente. L'esecuzione di questo backup è un'attività critica.	Per ulteriori informazioni su come eseguire il backup e ripristinare il sistema, vedere <a href="#">Backup dell'ambiente vRealize Automation 6.2.5 esistente</a> . Per informazioni dettagliate, vedere <i>Configurazione di backup e ripristino utilizzando Symantec Netbackup</i> all'indirizzo <a href="http://www.vmware.com/pdf/vrealize-backup-and-restore-netbackup.pdf">http://www.vmware.com/pdf/vrealize-backup-and-restore-netbackup.pdf</a>
 Preparare le macchine virtuali vRealize Automation 6.2.x per l'aggiornamento.	È necessario esaminare l' <a href="#">articolo della Knowledge Base 51531</a> ed eseguire eventuali correzioni rilevanti agli ambienti prima dell'aggiornamento.
 Arrestare i servizi di vRealize Automation nei server Windows di IaaS.	Vedere <a href="#">Arresto dei servizi di vRealize Automation nel server Windows IaaS</a> .
 Se il catalogo dei componenti comuni è installato, è necessario disinstallarlo prima di procedere con l'aggiornamento.	Per informazioni su come disinstallare i componenti del Catalogo dei componenti comuni, vedere la <i>guida all'installazione del catalogo di componenti comuni</i> . Se questa guida non è disponibile, eseguire questi passaggi in ciascun nodo IaaS. <ol style="list-style-type: none"> <li>1 Accedere al nodo IaaS.</li> <li>2 Fare clic su <b>Avvia</b>.</li> <li>3 Immettere <b>services</b> (servizi) nella casella di testo <b>Search programs and files</b> (Cerca programmi e file).</li> <li>4 Fare clic su <b>Servizi</b>.</li> <li>5 Nel riquadro destro della finestra Services, fare clic con il pulsante destro del mouse su ciascun servizio IaaS e selezionare <b>Stop</b> (Interrompi).</li> <li>6 Fare clic su <b>Start &gt; Control Panel &gt; Programs and Features</b> (Programmi e funzionalità).</li> <li>7 Fare clic su ciascun componente Common Components Catalog installato e selezionare <b>Uninstall</b> (Disinstalla).</li> <li>8 Fare clic su <b>Start &gt; Command Prompt</b> (Prompt dei comandi).</li> <li>9 Al prompt dei comandi, eseguire <b>iisreset</b>.</li> </ol>

**Tabella 1-64. Elenco di controllo per l'aggiornamento di un ambiente distribuito vRealize Automation (Continua)**

Attività	Istruzioni
<input type="checkbox"/> Configurare le risorse hardware per l'aggiornamento.	Vedere <a href="#">Incremento delle risorse hardware di vCenter Server per vRealize Automation 6.2.5</a> .
<input type="checkbox"/> Disattivare i bilanciamenti del carico.	<p>Disattivare ciascun nodo secondario e rimuovere i controlli di integrità di vRealize Automation per gli elementi seguenti.</p> <ul style="list-style-type: none"> <li>■ Appliance vRealize Automation</li> <li>■ Sito Web di IaaS</li> <li>■ Servizio di gestione di IaaS</li> </ul> <p>Per un aggiornamento corretto, verificare quanto segue:</p> <ul style="list-style-type: none"> <li>■ Il traffico del bilanciamento del carico viene indirizzato solo al nodo primario.</li> <li>■ I controlli di integrità di vRealize Automation vengono rimossi dall'appliance, dal sito Web e dal servizio di gestione.</li> </ul>
<input type="checkbox"/> Scaricare gli aggiornamenti nell'appliance vRealize Automation.	Vedere <a href="#">Download degli aggiornamenti delle appliance vRealize Automation</a> .
<input type="checkbox"/> Installare l'aggiornamento nella prima appliance vRealize Automation dell'installazione. Se è stata designata un'appliance come master, aggiornare prima questa appliance.	Vedere <a href="#">Installazione dell'aggiornamento su vRealize Automation Appliance</a> .
<input type="checkbox"/> Aggiornare l'utilità Single-Sign On all'utilità VMware Identity Manager.	Vedere <a href="#">Aggiornamento della password di Single Sign-On per VMware Identity Manager</a> .
<input type="checkbox"/> Aggiornare la chiave di licenza.	Vedere <a href="#">Aggiornamento della chiave di licenza</a> .
<input type="checkbox"/> Effettuare la migrazione dell'archivio identità all'utilità VMware Identity Manager.	<a href="#">Migrazione degli archivi identità in VMware Identity Manager</a>
<input type="checkbox"/> Installare l'aggiornamento nelle altre appliance vRealize Automation.	<a href="#">Installazione dell'aggiornamento su appliance vRealize Automation aggiuntive</a>
<input type="checkbox"/> Aggiornare i componenti di IaaS.	Vedere <a href="#">Aggiornamento dei componenti del server IaaS Server dopo l'aggiornamento di vRealize Automation</a> .
<input type="checkbox"/> Aggiornare l'istanza di vRealize Orchestrator esterna.	<p>Vedere <a href="#">Aggiornamento di un'appliance vRealize Orchestrator autonoma per l'utilizzo con vRealize Automation</a>.</p> <p>Vedere <a href="#">Aggiornamento di un cluster di appliance vRealize Orchestrator esterno per l'utilizzo con vRealize Automation</a></p>
<input type="checkbox"/> Attivare i bilanciamenti del carico.	<a href="#">Attivare i bilanciamenti del carico</a>

## Interfacce utente dell'ambiente vRealize Automation

È possibile utilizzare e gestire l'ambiente vRealize Automation con varie interfacce.

## Interfacce utente

Queste tabelle descrivono le interfacce che si utilizzano per gestire l'ambiente vRealize Automation.

**Tabella 1-65. vRealize Automation Console di amministrazione**

Scopo	Accesso	Credenziali necessarie
È possibile utilizzare la console vRealize Automation per queste attività di amministratore di sistema.	1 Avviare un browser e aprire la pagina iniziale dell'appliance vRealize Automation utilizzando il nome di dominio completo dell'appliance virtuale:	È necessario disporre del ruolo di amministratore di sistema.
<ul style="list-style-type: none"> <li>■ Aggiungere i tenant.</li> <li>■ Personalizzare l'interfaccia utente di vRealize Automation.</li> <li>■ Configurare i server email.</li> <li>■ Consente di visualizzare i registri degli eventi.</li> <li>■ Configurare vRealize Orchestrator.</li> </ul>	<p><a href="https://vra-virtual-hostname.domain.name">https://vra-virtual-hostname.domain.name</a>.</p> <p>2 Fare clic nella <b>console di vRealize Automation</b>.</p> <p>È inoltre possibile utilizzare questo URL per aprire la console di vRealize Automation:</p> <p><a href="https://vra-virtual-hostname.domain.name/vcac">https://vra-virtual-hostname.domain.name/vcac</a></p> <p>3 Accedere.</p>	

**Tabella 1-66. Console tenant vRealize Automation . Questa interfaccia è l'interfaccia utente principale utilizzata per creare e gestire i servizi e le risorse.**

Scopo	Accesso	Credenziali necessarie
È possibile utilizzare vRealize Automation per eseguire le attività seguenti.	1 Avviare un browser e immettere l'URL della tenancy utilizzando il nome di dominio completo dell'appliance virtuale e il nome URL del tenant:	È necessario disporre di uno o più dei ruoli seguenti:
<ul style="list-style-type: none"> <li>■ Richiedere nuovi blueprint dei servizi IT.</li> <li>■ Creare e gestire le risorse IT e cloud.</li> <li>■ Creare e gestire gruppi personalizzati.</li> <li>■ Consente di creare e gestire gruppi di business.</li> <li>■ Assegnare ruoli agli utenti.</li> </ul>	<p><a href="https://vra-virtual-hostname.domain.name/vcac/org/tenant_URL_name">https://vra-virtual-hostname.domain.name/vcac/org/tenant_URL_name</a>.</p> <p>2 Accedere.</p>	<ul style="list-style-type: none"> <li>■ Architetto dell'applicazione</li> <li>■ Amministratore approvazioni</li> <li>■ Amministratore del catalogo</li> <li>■ Amministratore contenitori</li> <li>■ Architetto di contenitori</li> <li>■ Consumatore di integrità</li> <li>■ Architetto dell'infrastruttura</li> <li>■ Consumatore esportazione sicura</li> <li>■ Architetto del software</li> <li>■ Amministratore tenant</li> <li>■ Architetto XaaS</li> </ul>

**Tabella 1-67. Console di gestione dell'appliance vRealize Automation . Questa interfaccia talvolta viene chiamata VAMI (Virtual Appliance Management Interface).**

Scopo	Accesso	Credenziali necessarie
<p>È possibile utilizzare la console di gestione dell'appliance vRealize Automation per eseguire le attività seguenti.</p> <ul style="list-style-type: none"> <li>■ Visualizzare lo stato dei servizi registrati.</li> <li>■ Visualizzare le informazioni di sistema ed eseguire riavvio o shutdown dell'appliance.</li> <li>■ Gestire la partecipazione al programma Analisi utilizzo software.</li> <li>■ Visualizzare lo stato della rete.</li> <li>■ Visualizzare lo stato dell'aggiornamento e installare gli aggiornamenti.</li> <li>■ Gestire le impostazioni di amministrazione.</li> <li>■ Gestire le impostazioni dell'host vRealize Automation.</li> <li>■ Gestire le impostazioni SSO.</li> <li>■ Gestire le licenze di prodotto.</li> <li>■ Configurare il database Postgres vRealize Automation.</li> <li>■ Configurare la messaggistica di vRealize Automation.</li> <li>■ Configurare la registrazione di vRealize Automation.</li> <li>■ Installare i componenti IaaS.</li> <li>■ Eseguire la migrazione da un'installazione vRealize Automation esistente.</li> <li>■ Gestire i certificati del componente IaaS.</li> <li>■ Configurare il servizio Xenon.</li> </ul>	<ol style="list-style-type: none"> <li>1 Avviare un browser e aprire la pagina iniziale dell'appliance vRealize Automation utilizzando il nome di dominio completo dell'appliance virtuale:  <code>https://vra-va-hostname.domain.name.</code></li> <li>2 Fare clic su <b>gestione dell'appliance vRealize Automation</b>  Per aprire vRealize Automation Appliance Management, è inoltre possibile utilizzare l'URL <code>https://vra-va-hostname.domain.name:5480.</code></li> <li>3 Accedere.</li> </ol>	<ul style="list-style-type: none"> <li>■ Nome utente: root</li> <li>■ Password: la password immessa durante la distribuzione dell'appliance vRealize Automation.</li> </ul>



Tabella 1-68. Client vRealize Orchestrator

Scopo	Accesso	Credenziali necessarie
<p>È possibile utilizzare il client vRealize Orchestrator per eseguire le attività seguenti.</p> <ul style="list-style-type: none"> <li>■ Sviluppare azioni.</li> <li>■ Sviluppare workflow.</li> <li>■ Gestire criteri</li> <li>■ Installare pacchetti.</li> <li>■ Gestire autorizzazioni di utenti e gruppi di utenti.</li> <li>■ Applicare tag a oggetti URI.</li> <li>■ Visualizzare l'inventario.</li> </ul>	<ol style="list-style-type: none"> <li>1 Avviare un browser e aprire la pagina iniziale di vRealize Automation utilizzando il nome di dominio completo dell'appliance virtuale:  <code>https://vra-virtual-hostname.domain.name</code>.</li> <li>2 Per scaricare il file <code>client.jnlp</code> nel computer locale, fare clic su <b>Client di vRealize Orchestrator</b>.</li> <li>3 Fare clic con il pulsante destro del mouse sul file <code>client.jnlp</code> e scegliere <b>Avvia</b>.</li> <li>4 Nella finestra di dialogo in cui viene chiesto se si desidera continuare, fare clic su <b>Continua</b>.</li> <li>5 Accedere.</li> </ol>	<p>È necessario essere un utente con ruolo di amministratore di sistema o far parte del gruppo <code>vcoadmins</code> configurato nelle impostazioni del provider di autenticazione di vRealize Orchestrator Control Center.</p>

Tabella 1-69. vRealize Orchestrator Control Center

Scopo	Accesso	Credenziali necessarie
<p>È possibile utilizzare vRealize Orchestrator Control Center per modificare la configurazione dell'istanza di vRealize Orchestrator predefinita incorporata in vRealize Automation.</p>	<ol style="list-style-type: none"> <li>1 Avviare un browser e aprire la pagina iniziale dell'appliance vRealize Automation utilizzando il nome di dominio completo dell'appliance virtuale:  <code>https://vra-virtual-hostname.domain.name</code>.</li> <li>2 Fare clic su <b>gestione dell'appliance vRealize Automation</b>  Per aprire vRealize Automation Appliance Management, è inoltre possibile utilizzare l'URL <code>https://vra-virtual-hostname.domain.name:5480</code>.</li> <li>3 Accedere.</li> <li>4 Fare clic su <b>Impostazioni vRA &gt; Orchestrator</b>.</li> <li>5 Selezionare <b>Interfaccia utente di Orchestrator</b>.</li> <li>6 Fare clic su <b>Avvia</b>.</li> <li>7 Fare clic sull'URL dell'interfaccia utente di Orchestrator.</li> <li>8 Accedere.</li> </ol>	<p>Nome utente</p> <ul style="list-style-type: none"> <li>■ Se non è configurata l'autenticazione basata sul ruolo, inserire <b>root</b>.</li> <li>■ Immettere il nome utente di vRealize Automation se è configurato per l'autenticazione basata sul ruolo.</li> </ul> <p>Password</p> <ul style="list-style-type: none"> <li>■ Inserire la password immessa durante la distribuzione dell'appliance vRealize Automation se non è configurata l'autenticazione basata sul ruolo.</li> <li>■ Inserire la password relativa al proprio nome utente se è configurato per l'autenticazione basata sul ruolo.</li> </ul>

**Tabella 1-70. Prompt dei comandi di Linux**

Scopo	Accesso	Credenziali necessarie
<p>È possibile utilizzare il prompt dei comandi di Linux in un host, ad esempio nell'host dell'appliance vRealize Automation, per eseguire le attività seguenti.</p> <ul style="list-style-type: none"> <li>■ Avviare o arrestare servizi</li> <li>■ Modificare file di configurazione</li> <li>■ Eseguire comandi</li> <li>■ Recuperare dati</li> </ul>	<p>1 Nell'host dell'appliance vRealize Automation, aprire un prompt dei comandi.</p> <p>Un modo per aprire il prompt dei comandi nel computer locale consiste nell'avviare una sessione nell'host utilizzando un'applicazione come PuTTY.</p> <p>2 Accedere.</p>	<ul style="list-style-type: none"> <li>■ Nome utente: root</li> <li>■ Password: la password creata durante la distribuzione dell'appliance vRealize Automation.</li> </ul>

**Tabella 1-71. Prompt dei comandi di Windows**

Scopo	Accesso	Credenziali necessarie
<p>È possibile utilizzare il prompt dei comandi di Windows in un host, ad esempio l'host IaaS, per eseguire script.</p>	<p>1 Nell'host IaaS, accedere a Windows.</p> <p>Un modo per effettuare l'accesso dal computer locale consiste nell'avviare una sessione desktop remota.</p> <p>2 Aprire il prompt dei comandi di Windows.</p> <p>Un modo per aprire il prompt dei comandi consiste nel fare clic con il pulsante destro del mouse sull'icona Start nell'host e selezionare <b>Prompt dei comandi</b> o <b>Prompt dei comandi (amministratore)</b>.</p>	<ul style="list-style-type: none"> <li>■ Nome utente: l'utente con privilegi amministrativi.</li> <li>■ Password: la password dell'utente.</li> </ul>

## Aggiornamento dei prodotti VMware integrati con vRealize Automation

È necessario gestire qualsiasi prodotto VMware integrato con l'ambiente vRealize Automation quando si aggiorna vRealize Automation.

Se l'ambiente vRealize Automation è integrato con uno o più prodotti aggiuntivi, è necessario eseguire l'aggiornamento di vRealize Automation prima di aggiornare i prodotti aggiuntivi. Se vRealize Business for Cloud è integrato con vRealize Automation, è necessario annullare la registrazione di vRealize Business for Cloud prima di procedere con l'aggiornamento di vRealize Automation.

Seguire il workflow suggerito per la gestione dei prodotti integrati quando si esegue l'aggiornamento di vRealize Automation.

- 1 Aggiornare vRealize Automation.
- 2 Aggiornare VMware vRealize Operations Manager.
- 3 Aggiornare VMware vRealize Log Insight.
- 4 Aggiornare VMware vRealize Business for Cloud.

In questa sezione vengono fornite istruzioni aggiuntive per la gestione di vRealize Business for Cloud quando è integrato con l'ambiente vRealize Automation.

## Aggiornamento di vRealize Operations Manager integrato con vRealize Automation

Aggiornare vRealize Operations Manager dopo aver aggiornato vRealize Automation.

### Procedura

- 1 Aggiornare vRealize Automation.
- 2 Aggiornare vRealize Operations Manager. Per informazioni, vedere *Aggiornamento del software* nella [documentazione di VMware vRealize Operations Manager](#).

## Aggiornamento di vRealize Log Insight integrato con vRealize Automation

Aggiornare vRealize Log Insight dopo aver aggiornato vRealize Automation.

### Procedura

- 1 Aggiornare vRealize Automation.
- 2 Aggiornare vRealize Log Insight. Per informazioni, vedere *Aggiornamento di vRealize Log Insight* nella [documentazione di VMware vRealize Log Insight](#).

## Aggiornamento di vRealize Business for Cloud integrato con vRealize Automation

Quando si effettua l'aggiornamento dell'ambiente vRealize Automation, è necessario annullare ed eseguire la registrazione della connessione a vRealize Business for Cloud.

Eseguire questa procedura per garantire la continuità del servizio con vRealize Business for Cloud quando si aggiorna l'ambiente vRealize Automation.

### Procedura

- 1 Annullare la registrazione di vRealize Business for Cloud da vRealize Automation. Vedere l'argomento relativo all'*annullamento della registrazione di vRealize Business for Cloud da vRealize Automation* nella [documentazione di VMware vRealize Business for Cloud](#).
- 2 Aggiornare vRealize Automation.
- 3 Se necessario, aggiornare vRealize Business for Cloud. Vedere l'argomento relativo all'*aggiornamento di vRealize Business for Cloud* nella [documentazione di VMware vRealize Business for Cloud](#).
- 4 Registrare vRealize Business for Cloud in vRealize Automation. Vedere l'argomento relativo alla *registrazione di vRealize Business for Cloud con vRealize Automation* nella [documentazione di VMware vRealize Business for Cloud](#).

## Preparazione per l'aggiornamento di vRealize Automation

Prima di eseguire l'aggiornamento di vRealize Automation dalla versione 6.2.5 alla versione 7.4, è necessario effettuare varie attività e procedure.

Eseguire le attività nell'ordine in cui sono disponibili nell'elenco di controllo dell'aggiornamento. Vedere [Elenco di controllo per l'aggiornamento di vRealize Automation](#).

## Prerequisiti di backup per l'aggiornamento di vRealize Automation

Assicurarsi che siano soddisfatti i prerequisiti di backup prima di procedere all'aggiornamento di vRealize Automation 6.2.5 alla versione 7.4.

### Prerequisiti

- Verificare che l'ambiente di origine sia completamente installato e configurato.
- Per ciascuna appliance nell'ambiente di origine, eseguire il backup di tutti i file di configurazione dell'appliance vRealize Automation nelle seguenti directory.
  - `/etc/vcac/`
  - `/etc/vco/`
  - `/etc/apache2/`
  - `/etc/rabbitmq/`
- Eseguire il backup dei file di configurazione del workflow esterno (xmldb) di vRealize Automation nel sistema. Archiviare i file di backup in una directory temporanea. I file si trovano nel percorso `VMware\VC\Server\ExternalWorkflows\xmldb\`. Dopo la migrazione, ripristinare i file xmldb nel nuovo sistema. Vedere [Ripristino dei file di timeout del workflow esterno](#).  
 Per un problema correlato, vedere [Le copie di backup dei file .xml causano il timeout del sistema](#).
- Eseguire il backup del database PostgreSQL di vRealize Automation esterno. Per verificare se il proprio database PostgreSQL è esterno, completare questi passaggi.
  - a Accedere alla console di gestione dell'appliance vRealize Automation utilizzando il relativo nome di dominio completo `https://va-hostname.domain.name:5480`.  
 Per un ambiente distribuito, accedere alla console di gestione dell'appliance vRealize Automation primaria.
  - b Selezionare **Impostazioni vRA > Database**.
  - c Se l'host del nodo del database PostgreSQL di vRealize Automation è diverso dall'host dell'appliance vRealize Automation, effettuare il backup del database. Se l'host del nodo del database è uguale all'host dell'appliance, non è necessario effettuare il backup del database.  
 Per informazioni sul backup del database PostgreSQL, visitare il sito <https://www.postgresql.org/>.
- Creare uno snapshot della configurazione del tenant e degli utenti assegnati.
- Eseguire il backup di ogni file personalizzato, ad esempio `DataCenterLocations.xml`.
- Creare uno snapshot di ciascuna appliance virtuale e server IaaS. Seguire le linee guida comuni per il backup dell'intero sistema nel caso in cui l'aggiornamento di vRealize Automation non venga eseguito correttamente. Vedere [Backup e ripristino per le installazioni di vRealize Automation](#).

### Backup dell'ambiente vRealize Automation 6.2.5 esistente

Prima di aggiornare, eseguire l'arresto e creare uno snapshot dei componenti dell'ambiente vRealize Automation 6.2.5.

Prima di eseguire l'aggiornamento, creare uno snapshot dei componenti mentre il sistema è in arresto.

- Server IaaS vRealize Automation (nodi Windows)
- Appliance vRealize Automation (nodi Linux)
- Nodo identità (SSO) vRealize Automation

Se l'aggiornamento non riesce, utilizzare lo snapshot per tornare all'ultima configurazione corretta nota e tentare un altro aggiornamento.

### Prerequisiti

- Verificare che il database PostgreSQL incorporato sia nella modalità ad alta disponibilità. In questo caso, individuare il nodo master corrente. Vedere l'articolo della knowledge base <http://kb.vmware.com/kb/2105809>.
- Se l'ambiente esistente comprende un database PostgreSQL esterno, creare un file di backup del database.
- Se il database Microsoft SQL vRealize Automation non è in hosting sul server IaaS, creare un file di backup del database. Per informazioni, cercare l'articolo disponibile in [Microsoft Developer Network](#) relativo alla creazione di un backup di database SQL Server completo.
- Verificare che i prerequisiti di backup per l'aggiornamento siano stati completati.
- Verificare di aver creato uno snapshot del sistema mentre è spento. Questo è il metodo preferibile per creare lo snapshot. Vedere la *documentazione di vSphere 6.0*.

---

**Nota** Quando si esegue il backup dell'appliance vRealize Automation e dei componenti IaaS, disabilitare gli snapshot in memoria e gli snapshot inattivi.

---

- Se è stato modificato il file `app.config`, eseguirne il backup. Vedere [Ripristino delle modifiche di registrazione nel file app.config](#).
- Creare un backup dei file di configurazione workflow esterni (xmldb). Vedere [Ripristino dei file di timeout del workflow esterno](#).
- Verificare di disporre di una posizione esterna alla cartella corrente in cui è possibile archiviare il file di backup. Vedere [Le copie di backup dei file .xml causano il timeout del sistema](#).

### Procedura

- 1 Accedere a vCenter Server.
- 2 Individuare i seguenti componenti di vRealize Automation 6.2.5.
  - Server IaaS vRealize Automation (nodi Windows)
  - Appliance vRealize Automation (nodi Linux)
  - Nodo identità (SSO) vRealize Automation

- 3 Per ciascuna delle seguenti macchine virtuali, selezionare la macchina virtuale, fare clic su **Esegui shutdown guest** e attendere l'arresto della macchina virtuale. Eseguire lo shutdown di queste macchine virtuali nell'ordine seguente.
  - a Macchine virtuali dell'agente proxy IaaS
  - b Macchine virtuali di DEM Worker
  - c Macchina virtuale di DEM Orchestrator
  - d Macchina virtuale Manager Service
  - e Macchine virtuali Web Services
  - f Appliance virtuali vRealize Automation secondarie
  - g Appliance virtuali vRealize Automation primarie
  - h Macchine virtuali Manager (se presenti)
  - i Identity Appliance
- 4 Eseguire uno snapshot di ogni macchina virtuale di vRealize Automation 6.2.5.
- 5 Clonare ciascun nodo dell'appliance vRealize Automation.

L'aggiornamento deve essere eseguito nelle macchine virtuali clonate.
- 6 Spegnere ciascuna macchina virtuale dell'appliance di vRealize Automation originale prima di aggiornare le macchine virtuali clonate.

Tenere spente le macchine virtuali originali e utilizzarle solo se è necessario ripristinare il sistema.

#### Operazioni successive

[Incremento delle risorse hardware di vCenter Server per vRealize Automation 6.2.5.](#)

#### Incremento delle risorse hardware di vCenter Server per vRealize Automation 6.2.5

Prima di eseguire l'aggiornamento da vRealize Automation 6.2.5, è necessario incrementare le risorse hardware per ciascuna appliance vRealize Automation.

In questa procedura si suppone che venga utilizzato il client Windows vCenter Server.

#### Prerequisiti

- Assicurarsi di disporre di un clone di ogni appliance vRealize Automation.
- Assicurarsi di disporre di almeno 140 GB di spazio libero su vCenter Server per ogni clone di appliance.
- Verificare che le appliance originali siano spente.

#### Procedura

- 1 Accedere a vCenter Server.
- 2 Fare clic con il pulsante destro del mouse sull'icona di un'appliance vRealize Automation clonata e selezionare **Modifica impostazioni**.

- 3 Selezionare **Memoria** e impostare il valore su 18 GB.
- 4 Selezionare **CPU** e impostare il **numero di socket virtuali** su 4.
- 5 Estendere la dimensione del disco virtuale 1 a 50 GB.
  - a Selezionare Disco 1.
  - b Impostare la dimensione su 50 GB.
  - c Fare clic su **OK**.
- 6 Se non si dispone del disco 3, procedere come segue per aggiungere un disco 3 con una dimensione di 25 GB.
  - a Fare clic su **Aggiungi** al di sopra della tabella Risorse per aggiungere un disco virtuale.
  - b Selezionare **Disco rigido** come **Tipo di dispositivo**, quindi fare clic su **Avanti**.
  - c Selezionare **Crea un nuovo disco virtuale**, quindi fare clic su **Avanti**.
  - d Impostare il valore della **dimensione del disco** su 25 GB.
  - e Selezionare **Archivia con macchina virtuale**, quindi fare clic su **Avanti**.
  - f Verificare che l'opzione **Indipendente** sia deselezionata per **Modalità** e che l'opzione **SCSI (0:2)** sia selezionata per **Modalità virtuale dispositivo**, quindi fare clic su **Avanti**.

Se viene richiesto di accettare le impostazioni consigliate, è sufficiente accettarle.
  - g Fare clic su **Fine**.
  - h Fare clic su **OK**.
- 7 In presenza di un disco virtuale 4 già esistente proveniente da una versione di vRealize Automation precedente, procedere come segue.
  - a Accendere il clone dell'appliance virtuale primaria e attendere 1 minuto.
  - b Accendere il clone dell'appliance virtuale secondaria.
  - c Sul clone dell'appliance virtuale primaria aprire un nuovo prompt dei comandi e passare a `/etc/fstab`.
  - d Sul clone dell'appliance virtuale primaria aprire il file `fstab` e rimuovere le righe che iniziano con `/dev/sdd` i cui registri sono precedenti dalla dicitura `Wal_Archive`.
  - e Sul clone dell'appliance virtuale primaria salvare il file.
  - f Sul clone dell'appliance virtuale secondaria aprire un nuovo prompt dei comandi e passare a `/etc/fstab`.
  - g Sul clone dell'appliance virtuale secondaria aprire il file `fstab` e rimuovere le righe che iniziano con `/dev/sdd` i cui registri sono precedenti dalla dicitura `Wal_Archive`.
  - h Sul clone dell'appliance virtuale secondaria salvare il file.
  - i Spegnerne il clone dell'appliance virtuale secondaria e attendere 1 minuto.

- j Spegner il clone dell'appliance virtuale primaria.
  - k Fare clic con il pulsante destro del mouse sull'icona dell'appliance vRealize Automation primaria clonata e selezionare **Modifica impostazioni**.
  - l Eliminare il disco 4 sulla macchina dell'appliance virtuale primaria clonata.
  - m Fare clic con il pulsante destro del mouse sull'icona dell'appliance vRealize Automation secondaria clonata e selezionare **Modifica impostazioni**.
  - n Eliminare il disco 4 sulla macchina dell'appliance virtuale secondaria clonata.
- 8 Per aggiungere un disco 4 con una dimensione di 50 GB alle macchine dell'appliance virtuale primaria e secondaria clonate, eseguire i passaggi seguenti.
- a Fare clic su **Aggiungi** al di sopra della tabella Risorse per aggiungere un disco virtuale.
  - b Selezionare **Disco rigido** come **Tipo di dispositivo**, quindi fare clic su **Avanti**.
  - c Selezionare **Crea un nuovo disco virtuale**, quindi fare clic su **Avanti**.
  - d Impostare il valore della **dimensione del disco** su 50 GB.
  - e Selezionare **Archivia con macchina virtuale**, quindi fare clic su **Avanti**.
  - f Verificare che l'opzione **Indipendente** sia deselezionata per **Modalità** e che l'opzione **SCSI (0:3)** sia selezionata per **Modalità dispositivo virtuale**, quindi fare clic su **Avanti**.
- Se viene richiesto di accettare le impostazioni consigliate, è sufficiente accettarle.
- g Fare clic su **Fine**.
  - h Fare clic su **OK**.
- 9 Creare uno snapshot della macchina dell'appliance virtuale primaria clonata e della macchina dell'appliance virtuale secondaria clonata.

#### Operazioni successive

[Accensione dell'intero sistema.](#)

#### Accensione dell'intero sistema

Dopo aver aumentato le risorse hardware di vCenter per l'aggiornamento, accendere il sistema prima di effettuare l'aggiornamento.

#### Prerequisiti

- [Backup dell'ambiente vRealize Automation 6.2.5 esistente.](#)
- [Incremento delle risorse hardware di vCenter Server per vRealize Automation 6.2.5.](#)



## Procedura

### 1 Accendere l'intero sistema.

Per istruzioni, vedere la versione vRealize Automation 6.2 dell'argomento sull'[avvio di vRealize Automation](#).

---

**Nota** Nel caso di un ambiente ad alta disponibilità, utilizzare questa procedura per accendere le appliance virtuali.

- a Accendere l'appliance virtuale che era stata spenta per ultima.
  - b Attendere un minuto.
  - c Accendere le appliance virtuali rimanenti.
- 

### 2 Verificare che il sistema funzioni in modo corretto.

## Operazioni successive

### [Arresto dei servizi di vRealize Automation nel server Windows IaaS.](#)

#### Arresto dei servizi di vRealize Automation nel server Windows IaaS

Quando necessario, è possibile utilizzare la seguente procedura per arrestare i servizi di vRealize Automation in ogni server che esegue servizi di IaaS.

Prima di iniziare l'aggiornamento, arrestare i servizi vRealize Automation in ciascun server Windows di IaaS.

---

**Nota** A eccezione di un'istanza di backup passiva del servizio di gestione, il tipo di avvio per tutti i servizi deve essere impostato su Automatico durante il processo di aggiornamento. Se si impostano i servizi su Manuale, il processo di aggiornamento non viene eseguito correttamente.

---

## Procedura

### 1 Accedere al server Windows di IaaS.

### 2 Selezionare **Start > Strumenti di amministrazione > Servizi**.

### 3 Arrestare i servizi nel seguente ordine. Fare attenzione a non arrestare la macchina virtuale.

Ogni macchina virtuale ha un agente di gestione, che deve essere arrestato con ogni insieme di servizi.

- a Tutti gli agenti di VMware vCloud Automation Center
- b Tutti i DEM Worker di VMware
- c Il servizio DEM Orchestrator di VMware
- d Il servizio VMware vCloud Automation Center

- 4 Per le distribuzioni distribuite con bilanciamenti del carico, disabilitare tutti i nodi secondari e rimuovere i monitoraggi di integrità di vRealize Automation per i seguenti elementi.

- a Appliance vRealize Automation
- b Sito Web IaaS
- c Servizio di gestione IaaS

Verificare che il traffico del bilanciamento del carico sia indirizzato esclusivamente ai nodi primari e che i controlli di integrità di vRealize Automation siano rimossi dall'appliance, dal sito Web e dal servizio di gestione. In caso contrario, l'aggiornamento non riesce.

- 5 Verificare che il servizio IaaS ospitato in Microsoft Internet Information Services (IIS) sia in esecuzione procedendo come segue.

- a Nel browser, andare all'URL **https://webhostname/Repository/Data/MetaModel.svc** per verificare che il repository Web sia in esecuzione. Se l'esito è positivo, non vengono restituiti errori e viene visualizzato un elenco dei modelli in formato XML.
- b Controllare lo stato registrato nel file `Repository.log` nel nodo Web della macchina virtuale IaaS per verificare che non segnali irregolarità. Il file si trova nella cartella home di VCAC all'indirizzo `/Server/Model Manager Web/Logs/Repository.log`.

Per un sito Web IaaS distribuito, accedere al sito Web secondario, senza MMD, e arrestare temporaneamente il server IIS Microsoft. Verificare la connettività di `MetaModel.svc`. Per verificare che il traffico del bilanciamento del carico stia attraversando solo il nodo Web primario, avviare il server IIS Microsoft.

## Operazioni successive

[Download degli aggiornamenti delle appliance vRealize Automation.](#)

### Download degli aggiornamenti delle appliance vRealize Automation

Nella console di gestione dell'appliance è possibile controllare la disponibilità di aggiornamenti ed eventualmente scaricarli in uno dei seguenti modi.

Per massimizzare le prestazioni dell'aggiornamento, utilizzare il metodo file ISO.

Per evitare la possibilità del verificarsi di problemi o nel caso in cui si verifichino effettivamente problemi durante l'aggiornamento dell'appliance, vedere l'[articolo della Knowledge Base di VMware](#) relativo alla *non riuscita dell'aggiornamento di vRealize Automation a causa di duplicati nel database di vRealize Orchestrator (54987)*.

- [Download di aggiornamenti di vRealize Automation appliance da un repository VMware](#)

È possibile scaricare l'aggiornamento per l'appliance vRealize Automation da un repository pubblico sul sito Web [vmware.com](http://vmware.com).

- [Download degli aggiornamenti delle appliance virtuali per l'uso tramite unità CD-ROM](#)

È possibile aggiornare l'appliance virtuale da un file ISO che l'appliance leggerà dall'unità CD-ROM virtuale. Questo è il metodo preferito.

## Download di aggiornamenti di vRealize Automation appliance da un repository VMware

È possibile scaricare l'aggiornamento per l'appliance vRealize Automation da un repository pubblico sul sito Web [vmware.com](http://vmware.com).

### Prerequisiti

- Backup dell'ambiente vRealize Automation esistente.
- Verificare che l'appliance vRealize Automation sia accesa.

### Procedura

- 1 Nell'appliance vRealize Automation primaria, accedere alla gestione dell'appliance di vRealize Automation come **root** utilizzando la password immessa durante la distribuzione dell'appliance vRealize Automation.
- 2 Fare clic sulla scheda **Aggiorna**.
- 3 Fare clic su **Impostazioni**.
- 4 (Facoltativo) Impostare la frequenza di controllo aggiornamenti nel pannello Aggiornamenti automatici.
- 5 Selezionare **Usa repository predefinito** nel pannello Aggiorna repository.  
Il repository predefinito è impostato all'URL VMware.com corretto.
- 6 Fare clic su **Salva impostazioni**.

## Download degli aggiornamenti delle appliance virtuali per l'uso tramite unità CD-ROM

È possibile aggiornare l'appliance virtuale da un file ISO che l'appliance leggerà dall'unità CD-ROM virtuale. Questo è il metodo preferito.

Scaricare il file ISO e configurare l'appliance primaria in modo che utilizzi questo file per aggiornare l'appliance in uso.

### Prerequisiti

- Eseguire il backup dell'ambiente vRealize Automation esistente.
- Verificare che tutte le unità CD-ROM utilizzate nell'aggiornamento siano abilitate prima di eseguire l'aggiornamento di un'appliance vRealize Automation. Fare riferimento alla documentazione di vSphere per informazioni sull'aggiunta di un'unità CD-ROM a una macchina virtuale nel client di vSphere.

### Procedura

- 1 Scaricare il file ISO del repository di aggiornamento.
  - a Avviare un browser e passare alla [pagina del prodotto vRealize Automation](#) sul sito [www.vmware.com](http://www.vmware.com).
  - b Fare clic su **Download di vRealize Automation** per passare alla pagina di download di VMware.
  - c Scaricare il file appropriato.

- 2 Individuare il file scaricato nel sistema per verificare che la dimensione del file corrisponda a quella del file sulla pagina di download di VMware. Utilizzare i checksum forniti nella pagina di download per convalidare l'integrità del file scaricato. Per ulteriori informazioni, vedere i collegamenti disponibili in fondo alla pagina di download di VMware.
- 3 Assicurarsi che l'appliance virtuale primaria sia accesa.
- 4 Collegare l'unità CD-ROM per l'appliance virtuale primaria al file ISO scaricato.
- 5 Nell'appliance vRealize Automation primaria, accedere alla gestione dell'appliance di vRealize Automation come **root** utilizzando la password immessa durante la distribuzione dell'appliance vRealize Automation.
- 6 Fare clic sulla scheda **Aggiorna**.
- 7 Fare clic su **Impostazioni**.
- 8 In **Aggiorna repository**, selezionare **Usa aggiornamenti CDROM**.
- 9 Fare clic su **Salva impostazioni**.

## Aggiornamento dell'appliance vRealize Automation

Dopo aver soddisfatto i prerequisiti di aggiornamento e aver scaricato l'aggiornamento dell'appliance virtuale, è possibile aggiornare l'appliance vRealize Automation 6.2.5 alla versione 7.4. È inoltre necessario riconfigurare alcune impostazioni dell'appliance vRealize Automation primaria.

Dopo aver aggiornato l'appliance vRealize Automation primaria, è necessario aggiornare gli altri nodi presenti nell'ambiente nel seguente ordine:

- 1 Ogni appliance vRealize Automation secondaria
- 2 Sito Web IaaS
- 3 Servizio di gestione IaaS
- 4 DEM di IaaS
- 5 Agente IaaS
- 6 Aggiornare o migrare ogni istanza di vRealize Orchestrator esterna

## Installazione dell'aggiornamento su vRealize Automation Appliance

È possibile installare l'aggiornamento di vRealize Automation nell'appliance vRealize Automation 6.2.5 e configurare le impostazioni dell'appliance.

L'assistenza per il database esterno PostgreSQL è stata interrotta a partire da vRealize Automation 7.1. Il processo di aggiornamento unisce i dati provenienti da un database PostgreSQL esterno esistente con il database PostgreSQL interno che fa parte di Appliance vRealize Automation.

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>.

Durante l'installazione dell'aggiornamento, non chiudere la console di gestione.

Se si verificano problemi durante il processo di aggiornamento, vedere [Risoluzione dei problemi relativi all'aggiornamento di vRealize Automation](#).

### Prerequisiti

- Verificare di aver selezionato un metodo di download e di aver scaricato l'aggiornamento. Vedere [Download degli aggiornamenti delle appliance vRealize Automation](#).
- Per distribuzioni distribuite ad alta disponibilità, vedere [Backup dell'ambiente vRealize Automation 6.2.5 esistente](#).
- Per le distribuzioni con bilanciamenti del carico, verificare che il traffico sia diretto esclusivamente al nodo principale e che i controlli di integrità siano disabilitati.
- Se è stato installato un componente del catalogo di componenti comuni nell'ambiente, disinstallarlo prima dell'aggiornamento. Per informazioni, consultare la *guida all'installazione del catalogo di componenti comuni*. Se la guida non è disponibile, utilizzare la procedura alternativa descritta nel paragrafo [Elenco di controllo per l'aggiornamento di vRealize Automation](#).
- Verificare che la connessione al database jdbc:postgresql punti all'indirizzo IP esterno del nodo PostgreSQL master.
  - a In ciascuna appliance vRealize Automation aprire un nuovo prompt dei comandi.
  - b Passare a `/etc/vcac/server.xml` ed eseguire una copia di backup di `server.xml`.
  - c Aprire `server.xml`.
  - d Se necessario, modificare la voce jdbc:postgresql del file `server.xml`, che punta al database Postgres e fare in modo che punti all'indirizzo IP esterno del nodo PostgreSQL master per il database PostgreSQL esterno o l'appliance virtuale primaria per PostgreSQL incorporato.  
  
Ad esempio `jdbc:postgresql://198.15.100.60:5432/vcac`
- Prima di effettuare l'aggiornamento, assicurarsi che tutte le richieste salvate e in corso siano state completate correttamente.

### Procedura

- 1 Aprire la console di gestione dell'appliance vRealize Automation.
  - a Nell'appliance vRealize Automation primaria, accedere alla gestione dell'appliance di vRealize Automation come **root** utilizzando la password immessa durante la distribuzione dell'appliance vRealize Automation.
  - b Accedere con il nome utente **root** e la password immessa durante la distribuzione dell'appliance.
- 2 Fare clic su **Servizi** e verificare che tutti i servizi siano elencati come REGISTRATI, ad eccezione del servizio IaaS.
- 3 Selezionare **Aggiorna > Impostazioni**.
- 4 Selezionare una delle seguenti opzioni:
  - **Usa repository predefinito.**

- **Usa aggiornamenti da CDROM.**

5 Fare clic su **Salva impostazioni**.

6 Selezionare **Stato**.

7 Fare clic su **Controlla aggiornamenti** per verificare l'accessibilità di un aggiornamento.

8 (Facoltativo) Per le istanze dell'appliance vRealize Automation, fare clic su **Dettagli** nell'area della versione dell'appliance per visualizzare informazioni sulla posizione delle note di rilascio.

9 Fare clic su **Installa aggiornamenti**.

10 Fare clic su **OK**.

Viene visualizzato un messaggio che segnala l'aggiornamento in corso.

11 (Facoltativo) Se il disco 1 non è stato ridimensionato manualmente a 50 GB, procedere come segue.

a Quando il sistema chiede di riavviare l'appliance virtuale, fare clic su **Sistema**, quindi su **Riavvia**.

Durante il riavvio, il sistema regola lo spazio richiesto per l'aggiornamento.

b Dopo il riavvio del sistema, accedere di nuovo alla console di gestione dell'appliance vRealize Automation, verificare che ciascun servizio, ad eccezione del servizio IaaS, sia elencato come REGISTRATO e selezionare **Aggiorna > Stato**.

c Fare clic su **Controlla aggiornamenti** e su **Installa aggiornamenti**.

12 Per visualizzare lo stato di avanzamento dell'aggiornamento, aprire i seguenti file registro.

- `/opt/vmware/var/log/vami/updatecli.log`
- `/opt/vmware/var/log/vami/vami.log`
- `/var/log/vmware/horizon/horizon.log`
- `/var/log/bootstrap/*.log`

Se ci si disconnette durante il processo di aggiornamento e si accede di nuovo prima che l'aggiornamento sia concluso, è possibile continuare a seguire l'avanzamento dell'aggiornamento nel file registro. Il file `updatecli.log` potrebbe visualizzare informazioni sulla versione di vRealize Automation dalla quale si sta eseguendo l'aggiornamento. La versione visualizzata passa alla versione corretta più avanti nel corso dell'aggiornamento.

Il tempo necessario per completare l'aggiornamento varia a seconda dell'ambiente.

13 Fare clic su **Telemetria** nella console di gestione dell'appliance. Leggere la nota sulla partecipazione al programma CEIP (Customer Experience Improvement Program) e scegliere se partecipare o meno al programma.

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>.

Per ulteriori informazioni sul programma CEIP, vedere [Partecipazione o uscita dal programma CEIP per vRealize Automation](#).

## Operazioni successive

[Aggiornamento della password di Single Sign-On per VMware Identity Manager.](#)

### Aggiornamento della password di Single Sign-On per VMware Identity Manager

Dopo aver installato gli aggiornamenti, è necessario aggiornare la password di Single Sign-On per VMware Identity Manager.

VMware Identity Manager sostituisce i componenti SSO Identity Appliance e vSphere.

#### Procedura

- 1 Disconnettersi dalla console di gestione dell'appliance vRealize Automation, chiudere e riaprire il browser ed eseguire nuovamente l'accesso.
- 2 Selezionare **Impostazioni vRA > SSO**.
- 3 Inserire una nuova password per VMware Identity Manager e fare clic su **Salva impostazioni**.  
  
Non utilizzare password semplici. È possibile ignorare il messaggio di errore Server SSO non connesso. Il riavvio dei servizi può richiedere diversi minuti.  
  
La password viene accettata.  
  
In una distribuzione ad alta disponibilità, la password viene applicata al primo nodo dell'appliance vRealize Automation e propagata a tutti i nodi dell'appliance vRealize Automation secondari.
- 4 Riavviare l'appliance virtuale.
  - a Fare clic sulla scheda **System**.
  - b Fare clic su **Riavvia** e confermare la selezione.
- 5 Verificare che tutti i servizi siano in esecuzione.
  - a Accedere alla console di gestione dell'appliance vRealize Automation.
  - b Fare clic sulla scheda **Servizi** nella console.
  - c Fare clic sulla scheda **Aggiorna** per monitorare l'avanzamento dell'avvio dei servizi.  
  
Dovrebbero esserci almeno 35 servizi.
- 6 Verificare che tutti i servizi siano registrati, ad eccezione del servizio IaaS.  
  
Il servizio di gestione versioni non si avvia senza una chiave di licenza vRealize Code Stream.

## Operazioni successive

[Aggiornamento della chiave di licenza.](#)

### Aggiornamento della chiave di licenza

È necessario aggiornare la chiave di licenza in modo che utilizzi la versione più recente dell'appliance vRealize Automation.

## Procedura

- 1 Aprire la console di gestione della propria appliance virtuale utilizzando il suo nome di dominio completo, `https://va-hostname.domain.name:5480`.
- 2 Accedere utilizzando il nome utente **root** e la password immessi al momento della distribuzione dell'appliance.
- 3 Selezionare **Impostazioni vRA > Gestione licenze**.  
 Se la scheda **Gestione licenze** non è disponibile, eseguire i passaggi seguenti e ripetere la procedura.
  - a Uscire dalla console di gestione.
  - b Svuotare la cache del browser.
- 4 Immettere la nuova chiave di licenza nella casella di testo **Nuova chiave di licenza**.  
 Gli endpoint e le quote sono contrassegnati in base all'accordo di licenza con l'utente finale (EULA).
- 5 Fare clic su **Invia chiave**.

## Operazioni successive

[Migrazione degli archivi identità in VMware Identity Manager.](#)

### Migrazione degli archivi identità in VMware Identity Manager

Quando si esegue l'aggiornamento da vRealize Automation 6.2.5 alla versione corrente, è necessario migrare gli archivi identità.

Come richiesto nelle procedure seguenti, fare riferimento allo snapshot delle informazioni di configurazione del tenant 6.2.5.

---

**Nota** Dopo aver eseguito la migrazione degli archivi identità, gli utenti di vRealize Code Stream devono riassegnare manualmente i ruoli di vRealize Code Stream.

---

## Procedura

- 1 [Creare un account utente locale per i propri tenant](#)  
 È necessario configurare un tenant con un account utente locale e assegnare privilegi di amministratore tenant all'account utente locale.
- 2 [Sincronizzazione di utenti e gruppi per un collegamento Active Directory](#)  
 Per importare i propri utenti e gruppi in vRealize Automation utilizzando la funzionalità Gestione directory, è necessario connettersi al collegamento di Active Directory.
- 3 [Migrazione di gruppi personalizzati nell'istanza di VMware Identity Manager di destinazione](#)  
 È necessario migrare tutti i gruppi personalizzati dall'ambiente di origine a VMware Identity Manager (vIDM) nella distribuzione di destinazione.
- 4 [Migrazione di più tenant e amministratori IaaS](#)  
 Per ciascun tenant vRealize Automation con amministratori Tenant o IaaS, è necessario eliminare e ripristinare manualmente ciascun amministratore.



## Creare un account utente locale per i propri tenant

È necessario configurare un tenant con un account utente locale e assegnare privilegi di amministratore tenant all'account utente locale.

Ripetere questa procedura per ogni tenant.

### Prerequisiti

Verificare di aver impostato una nuova password per VMware Identity Manager. Vedere [Aggiornamento della password di Single Sign-On per VMware Identity Manager](#).

### Procedura

- 1 Accedere alla console vRealize Automation con il nome utente (**administrator**) e la password dell'amministratore di sistema predefinito.

Il percorso della console è `https://vra-appliance/vcac/`.

- 2 Fare clic sul proprio tenant.

Ad esempio, per il tenant predefinito, fare clic su **vsphere.local**.

- 3 Selezionare la scheda **Utenti locali**.

- 4 Fare clic su **Nuovo**.

- 5 Creare un account utente locale.

A questo utente viene assegnato il ruolo di amministratore tenant. Verificare che il nome utente locale sia univoco nell'istanza di Active Directory di vsphere.local.

- 6 Fare clic su **OK**.

- 7 Fare clic su **Amministratori**.

- 8 Immettere il nome utente locale nella casella di ricerca **Amministratori tenant** e premere Invio.

- 9 Fare clic su **Fine**.

- 10 Uscire dalla console.

### Operazioni successive

[Sincronizzazione di utenti e gruppi per un collegamento Active Directory](#).

## Sincronizzazione di utenti e gruppi per un collegamento Active Directory

Per importare i propri utenti e gruppi in vRealize Automation utilizzando la funzionalità Gestione directory, è necessario connettersi al collegamento di Active Directory.

Eseguire questa procedura per ciascuno dei propri tenant.

### Prerequisiti

Verificare di disporre dei privilegi di accesso ad Active Directory.

## Procedura

- 1 Accedere alla console di vRealize Automation all'indirizzo:  
**`https://vra-appliance/vcac/org/tenant_name`**.
- 2 Selezionare **Amministrazione > Gestione directory > Directory**.
- 3 Fare clic su **Aggiungi directory** e selezionare **Aggiungi Active Directory su LDAP/IWA**.
- 4 Immettere le impostazioni dell'account di Active Directory.

### ◆ Istanze di Active Directory non native

Opzione	Input di esempio
<b>Nome directory</b>	Immettere un nome di directory univoco. Selezionare Active Directory su LDAP quando si utilizza un'istanza di Active Directory non nativa.
<b>Questa directory supporta i servizi DNS</b>	Deselezionare questa opzione.
<b>DN di base</b>	Immettere il DN (Distinguished Name) del punto di inizio per le ricerche nel server della directory. Ad esempio, <b>cn=users,dc=rainpole,dc=local</b> .
<b>DN di binding</b>	Immettere il DN (Distinguished Name) completo, incluso il CN (Common Name), di un account utente di Active Directory che disponga di privilegi per la ricerca degli utenti. Ad esempio, <b>cn=config_admin infra,cn=users,dc=rainpole,dc=local</b> .
<b>Password DN di binding</b>	Immettere la password di Active Directory per l'account che può effettuare la ricerca di utenti.

### ◆ Istanze di Active Directory native

Opzione	Input di esempio
<b>Nome directory</b>	Immettere un nome di directory univoco. Selezionare Active Directory (autenticazione integrata di Windows) quando si utilizza un'istanza di Active Directory nativa.
<b>Nome di dominio</b>	Immettere il nome del dominio da unire.
<b>Nome utente amministratore di dominio</b>	Immettere il nome utente dell'amministratore del dominio.
<b>Password amministratore di dominio</b>	Immettere la password dell'account dell'amministratore del dominio.
<b>UPN utente di binding</b>	Utilizzare il formato di indirizzo email per inserire il nome dell'utente autorizzato ad autenticare il dominio.
<b>Password DN di binding</b>	Immettere la password dell'account di binding di Active Directory per l'account che può effettuare la ricerca di utenti.

- 5 Fare clic su **Prova connessione** per verificare la connessione alla directory configurata.
- 6 Fare clic su **Salva e avanti**.  
Viene visualizzata la pagina **Seleziona domini** con l'elenco dei domini.
- 7 Accettare l'impostazione del dominio predefinito e fare clic su **Avanti**.

- 8 Verificare che i nomi di attributo siano mappati agli attributi di Active Directory corretti e fare clic su **Avanti**.
- 9 Selezionare i gruppi e gli utenti da sincronizzare.
  - a Fare clic sull'icona **Nuovo**.
  - b Immettere il dominio dell'utente e fare clic su **Trova gruppi**.  
Ad esempio, inserire **dc=vcac,dc=local**.
  - c Per selezionare i gruppi da sincronizzare, fare clic su **Seleziona**, quindi su **Avanti**.
  - d Nella pagina di **selezione degli utenti**, selezionare gli utenti da sincronizzare e fare clic su **Avanti**.
- 10 Verificare che gli utenti e i gruppi siano sincronizzati con la directory e fare clic su **Sincronizza directory**.  
La sincronizzazione della directory richiede un po' di tempo e viene eseguita in background.
- 11 Selezionare **Amministrazione > Gestione directory > Provider di identità** e fare clic sul nuovo provider di identità.  
Ad esempio, **WorkspaceIDP\_\_1**.
- 12 Scorrere fino in fondo alla pagina e aggiornare il valore della proprietà Nome host IdP in modo che punti al nome di dominio completo del bilanciamento del carico di vRealize Automation.
- 13 Fare clic su **Salva**.
- 14 Ripetere i passaggi 11-13 per ogni tenant e provider di identità.
- 15 Dopo aver aggiornato tutti i nodi di vRealize Automation, accedere a ogni tenant e selezionare **Amministrazione > Gestione directory > Provider di identità**.  
A ogni provider di identità sono stati aggiunti tutti i connettori di vRealize Automation.  
Se ad esempio la distribuzione include due appliance vRealize Automation, i connettori associati al provider di identità sono due.

### Migrazione di gruppi personalizzati nell'istanza di VMware Identity Manager di destinazione

È necessario migrare tutti i gruppi personalizzati dall'ambiente di origine a VMware Identity Manager (vIDM) nella distribuzione di destinazione.

Completare questa procedura per eseguire la migrazione dei gruppi personalizzati.

#### Prerequisiti

- [Creare un account utente locale per i propri tenant](#).
- Verificare che il servizio horizon-workspace sia in esecuzione nell'appliance virtuale vRealize Automation.

#### Procedura

- 1 Avviare una sessione SSH nell'appliance virtuale vRealize Automation.

- 2 Al prompt dei comandi, accedere come **root** utilizzando la password creata quando è stata installata l'appliance virtuale vRealize Automation.
- 3 Eseguire il comando seguente.

```
vcac-config migrate-custom-groups
```

- Al termine della migrazione viene visualizzato un messaggio che indica che la migrazione dei gruppi personalizzati è stata completata correttamente.
- Se nell'ambiente di origine non sono presenti gruppi personalizzati, viene visualizzato un messaggio che indica che non sono stati trovati gruppi personalizzati nel database di vRA e che il processo di migrazione verrà ignorato.

---

**Nota** Se la migrazione dei gruppi personalizzati non riesce, visualizzare il file di registro in `/var/log/vmware/vcac/vcac-config.log` per ulteriori dettagli.

---

### Migrazione di più tenant e amministratori IaaS

Per ciascun tenant vRealize Automation con amministratori Tenant o IaaS, è necessario eliminare e ripristinare manualmente ciascun amministratore.

Eseguire la procedura seguente per ogni tenant nella console di vRealize Automation.

#### Prerequisiti

Accedere alla console di vRealize Automation nell'appliance virtuale aggiornata.

- 1 Aprire la console di vRealize Automation nell'appliance virtuale aggiornata utilizzando il nome di dominio completo, `https://va-hostname.domain_name/vcac`.

Per un ambiente distribuito, aprire la console nell'appliance virtuale master.

- 2 Selezionare il dominio **vsphere.local**.
- 3 Accedere con il nome utente **administrator** e la password immessa durante la distribuzione dell'appliance virtuale.

#### Procedura

- 1 Selezionare **Amministrazione > Tenant**.
- 2 Fare clic su un nome di tenant.
- 3 Fare clic su **Amministratori**.
- 4 Creare un elenco per ciascun nome e nome utente di amministratore tenant e IaaS.
- 5 Puntare su ciascun amministratore e fare clic sull'icona di eliminazione **X** fino a eliminare tutti gli amministratori.
- 6 Fare clic su **Fine**.
- 7 Nella pagina Tenant fare clic nuovamente sul nome del tenant.
- 8 Fare clic su **Amministratori**.

- 9 Immettere nella casella di ricerca appropriata il nome di ciascun utente eliminato e premere Invio.
- 10 Fare clic sul nome dell'utente appropriato dai risultati della ricerca per aggiungere nuovamente l'utente come amministratore.

Al termine, l'elenco degli amministratori tenant e laaS sarà uguale all'elenco degli amministratori eliminati.

- 11 Fare clic su **Fine**.

### Operazioni successive

Aggiornare le appliance secondarie. Vedere [Installazione dell'aggiornamento su appliance vRealize Automation aggiuntive](#).

### Installazione dell'aggiornamento su appliance vRealize Automation aggiuntive

In un ambiente ad alta disponibilità, l'appliance virtuale master rappresenta il nodo che esegue il database PostgreSQL incorporato in modalità Master. Gli altri nodi dell'ambiente eseguono il database PostgreSQL incorporato in modalità Replica. Durante l'aggiornamento, l'appliance virtuale di replica della versione 6.2.5 non richiede modifiche del database.

Durante l'installazione dell'aggiornamento, non chiudere la console di gestione.

### Prerequisiti

- Assicurarsi di aver scaricato gli aggiornamenti dell'appliance virtuale. Vedere [Download degli aggiornamenti delle appliance vRealize Automation](#).
- Verificare che la connessione al database jdbc:postgresql punti all'indirizzo IP esterno del nodo PostgreSQL master.
  - a Nell'appliance vRealize Automation aprire un nuovo prompt dei comandi.
  - b Passare a `/etc/vcac/server.xml` ed eseguire il backup del file `server.xml`.
  - c Aprire il file `server.xml`.
  - d Se necessario, modificare la voce `jdbc:postgresql` del file `server.xml` per indicare il database PostgreSQL che si desidera utilizzare.
    - Per un database PostgreSQL esterno, immettere l'indirizzo IP esterno del nodo PostgreSQL master.
    - Per un database PostgreSQL incorporato, immettere l'indirizzo IP dell'appliance virtuale master.

Ad esempio `jdbc:postgresql://198.15.100.60:5432/vcac`

## Procedura

- 1 Aprire la console di gestione dell'appliance vRealize Automation per l'aggiornamento.
  - a Nell'appliance vRealize Automation secondaria, accedere alla console di gestione dell'appliance vRealize Automation come **root** utilizzando la password immessa durante la distribuzione dell'appliance vRealize Automation.
  - b Accedere con il nome utente **root** e la password immessa durante la distribuzione dell'appliance.
  - c Fare clic su **Aggiorna**.
- 2 Fare clic su **Impostazioni**.
- 3 Nella sezione **Aggiorna repository**, scegliere se scaricare gli aggiornamenti dal repository VMware o da un CD-ROM.
- 4 Fare clic su **Stato**.
- 5 Fare clic su **Controlla aggiornamenti** per verificare l'accessibilità di un aggiornamento.
- 6 Fare clic su **Installa aggiornamenti**.
- 7 Fare clic su **OK**.

Viene visualizzato un messaggio che segnala l'aggiornamento in corso.

- 8 (Facoltativo) Se il disco 1 non è stato ridimensionato manualmente a 50 GB, eseguire i passaggi seguenti.
  - a Quando il sistema chiede di riavviare l'appliance virtuale, fare clic su **Sistema**, quindi su **Riavvia**.  
Durante il riavvio, il sistema regola lo spazio sul disco 1 necessario per l'aggiornamento.
  - b Dopo il riavvio del sistema, disconnettersi e accedere di nuovo alla console di gestione di Appliance vRealize Automation e selezionare **Aggiorna > Stato**.
  - c Fare clic su **Controlla aggiornamenti** e su **Installa aggiornamenti**.

- 9 Per verificare se l'aggiornamento sta procedendo in modo corretto, aprire i file di registro.

- /opt/vmware/var/log/vami/vami.log
- /opt/vmware/var/log/vami/updatecli.log
- /var/log/vmware/horizon/horizon.log
- /var/log/bootstrap/\*.log

Se si esce durante il processo di aggiornamento e successivamente si accede nuovamente, è possibile continuare a seguire l'avanzamento dell'aggiornamento nel file registro /opt/vmware/var/log/vami/updatecli.log.

Il tempo necessario per completare l'aggiornamento dipende dall'ambiente.

- 10 Al termine dell'aggiornamento, disconnettersi dalla console di gestione di Appliance vRealize Automation, cancellare la cache del browser Web e accedere alla console di gestione di Appliance vRealize Automation.

- 11 Riavviare l'appliance virtuale.
  - a Fare clic su **Sistema**.
  - b Fare clic su **Riavvia** e confermare la selezione.
- 12 Dopo aver riavviato l'appliance virtuale, accedere alla console di gestione dell'appliance Appliance vRealize Automation di replica.
- 13 Selezionare **Impostazioni vRA > Cluster**.
- 14 Immettere il nome utente e la password dell'appliance Appliance vRealize Automation master.
- 15 Fare clic su **Unisci cluster**.
- 16 Fare clic su **Servizi** e verificare che tutti i servizi siano elencati come REGISTRATI, ad eccezione del servizio IaaS.

#### Operazioni successive

[Aggiornamento dei componenti del server IaaS Server dopo l'aggiornamento di vRealize Automation.](#)

### Aggiornamento dei componenti del server IaaS Server dopo l'aggiornamento di vRealize Automation

Dopo l'aggiornamento di vRealize Automation 6.2.5 alla versione 7.4, l'amministratore di sistema deve aggiornare i componenti del server IaaS, incluso il database di Microsoft SQL Server.

Per aggiornare i componenti del server IaaS si possono utilizzare due metodi.

- Utilizzare lo script della shell dell'aggiornamento IaaS automatico.
- Utilizzare il file eseguibile del programma di installazione IaaS di vRealize Automation 7.4.

Se è stato installato un componente del catalogo di componenti comuni, disinstallarlo prima dell'aggiornamento. Terminato l'aggiornamento, è possibile reinstallare la versione appropriata del componente. Per ulteriori informazioni, consultare la *guida all'installazione del catalogo di componenti comuni*. Se la guida non è disponibile, utilizzare la procedura alternativa descritta nel paragrafo [Elenco di controllo per l'aggiornamento di vRealize Automation](#).

#### Aggiornamento dei componenti IaaS tramite lo script della shell di aggiornamento

Utilizzare lo script della shell di aggiornamento per aggiornare i componenti IaaS dopo aver aggiornato ciascuna appliance vRealize Automation 6.2.5 alla versione 7.4.

L' Appliance vRealize Automationmaster o principale aggiornata contiene uno script della shell da utilizzare per aggiornare ciascun nodo e componente IaaS.

È possibile eseguire lo script di aggiornamento utilizzando la console di vSphere per la macchina virtuale oppure una sessione console SSH. Utilizzando la console di vSphere si evitano i problemi di connettività di rete intermittente, che possono interrompere l'esecuzione dello script.

Se si interrompe l'esecuzione dello script mentre sta aggiornando un componente, l'esecuzione dello script continua fino al completamento dell'aggiornamento nel componente. Se nel nodo sono presenti componenti non aggiornati, è necessario eseguire di nuovo lo script.

Al termine dell'aggiornamento, è possibile esaminare il risultato dell'aggiornamento aprendo il file di registro dell'aggiornamento nel percorso `/usr/lib/vcac/tools/upgrade/upgrade.log`.

### Prerequisiti

- Verificare che tutte le appliance vRealize Automation siano state aggiornate.
- Se si riavvia un server IaaS dopo aver aggiornato tutte le appliance vRealize Automation, è necessario arrestare i servizi Windows IaaS. Prima di aggiornare i componenti di IaaS, arrestare tutti i servizi Windows IaaS nel server, ad eccezione del servizio dell'agente di gestione.
- Prima di eseguire lo script della shell di aggiornamento nel nodo master o primario di Appliance vRealize Automation, verificare che ciascun servizio sia REGISTRATO.
  - a Passare alla console di gestione dell'appliance virtuale utilizzando il nome di dominio completo, ovvero `https://va-hostname.domain.name:5480`.
  - b Accedere utilizzando il nome utente **root** e la password immessi al momento della distribuzione dell'appliance.
  - c Fare clic su **Servizi**.
  - d Verificare che ogni servizio, ad eccezione di `iaas-service`, sia REGISTRATO.
- Aggiornare l'agente di gestione in ogni macchina virtuale IaaS vRealize Automation.
  - a Aprire un browser e passare alla pagina Installazione IaaS di VMware vRealize Automation nell'appliance vRealize Automation utilizzando il nome di dominio completo, ovvero `https://virtual_appliance_host:5480/installer`.
  - b Fare clic su **Management Agent Installer**.  
  
Per impostazione predefinita, il programma di installazione viene scaricato nella cartella Downloads.
  - c Accedere a ciascuna macchina virtuale IaaS vRealize Automation e aggiornare l'agente di gestione utilizzando il file del **programma di installazione dell'agente di gestione**.
- Verificare che nel nodo Web IaaS primario in cui sono installati i dati Model Manager sia installato JAVA SE Runtime Environment 8, a 64 bit, aggiornamento 161 o versione successiva. Dopo aver installato Java, è necessario impostare la variabile di ambiente `JAVA_HOME` sulla nuova versione.
- Accedere a ogni nodo del sito Web IaaS e verificare che la data di creazione sia antecedente alla data di modifica nel file `web.config`. Se la data di creazione del file `web.config` coincide o è successiva alla data di modifica, eseguire la procedura in [Aggiornamento non riuscito per il componente sito Web di IaaS](#).
- Per verificare che in ogni nodo IaaS sia presente un agente di gestione aggiornato, eseguire questi passaggi in ciascun nodo IaaS.
  - a Accedere alla console di gestione dell'appliance vRealize Automation.
  - b Selezionare **Impostazioni vRA > Cluster**.
  - c Espandere l'elenco di tutti i componenti installati su ciascun nodo IaaS e individuare l'agente di gestione IaaS.



d Verificare che la versione dell'agente di gestione sia corrente.

- Verificare che il backup del database Microsoft SQL Server IaaS sia accessibile qualora si rendesse necessario un ripristino dello stato precedente.
- Eliminare tutti i nodi IaaS orfani. Vedere [Eliminazione di nodi orfani in vRealize Automation](#).
- Verificare che gli snapshot dei server IaaS nella distribuzione siano disponibili.

Se l'aggiornamento non riesce, tornare allo snapshot e al backup del database e provare a eseguire un altro aggiornamento.

## Procedura

- 1 Aprire una nuova sessione console nel nodo primario o master di Appliance vRealize Automation e accedere con l'account root.

Se si intende eseguire lo script di aggiornamento con SSH, aprire una sessione della console SSH.

- 2 Cambiare le directory in `/usr/lib/vcac/tools/upgrade/`.
- 3 Al prompt, eseguire questo comando per creare il file `upgrade.properties`.  
`./generate_properties`

- 4 Aprire il file `upgrade.properties` e inserire i valori richiesti.

Nella tabella sono indicati i valori richiesti che variano in base all'ambiente. Ad esempio, su un nodo che contiene un DEM Worker o un DEM Orchestrator, sono richieste le credenziali DEM.

Valore obbligatorio	Descrizione	Formato credenziali	Valore di esempio
web_username	Il nome utente del nodo Web primario. Richiesto solo una volta.	Dominio\utente	iaasDomain\webuser
web_password	La password del nodo Web primario. Richiesto solo una volta.	Password	pa\$\$w0rd!
dem_username	Il nome utente di DEM Worker o DEM Orchestrator. Richiesto per ogni nodo su cui viene installato un componente DEM.	Dominio\utente	iaasDomain\demuser
dem_password	La password di DEM Worker o DEM Orchestrator. Richiesto per ogni nodo su cui viene installato un componente DEM.	Password	pa\$\$w0rd!
agent_username	Il nome utente di un agente, quale ad esempio un agente vSphere. Richiesto per ogni nodo su cui viene installato un componente agente.	Dominio\utente	iaasDomain\agent_user

Valore obbligatorio	Descrizione	Formato credenziali	Valore di esempio
agent_password	La password di un agente, quale ad esempio un agente vSphere. Richiesto per ogni nodo su cui viene installato un componente agente.	Password	pa\$\$w0rd!
vidm_admin_password	La password dell'amministratore VIDM. Richiesta solo quando si esegue l'aggiornamento da vRealize Automation 6.2.5.	vidm_password	pa\$\$w0rd!

Per motivi di sicurezza, il file `upgrade.properties` viene rimosso quando si esegue lo script di shell di aggiornamento. Le proprietà del file vengono definite utilizzando le informazioni di ogni componente IaaS che passa attraverso gli agenti di gestione IaaS. Prima di eseguire lo script della shell `./generate_properties` o `./upgrade_from_62x`, è importante che tutti gli agenti di gestione di IaaS siano aggiornati e integri. Se un agente di gestione IaaS presenta problemi quando si esegue lo script di shell di aggiornamento, vedere [L'aggiornamento dell'agente di gestione non riesce](#). Per ricreare il file `upgrade.properties` ripetere i passaggi 2 e 3.

## 5 Eseguire lo script di aggiornamento.

- Al prompt dei comandi, inserire `./upgrade_from_62x`.
- Premere Invio.

Lo script visualizza i singoli nodi IaaS e tutti i componenti installati su ciascuno. Lo script convalida ogni componente prima di installare l'aggiornamento. Se nel file `upgrade.properties` sono presenti valori non corretti, lo script fallisce, lo script non riesce.

L'aggiornamento del primo componente del server IaaS richiede almeno 30 minuti. Durante l'aggiornamento, viene visualizzato un messaggio simile al seguente `Upgrading server components for node web1-vra.mycompany.com`.

Se lo script della shell di aggiornamento non viene eseguito correttamente, esaminare il file `upgrade.log`.

Dopo aver risolto il problema è possibile eseguire di nuovo lo script di aggiornamento. Prima di eseguire di nuovo lo script di aggiornamento, ricreare il file `upgrade.properties`, aprirlo e inserire tutti i valori richiesti.

## 6 (Facoltativo) Attivare il failover automatico del servizio di gestione. Vedere [Abilitazione del failover automatico del servizio di gestione dopo l'aggiornamento](#).

### Operazioni successive

[Ripristino dell'accesso al Control Center di vRealize Orchestrator integrato.](#)

### Aggiornamento dei componenti IaaS tramite il programma di installazione di IaaS

È possibile utilizzare questo metodo alternativo per aggiornare i componenti IaaS dopo l'aggiornamento di vRealize Automation 6.2.5 alla versione 7.4.

## Download del programma di installazione di IaaS per aggiornare i componenti di IaaS

Dopo l'aggiornamento da vRealize Automation 6.2.5 alla versione 7.4, scaricare il programma di installazione di IaaS nella macchina virtuale in cui sono installati i componenti di IaaS da aggiornare.

Se durante questa procedura vengono visualizzati avvisi relativi ai certificati, è possibile ignorarli.

---

**Nota** A eccezione di un'istanza di backup passiva del servizio di gestione, il tipo di avvio per tutti i servizi deve essere impostato su Automatico durante il processo di aggiornamento. Se si impostano i servizi su Manuale, il processo di aggiornamento non viene eseguito correttamente.

---

### Prerequisiti

- Verificare che nella macchina virtuale dell'installazione di IaaS sia installato Microsoft .NET Framework 4.5.2 o versioni successive. È possibile scaricare il programma di installazione di .NET dalla pagina di installazione di IaaS di VMware vRealize Automation. Se si aggiorna .NET alla versione 4.5.2 dopo lo shutdown dei servizi, è possibile che la macchina virtuale venga riavviata durante l'installazione. Quando ciò accade, è necessario arrestare manualmente tutti i servizi IaaS nella macchina virtuale ad eccezione dell'agente di gestione.
- Se si utilizza Internet Explorer per il download, verificare che non sia abilitata la configurazione di sicurezza avanzata. Immettere `res://iesetup.dll/SoftAdmin.htm` nella barra di ricerca e premere Invio.
- Accedere in qualità di amministratore locale al server Windows in cui sono installati uno o più componenti IaaS da aggiornare.

### Procedura

- 1 Aprire un browser.
- 2 Immettere l'URL per la pagina di installazione di IaaS di VMware vRealize Automation.  
Ad esempio, `https://vcac-va-hostname.domain.name:5480/installer`, dove `vcac-va-hostname.domain.name` è il nome del nodo primario o master dell'appliance vRealize Automation.
- 3 Fare clic sul **programma di installazione di IaaS**.
- 4 Il file del programma di installazione `setup__vcac-va-hostname.domain.name@5480.exe` viene inviato alla cartella Downloads per impostazione predefinita.  
Non modificare il nome del file. poiché viene utilizzato per collegare l'installazione all'appliance vRealize Automation.

### Operazioni successive

- Se si dispone di un'istanza autonoma di vRealize Orchestrator, vedere [Aggiornamento di un'appliance vRealize Orchestrator autonoma per l'utilizzo con vRealize Automation](#).
- Se si dispone di un cluster di appliance vRealize Orchestrator esterno, vedere [Aggiornamento di un cluster di appliance vRealize Orchestrator esterno per l'utilizzo con vRealize Automation](#).
- Vedere [Aggiornamento dei componenti IaaS dopo l'aggiornamento di vRealize Automation](#).

## Aggiornamento dei componenti IaaS dopo l'aggiornamento di vRealize Automation

Dopo l'aggiornamento di vRealize Automation 6.2.5 alla versione 7.4, è necessario aggiornare il database SQL e configurare tutti i sistemi in cui sono installati componenti IaaS. È possibile utilizzare questi passaggi per installazioni minime e distribuite.

---

**Nota** Il programma di installazione di IaaS deve trovarsi nella macchina virtuale che contiene i componenti IaaS che si desidera aggiornare. Non è possibile eseguire il programma di installazione da una posizione esterna, ad eccezione del database Microsoft SQL che può essere aggiornato anche in remoto rispetto al nodo Web.

---

Verificare che gli snapshot dei server IaaS nella distribuzione siano disponibili. Se l'aggiornamento non riesce, è possibile tornare allo snapshot e tentare un altro aggiornamento.

Eseguire l'aggiornamento in modo che i servizi siano aggiornati nell'ordine seguente:

### 1 Siti Web di IaaS

Se si utilizza un bilanciamento del carico, disabilitare il traffico su tutti i nodi non primari.

Completare l'aggiornamento su un server prima di aggiornare quello successivo che esegue un servizio sito Web. Iniziare da quello in cui è installato il componente Model Manager Data.

Se si sta eseguendo un aggiornamento manuale del database Microsoft SQL esterno, è necessario aggiornare l'applicazione SQL esterna prima di aggiornare il nodo Web. È possibile eseguire l'aggiornamento del database SQL esterno in remoto da un nodo Web.

### 2 Servizi di gestione

Aggiornare il servizio di gestione attivo prima di aggiornare il servizio di gestione passivo.

Se la codifica SSL non è abilitata nell'istanza di SQL, deselezionare l'opzione relativa alla **codifica SSL** nella finestra di dialogo per la configurazione dell'aggiornamento di IaaS.

### 3 DEM Orchestrator e DEM Worker

Aggiornare tutti i DEM Orchestrator e i DEM Worker. Completare l'aggiornamento su un server prima di aggiornare quello successivo.

### 4 Agenti

Completare l'aggiornamento su un server prima di aggiornare quello successivo che esegue un agente.

### 5 Agente di gestione

Aggiornato come parte del processo di aggiornamento.

I diversi servizi eventualmente presenti su un unico server vengono aggiornati nell'ordine corretto. Se ad esempio nel sito sono presenti nello stesso server il sito Web e i servizi di gestione, selezionare entrambi per l'aggiornamento. Il programma di installazione dell'aggiornamento applica gli aggiornamenti nell'ordine corretto. È necessario completare l'aggiornamento su un server prima di iniziare ad aggiornarne un altro.

---

**Nota** se la distribuzione utilizza un bilanciamento del carico, la prima appliance che si intende aggiornare deve essere connessa al bilanciamento del carico. Per evitare errori della cache, tutte le altre istanze di Appliance vRealize Automation devono essere disabilite per il traffico del bilanciamento del carico prima di applicare l'aggiornamento.

---

### Prerequisiti

- Eseguire il backup dell'ambiente vRealize Automation 6.2.5 esistente.
- Se si riavvia un server IaaS dopo aver aggiornato tutte le appliance vRealize Automation, è necessario arrestare i servizi Windows IaaS. Prima di aggiornare i componenti di IaaS, arrestare tutti i servizi Windows IaaS nel server, ad eccezione del servizio dell'agente di gestione.
- [Download del programma di installazione di IaaS per aggiornare i componenti di IaaS.](#)
- Verificare che nel nodo primario del sito Web di IaaS dove si trovano i dati di Model Manager sia installata la versione corretta di Java. È necessario che sia installato JAVA SE Runtime Environment 8, a 64 bit, aggiornamento 161 o versioni successive. Dopo aver installato Java, impostare la variabile di ambiente JAVA\_HOME sulla nuova versione.
- Verificare che la data di creazione sia antecedente alla data di modifica nel file `web.config`. Se la data di creazione del file `web.config` coincide o è successiva alla data di modifica, eseguire la procedura in [Aggiornamento non riuscito per il componente sito Web di IaaS](#).
- Se si sta eseguendo l'aggiornamento da vRealize Automation 6.2.5 e si utilizza un database Microsoft SQL esterno, è necessario disporre della versione corretta dell'agente di gestione. Prima di poter eseguire l'aggiornamento del sito Web di IaaS, la versione dell'agente di gestione nel database esterno deve essere 7.0 o successiva. È possibile verificare la versione dell'agente di gestione nel Pannello di controllo della macchina virtuale SQL esterna. Se la versione dell'agente di gestione non è 7.0 o successiva, eseguire i passaggi seguenti per aggiornarlo.
  - a Aprire un browser e passare alla pagina Installazione IaaS di VMware vRealize Automation in Appliance vRealize Automation utilizzando il nome di dominio completo, ovvero `https://virtual_appliance_host:5480/installer`.
  - b Fare clic su **Management Agent Installer**.  
Per impostazione predefinita, il programma di installazione viene scaricato nella cartella Downloads.
  - c Accedere al database esterno, aggiornare l'agente di gestione mediante il file del **programma di installazione dell'agente di gestione** e riavviare il servizio dell'agente di gestione di Windows.

- Se è stato installato un componente del catalogo di componenti comuni, disinstallarlo prima dell'aggiornamento. Per ulteriori informazioni, vedere la *guida all'installazione del catalogo di componenti comuni* o seguire la procedura descritta nell'[Elenco di controllo per l'aggiornamento di vRealize Automation](#).

## Procedura

- 1 Se si utilizza il bilanciamento del carico, preparare l'ambiente.
  - a Verificare che il nodo del sito Web IaaS che contiene i dati di Model Manager sia abilitato per il traffico del bilanciamento del carico.  
È possibile identificare questo nodo dalla presenza della *cartella* `vCAC\Server\ConfigTool`.
  - b Disabilitare tutti gli altri siti Web IaaS e i servizi di gestione non primari per il traffico del bilanciamento del carico.
- 2 Fare clic con il pulsante destro del mouse sul file d'installazione `setup__vrealize-automation-appliance-FQDN@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, immettere le credenziali di amministratore per la distribuzione corrente.  
Il nome utente è **root** e la password corrisponde a quella immessa durante la distribuzione dell'appliance.
- 6 Selezionare **Accetta certificato**.
- 7 Nella pagina **Tipo di installazione**, verificare che sia selezionato **Aggiorna**.  
Se **Aggiorna** non è selezionato, i componenti del sistema sono già aggiornati a questa versione.
- 8 Fare clic su **Avanti**.
- 9 Configurare le impostazioni di aggiornamento.

Opzione	Azione
<b>Se si sta aggiornando Model Manager Data</b>	<p>Selezionare la casella di controllo <b>Model Manager Data</b> nella sezione vCAC Server.</p> <p>La casella di controllo è selezionata per impostazione predefinita. Aggiornare Model Manager Data una sola volta. Quando si aggiorna un'installazione distribuita, nell'intervallo di tempo in cui le versioni dei dati di Model Manager e quelle dei dati dei server Web non corrispondono, i server Web smettono di funzionare. Una volta completato l'aggiornamento di Model Manager, i server Web riprendono a funzionare normalmente.</p>
<b>Se non si sta aggiornando Model Manager Data</b>	<p>Deselezionare la casella di controllo <b>Model Manager Data</b> nella sezione vCAC Server.</p>

Opzione	Azione
<b>Per preservare i workflow personalizzati nell'ultima versione in Model Manager Data</b>	<p>Se si sta aggiornando Model Manager Data, selezionare la casella di controllo <b>Preserva ultime versioni dei workflow</b> nella sezione Workflow di estendibilità.</p> <p>La casella di controllo è selezionata per impostazione predefinita. I workflow personalizzati vengono sempre preservati. La selezione della casella di controllo determina solo l'ordine delle versioni. Se sono stati personalizzati workflow in Model Manager, selezionare questa opzione in modo che il workflow più recente rimanga nella versione più recente dopo l'aggiornamento.</p> <p>Se non si seleziona questa opzione, la versione di ogni workflow fornito con vRealize Automation Designer diventa la più recente dopo l'aggiornamento. La versione che prima dell'aggiornamento era la più recente diventa la seconda più recente.</p> <p>Per informazioni su vRealize Automation Designer, vedere <i>Estensibilità del ciclo di vita</i>.</p>
<b>Se si sta aggiornando un Distributed Execution Manager o un agente proxy</b>	<p>Immettere le credenziali dell'account di amministratore nella sezione Account servizio.</p> <p>Tutti i servizi aggiornati vengono eseguiti con questo account.</p>
<b>Per specificare il database di Microsoft SQL Server</b>	<p>Se si aggiorna Model Manager Data, immettere i nomi del server e dell'istanza del database nella casella di testo <b>Server</b>. Immettere il nome di dominio completo (FQDN) del nome del server di database nella casella di testo <b>Nome database</b>.</p> <p>Se l'istanza del database si trova su una porta SQL non predefinita, includere il numero della porta nella definizione dell'istanza del server. La porta predefinita di Microsoft SQL è 1433.</p> <p>Quando si aggiornano i nodi di gestione, l'opzione SSL di MSSQL è selezionata per impostazione predefinita. Se il database non utilizza SSL, deselezionare <b>Usa SSL per la connessione al database</b>.</p>

10 Fare clic su **Avanti**.

11 Verificare che tutti i servizi da aggiornare appaiano nella pagina Pronto per l'aggiornamento e fare clic su **Aggiorna**.

Viene visualizzata la pagina dell'aggiornamento e un indicatore di avanzamento. Terminato il processo di aggiornamento, il pulsante **Avanti** viene abilitato.

12 Fare clic su **Avanti**.

13 Fare clic su **Fine**.

14 Verificare che tutti i servizi vengano riavviati.

15 Ripetere i passaggi per ogni server IaaS della distribuzione nell'ordine indicato.

16 Dopo aver aggiornato tutti i componenti, accedere alla console di gestione dell'appliance e verificare che tutti i servizi, incluso IaaS, ora siano registrati.

Tutti i componenti selezionati sono aggiornati alla nuova versione.

#### Operazioni successive

- [Ripristino dell'accesso al Control Center di vRealize Orchestrator integrato.](#)

- Se la distribuzione utilizza un bilanciamento del carico, aggiornare ogni nodo del bilanciamento del carico in modo che utilizzi i controlli di integrità di vRealize Automation. Riabilitare il traffico del bilanciamento del carico per tutti i nodi non connessi. Se la distribuzione precedente utilizzava un database PostgreSQL incorporato con bilanciamento del carico, disattivare tutti i nodi del pool di PostgreSQL in quanto non sono necessari. Eliminare il pool in un secondo momento.

Per ulteriori informazioni, vedere [Bilanciamento del carico di vRealize Automation](#).

- (Facoltativo) Attivare il failover automatico del servizio di gestione. Vedere [Abilitazione del failover automatico del servizio di gestione dopo l'aggiornamento](#).

### Ripristino dell'accesso al Control Center di vRealize Orchestrator integrato

Dopo aver aggiornato i componenti del server IaaS, è necessario ripristinare l'accesso a vRealize Orchestrator.

Quando si aggiorna vRealize Automation 6.2.5 alla versione 7.4, è necessario eseguire la seguente procedura per integrare la nuova funzionalità di controllo dell'accesso in base al ruolo. Questa procedura è stata scritta per un ambiente ad alta disponibilità.

#### Prerequisiti

Creare uno snapshot dell'ambiente di vRealize Automation.

#### Procedura

- 1 Accedere alla console di gestione di Appliance vRealize Automation come root utilizzando il nome di dominio completo dell'host dell'appliance, `https://va-hostname.domain.name:5480`.
- 2 Selezionare **Impostazioni vRA > Database**.
- 3 Identificare i nodi master e replica.
- 4 Su ogni nodo di replica, aprire una sessione SSH, accedere come amministratore ed eseguire questo comando:  
  
`service vco-server stop && service vco-configurator stop`
- 5 Nel nodo master, aprire una sessione SSH, accedere come amministratore ed eseguire questo comando:  
  
`rm /etc/vco/app-server/vco-registration-id`
- 6 Sul nodo master, passare alla directory `/etc/vco/app-server/`.
- 7 Aprire il file `sso.properties`.



- 8 Se il nome della proprietà `com.vmware.o11n.sso.admin.group.name` contiene spazi o qualsiasi altro carattere correlato alla Bash, ovvero accettati come carattere speciale in un comando Bash come ad esempio un apostrofo (') o un segno di dollaro (\$), continuare con questa procedura.
  - a Copiare la riga con la proprietà `com.vmware.o11n.sso.admin.group.name` e immettere `AdminGroup` come valore.
  - b Aggiungere `#` all'inizio della riga originale contenente la proprietà `com.vmware.o11n.sso.admin.group.name` per impostare la riga come commento.
  - c Salvare e chiudere il file `sso.properties`.
- 9 Eseguire il comando seguente:  

```
vcac-vami vco-service-reconfigure
```
- 10 Se è stato completato il passaggio 8, aprire il file `sso.properties` e completare i passaggi seguenti.
  - a Rimuovere l'asterisco `#` dall'inizio della riga originale contenente la proprietà `com.vmware.o11n.sso.admin.group.name` per rimuovere il commento dalla riga.
  - b Rimuovere la copia della riga con la proprietà `com.vmware.o11n.sso.admin.group.name`.
  - c Salvare e chiudere il file `sso.properties`.
- 11 Per riavviare il servizio `vco-server`, eseguire il comando seguente:  

```
service vco-server restart
```
- 12 Per riavviare il servizio `vco-configurator`, eseguire il comando seguente:  

```
service vco-configurator restart
```
- 13 Nella console di gestione di Appliance vRealize Automation, fare clic su **Servizi** e attendere che tutti i servizi nel nodo master siano REGISTRATI.
- 14 Quando tutti i servizi sono registrati, unire i nodi replica di vRealize Automation al cluster vRealize Automation per sincronizzare la configurazione di vRealize Orchestrator. Per informazioni, vedere [Riconfigurazione del vRealize Orchestrator incorporato per il supporto dell'alta disponibilità](#).

#### Operazioni successive

[Aggiornamento di vRealize Orchestrator dopo l'aggiornamento di vRealize Automation.](#)

### Aggiornamento di vRealize Orchestrator dopo l'aggiornamento di vRealize Automation

È necessario aggiornare l'istanza di vRealize Orchestrator dopo l'aggiornamento di vRealize Automation 6.2.5 alla versione 7.4.

Con il rilascio di vRealize Orchestrator 7.4, sono disponibili due opzioni per aggiornare vRealize Orchestrator dopo aver completato l'aggiornamento a vRealize Automation 7.4.

- È possibile eseguire la migrazione del server vRealize Orchestrator esterno esistente all'istanza di vRealize Orchestrator incorporata inclusa in vRealize Automation 7.4.

- È possibile aggiornare il server vRealize Orchestrator autonomo o in cluster per consentirne il funzionamento con vRealize Automation 7.4.

### Migrazione di un server vRealize Orchestrator esterno in vRealize Automation

È possibile migrare il server vRealize Orchestrator esterno esistente in un'istanza di vRealize Orchestrator incorporata in vRealize Automation 7.4.

È possibile distribuire vRealize Orchestrator come istanza esterna del server e configurare vRealize Automation per il funzionamento con tale istanza esterna oppure configurare e utilizzare il server vRealize Orchestrator incluso in Appliance vRealize Automation.

VMware consiglia di effettuare la migrazione del server vRealize Orchestrator esterno nel server Orchestrator integrato in vRealize Automation. La migrazione da un server Orchestrator esterno a uno incorporato offre i seguenti vantaggi:

- Riduce il costo totale di proprietà.
- Semplifica il modello di distribuzione.
- Migliora l'efficienza operativa.

---

**Nota** È consigliabile utilizzare il server vRealize Orchestrator esterno nei casi seguenti:

- Tenant multipli nell'ambiente vRealize Automation
  - Ambiente diffuso geograficamente
  - Gestione del carico di lavoro
  - Uso di plug-in specifici, ad esempio vecchie versioni del plug-in Site Recovery Manager
- 

### Differenze di Control Center tra server Orchestrator esterni e incorporati

Alcune delle voci di menu disponibili in Control Center per un server vRealize Orchestrator esterno non sono incluse nella vista di Control Center predefinita di un'istanza di Orchestrator incorporata.

In un server Orchestrator incorporato, alcune opzioni di Control Center sono nascoste per impostazione predefinita.

Voce di menu	Dettagli
<b>Gestione licenze</b>	Il server Orchestrator incorporato è preconfigurato per l'utilizzo di vRealize Automation come provider di licenze.
<b>Esporta/Importa configurazione</b>	La configurazione del server Orchestrator incorporato è inclusa nei componenti di vRealize Automation esportati.
<b>Consente di configurare database</b>	Il server Orchestrator incorporato utilizza il database usato da vRealize Automation.
<b>Programma per il miglioramento dell'esperienza del cliente (CEIP)</b>	È possibile partecipare al programma CEIP dall'interfaccia di gestione dell'appliance vRealize Automation. <i>Vedere <a href="#">Programma per il miglioramento dell'esperienza del cliente</a> in <a href="#">Gestione di vRealize Automation</a>.</i>

---

Altre opzioni nascoste dalla vista di Control Center predefinita sono la casella di testo **Indirizzo host** e il pulsante **ANNULLA REGISTRAZIONE** nella pagina **Configura provider di autenticazione**.

---

**Nota** Per vedere l'intera serie di opzioni di Control Center in vRealize Orchestrator integrato in vRealize Automation, è necessario accedere alla pagina di gestione avanzata di Orchestrator all'indirizzo `https://vra-va-hostname.domain.name_or_load_balancer_address:8283/vco-controlcenter/#/?advanced` e premere il pulsante F5 sulla tastiera per aggiornare la pagina.

---

### Migrazione di un server vRealize Orchestrator esterno su Windows in vRealize Automation

Dopo aver aggiornato vRealize Automation dalla versione 6.x alla versione 7.4, è possibile effettuare la migrazione del server Orchestrator 6.x esterno esistente installato su Windows nel server Orchestrator integrato in vRealize Automation 7.4.

---

**Nota** Se è presente un ambiente vRealize Automation distribuito con più nodi di vRealize Automation, eseguire la procedura di migrazione solo nel nodo di vRealize Automation primario.

---

#### Prerequisiti

- Migrazione a vRealize Automation 7.4 riuscita.
- Arrestare il servizio nel server Orchestrator esterno.
- Eseguire il backup del database del server Orchestrator esterno, incluso lo schema di database.

#### Procedura

- 1 Scaricare lo strumento di migrazione dal server Orchestrator di destinazione.
  - a Accedere all'appliance vRealize Automation tramite SSH come **root**.
  - b Scaricare l'archivio `migration-tool.zip` che si trova nella directory `/var/lib/vco/downloads`.
- 2 Esportare la configurazione di Orchestrator dal server Orchestrator di origine.
  - a Impostare la variabile di ambiente `PATH` in modo che punti alla cartella `bin` di Java JRE installato con Orchestrator.
  - b Caricare lo strumento di migrazione nel server Windows in cui è installato il server Orchestrator esterno.
  - c Estrarre l'archivio scaricato nella cartella di installazione di Orchestrator.

Il percorso predefinito della cartella di installazione di Orchestrator in un'installazione basata su Windows è `C:\Program Files\VMware\Orchestrator`.

- d Eseguire il prompt dei comandi di Windows come amministratore e passare alla cartella bin nella cartella di installazione di Orchestrator.

Per impostazione predefinita, il percorso della cartella bin è C:\Program Files\VMware\Orchestrator\migration-cli\bin.

- e Eseguire il comando export dalla riga di comando.

```
C:\Program Files\VMware\Orchestrator\migration-cli\bin\vro-migrate.bat export
```

Questo comando combina i file di configurazione e i plug-in di vRealize Orchestrator in un archivio di esportazione.

L'archivio viene creato nella stessa cartella migration-cli.

- 3 Effettuare la migrazione della configurazione esportata nel server Orchestrator integrato in vRealize Automation 7.4.

- a Caricare il file di configurazione esportato nella directory /usr/lib/vco/tools/configuration-cli/bin in Appliance vRealize Automation.
- b Nella directory /usr/lib/vco/tools/configuration-cli/bin, modificare la proprietà del file di configurazione di Orchestrator esportato.

```
chown vco:vco orchestrator-config-export-orchestrator_ip_address-date_hour.zip
```

- c Importare il file di configurazione del server Orchestrator nel server vRealize Orchestrator integrato eseguendo lo script vro-configure con il comando import.

```
./vro-configure.sh import --skipDatabaseSettings --skipLicense --skipSettings --skipSslCertificate --notForceImportPlugins --notRemoveMissingPlugins --skipTrustStore --path orchestrator-config-export-orchestrator_appliance_ip-date_hour.zip
```

- 4 Migrare il database nel database PostgreSQL interno mediante l'esecuzione dello script vro-configure con il comando db-migrate.

```
./vro-configure.sh db-migrate --sourceJdbcUrl JDBC_connection_URL --sourceDbUsername database_user
--sourceDbPassword database_user_password
```

**Nota** Racchiudere tra apici le password contenenti caratteri speciali.

Il valore di *JDBC\_connection\_URL* dipende dal tipo di database utilizzato.

PostgreSQL: *jdbc:postgresql://host:port/database\_name*

MSSQL: *jdbc:jtds:sqlserver://host:port/database\_name\*; if using SQL authentication and MSSQL: *jdbc:jtds:sqlserver://host:port/database\_name\;domain=domain\;useNTLMv2=TRUE* if using Windows authentication.

Oracle: *jdbc:oracle:thin:@host:port:database\_name*

Le informazioni di accesso del database predefinite sono:

<i>database_name</i>	vmware
<i>database_user</i>	vmware
<i>database_user_password</i>	vmware

- 5 Se vRealize Automation è stato migrato e non aggiornato, eliminare i certificati Single Sign-On attendibili dal database dell'istanza di Orchestrator incorporata.

```
sudo -u postgres -i -- /opt/vmware/vpostgres/current/bin/psql vcac -c "DELETE FROM vmo_keystore
WHERE id='cakeystore-id';"
```

La migrazione di un server vRealize Orchestrator 6.x esterno installato su Windows in un'istanza di vRealize Orchestrator incorporata in vRealize Automation 7.4 è stata eseguita correttamente.

### Operazioni successive

Configurare il server vRealize Orchestrator integrato. Vedere [Configurazione del server vRealize Orchestrator integrato](#).

### Migrazione di un'appliance virtuale vRealize Orchestrator 6.x esterna in vRealize Automation 7.4

Una volta aggiornato vRealize Automation dalla versione 6.x alla versione 7.4, è possibile effettuare la migrazione dell'appliance virtuale Orchestrator 6.x esterna nel server Orchestrator integrato in vRealize Automation 7.4.

**Nota** Se è presente un ambiente vRealize Automation distribuito con più nodi di Appliance vRealize Automation, eseguire la procedura di migrazione solo nel nodo di vRealize Automation primario.

## Prerequisiti

- Migrazione a vRealize Automation 7.4 riuscita.
- Arrestare il servizio nel server Orchestrator esterno.
- Eseguire il backup del database del server Orchestrator esterno, incluso lo schema di database.

## Procedura

- 1 Scaricare lo strumento di migrazione dal server Orchestrator di destinazione al server Orchestrator di origine.

- a Accedere all'appliance virtuale vRealize Orchestrator 6.x su SSH come **root**.
- b Nella directory `/var/lib/vco`, eseguire il comando `scp` per scaricare l'archivio `migration-tool.zip`.

```
scp root@vra-va-hostname.domain.name:/var/lib/vco/downloads/migration-tool.zip ./
```

- c Eseguire il comando `unzip` per estrarre l'archivio dello strumento di migrazione.

```
unzip migration-tool.zip
```

- 2 Esportare la configurazione di Orchestrator dal server Orchestrator di origine.

- a Nella directory `/var/lib/vco/migration-cli/bin`, eseguire il comando `export`.

```
./vro-migrate.sh export
```

Questo comando combina i file di configurazione e i plug-in di VMware vRealize Orchestrator in un archivio di esportazione.

Viene creato un archivio con nome di file `orchestrator-config-export-orchestrator_ip_address-date_hour.zip` nella cartella `/var/lib/vco`.

- 3 Effettuare la migrazione della configurazione esportata nel server Orchestrator integrato in vRealize Automation 7.4.

- a Accedere all'Appliance vRealize Automation su SSH come **root**.
- b Nella directory `/usr/lib/vco/tools/configuration-cli/bin`, eseguire il comando `scp` per scaricare l'archivio di configurazione esportato.

```
scp root@orchestrator_ip_or_DNS_name:/var/lib/vco/orchestrator-config-export-orchestrator_ip_address-date_hour.zip ./
```

- c Modificare la proprietà del file di configurazione del server Orchestrator esportato.

```
chown vco:vco orchestrator-config-export-orchestrator_ip_address-date_hour.zip
```

- d Arrestare il servizio del server Orchestrator e il servizio Control Center del server vRealize Orchestrator integrato.

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

- e Importare il file di configurazione del server Orchestrator nel server vRealize Orchestrator integrato eseguendo lo script vro-configure con il comando import.

```
./vro-configure.sh import --skipDatabaseSettings --skipLicense --skipSettings --  
skipSslCertificate --notForceImportPlugins --notRemoveMissingPlugins --skipTrustStore --path  
orchestrator-config-export-orchestrator_appliance_ip-date_hour.zip
```

- 4 Se il server Orchestrator esterno da cui si desidera effettuare la migrazione utilizza il database PostgreSQL integrato, modificare i suoi file di configurazione del database.

- a Nel file /var/vmware/vpostgres/current/pgdata/postgresql.conf, rimuovere il commento per la riga listen\_addresses.
- b Impostare i valori di listen\_addresses su un carattere jolly (\*).

```
listen_addresses = '*'
```

- c Aggiungere una riga al file /var/vmware/vpostgres/current/pgdata/pg\_hba.conf.

```
host all all vra-va-ip-address/32 md5
```

---

**Nota** Il file pg\_hba.conf richiede l'uso di un formato di prefisso CIDR al posto di un indirizzo IP e di una subnet mask.

---

- d Riavviare il servizio del server PostgreSQL.

```
service vpostgres restart
```

- 5 Migrare il database nel database PostgreSQL interno mediante l'esecuzione dello script vro-configure con il comando db-migrate.

```
./vro-configure.sh db-migrate --sourceJdbcUrl JDBC_connection_URL --sourceDbUsername database_user
--sourceDbPassword database_user_password
```

**Nota** Racchiudere tra apici le password contenenti caratteri speciali.

Il valore di *JDBC\_connection\_URL* dipende dal tipo di database utilizzato.

PostgreSQL: `jdbc:postgresql://host:port/database_name`

MSSQL: `jdbc:jtds:sqlserver://host:port/database_name\;` if using SQL authentication and MSSQL: `jdbc:jtds:sqlserver://host:port/database_name\;domain=domain\;useNTLMv2=TRUE` if using Windows authentication.

Oracle: `jdbc:oracle:thin:@host:port:database_name`

Le informazioni di accesso del database predefinite sono:

<i>database_name</i>	vmware
<i>database_user</i>	vmware
<i>database_user_password</i>	vmware

- 6 Se vRealize Automation è stato migrato e non aggiornato, eliminare i certificati Single Sign-On attendibili dal database dell'istanza di Orchestrator incorporata.

```
sudo -u postgres -i -- /opt/vmware/vpostgres/current/bin/psql vcac -c "DELETE FROM vmo_keystore
WHERE id='cakeystore-id';"
```

- 7 Ripristinare la configurazione predefinita dei file `postgresql.conf` e `pg_hba.conf`.

- a Riavviare il servizio del server PostgreSQL.

La migrazione di un'appliance virtuale vRealize Orchestrator 6.x esterna in un'istanza di vRealize Orchestrator incorporata in vRealize Automation 7.4 è stata eseguita correttamente.

### Operazioni successive

Configurare il server vRealize Orchestrator integrato. Vedere [Configurazione del server vRealize Orchestrator integrato](#).

### Configurazione del server vRealize Orchestrator integrato

Dopo aver esportato la configurazione di un server Orchestrator esterno e averla importata in vRealize Automation 7.4, è necessario configurare il server Orchestrator integrato in vRealize Automation.



## Prerequisiti

Migrazione della configurazione dal server vRealize Orchestrator esterno a quello interno.

## Procedura

- 1 Accedere all'Appliance vRealize Automation su SSH come **root**.
- 2 Avviare il servizio Control Center e il servizio del server Orchestrator del server vRealize Orchestrator integrato.

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

- 3 Accedere al servizio Control Center del server Orchestrator integrato come **amministratore**.

---

**Nota** Se si effettua la migrazione da un'istanza di vRealize Orchestrator 7.4 esterna, andare al passaggio 5.

---

- 4 Verificare che Orchestrator sia configurato correttamente nella pagina **Convalida configurazione** in Control Center.
- 5 Se il server Orchestrator esterno è stato configurato per l'utilizzo in modalità cluster, riconfigurare il cluster Orchestrator in vRealize Automation.

- a Passare alla pagina **Orchestrator Cluster Management** avanzata all'indirizzo `https://vra-vr-hostname.domain.name_or_load_balancer_address:8283/vco-controlcenter/#!/control-app/ha?remove-nodes`.

---

**Nota** Se non vengono visualizzate le caselle di controllo **Rimuovi** accanto ai nodi esistenti nel cluster, sarà necessario aggiornare la pagina del browser premendo il pulsante F5 sulla tastiera.

---

- b Selezionare le caselle di controllo accanto ai nodi Orchestrator esterni e fare clic su **Rimuovi** per rimuoverli dal cluster.
- c Per uscire dalla pagina di gestione del cluster avanzata, eliminare la stringa `remove-nodes` dall'URL e aggiornare la pagina del browser premendo il pulsante F5 sulla tastiera.
- d Nella pagina **Convalida configurazione** di Control Center verificare che il server Orchestrator sia configurato correttamente.
- 6 (Facoltativo) Nella scheda **Certificato di firma pacchetto** nella pagina **Certificati**, generare un nuovo certificato di firma del pacchetto.
- 7 (Facoltativo) Modificare i valori per **Tenant predefinito** e **Gruppo Amministratori** nella pagina **Configura provider di autenticazione**.
- 8 Verificare che il servizio `vco-server` sia contrassegnato come REGISTRATO nella scheda **Servizi** nella console di gestione dell'appliance Appliance vRealize Automation.
- 9 Selezionare i servizi `vco` del server Orchestrator esterno e fare clic su **Annulla registrazione**.

## Operazioni successive

- Importare i certificati considerati attendibili dal server Orchestrator esterno nell'archivio Attendibilità del server Orchestrator integrato.
- Unire i nodi di replica di vRealize Automation al cluster di vRealize Automation per sincronizzare la configurazione del server Orchestrator.

Per ulteriori informazioni, vedere la *sezione relativa alla riconfigurazione del server vRealize Orchestrator integrato di destinazione per il supporto dell'alta disponibilità* in *Installazione o aggiornamento di vRealize Automation*.

---

**Nota** Le istanze di vRealize Orchestrator vengono incluse automaticamente nel cluster e sono disponibili per l'utilizzo.

---

- Riavviare il servizio vco-configurator in tutti i nodi del cluster.
- Aggiornare l'endpoint di vRealize Orchestrator in modo che punti al server Orchestrator integrato di cui è stata eseguita la migrazione.
- Aggiungere l'host vRealize Automation e l'host IaaS all'inventario del plug-in vRealize Automation, eseguendo i workflow per l'aggiunta di un host vRA e l'aggiunta dell'host IaaS di un host vRA.

## Aggiornamento di un'appliance vRealize Orchestrator autonoma per l'utilizzo con vRealize Automation

Se si gestisce un'appliance vRealize Orchestrator autonoma per l'utilizzo con vRealize Automation, è necessario aggiornare l'appliance autonoma quando si aggiorna vRealize Automation dalla versione 6.2.5 alla versione 7.4.

Le istanze incorporate di vRealize Orchestrator vengono aggiornate come parte dell'aggiornamento di vRealize Automation appliance. Per un'istanza incorporata non è necessario eseguire altre operazioni.

Se si sta aggiornando un cluster di appliance vRealize Orchestrator, vedere [Aggiornamento di un cluster di appliance vRealize Orchestrator esterno per l'utilizzo con vRealize Automation](#).

## Prerequisiti

- [Installazione dell'aggiornamento su vRealize Automation Appliance](#).
- Aggiornare i componenti IaaS come descritto in [Aggiornamento dei componenti del server IaaS Server dopo l'aggiornamento di vRealize Automation](#).
- Smontare tutti i file system di rete. Vedere *Amministrazione delle macchine virtuali vSphere* nella documentazione di vSphere.
- Aumentare la memoria dell'appliance vSphere Orchestrator fino ad almeno 6 GB. Vedere *Amministrazione delle macchine virtuali vSphere* nella documentazione di vSphere.
- Creare uno snapshot della macchina virtuale vSphere Orchestrator. Vedere *Amministrazione delle macchine virtuali vSphere* nella documentazione di vSphere.
- Se si utilizza un database esterno, eseguirne il backup.

- Se si utilizza il database PostgreSQL preconfigurato in vSphere Orchestrator, eseguire il backup del database utilizzando il menu per l'**esportazione del database** in vSphere Control Center.

#### Procedura

- 1 Utilizzare uno dei metodi descritti nella documentazione per aggiornare l'istanza di vRealize Orchestrator autonoma.
  - [Aggiornamento di Orchestrator Appliance mediante il repository predefinito di VMware.](#)
  - [Aggiornamento di Orchestrator Appliance utilizzando un'immagine ISO.](#)
  - [Aggiornamento di Orchestrator Appliance mediante un repository specificato.](#)
- 2 Da Control Center, aggiornare il plugin NSX di vRealize Automation.

#### Aggiornamento di Orchestrator Appliance mediante il repository predefinito di VMware

È possibile configurare Orchestrator in modo che scarichi il pacchetto di aggiornamento del repository predefinito di VMware.

#### Prerequisiti

- Smontare tutti i file system di rete. Per ulteriori informazioni, vedere la documentazione *Amministrazione delle macchine virtuali vSphere*.
- Aumentare la memoria di Orchestrator Appliance fino ad almeno 6 GB. Per ulteriori informazioni, vedere la documentazione *Amministrazione delle macchine virtuali vSphere*.
- Aumentare le dimensioni del disco della macchina virtuale di vRealize Orchestrator: disco 1 = 7 GB, disco 2 = 10 GB.
- Accertarsi che la partizione radice di Orchestrator Appliance disponga di almeno 3 GB di spazio libero. Per ulteriori informazioni sull'aumento della dimensione di una partizione del disco, vedere KB 1004071: <http://kb.vmware.com/kb/1004071>.
- Creare uno snapshot della macchina virtuale Orchestrator. Per ulteriori informazioni, vedere la documentazione *Amministrazione delle macchine virtuali vSphere*.
- Se si utilizza un database esterno, eseguirne il backup.
- Se si utilizza il database PostgreSQL preconfigurato in Orchestrator, eseguire il backup del database utilizzando il menu per l'**esportazione del database** in Control Center.

#### Procedura

- 1 Passare a VAMI (Virtual Appliance Management Interface) all'indirizzo `https://orchestrator_server:5480` e accedere come **root**.
- 2 Nella scheda **Aggiorna**, fare clic su **Impostazioni**.  
Il pulsante di opzione accanto all'opzione **Usa repository predefinito** è selezionato.
- 3 Nella pagina **Stato**, fare clic su **Verifica aggiornamenti**.
- 4 Se sono disponibili aggiornamenti, fare clic su **Installa aggiornamenti**.

- 5 Accettare l'accordo di licenza con l'utente finale (EULA) di VMware e confermare che si desidera installare l'aggiornamento.
- 6 Per completare l'aggiornamento, riavviare Orchestrator Appliance.
  - a Accedere nuovamente a VAMI come **root**.
- 7 (Facoltativo) Nella scheda **Aggiorna**, verificare che la versione più recente di Orchestrator Appliance sia stata installata correttamente.
- 8 Accedere a Control Center come **root**.
- 9 Se si intende creare un cluster delle istanze di Orchestrator, riconfigurare le impostazioni degli host.
  - a Nella pagina **Impostazioni host** in Control Center fare clic su **MODIFICA**.
  - b Sostituire il nome dell'appliance vRealize Orchestrator con il nome host del server di bilanciamento del carico.
- 10 Riconfigurare l'autenticazione.
  - a Se prima dell'aggiornamento il server Orchestrator è stato configurato per l'utilizzo di **LDAP** o **SSO (legacy)** come metodo di autenticazione, configurare **vSphere** o **vRealize Automation** come provider di autenticazione.
  - b Se l'autenticazione è già impostata su **vSphere** o su **vRealize Automation**, annullare la registrazione delle impostazioni e registrarle nuovamente.

---

**Nota** Se prima dell'aggiornamento, l'Orchestrator ha utilizzato **vSphere** come provider di autenticazione ed è stato configurato per connettersi al nome di dominio completo o all'indirizzo IP di vCenter Server, nel caso in cui si disponga di un Platform Services Controller esterno, dopo l'aggiornamento è necessario configurare Orchestrator per connettersi al nome di dominio completo o all'indirizzo IP dell'istanza di Platform Services Controller che contiene il vCenter Single Sign-On. È inoltre necessario importare manualmente in Orchestrator i certificati di tutti i Platform Services Controller che condividono lo stesso dominio vCenter Single Sign-On.

---

L'aggiornamento di Orchestrator Appliance è stato eseguito correttamente.

### Operazioni successive

Verificare che Orchestrator sia configurato correttamente nella pagina **Convalida configurazione** in Control Center.

### Aggiornamento di Orchestrator Appliance utilizzando un'immagine ISO

È possibile configurare Orchestrator in modo che scarichi il pacchetto di aggiornamento da un file di immagine ISO montata nell'unità CD-ROM dell'appliance.

### Prerequisiti

- Smontare tutti i file system di rete. Per ulteriori informazioni, vedere la documentazione *Amministrazione delle macchine virtuali vSphere*.

- Aumentare la memoria di Orchestrator Appliance fino ad almeno 6 GB. Per ulteriori informazioni, vedere la documentazione *Amministrazione delle macchine virtuali vSphere*.
- Aumentare le dimensioni del disco della macchina virtuale di vRealize Orchestrator: disco 1 = 7 GB, disco 2 = 10 GB.
- Accertarsi che la partizione radice di Orchestrator Appliance disponga di almeno 3 GB di spazio libero. Per ulteriori informazioni sull'aumento della dimensione di una partizione del disco, vedere KB 1004071: <http://kb.vmware.com/kb/1004071>.
- Creare uno snapshot della macchina virtuale Orchestrator. Per ulteriori informazioni, vedere la documentazione *Amministrazione delle macchine virtuali vSphere*.
- Se si utilizza un database esterno, eseguirne il backup.
- Se si utilizza il database PostgreSQL preconfigurato in Orchestrator, eseguire il backup del database utilizzando il menu per l'**esportazione del database** in Control Center.

## Procedura

- 1 Scaricare l'archivio VMware-vRO-Appliance-version-build\_number-updaterepo.iso dal sito di download ufficiale di VMware.
- 2 Connettere l'unità CD-ROM della macchina virtuale Orchestrator Appliance. Per ulteriori informazioni, vedere la documentazione *Amministrazione delle macchine virtuali vSphere*.
- 3 Montare il file di immagine ISO nell'unità CD-ROM dell'appliance. Per ulteriori informazioni, vedere la documentazione *Amministrazione delle macchine virtuali vSphere*.
- 4 Passare a VAMI (Virtual Appliance Management Interface) all'indirizzo [https://orchestrator\\_server:5480](https://orchestrator_server:5480) e accedere come **root**.
- 5 Nella scheda **Aggiorna**, fare clic su **Impostazioni**.
- 6 Selezionare il pulsante di opzione accanto all'opzione **Usa aggiornamenti da CD-ROM**.
- 7 Tornare alla pagina **Stato**.  
Viene visualizzata la versione dell'aggiornamento disponibile.
- 8 Fare clic su **Installa aggiornamenti**.
- 9 Accettare l'accordo di licenza con l'utente finale (EULA) di VMware e confermare che si desidera installare l'aggiornamento.
- 10 Per completare l'aggiornamento, riavviare Orchestrator Appliance.
  - a Accedere nuovamente a VAMI come **root**.
- 11 (Facoltativo) Nella scheda **Aggiorna**, verificare che la versione più recente di Orchestrator Appliance sia stata installata correttamente.
- 12 Accedere a Control Center come **root**.

- 13 Se si intende creare un cluster delle istanze di Orchestrator, riconfigurare le impostazioni degli host.
  - a Nella pagina **Impostazioni host** in Control Center fare clic su **MODIFICA**.
  - b Sostituire il nome dell'appliance vRealize Orchestrator con il nome host del server di bilanciamento del carico.
- 14 Riconfigurare l'autenticazione.
  - a Se prima dell'aggiornamento il server Orchestrator è stato configurato per l'utilizzo di **LDAP** o **SSO (legacy)** come metodo di autenticazione, configurare **vSphere** o **vRealize Automation** come provider di autenticazione.
  - b Se l'autenticazione è già impostata su **vSphere** o su **vRealize Automation**, annullare la registrazione delle impostazioni e registrarle nuovamente.

---

**Nota** Se prima dell'aggiornamento, l'Orchestrator ha utilizzato **vSphere** come provider di autenticazione ed è stato configurato per connettersi al nome di dominio completo o all'indirizzo IP di vCenter Server, nel caso in cui si disponga di un Platform Services Controller esterno, dopo l'aggiornamento è necessario configurare Orchestrator per connettersi al nome di dominio completo o all'indirizzo IP dell'istanza di Platform Services Controller che contiene il vCenter Single Sign-On. È inoltre necessario importare manualmente in Orchestrator i certificati di tutti i Platform Services Controller che condividono lo stesso dominio vCenter Single Sign-On.

---

L'aggiornamento di Orchestrator Appliance è stato eseguito correttamente.

#### Operazioni successive

Verificare che Orchestrator sia configurato correttamente nella pagina **Convalida configurazione** in Control Center.

#### Aggiornamento di Orchestrator Appliance mediante un repository specificato

È possibile configurare Orchestrator in modo che utilizzi un repository locale, in cui è stato caricato l'archivio di aggiornamento.

#### Prerequisiti

- Smontare tutti i file system di rete. Per ulteriori informazioni, vedere la documentazione *Amministrazione delle macchine virtuali vSphere*.
- Aumentare la memoria di Orchestrator Appliance fino ad almeno 6 GB. Per ulteriori informazioni, vedere la documentazione *Amministrazione delle macchine virtuali vSphere*.
- Aumentare le dimensioni del disco della macchina virtuale di vRealize Orchestrator: disco 1 = 7 GB, disco 2 = 10 GB.
- Accertarsi che la partizione radice di Orchestrator Appliance disponga di almeno 3 GB di spazio libero. Per ulteriori informazioni sull'aumento della dimensione di una partizione del disco, vedere KB 1004071: <http://kb.vmware.com/kb/1004071>.
- Creare uno snapshot della macchina virtuale Orchestrator. Per ulteriori informazioni, vedere la documentazione *Amministrazione delle macchine virtuali vSphere*.

- Se si utilizza un database esterno, eseguirne il backup.
- Se si utilizza il database PostgreSQL preconfigurato in Orchestrator, eseguire il backup del database utilizzando il menu per l'**esportazione del database** in Control Center.

## Procedura

- 1 Preparare il repository locale per gli aggiornamenti.
  - a Installare e configurare un server Web locale.
  - b Scaricare l'archivio VMware-vRO-Appliance-version-build\_number-updaterepo.zip dal sito di download ufficiale di VMware.
  - c Estrarre l'archivio .ZIP nel repository locale.
- 2 Passare a VAMI (Virtual Appliance Management Interface) all'indirizzo `https://orchestrator_server:5480` e accedere come **root**.
- 3 Nella scheda **Aggiorna**, fare clic su **Impostazioni**.
- 4 Selezionare il pulsante di opzione accanto all'opzione **Usa repository specificato**.
- 5 Immettere l'indirizzo URL del repository locale puntando alla directory Update\_Repo.  
`http://local_web_server:port/build/mts/release/bora-build_number/publish/exports/Update_Repo`
- 6 Se il repository locale richiede l'autenticazione, immettere nome utente e password.
- 7 Fare clic su **Salva impostazioni**.
- 8 Nella pagina **Stato**, fare clic su **Verifica aggiornamenti**.
- 9 Se sono disponibili aggiornamenti, fare clic su **Installa aggiornamenti**.
- 10 Accettare l'accordo di licenza con l'utente finale (EULA) di VMware e confermare che si desidera installare l'aggiornamento.
- 11 Per completare l'aggiornamento, riavviare Orchestrator Appliance.
  - a Accedere nuovamente a VAMI come **root**.
- 12 (Facoltativo) Nella scheda **Aggiorna**, verificare che la versione più recente di Orchestrator Appliance sia stata installata correttamente.
- 13 Accedere a Control Center come **root**.
- 14 Se si intende creare un cluster delle istanze di Orchestrator, riconfigurare le impostazioni degli host.
  - a Nella pagina **Impostazioni host** in Control Center fare clic su **MODIFICA**.
  - b Sostituire il nome dell'appliance vRealize Orchestrator con il nome host del server di bilanciamento del carico.

**15** Riconfigurare l'autenticazione.

- a Se prima dell'aggiornamento il server Orchestrator è stato configurato per l'utilizzo di **LDAP** o **SSO (legacy)** come metodo di autenticazione, configurare **vSphere** o **vRealize Automation** come provider di autenticazione.
- b Se l'autenticazione è già impostata su **vSphere** o su **vRealize Automation**, annullare la registrazione delle impostazioni e registrarle nuovamente.

---

**Nota** Se prima dell'aggiornamento, l'Orchestrator ha utilizzato **vSphere** come provider di autenticazione ed è stato configurato per connettersi al nome di dominio completo o all'indirizzo IP di vCenter Server, nel caso in cui si disponga di un Platform Services Controller esterno, dopo l'aggiornamento è necessario configurare Orchestrator per connettersi al nome di dominio completo o all'indirizzo IP dell'istanza di Platform Services Controller che contiene il vCenter Single Sign-On. È inoltre necessario importare manualmente in Orchestrator i certificati di tutti i Platform Services Controller che condividono lo stesso dominio vCenter Single Sign-On.

---

L'aggiornamento di Orchestrator Appliance è stato eseguito correttamente.

**Operazioni successive**

Verificare che Orchestrator sia configurato correttamente nella pagina **Convalida configurazione** in Control Center.

**Aggiornamento di un cluster di appliance vRealize Orchestrator esterno per l'utilizzo con vRealize Automation**

Se si utilizza un cluster di appliance vRealize Orchestrator con vRealize Automation, è necessario aggiornare il cluster di appliance Orchestrator alla versione 7.4 aggiornando una singola istanza e unendo i nodi della versione 7.4 appena installata all'istanza aggiornata.

**Prerequisiti**

- [Installazione dell'aggiornamento su vRealize Automation Appliance.](#)
- Aggiornare i componenti di IaaS. Vedere [Aggiornamento dei componenti del server IaaS Server dopo l'aggiornamento di vRealize Automation.](#)
- Configurare un bilanciamento del carico per distribuire il traffico tra più istanze di vRealize Orchestrator. Vedere la [guida alla configurazione del bilanciamento del carico di vRealize Orchestrator.](#)
- Creare uno snapshot di tutti i nodi del server vRealize Orchestrator.
- Eseguire il backup del database condiviso di vRealize Orchestrator.

**Procedura**

- 1 Da Control Center, aggiornare il plugin NSX di vRealize Automation.
- 2 Arrestare i servizi di Orchestrator vco-server e vco-configurator in tutti i nodi del cluster.



- 3 Aggiornare una sola istanza del server Orchestrator nel cluster utilizzando una delle procedure documentate.
- 4 Distribuire una nuova appliance Orchestrator nella versione 7.4.
  - a Configurare il nuovo nodo con le impostazioni di rete di un'istanza esistente non aggiornata che fa parte del cluster.
- 5 Accedere a Control Center del secondo nodo per avviare la configurazione guidata.
  - a Passare a `https://your_orchestrator_server_IP_or_DNS_name:8283/vco-controlcenter`.
  - b Accedere come **root** utilizzando la password immessa durante la distribuzione di OVA.
- 6 Selezionare il tipo di distribuzione **Orchestrator in cluster**.

Selezionando questo tipo, si sceglie di unire il nodo a un cluster Orchestrator esistente.
- 7 Nella casella di testo **Nome host**, immettere il nome host o l'indirizzo IP della prima istanza del server Orchestrator.

---

**Nota** Deve essere l'IP o il nome host locale dell'istanza di Orchestrator a cui unire il secondo nodo. Non utilizzare l'indirizzo del bilanciamento del carico.

---

- 8 Nelle caselle di testo **Nome utente** e **Password**, immettere le credenziali di root della prima istanza del server Orchestrator.
- 9 Fare clic su **Unisci**. L'istanza di Orchestrator clona la configurazione del nodo a cui si unisce.

Il servizio del server Orchestrator di entrambi i nodi viene riavviato automaticamente.
- 10 Accedere a Control Center del cluster Orchestrator aggiornato mediante l'indirizzo del bilanciamento del carico e accedere come **amministratore**.
- 11 Nella pagina **Gestione cluster Orchestrator** verificare che la stringa dell'**impronta digitale della configurazione attiva** corrisponda a quella dell'**impronta digitale della configurazione in sospeso** in tutti i nodi del cluster.

---

**Nota** Potrebbe essere necessario aggiornare la pagina più volte fino a quando le due stringhe non corrispondono.

---

- 12 Verificare che il cluster vRealize Orchestrator sia configurato in modo appropriato aprendo la pagina **Convalida configurazione** in Control Center.
- 13 (Facoltativo) Ripetere i passaggi da 3 a 8 per ogni nodo aggiuntivo nel cluster.
- 14 Da Control Center, aggiornare il plugin NSX di vRealize Automation.

Il cluster di Orchestrator è stato aggiornato.

#### Operazioni successive

[Attivare i bilanciamenti del carico.](#)

## Aggiunta di utenti o gruppi a una connessione Active Directory

È possibile aggiungere utenti o gruppi a una connessione Active Directory esistente.

Il sistema di autenticazione utenti di Gestione directory importa i dati da Active Directory quando vengono aggiunti gruppi e utenti. La velocità del trasporto dei dati dipende dai limiti di capacità di Active Directory. Questa operazione può quindi richiedere molto tempo, in base al numero di gruppi e utenti aggiunti. Per ridurre al minimo i problemi, aggiungere solo i gruppi e gli utenti necessari per un'azione di vRealize Automation. In caso di problemi, chiudere le applicazioni non necessarie e verificare che nella distribuzione sia stata allocata memoria sufficiente ad Active Directory. Se i problemi persistono, aumentare la quantità di memoria allocata ad Active Directory. Per le distribuzioni con un elevato numero di utenti e gruppi, potrebbe essere necessario allocare fino a 24 GB di memoria ad Active Directory.

Quando viene sincronizzata una distribuzione di vRealize Automation con molti utenti e gruppi, è possibile che si verifichi un ritardo prima che i dettagli del registro risultino disponibili. Il timestamp nel file di registro può essere diverso dall'orario completo visualizzato nella console.

Se i membri di un gruppo non sono presenti nell'elenco Utenti, quando si aggiunge il gruppo da Active Directory, tali membri vengono aggiunti all'elenco. Quando si sincronizza un gruppo, gli utenti che non hanno Utenti del dominio come gruppo primario in Active Directory non vengono sincronizzati.

---

**Nota** Una volta avviata l'operazione di sincronizzazione, non è possibile annullarla.

---

### Prerequisiti

- Connettore installato e codice di attivazione attivato. Selezionare gli attributi predefiniti obbligatori e aggiungere ulteriori attributi nella pagina Attributi utente.  
  
Vedere [PLUGINS\\_ROOT/com.vmware.vra.prepare.use.doc/GUID-9B25F502-EC8C-40CF-8ACF-4731B5A6903A.html](https://docs.vmware.com/en/VMware-vRealize-Automation/7.0/Plugins/com.vmware.vra.prepare.use.doc/GUID-9B25F502-EC8C-40CF-8ACF-4731B5A6903A.html).
- Elenco di gruppi e utenti Active Directory da sincronizzare da Active Directory.
- Per Active Directory su LDAP, le informazioni obbligatorie includono DN di base, DN di binding e password del DN di binding.
- Per l'autenticazione integrata di Windows in Active Directory, le informazioni obbligatorie sono l'indirizzo UPN dell'utente di binding del dominio e la relativa password.
- Se si accede ad Active Directory su SSL, è necessaria una copia del certificato SSL.
- Se si dispone di un'istanza di Active Directory a più foreste integrata con l'autenticazione di Windows e il gruppo locale di dominio contiene membri di foreste diverse, eseguire le operazioni seguenti. Aggiungere l'utente di binding al gruppo Amministratori del gruppo locale di dominio. In caso contrario, tali membri risulteranno mancanti dal gruppo locale di dominio.
- Accedere a vRealize Automation come **amministratore tenant**.

### Procedura

- 1 Selezionare **Amministrazione > Gestione directory > Directory**.

- 2 Fare clic sul nome della directory desiderata.
- 3 Fare clic su **Impostazioni di sincronizzazione** per aprire la finestra di dialogo contenente le opzioni di sincronizzazione.
- 4 Fare clic sull'icona appropriata per modificare la configurazione di utenti o gruppi.

Per modificare la configurazione di gruppi:

- Per aggiungere gruppi, fare clic sull'icona **+** per aggiungere una riga per le definizioni DN del gruppo e inserire il DN del gruppo appropriato.
- Per eliminare la definizione DN di un gruppo, fare clic sull'icona **x** corrispondente.

Per modificare la configurazione di utenti:

- ◆ Per aggiungere utenti, fare clic sull'icona **+** per aggiungere una riga per la definizione DN di un utente e inserire il DN dell'utente appropriato.

Per eliminare la definizione DN di un utente, fare clic sull'icona **x** corrispondente.

- 5 Fare clic su **Salva** per salvare le modifiche senza sincronizzare immediatamente gli aggiornamenti. Fare clic su **Salva e sincronizza** per salvare le modifiche e sincronizzare immediatamente gli aggiornamenti.

## Attivare i bilanciamenti del carico

Se la distribuzione utilizza bilanciamenti del carico, riabilitare i nodi secondari e i controlli di integrità e ripristinare le impostazioni del timeout dei bilanciamenti del carico.

I controlli di integrità per vRealize Automation variano in base alla versione. Per informazioni, consultare *Guida alla configurazione del bilanciamento del carico di vRealize Automation* nella [Documentazione di VMware vRealize Automation](#).

Ripristinare il valore predefinito delle impostazioni del timeout dei bilanciamenti del carico il cui valore è 10 minuti.

## Attività successive all'aggiornamento di vRealize Automation

Dopo aver aggiornato vRealize Automation 6.2.5 alla versione 7.4, eseguire le attività successive all'aggiornamento necessarie.

### Configurazione della porta per distribuzioni ad alta disponibilità

Dopo aver completato un aggiornamento in una distribuzione ad alta disponibilità, è necessario configurare il bilanciamento del carico per consentire il passaggio del traffico dalla porta 8444 verso l'appliance vRealize Automation per il supporto delle funzionalità della console remota.

Per ulteriori informazioni, consultare *Guida alla configurazione del bilanciamento del carico di vRealize Automation* nella [Documentazione di vRealize Automation](#).

## Riconfigurazione del vRealize Orchestrator incorporato per il supporto dell'alta disponibilità

Per una distribuzione ad alta disponibilità, è necessario ricongiungere manualmente ogni appliance vRealize Automation di replica target al cluster per abilitare il supporto dell'alta disponibilità per il componente vRealize Orchestrator incorporato.

### Prerequisiti

Accedere alla console di gestione dell'appliance vRealize Automation di replica target.

- 1 Avviare un browser e aprire la console di gestione dell'appliance vRealize Automation di replica target utilizzando il nome di dominio completo (FQDN) dell'appliance virtuale di replica target: `https://vra-va-hostname.domain.name:5480`.
- 2 Accedere con il nome utente **root** e la password impostata quando è stata effettuata la distribuzione dell'appliance vRealize Automation di replica target.

### Procedura

- 1 Selezionare **Impostazioni vRA > Cluster**.
- 2 Nella casella di testo **Nodo di cluster iniziale**, immettere il nome di dominio completo dell'appliance vRealize Automation master target.
- 3 Immettere la password root nella casella di testo **Password**.
- 4 Fare clic su **Unisci cluster**.  
  
Continuare indipendentemente dall'eventuale visualizzazione di avvisi sui certificati. Il sistema riavvia i servizi per il cluster.
- 5 Verificare che i servizi siano in esecuzione.
  - a Nella barra delle schede in alto fare clic su **Servizi**.
  - b Fare clic su **Aggiorna** per monitorare lo stato di avanzamento dell'avvio dei servizi.

### Abilitazione dell'azione Connetti a console remota per i clienti

L'azione della console remota per i clienti è supportata per le appliance il cui provisioning viene eseguito da vSphere in vRealize Automation.

Modificare il blueprint dopo aver aggiornato la versione e selezionare l'azione **Connetti a console remota** nella scheda **Azione**.

Per ulteriori informazioni, consultare l'[articolo 2109706 della Knowledge Base](#).

### Ripristino dei file di timeout del workflow esterno

È necessario riconfigurare i file di timeout del workflow esterno di vRealize Automation perché il processo di aggiornamento sovrascrive i file xmldb.

### Procedura

- 1 Aprire i file di configurazione (xmldb) workflow esterni sul sistema dalla directory seguente.  
`\\VMware\\vCAC\\Server\\ExternalWorkflows\\xmldb\\`.

- 2 Sostituire i file xmldb con i file di cui è stato eseguito il backup prima della migrazione. Se non si dispone dei file di backup, riconfigurare le impostazioni di timeout del workflow esterno.
- 3 Salvare le impostazioni.

### Verifica della disponibilità del servizio vRealize Orchestrator

Dopo aver eseguito l'aggiornamento all'ultima versione di vRealize Automation, è necessario verificare il collegamento tra vRealize Automation e vRealize Orchestrator. A volte è necessario ripristinare la connessione dopo l'aggiornamento.

#### Prerequisiti

Accedere all'interfaccia di configurazione di vRealize Orchestrator.

#### Procedura

- 1 Fare clic su **Convalida configurazione**.
- 2 Se nella sezione Autenticazione è presente il segno di spunta verde, saltare al passaggio 5.
- 3 Se la sezione Autenticazione non ha il segno di spunta verde, attenersi ai passaggi seguenti per ripristinare la connessione a vRealize Orchestrator.
  - a Fare clic su **Home**.
  - b Fare clic su **Configura provider autenticazione**.
  - c Nella casella di testo **Gruppo Admin**, selezionare **Cambia** e scegliere un nuovo gruppo Admin che possa essere correttamente risolto.

Il gruppo vcoadmins è disponibile solo al tenant vsphere.local predefinito. Se si utilizza un altro tenant per vRealize Orchestrator, è necessario selezionare un altro gruppo.
  - d Fare clic su **Salva modifiche** e, se richiesto, riavviare il server vRealize Orchestrator.
  - e Fare clic su **Home**.
- 4 Ripetere il passaggio 1 per verificare che sulla sezione Autenticazione sia ancora presente il segno di spunta verde.
- 5 Fare clic su **Home** e chiudere vRealize Orchestrator Control Center.

### Riconfigurazione dell'endpoint dell'infrastruttura vRealize Orchestrator incorporata nel componente vRealize Automation target

Quando si esegue la migrazione da un ambiente vRealize Automation 6.2.x, è necessario aggiornare l'URL dell'endpoint dell'infrastruttura che punta al server vRealize Orchestrator target incorporato.

#### Prerequisiti

- Effettuare la migrazione a vRealize Automation 7.4 correttamente.
- Accedere alla console di vRealize Automation di destinazione.
  - a Aprire la console di vRealize Automation utilizzando il nome di dominio completo dell'appliance virtuale di destinazione: `https://vra-va-hostname.domain.name/vcac`.

Per un ambiente ad alta disponibilità, aprire la console utilizzando il nome di dominio completo del bilanciamento del carico dell'appliance virtuale di destinazione: `https://vra-vb-hostname.domain.name/vcac`.

- b Accedere come utente amministratore laaS.

#### Procedura

- 1 Selezionare **Infrastruttura > Endpoint > Endpoint**.
- 2 Nella pagina Endpoint selezionare l'endpoint vRealize Orchestrator e fare clic su **Modifica**.
- 3 Nella casella di testo Indirizzo modificare l'URL dell'endpoint vRealize Orchestrator.
  - Se è stata effettuata la migrazione a un ambiente minimo, sostituire l'URL dell'endpoint vRealize Orchestrator con `https://vra-vb-hostname.domain.name:443/vco`.
  - Se è stata effettuata la migrazione a un ambiente ad alta disponibilità, sostituire l'URL dell'endpoint vRealize Orchestrator con `https://vra-vb-lb-hostname.domain.name:443/vco`.
- 4 Fare clic su **OK**.
- 5 Eseguire manualmente una raccolta dati sull'endpoint vRealize Orchestrator.
  - a Nella pagina Endpoint, selezionare l'endpoint vRealize Orchestrator.
  - b Selezionare **Azioni > Raccolta dati**.

Verificare la corretta esecuzione della raccolta dati.

#### Ripristino delle modifiche di registrazione nel file `app.config`

Il processo di aggiornamento sovrascrive le modifiche apportate durante la registrazione nei file di configurazione. Al termine dell'aggiornamento, è necessario ripristinare le eventuali modifiche apportate al file `app.config` prima dell'aggiornamento.

#### Abilitazione del failover automatico del servizio di gestione dopo l'aggiornamento

Per impostazione predefinita, il failover automatico del servizio di gestione è disabilitato quando si esegue l'aggiornamento di vRealize Automation.

Per abilitare il servizio di gestione automatico dopo l'aggiornamento, completare la procedura che segue.

#### Procedura

- 1 Aprire un prompt dei comandi come root nell'appliance vRealize Automation.
- 2 Modificare le directory in `/usr/lib/vcac/tools/vami/commands`.
- 3 Per abilitare il failover automatico del servizio di gestione, eseguire il comando che segue.
 

```
python ./manager-service-automatic-failover ENABLE
```

Per disabilitare il failover automatico all'interno di una distribuzione IaaS, eseguire il comando che segue.

```
python ./manager-service-automatic-failover DISABLE
```

### Informazioni sul failover automatico del servizio di gestione

È possibile configurare il servizio di gestione IaaS di vRealize Automation per il failover automatico in un backup in caso di arresto del servizio di gestione primario.

A partire da vRealize Automation 7.3, non è più necessario avviare o arrestare manualmente il servizio di gestione su ciascun server Windows per scegliere quale utilizzare come servizio primario o di backup. Il failover automatico del servizio di gestione è disattivato per impostazione predefinita quando si aggiorna IaaS utilizzando lo script della shell di aggiornamento o il file eseguibile del programma di installazione di IaaS.

Quando è attivato il failover automatico, il servizio di gestione viene avviato automaticamente in tutti gli host del servizio di gestione, inclusi i backup. La funzionalità di failover automatico consente agli host di monitorarsi a vicenda in modo trasparente e di eseguire il failover quando necessario, ma è necessario che il servizio Windows sia in esecuzione in tutti gli host.

---

**Nota** Non è richiesto l'uso del failover automatico. È infatti possibile disattivarlo e continuare ad avviare e arrestare manualmente il servizio Windows per scegliere quale host utilizzare come primario o di backup. Se si segue l'approccio del failover manuale, è necessario avviare il servizio su un solo host alla volta. Con la disattivazione del failover automatico, l'esecuzione simultanea del servizio in più server IaaS non consente di utilizzare vRealize Automation.

---

Evitare di attivare o disattivare il failover in modo selettivo. È necessario che il failover automatico venga sempre sincronizzato come attivo o disattivo attraverso ogni host del servizio di gestione in una distribuzione IaaS.

### Esecuzione di Prova connessione e verifica degli endpoint aggiornati

L'aggiornamento da vRealize Automation 7.3 o versioni precedenti alla versione 7.4 apporta modifiche agli endpoint nell'ambiente di destinazione.

Dopo aver effettuato l'aggiornamento a vRealize Automation 7.4, è necessario utilizzare l'azione **Prova connessione** per tutti gli endpoint applicabili. Potrebbe anche essere necessario apportare modifiche ad alcuni endpoint aggiornati. Per ulteriori informazioni, vedere [Considerazioni sull'utilizzo degli endpoint aggiornati o migrati](#).

L'impostazione di sicurezza predefinita per gli endpoint aggiornati o migrati prevede che i certificati non attendibili non vengano accettati.

Dopo l'aggiornamento o la migrazione da un'installazione precedente di vRealize Automation, se venivano utilizzati certificati non attendibili, è necessario eseguire la procedura che segue per tutti gli endpoint vSphere e NSX per consentire la convalida dei certificati. In caso contrario, le operazioni sugli endpoint non riusciranno e verranno restituiti errori di certificato. Per ulteriori informazioni, vedere gli

articoli della Knowledge Base di VMware *Endpoint communication is broken after upgrade to vRA 7.3* (2150230) all'indirizzo <http://kb.vmware.com/kb/2150230> e *How to download and install vCenter Server root certificates to avoid Web Browser certificate warnings* (2108294) all'indirizzo <http://kb.vmware.com/kb/2108294>.

- 1 Dopo l'aggiornamento o la migrazione, accedere alla macchina dell'agente vRealize Automation vSphere e riavviare gli agenti vSphere utilizzando la scheda **Servizi**.

La migrazione potrebbe non riavviare tutti gli agenti, pertanto è necessario riavviarli manualmente se richiesto.

- 2 Attendere il completamento di almeno un report di ping. Questa operazione richiede uno o due minuti.
- 3 Dopo che gli agenti vSphere avranno avviato la raccolta dati, accedere a vRealize Automation come amministratore IaaS.
- 4 Fare clic su **Infrastruttura > Endpoint > Endpoint**.
- 5 Modificare un endpoint vSphere e fare clic su **Prova connessione**.
- 6 Se viene visualizzato un prompt sul certificato, fare clic su **OK** per accettare il certificato.  
  
In caso contrario, è possibile che al momento il certificato sia correttamente archiviato presso un'autorità root attendibile del servizio di hosting della macchina Windows per l'endpoint, ad esempio come macchina agente proxy o come macchina DEM.
- 7 Fare clic su **OK** per accettare il certificato e salvare l'endpoint.
- 8 Ripetere questa procedura per ogni endpoint vSphere.
- 9 Ripetere questa procedura per ogni endpoint NSX.

Se l'azione **Prova connessione** riesce ma alcune operazioni di provisioning o di raccolta dati hanno esito negativo, è possibile installare lo stesso certificato in tutte le macchine agente che servono l'endpoint e su tutte le macchine DEM. In alternativa, è possibile disinstallare il certificato dalle macchine esistenti e ripetere la procedura precedente per l'endpoint in cui si verifica l'errore.

### Importazione del plug-in DynamicTypes

Se si utilizza il plug-in DynamicTypes e si esporta la configurazione come pacchetto prima dell'aggiornamento, è necessario importare il workflow seguente:

```
/Library/Dynamic Types/Configuration/Import Configuration From Package
```

Nel client Java di vRealize Orchestrator viene eseguito il comando `/Library`.

### Risoluzione dei problemi relativi all'aggiornamento di vRealize Automation

Gli argomenti che riguardano la risoluzione dei problemi relativi all'aggiornamento includono soluzioni ai problemi che possono verificarsi durante l'aggiornamento di vRealize Automation 6.2.5 alla versione 7.4.



## **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.
- 2 Eseguire nuovamente l'installazione o l'aggiornamento.

## **Aggiornamento non riuscito per il componente sito Web di IaaS**

L'aggiornamento di IaaS non riesce ed è impossibile continuare l'operazione.

### **Problema**

L'aggiornamento di IaaS non riesce per il componente sito Web. Il file di registro del programma di installazione include i seguenti messaggi di errore.

- System.Data.Services.Client.DataServiceQueryException:  
An error occurred while processing this request. --->  
System.Data.Services.Client.DataServiceClientException: <!DOCTYPE html>
- **Description:** An application error  
occurred on the server. The current custom error settings for this application  
prevent the details of the application error from being viewed remotely (for  
security reasons). It could, however, be viewed by browsers running on the  
local server machine.
- Warning: Non-zero return code. Command failed.
- Done Building Project "C:\Program Files  
(x86)\VMware\VCAC\Server\Model Manager Data\DeployRepository.xml"  
(InstallRepoModel target(s)) -- FAILED.

Il file di registro del repository include i seguenti messaggi di errore.

- [Error]: [sub-thread-Id="20"  
context="" token=""] Failed to start repository service. Reason:  
System.InvalidOperationException: Configuration section encryptionKey is not  
protected  
at  
DynamicOps.Common.Utils.EncryptionHelpers.ReadKeyFromConfiguration(Configuration  
config)  
at DynamicOps.Common.Utils.EncryptionHelpers.Decrypt(String value)  
at DynamicOps.Repository.Runtime.CoreModel.GlobalPropertyItem.Decrypt(Func`2  
decryptFunc)  
at  
DynamicOps.Common.Entity.ContextHelpers.OnObjectMaterializedCallbackEncryptable(Object  
sender, ObjectMaterializedEventArgs e)  
at  
System.Data.Common.Internal.Materialization.Shaper.RaiseMaterializedEvents()  
at  
System.Data.Common.Internal.Materialization.Shaper`1.SimpleEnumerator.MoveNext()  
at System.Linq.Enumerable.FirstOrDefault[TSource](IEnumerable`1 source)  
at System.Linq.Queryable.FirstOrDefault[TSource](IQueryable`1 source)  
at  
DynamicOps.Repository.Runtime.Common.GlobalPropertyHelper.GetGlobalPropertyItemValue(Core  
ModelEntities  
coreModelContext, String propertyName, Boolean throwIfPropertyNotFound)  
at  
DynamicOps.Repository.Runtime.CafeClientAbstractFactory.LoadSolutionUserCertificate()  
at  
DynamicOps.Repository.Runtime.CafeClientAbstractFactory.InitializeFromDb(String  
coreModelConnectionString)  
at DynamicOps.Repository.Runtime.Common.RepositoryRuntime.Initialize().

### Causa

L'aggiornamento di IaaS non riesce quando la data di creazione del file `web.config` coincide o è successiva alla data di modifica.

### Soluzione

- 1 Nell'host IaaS, accedere a Windows.
- 2 Aprire il prompt dei comandi di Windows.
- 3 Passare alla cartella di installazione di vRealize Automation.
- 4 Avviare l'editor di test preferito con l'opzione **Esegui come amministratore**.
- 5 Individuare e selezionare il file `web.config` e salvarlo per modificare la data dell'ultima modifica.
- 6 Esaminare le proprietà del file `web.config` per verificare che la data di modifica del file sia successiva alla data di creazione.
- 7 Aggiornare IaaS.

### Errore di esecuzione del servizio di gestione a causa di errori di convalida SSL durante il runtime

Si verificano errori nel servizio di gestione a causa di errori di convalida SSL.

### Problema

Nel file registro del servizio di gestione viene visualizzato il messaggio di errore seguente:

```
[Info]: Thread-Id="6" - context="" token="" Connessione non riuscita al database core. Verrà effettuato un nuovo tentativo in 00:00:05. Dettagli dell'errore: è stata correttamente stabilita una connessione con il server, ma si è verificato successivamente un errore durante il processo di accesso. (provider: Provider SSL, errore: 0 - La catena di certificati è stata rilasciata da un'autorità non attendibile.)
```

### Causa

Durante il runtime, si verificano errori nel servizio di gestione a causa di errori di convalida SSL.

### Soluzione

- 1 Aprire il file di configurazione `ManagerService.config`.
- 2 Aggiornare **Encrypt=False** nella riga seguente:  

```
<add name="vcac-repository" providerName="System.Data.SqlClient"
connectionString="Data Source=iaas-db.sqa.local;Initial Catalog=vcac;Integrated
Security=True;Pooling=True;Max Pool
Size=200;MultipleActiveResultSets=True;Connect Timeout=200, Encrypt=True" />
```

### L'accesso non riesce dopo l'aggiornamento

È necessario chiudere il browser e accedere nuovamente dopo un aggiornamento per sessioni che utilizzano account utente sincronizzati.

### Problema

Dopo aver eseguito l'aggiornamento di vRealize Automation, il sistema nega l'accesso agli account utente non sincronizzati quando eseguono l'accesso.

### Soluzione

Chiudere il browser ed eseguire nuovamente vRealize Automation.

### Gli elementi del catalogo vengono visualizzati nel catalogo dei servizi dopo l'aggiornamento, ma non sono disponibili per la richiesta

Gli elementi del catalogo che utilizzano determinate definizioni delle proprietà dalle versioni precedenti vengono visualizzati nel catalogo dei servizi, ma non sono disponibili per la richiesta dopo l'aggiornamento alla versione più recente di vRealize Automation.

### Problema

Se si effettua l'aggiornamento dalla versione 6.2.x o una versione precedente e si dispone di definizioni delle proprietà con i tipi di controllo o attributi indicati di seguito, gli attributi non saranno presenti nelle definizioni delle proprietà e tutti gli elementi del catalogo che utilizzano le definizioni non funzioneranno come prima dell'aggiornamento.

- Tipi di controllo. Casella di controllo o collegamento.
- Attributi. Relazione, espressioni regolari o layout delle proprietà.

### Causa

In vRealize Automation 7.0 e versioni successive le definizioni delle proprietà non utilizzano più gli attributi. È necessario ricreare la definizione della proprietà o configurarla in modo che utilizzi un'azione di script di vRealize Orchestrator anziché i tipi di controllo o gli attributi incorporati.

Eseguire la migrazione del tipo di controllo o degli attributi a vRealize Automation 7.x utilizzando un'azione di script.

### Soluzione

- 1 In vRealize Orchestrator creare un'azione di script che restituisca i valori delle proprietà. L'azione deve restituire un tipo semplice. Ad esempio, stringhe di ritorno, numeri interi o altri tipi supportati. L'azione può acquisire le altre proprietà da cui dipende come parametro di input.
- 2 Nella console di vRealize Automation configurare la definizione del prodotto.
  - a Selezionare **Amministrazione > Dizionario proprietà > Definizioni proprietà**.
  - b Selezionare la definizione della proprietà e fare clic su **Modifica**.
  - c Dal menu a discesa Visualizza consiglio selezionare **Elenco a discesa**.
  - d Dal menu a discesa Valori, selezionare **Valori esterni**.
  - e Selezionare l'azione di script.
  - f Fare clic su **OK**.

- g Configurare i parametri di input che vengono inclusi nell'azione di script. Per mantenere la relazione esistente, effettuare il binding del parametro all'altra proprietà.
- h Fare clic su **OK**.

### **Unione non riuscita del database esterno PostgreSQL**

L'unione del database PostgreSQL esterno con il database PostgreSQL incorporato non viene eseguita.

#### **Problema**

Se la versione del database PostgreSQL esterno è successiva a quella del database PostgreSQL incorporato, l'unione non avviene.

#### **Soluzione**

1 Accedere all'host per il database PostgreSQL esterno.

2 Eseguire il comando `psql --version`.

Annotare la versione di PostgreSQL per il database esterno.

3 Accedere all'host per il database PostgreSQL incorporato.

4 Eseguire il comando `psql --version`.

Annotare la versione di PostgreSQL per il database incorporato.

Se la versione del PostgreSQL esterno è successiva a quella del PostgreSQL incorporato, contattare l'assistenza per ricevere aiuto sull'unione del database PostgreSQL esterno.

### **Il comando Unisci cluster sembra non avere esito positivo dopo aver aggiornato un ambiente ad alta disponibilità**

Dopo aver fatto clic su **Unisci cluster** nella console di gestione di un nodo di cluster secondario, scompare l'indicatore di avanzamento.

#### **Problema**

Quando si utilizza la console di gestione dell'appliance vRealize Automation dopo l'aggiornamento per unire un nodo di cluster secondario al nodo primario, l'indicatore di avanzamento scompare e non viene visualizzato alcun messaggio di errore o di corretta esecuzione. Questo problema si verifica in modo intermittente.

#### **Causa**

L'indicatore di avanzamento scompare perché alcuni browser smettono di attendere una risposta dal server. Questo funzionamento non arresta il processo di unione dei cluster. È possibile confermare che il processo di unione dei cluster ha avuto esito positivo visualizzando il file di registro in `/var/log/vmware/vcac/vcac-config.log`.

### **Aggiornamento non riuscito se la partizione root non dispone di sufficiente spazio libero**

Se non è disponibile sufficiente spazio libero nella partizione root dell'host dell'appliance di vRealize Automation, non si può procedere all'aggiornamento.

## Soluzione

Questa procedura aumenta lo spazio libero nella partizione root del Disco 1 dell'host dell'appliance di vRealize Automation. In una distribuzione distribuita, eseguire questa procedura per aumentare lo spazio libero in ogni nodo di replica in modo sequenziale, quindi aumentare lo spazio libero del nodo master.

**Nota** Durante l'esecuzione della procedura, è possibile che vengano visualizzati i seguenti messaggi di avviso:

- `WARNING: Re-reading the partition table failed with error 16:  
Device or resource busy. The kernel still uses the old table. The  
new table will be used at the next reboot or after you run  
partprobe(8) or kpartx(8) Syncing disks.`
- `Error: Partition(s) 1 on /dev/sda have been written, but we have been unable to inform the kernel  
of the change, probably because it/they are in use. As a result, the old partition(s) will remain  
in use. You should reboot now before making further changes.`

Ignorare il messaggio che avvisa di riavviare subito il sistema prima di effettuare ulteriori modifiche. Se il sistema viene riavviato prima del passaggio 10, il processo di aggiornamento viene danneggiato.

### Procedura

- 1 Accendere la macchina virtuale host dell'appliance di vRealize Automation e accedere con connessione shell protetta come utente root.
- 2 Eseguire questi comandi per arrestare i servizi.
  - a `service vcac-server stop`
  - b `service vco-server stop`
  - c `service vpostgres stop`
- 3 Eseguire questi comandi per smontare la partizione di swap.
 

```
swapoff -a
```
- 4 Eseguire questi comandi per eliminare le partizioni esistenti del disco 1 e creare una partizione root da 44 GB e una partizione di swap da 6 GB:
 

```
(echo d; echo 2; echo d; echo 1; echo n; echo p; echo ; echo ; echo '+44G';  
echo n; echo p; echo ; echo ; echo ; echo w; echo p; echo q) | fdisk /dev/sda
```
- 5 Eseguire questi comandi per cambiare il tipo di partizione di scambio.
 

```
(echo t; echo 2; echo 82; echo w; echo p; echo q) | fdisk /dev/sda
```
- 6 Eseguire questi comandi per impostare il flag avviabile del disco 1.
 

```
(echo a; echo 1; echo w; echo p; echo q) | fdisk /dev/sda
```

- 7 Eseguire questi comandi per registrare le modifiche di partizione con il kernel Linux.

```
partprobe
```

Se viene visualizzato un avviso che richiede il riavvio del sistema prima di effettuare ulteriori modifiche, ignorare il messaggio. Il riavvio del sistema prima del passaggio 10 danneggia il processo di aggiornamento.

- 8 Eseguire questi comandi per formattare la nuova partizione di swap.

```
mkswap /dev/sda2
```

- 9 Eseguire questi comandi per montare la partizione di swap.

```
swapon -a
```

- 10 Riavviare l'appliance vRealize Automation.

- 11 Dopo il riavvio dell'appliance, eseguire questo comando per ridimensionare la tabella di partizione del disco 1.

```
resize2fs /dev/sda1
```

- 12 Per verificare che l'espansione del disco sia corretta, eseguire `df -h` e controllare che lo spazio disponibile su disco in `/dev/sda1` superi 30 GB.

### Le copie di backup dei file .xml causano il timeout del sistema

vRealize Automation registra qualsiasi file con un'estensione .xml nella directory `\VMware\vmCAC\Server\External\Workflows\xml\`. Se questa directory contiene file di backup con un'estensione .xml, il sistema esegue workflow duplicati che causano il timeout del sistema.

#### Soluzione

Soluzione: quando si esegue il backup dei file in questa directory, spostare i backup in un'altra directory oppure modificare l'estensione del file di backup in un'estensione diversa da .xml.

### Eliminazione di nodi orfani in vRealize Automation

Un nodo orfano è un nodo duplicato che viene segnalato nell'host ma non esiste nell'host.

#### Problema

Quando si verifica se tutti i nodi IaaS e dell'appliance virtuale sono integri, è possibile scoprire che un host ha uno o più nodi orfani. Tutti i nodi orfani devono essere eliminati.

#### Soluzione

- 1 Nell'appliance vRealize Automation primaria, accedere alla gestione dell'appliance di vRealize Automation come **root** utilizzando la password immessa durante la distribuzione dell'appliance vRealize Automation.
- 2 Selezionare **Impostazioni vRA > Cluster**.
- 3 Per ogni nodo orfano nella tabella, fare clic su **Elimina**.

## Impossibile creare una nuova directory in vRealize Automation

Il tentativo di aggiungere una nuova directory con il primo connettore di sincronizzazione non riesce.

### Problema

Questo problema si verifica a causa di un `config-state.json` file errato ubicato in `usr/local/horizon/conf/states/VSPHERE.LOCAL/3001/`.

Per ulteriori informazioni sulla risoluzione di questo problema, vedere l'[articolo della Knowledge Base 2145438](#).

## Per alcune macchine virtuali non viene creata una distribuzione durante l'aggiornamento

Per le macchine virtuali il cui stato al momento dell'aggiornamento risulta mancante non viene creata una distribuzione corrispondente nell'ambiente target.

### Problema

Se durante l'aggiornamento lo stato di una macchina virtuale risulta mancante nell'ambiente di origine, nell'ambiente target non viene creata una distribuzione corrispondente. Se dopo l'aggiornamento lo stato di una macchina virtuale non risulta più mancante, è possibile importare la macchina nella distribuzione target utilizzando l'importazione di massa.

## Errore di certificato non attendibile

Quando viene visualizzata la pagina Visualizzatore registro dell'infrastruttura nella console Appliance vRealize Automation, è possibile che venga visualizzato un report di errore di connessione dell'endpoint contenente la frase seguente: `Certificate is not trusted`.

### Problema

Nella console Appliance vRealize Automation, selezionare **Infrastruttura > Monitoraggio > Registro**. Nella pagina Visualizzatore registro, è possibile che venga visualizzato un report simile al seguente:

Connessione all'endpoint non riuscita. Per convalidare la possibilità di stabilire una connessione protetta a questo endpoint, andare all'endpoint vSphere nella pagina Endpoint e fare clic sul pulsante Prova connessione.

Inner Exception: Certificate is not trusted (RemoteCertificateChainErrors). Subject: C=US, CN=vc6.mycompany.com Thumbprint: DC5A8816231698F4C9013C42692B0AF93D7E35F1

### Causa

L'aggiornamento da vRealize Automation 7.3 o versioni precedenti alla versione 7.4 comporta modifiche degli endpoint dell'ambiente originale. Per gli ambienti aggiornati di recente a vRealize Automation 7.4, l'amministratore IaaS deve controllare tutti gli endpoint esistenti che utilizzano una connessione https protetta. Se in un endpoint si presenta l'errore `Certificate is not trusted`, significa che l'endpoint non funziona correttamente.

### Soluzione

- 1 Accedere alla console vRealize Automation come amministratore di infrastruttura.



- 2 Selezionare **Infrastruttura > Endpoint > Endpoint**.
- 3 Completare questi passaggi per ciascun endpoint con connessione sicura.
  - a Fare clic su **Modifica**.
  - b Fare clic su **Prova connessione**.
  - c Controllare i dettagli del certificato e fare clic su **OK** se si considera attendibile il certificato.
  - d Riavviare i servizi Windows per tutti gli agenti proxy IaaS utilizzati da questo endpoint.
- 4 Verificare che non vengano più visualizzati errori Certificate is not trusted nella pagina Visualizzatore registro dell'infrastruttura.

### L'installazione o l'aggiornamento a vRealize Automation non riesce

L'installazione o l'aggiornamento di vRealize Automation non riesce e nel file di registro viene visualizzato un messaggio di errore.

#### Problema

Quando si esegue l'installazione o l'aggiornamento di vRealize Automation, la procedura non riesce. Ciò avviene in genere quando una correzione applicata durante l'installazione o l'aggiornamento non va a buon fine. Nel file di registro viene visualizzato un messaggio di errore simile al seguente: Security error. Applying automatic fix for FIREWALL prerequisite failed. RPM Status 1: Pre install script failed, package test and installation skipped.

#### Causa

L'ambiente Windows dispone di criteri di gruppo abilitati per l'esecuzione dello script PowerShell.

#### Soluzione

- 1 Nella macchina host di Windows, eseguire `gpedit.msc` per aprire l'Editor Criteri di gruppo locali.
- 2 Nel riquadro a sinistra sotto **Configurazione computer**, fare clic sul pulsante Espandi per aprire **Modelli amministrativi > Componenti di Windows > Windows PowerShell**.
- 3 In **Attiva l'esecuzione di script**, modificare lo stato da Enabled a Not Configured.

### L'aggiornamento dell'agente di gestione non riesce

Quando si fa clic su **Installa aggiornamenti** nella pagina dello stato dell'aggiornamento della console di gestione di Appliances vRealize Automation, viene visualizzato un messaggio di errore relativo all'agente di gestione.

#### Problema

Il processo di aggiornamento non va a buon fine. Viene visualizzato il messaggio che informa che è impossibile aggiornare l'agente di gestione nel nodo x. In alcuni casi, il messaggio riporta più nodi.

## Causa

Questo problema può essere causato da diverse condizioni. Il messaggio di errore identifica solo l'ID del nodo della macchina interessata. Ulteriori informazioni sono disponibili nel file All.log per l'agente di gestione nella macchina in cui si è verificato l'errore di comando.

Eseguire queste attività sui nodi interessati in base alle proprie circostanze:

## Soluzione

- Se il servizio dell'agente di gestione non è in esecuzione, avviare il servizio e riavviare l'aggiornamento sull'appliance virtuale.
- Se il servizio dell'agente di gestione è in esecuzione e l'agente di gestione viene aggiornato, riavviare l'aggiornamento sull'appliance virtuale.
- Se il servizio dell'agente di gestione è in esecuzione ma l'agente di gestione non viene aggiornato, eseguire un aggiornamento manuale.
  - a Aprire un browser e passare alla pagina d'installazione dell'laaS di vRealize Automation sull'appliance vRealize Automation all'indirizzo `https:// va-hostname.domain.name:5480/install`.
  - b Scaricare ed eseguire il programma di installazione dell'agente di gestione.
  - c Riavviare la macchina dell'agente di gestione.
  - d Riavviare l'aggiornamento sull'appliance virtuale.

## Aggiornamento dell'agente di gestione non riuscito

L'aggiornamento dell'agente di gestione ha esito negativo se viene eseguito da vRealize Automation alla versione 7.2. - 7.3.x.

## Problema

Se un incidente di failover ha scambiato l'host primario con l'host secondario dell'agente di gestione, l'aggiornamento non riesce perché il processo di aggiornamento automatico non trova l'host previsto. Eseguire questa procedura in ciascun nodo laaS in cui l'agente di gestione non è aggiornato.

## Soluzione

- 1 Aprire il file All.log nella cartella dei file di registro dell'agente di gestione, disponibile all'indirizzo `C:\Programmi (x86)\VMware\VCAC\Management Agent\Logs\`.

Il percorso della cartella di installazione potrebbe essere diverso da quello predefinito.

- 2 Cercare nel file di registro un messaggio relativo a un'appliance virtuale obsoleta o spenta.

Ad esempio, INNER EXCEPTION: System.Net.WebException: Impossibile effettuare la connessione al server remoto ---> System.Net.Sockets.SocketException: Impossibile stabilire la connessione. Risposta non corretta della parte connessa dopo l'intervallo di tempo oppure mancata risposta dall'host collegato `IP_Address:5480`

- 3 Modificare il file di configurazione dell'agente di gestione all'indirizzo C:\Programmi Files (x86)\VMware\VCAC\Management Agent\VMware.IaaS.Management.Agent.exe.config per sostituire il valore `alternativeEndpointaddress` esistente con l'URL dell'endpoint primario dell'appliance virtuale.

Il percorso della cartella di installazione potrebbe essere diverso da quello predefinito.

Esempio di `alternativeEndpointaddress` in `VMware.IaaS.Management.Agent.exe.config`.

```
<alternativeEndpoint address="https://FQDN:5480/" thumbprint="numero
thumbprint" />
```

- 4 Riavviare il servizio Agente di gestione di Windows e controllare il file `All.log` per verificare che funzioni.
- 5 Eseguire la procedura di aggiornamento nell'appliance vRealize Automation primaria.

### L'aggiornamento di vRealize Automation ha esito negativo a causa delle impostazioni di timeout predefinite

È possibile aumentare l'impostazione del tempo per l'aggiornamento se l'impostazione predefinita per la sincronizzazione dei database è troppo breve per il proprio ambiente.

#### Problema

L'impostazione del timeout per il comando `Vcac-Config SynchronizeDatabases` non è sufficiente per alcuni ambienti in cui la sincronizzazione dei database richiede più tempo rispetto al valore predefinito di 3600 secondi.

I valori delle proprietà `cafeTimeoutInSeconds` e `cafeRequestPageSize` nel file `Vcac-Config.exe.config` regolano la comunicazione tra l'API e lo strumento di utilità `Vcac-config.exe`. Il file si trova in `IaaS installation location\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe.config`.

È possibile sovrascrivere il valore di timeout predefinito solo per il comando `SynchronizeDatabases` specificando un valore per questi parametri facoltativi.

Parametro	Nome breve	Descrizione
<code>--DatabaseSyncTimeout</code>	<code>-dstm</code>	Imposta il valore di timeout della richiesta http solo per <code>SynchronizeDatabases</code> in secondi.
<code>--DatabaseSyncPageSize</code>	<code>-dsps</code>	Imposta le dimensioni della pagina di richiesta solo per la sincronizzazione di Prenotazione o Criterio di prenotazione. Il valore predefinito è 10.

Se questi parametri non sono impostati nel file `Vcac-Config.exe.config`, il sistema utilizza il valore di timeout predefinito.

## L'aggiornamento di IaaS in un ambiente ad alta disponibilità non riesce

Il processo di aggiornamento di IaaS nel nodo del server Web primario con bilanciamento del carico abilitato non riesce. Potrebbero venire visualizzati i seguenti messaggi di errore:

"System.Net.WebException: timeout dell'operazione" o "401 - Autorizzazione negata: accesso negato a causa di credenziali non valide".

### Problema

L'aggiornamento di IaaS con il bilanciamento del carico abilitato può causare un errore intermittente. In questo caso, è necessario eseguire nuovamente l'aggiornamento di vRealize Automation con il bilanciamento del carico disabilitato.

### Soluzione

- 1 Ripristinare gli snapshot dell'ambiente precedenti all'aggiornamento.
- 2 Aprire una connessione desktop remoto al nodo del server Web IaaS primario.
- 3 Passare al file degli host di Windows in c:\windows\system32\drivers\etc.
- 4 Aprire il file degli host e aggiungere la seguente riga per disabilitare il bilanciamento del carico del server Web.

*IP\_address\_of\_primary\_iaas\_website\_node vrealizeautomation\_iaas\_website\_lb\_fqdn*

Esempio:

10.10.10.5 vra-iaas-web-lb.domain.com

- 5 Salvare il file degli host e riprovare a eseguire l'aggiornamento di vRealize Automation.
- 6 Al termine dell'aggiornamento di vRealize Automation, aprire il file degli host e rimuovere la riga aggiunta al passaggio 4.

## Risoluzione dei problemi di aggiornamento

È possibile modificare il processo di aggiornamento per risolvere problemi di aggiornamento.

### Soluzione

Quando si verificano problemi durante l'aggiornamento dell'ambiente di vRealize Automation, utilizzare questa procedura per modificare il processo di aggiornamento selezionando uno dei flag disponibili.

#### Procedura

- 1 Aprire una connessione shell protetta al nodo dell'appliance vRealize Automation primaria.

- 2 Al prompt dei comandi, eseguire questo comando per creare il file di commutazione::

**touch available\_flag**

Ad esempio: **touch /tmp/disable-iaas-upgrade**

**Tabella 1-72. Flag disponibili**

Flag	Descrizione
/tmp/disable-iaas-upgrade	<ul style="list-style-type: none"> <li>■ Impedisce il processo di aggiornamento di IaaS dopo il riavvio dell'appliance virtuale.</li> <li>■ Impedisce l'aggiornamento dell'agente di gestione.</li> <li>■ Impedisce il controllo automatico dei prerequisiti e le correzioni.</li> <li>■ Impedisce l'arresto dei servizi di IaaS.</li> </ul>
/tmp/do-not-upgrade-ma	Impedisce l'aggiornamento dell'agente di gestione. Questo flag è utile quando l'agente di gestione viene aggiornato manualmente.
/tmp/skip-prereq-checks	Impedisce il controllo automatico dei prerequisiti e le correzioni. Questo flag è utile quando si verifica un problema con le correzioni automatiche dei prerequisiti e le correzioni vengono applicate manualmente.
/tmp/do-not-stop-services	Impedisce l'arresto dei servizi di IaaS. L'aggiornamento non arresta i servizi Windows di IaaS, ad esempio il servizio di gestione, DEM e gli agenti.
/tmp/do-not-upgrade-servers	<p>Impedisce l'aggiornamento automatico di tutti i componenti IaaS server, ad esempio il database, il sito Web, WAPI, il repository, i dati di Model Mfrontanager e il servizio di gestione.</p> <p><b>Nota</b> Questo flag impedisce inoltre l'abilitazione della modalità di failover automatica del servizio di gestione.</p>
/tmp/do-not-upgrade-dems	Impedisce l'aggiornamento di DEM.
/tmp/do-not-upgrade-agents	Impedisce l'aggiornamento dell'agente proxy di IaaS.

### 3 Completare le attività per il flag scelto.

**Tabella 1-73. Attività aggiuntive**

Flag	Attività
/tmp/disable-iaas-upgrade	<ul style="list-style-type: none"> <li>■ Aggiornare manualmente l'agente di gestione.</li> <li>■ Applicare manualmente tutti i prerequisiti di IaaS necessari.</li> <li>■ Arrestare manualmente i servizi IaaS.               <ol style="list-style-type: none"> <li>a Accedere al server Windows di IaaS.</li> <li>b Selezionare <b>Start &gt; Strumenti di amministrazione &gt; Servizi</b>.</li> <li>c Arrestare tali servizi rispettando il seguente ordine.</li> </ol> <p><b>Nota</b> Non spegnere il server Windows di IaaS.</p> <ol style="list-style-type: none"> <li>a Tutti gli agenti proxy di VMware vRealize Automation.</li> <li>b Tutte le istanze di DEM Worker VMware.</li> <li>c L'istanza di DEM Orchestrator VMware.</li> <li>d Il servizio VMware vCloud Automation Center.</li> </ol> </li> <li>■ Avviare manualmente l'aggiornamento di IaaS al termine dell'aggiornamento dell'appliance virtuale.</li> </ul>
/tmp/do-not-upgrade-ma	Aggiornare manualmente l'agente di gestione.
/tmp/skip-prereq-checks	Applicare manualmente tutti i prerequisiti di IaaS necessari.
/tmp/do-not-stop-services	<p>Arrestare manualmente i servizi IaaS.</p> <ol style="list-style-type: none"> <li>1 Accedere al server Windows di IaaS.</li> <li>2 Selezionare <b>Start &gt; Strumenti di amministrazione &gt; Servizi</b>.</li> <li>3 Arrestare tali servizi rispettando il seguente ordine.</li> </ol> <p><b>Nota</b> Non spegnere il server Windows di IaaS.</p> <ol style="list-style-type: none"> <li>a Tutti gli agenti proxy di VMware vRealize Automation.</li> <li>b Tutte le istanze di DEM Worker VMware.</li> <li>c L'istanza di DEM Orchestrator VMware.</li> <li>d Il servizio VMware vCloud Automation Center.</li> </ol>
/tmp/do-not-upgrade-servers	
/tmp/do-not-upgrade-dems	
/tmp/do-not-upgrade-agents	

- 4 Accedere alla console di gestione dell'appliance vRealize Automation primaria e aggiornare l'appliance vRealize Automation primaria.

---

**Nota** Poiché ogni flag resta attivo finché non viene rimosso, eseguire questo comando per rimuovere il flag scelto dopo l'aggiornamento: `rm /flag_path/flag_name`. Ad esempio `rm /tmp/disable-iaas-upgrade`.

---

## Migrazione a vRealize Automation 7.4

È possibile eseguire un aggiornamento affiancato dell'ambiente vRealize Automation corrente all'ultima versione mediante migrazione.

Queste informazioni si riferiscono specificamente all'aggiornamento di vRealize Automation 7.4 mediante migrazione. Per informazioni su altri percorsi di aggiornamento supportati, vedere [Aggiornamento di vRealize Automation](#)

### Migrazione di vRealize Automation

È possibile eseguire un aggiornamento affiancato dell'ambiente vRealize Automation corrente mediante migrazione.

La migrazione consente di spostare tutti i dati, ad eccezione dei tenant e degli archivi identità, dall'ambiente di origine corrente di vRealize Automation in una distribuzione target della versione più recente di vRealize Automation. Inoltre, la migrazione sposta tutti i dati da vRealize Orchestrator 7.x incorporato alla distribuzione di destinazione.

Questo processo non modifica l'ambiente di origine, ma semplicemente interrompe i servizi vRealize Automation per il tempo necessario affinché sia possibile raccogliere e copiare i dati in modo sicuro nell'ambiente target. A seconda delle dimensioni del database vRealize Automation di origine, la migrazione può richiedere da pochi minuti ad alcune ore.

È possibile migrare l'ambiente di origine in una distribuzione minima o ad alta disponibilità.

Se si intende trasferire l'ambiente target alla fase di produzione dopo la migrazione, non effettuare la messa in servizio dell'ambiente di origine. Eventuali modifiche apportate all'ambiente di origine dopo la migrazione non verranno sincronizzate con l'ambiente target.

Se l'ambiente di origine è integrato con vCloud Air o vCloud Director oppure dispone di endpoint fisici, è necessario utilizzare la migrazione per eseguire un aggiornamento. La migrazione rimuove questi endpoint e tutti gli elementi associati ad essi dall'ambiente target. Rimuove inoltre l'integrazione di VMware vRealize Application Services 6.x dall'ambiente di destinazione.

---

**Nota** È necessario completare attività aggiuntive per preparare le macchine virtuali vRealize Automation prima della migrazione. Prima di effettuare la migrazione, leggere l'articolo della Knowledge Base [51531](#).

---

Se si effettua la migrazione da vRealize Automation 6.2.x alla versione più recente, si potrebbero riscontrare questi problemi.

Problema	Risoluzione
<p>Dopo la migrazione da vRealize Automation 6.2.x alla versione più recente, gli elementi del catalogo che utilizzano queste definizioni di proprietà vengono visualizzati all'interno del catalogo dei servizi, ma non sono disponibili per la richiesta.</p> <ul style="list-style-type: none"> <li>Tipi di controllo: casella di controllo o collegamento.</li> <li>Attributi: relazione, espressioni regolari o layout delle proprietà.</li> </ul> <p>In vRealize Automation 7.x, le definizioni delle proprietà non utilizzano più questi elementi.</p>	<p>È necessario ricreare la definizione della proprietà o configurarla in modo che utilizzi un'azione di script di vRealize Orchestrator anziché i tipi di controllo o gli attributi incorporati. Per ulteriori informazioni, vedere <a href="#">Gli elementi del catalogo vengono visualizzati nel catalogo dei servizi dopo la migrazione, ma non sono disponibili per la richiesta.</a></p>
<p>Le espressioni regolari utilizzate per definire le relazioni padre-figlio in un menu a discesa di vRealize Automation 6.2.x non sono supportate nella versione 7.x. Nella versione 6.2.x, è possibile utilizzare espressioni regolari per definire una o più voci di menu figlio che sono disponibili solo per una determinata voce di menu padre. Quando si seleziona la voce di menu padre, vengono visualizzati solo tali voci di menu figlio.</p> <p>Dopo la migrazione alla versione 7.x, nel menu a discesa figlio vengono visualizzate tutte le voci di menu disponibili, indipendentemente dalla scelta effettuata nel menu a discesa padre. Per segnalare che i valori dinamici precedentemente definiti non funzionano più, la prima voce del menu a discesa figlio è "Avviso. Utilizzare i workflow di vRO per definire valori dinamici".</p>	<p>Dopo la migrazione, è necessario ricreare la definizione della proprietà per ripristinare i valori dinamici precedenti. Per informazioni sulla creazione di una relazione padre-figlio tra il menu a discesa padre e il menu a discesa figlio, vedere <a href="#">l'argomento che spiega come utilizzare le definizioni delle proprietà dinamiche in vRA 7.2.</a></p>

## Interfacce utente dell'ambiente vRealize Automation

È possibile utilizzare e gestire l'ambiente vRealize Automation con varie interfacce.

### Interfacce utente

Queste tabelle descrivono le interfacce che si utilizzano per gestire l'ambiente vRealize Automation.

**Tabella 1-74. vRealize Automation Console di amministrazione**

Scopo	Accesso	Credenziali necessarie
È possibile utilizzare la console vRealize Automation per queste attività di amministratore di sistema.	1	Avviare un browser e aprire la pagina iniziale dell'appliance vRealize Automation utilizzando il nome di dominio completo dell'appliance virtuale:
<ul style="list-style-type: none"> <li>Aggiungere i tenant.</li> </ul>		<code>https://vra-va-hostname.domain.name.</code>
<ul style="list-style-type: none"> <li>Personalizzare l'interfaccia utente di vRealize Automation.</li> </ul>	2	Fare clic nella <b>console di vRealize Automation</b> .
<ul style="list-style-type: none"> <li>Configurare i server email.</li> </ul>		È inoltre possibile utilizzare questo URL per aprire la console di vRealize Automation:
<ul style="list-style-type: none"> <li>Consente di visualizzare i registri degli eventi.</li> </ul>		<code>https://vra-va-hostname.domain.name/vcac</code>
<ul style="list-style-type: none"> <li>Configurare vRealize Orchestrator.</li> </ul>	3	Accedere.



**Tabella 1-75. Console tenant vRealize Automation . Questa interfaccia è l'interfaccia utente principale utilizzata per creare e gestire i servizi e le risorse.**

Scopo	Accesso	Credenziali necessarie
<p>È possibile utilizzare vRealize Automation per eseguire le attività seguenti.</p> <ul style="list-style-type: none"> <li>■ Richiedere nuovi blueprint dei servizi IT.</li> <li>■ Creare e gestire le risorse IT e cloud.</li> <li>■ Creare e gestire gruppi personalizzati.</li> <li>■ Consente di creare e gestire gruppi di business.</li> <li>■ Assegnare ruoli agli utenti.</li> </ul>	<p>1 Avviare un browser e immettere l'URL della tenancy utilizzando il nome di dominio completo dell'appliance virtuale e il nome URL del tenant:</p> <p><code>https://vra-va-hostname.domain.name/vcac/org/tenant_URL_name</code></p> <p>2 Accedere.</p>	<p>È necessario disporre di uno o più dei ruoli seguenti:</p> <ul style="list-style-type: none"> <li>■ Architetto dell'applicazione</li> <li>■ Amministratore approvazioni</li> <li>■ Amministratore del catalogo</li> <li>■ Amministratore contenitori</li> <li>■ Architetto di contenitori</li> <li>■ Consumatore di integrità</li> <li>■ Architetto dell'infrastruttura</li> <li>■ Consumatore esportazione sicura</li> <li>■ Architetto del software</li> <li>■ Amministratore tenant</li> <li>■ Architetto XaaS</li> </ul>

**Tabella 1-76. Console di gestione dell'appliance vRealize Automation . Questa interfaccia talvolta viene chiamata VAMI (Virtual Appliance Management Interface).**

Scopo	Accesso	Credenziali necessarie
<p>È possibile utilizzare la console di gestione dell'appliance vRealize Automation per eseguire le attività seguenti.</p> <ul style="list-style-type: none"> <li>■ Visualizzare lo stato dei servizi registrati.</li> <li>■ Visualizzare le informazioni di sistema ed eseguire riavvio o shutdown dell'appliance.</li> <li>■ Gestire la partecipazione al programma Analisi utilizzo software.</li> <li>■ Visualizzare lo stato della rete.</li> <li>■ Visualizzare lo stato dell'aggiornamento e installare gli aggiornamenti.</li> <li>■ Gestire le impostazioni di amministrazione.</li> <li>■ Gestire le impostazioni dell'host vRealize Automation.</li> <li>■ Gestire le impostazioni SSO.</li> <li>■ Gestire le licenze di prodotto.</li> <li>■ Configurare il database Postgres vRealize Automation.</li> <li>■ Configurare la messaggistica di vRealize Automation.</li> <li>■ Configurare la registrazione di vRealize Automation.</li> <li>■ Installare i componenti IaaS.</li> <li>■ Eseguire la migrazione da un'installazione vRealize Automation esistente.</li> <li>■ Gestire i certificati del componente IaaS.</li> <li>■ Configurare il servizio Xenon.</li> </ul>	<ol style="list-style-type: none"> <li>1 Avviare un browser e aprire la pagina iniziale dell'appliance vRealize Automation utilizzando il nome di dominio completo dell'appliance virtuale:  <code>https://vra-va-hostname.domain.name.</code></li> <li>2 Fare clic su <b>gestione dell'appliance vRealize Automation</b>  Per aprire vRealize Automation Appliance Management, è inoltre possibile utilizzare l'URL <code>https://vra-va-hostname.domain.name:5480.</code></li> <li>3 Accedere.</li> </ol>	<ul style="list-style-type: none"> <li>■ Nome utente: root</li> <li>■ Password: la password immessa durante la distribuzione dell'appliance vRealize Automation.</li> </ul>

Tabella 1-77. Client vRealize Orchestrator

Scopo	Accesso	Credenziali necessarie
<p>È possibile utilizzare il client vRealize Orchestrator per eseguire le attività seguenti.</p> <ul style="list-style-type: none"> <li>■ Sviluppare azioni.</li> <li>■ Sviluppare workflow.</li> <li>■ Gestire criteri</li> <li>■ Installare pacchetti.</li> <li>■ Gestire autorizzazioni di utenti e gruppi di utenti.</li> <li>■ Applicare tag a oggetti URI.</li> <li>■ Visualizzare l'inventario.</li> </ul>	<ol style="list-style-type: none"> <li>1 Avviare un browser e aprire la pagina iniziale di vRealize Automation utilizzando il nome di dominio completo dell'appliance virtuale:  <code>https://vra-va-hostname.domain.name.</code></li> <li>2 Per scaricare il file <code>client.jnlp</code> nel computer locale, fare clic su <b>Client di vRealize Orchestrator</b>.</li> <li>3 Fare clic con il pulsante destro del mouse sul file <code>client.jnlp</code> e scegliere <b>Avvia</b>.</li> <li>4 Nella finestra di dialogo in cui viene chiesto se si desidera continuare, fare clic su <b>Continua</b>.</li> <li>5 Accedere.</li> </ol>	<p>È necessario essere un utente con ruolo di amministratore di sistema o far parte del gruppo <code>vcoadmins</code> configurato nelle impostazioni del provider di autenticazione di vRealize Orchestrator Control Center.</p>

Tabella 1-78. vRealize Orchestrator Control Center

Scopo	Accesso	Credenziali necessarie
<p>È possibile utilizzare vRealize Orchestrator Control Center per modificare la configurazione dell'istanza di vRealize Orchestrator predefinita incorporata in vRealize Automation.</p>	<ol style="list-style-type: none"> <li>1 Avviare un browser e aprire la pagina iniziale dell'appliance vRealize Automation utilizzando il nome di dominio completo dell'appliance virtuale:  <code>https://vra-va-hostname.domain.name.</code></li> <li>2 Fare clic su <b>gestione dell'appliance vRealize Automation</b>  Per aprire vRealize Automation Appliance Management, è inoltre possibile utilizzare l'URL <code>https://vra-va-hostname.domain.name:5480.</code></li> <li>3 Accedere.</li> <li>4 Fare clic su <b>Impostazioni vRA &gt; Orchestrator</b>.</li> <li>5 Selezionare <b>Interfaccia utente di Orchestrator</b>.</li> <li>6 Fare clic su <b>Avvia</b>.</li> <li>7 Fare clic sull'URL dell'interfaccia utente di Orchestrator.</li> <li>8 Accedere.</li> </ol>	<p>Nome utente</p> <ul style="list-style-type: none"> <li>■ Se non è configurata l'autenticazione basata sul ruolo, inserire <b>root</b>.</li> <li>■ Immettere il nome utente di vRealize Automation se è configurato per l'autenticazione basata sul ruolo.</li> </ul> <p>Password</p> <ul style="list-style-type: none"> <li>■ Inserire la password immessa durante la distribuzione dell'appliance vRealize Automation se non è configurata l'autenticazione basata sul ruolo.</li> <li>■ Inserire la password relativa al proprio nome utente se è configurato per l'autenticazione basata sul ruolo.</li> </ul>

**Tabella 1-79. Prompt dei comandi di Linux**

Scopo	Accesso	Credenziali necessarie
<p>È possibile utilizzare il prompt dei comandi di Linux in un host, ad esempio nell'host dell'appliance vRealize Automation, per eseguire le attività seguenti.</p> <ul style="list-style-type: none"> <li>■ Avviare o arrestare servizi</li> <li>■ Modificare file di configurazione</li> <li>■ Eseguire comandi</li> <li>■ Recuperare dati</li> </ul>	<p>1 Nell'host dell'appliance vRealize Automation, aprire un prompt dei comandi.</p> <p>Un modo per aprire il prompt dei comandi nel computer locale consiste nell'avviare una sessione nell'host utilizzando un'applicazione come PuTTY.</p> <p>2 Accedere.</p>	<ul style="list-style-type: none"> <li>■ Nome utente: root</li> <li>■ Password: la password creata durante la distribuzione dell'appliance vRealize Automation.</li> </ul>

**Tabella 1-80. Prompt dei comandi di Windows**

Scopo	Accesso	Credenziali necessarie
<p>È possibile utilizzare il prompt dei comandi di Windows in un host, ad esempio l'host IaaS, per eseguire script.</p>	<p>1 Nell'host IaaS, accedere a Windows.</p> <p>Un modo per effettuare l'accesso dal computer locale consiste nell'avviare una sessione desktop remota.</p> <p>2 Aprire il prompt dei comandi di Windows.</p> <p>Un modo per aprire il prompt dei comandi consiste nel fare clic con il pulsante destro del mouse sull'icona Start nell'host e selezionare <b>Prompt dei comandi</b> o <b>Prompt dei comandi (amministratore)</b>.</p>	<ul style="list-style-type: none"> <li>■ Nome utente: l'utente con privilegi amministrativi.</li> <li>■ Password: la password dell'utente.</li> </ul>

## Prerequisiti della migrazione

I prerequisiti della migrazione cambiano in base all'ambiente di destinazione.

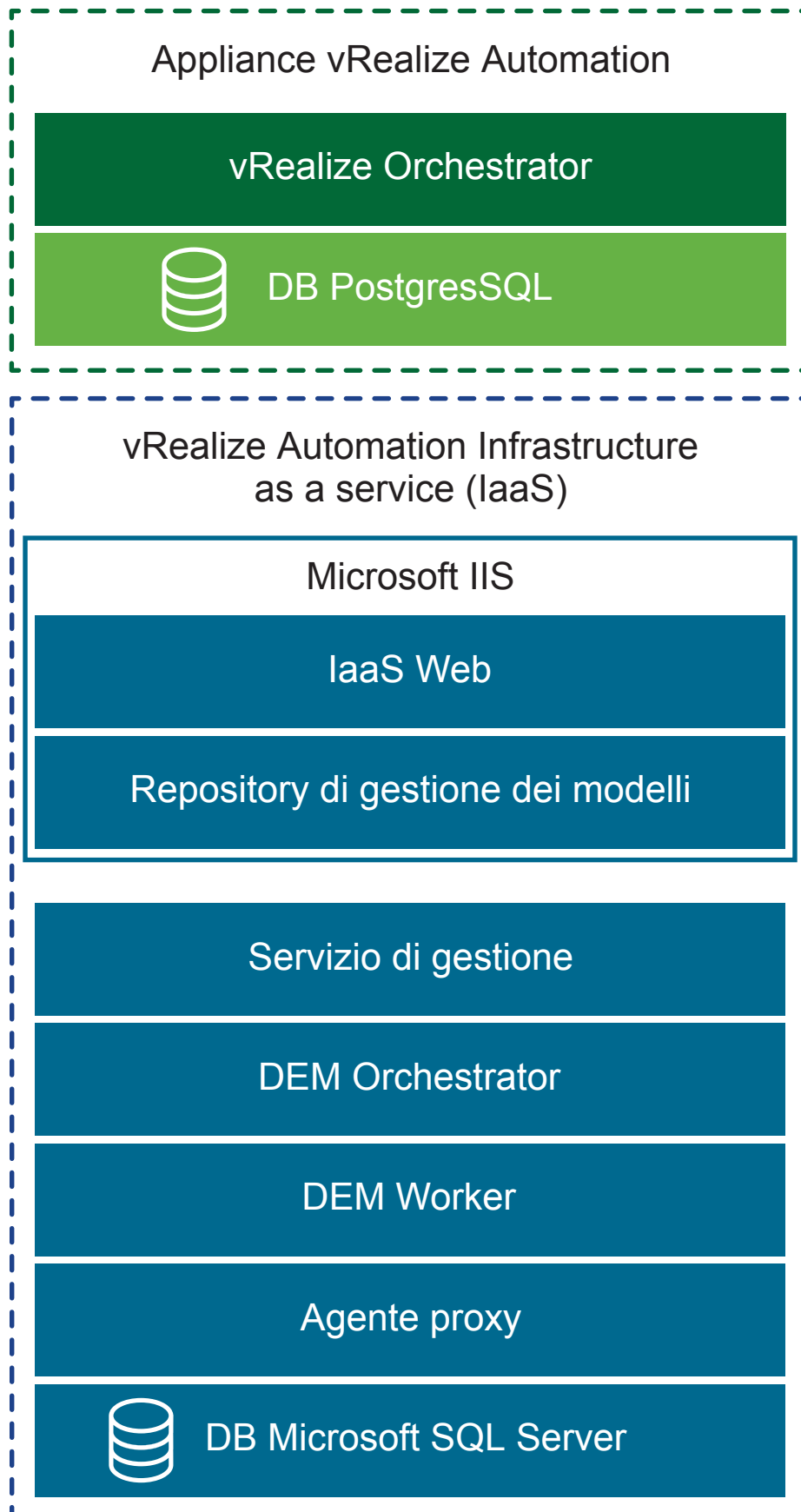
È possibile effettuare la migrazione in un ambiente minimo o in un ambiente ad alta disponibilità.

### Prerequisiti per la migrazione in un ambiente minimo

Per garantire la corretta migrazione in un ambiente minimo, esaminare i requisiti riportati di seguito.

Le distribuzioni minime includono un'appliance vRealize Automation e un server Windows che ospita i componenti IaaS. In una distribuzione minima, il database SQL Server di vRealize Automation può trovarsi sullo stesso server Windows IaaS con i componenti IaaS oppure su un server Windows separato.

Figura 1-17. Distribuzione minima di vRealize Automation



## Prerequisiti

- Verificare di disporre di un nuovo ambiente target di vRealize Automation.
- Installare gli agenti proxy rilevanti nell'ambiente target in base ai requisiti riportati di seguito.
  - Il nome dell'agente proxy target deve corrispondere al nome dell'agente proxy di origine per gli agenti proxy vSphere, Hyper-V, Citrix XenServer e Test.

---

**Nota** Per ottenere un nome di agente, completare i passaggi descritti di seguito.

- 1 Nell'host IaaS, accedere a Windows come utente locale con privilegi di **amministratore**.
  - 2 Utilizzare Esplora risorse per passare alla directory di installazione dell'agente.
  - 3 Aprire il file VRMAgent.exe.config.
  - 4 Nel tag serviceConfiguration cercare il valore dell'attributo agentName.
- 

- Consultare l'articolo della Knowledge Base [51531](#).
- Il nome dell'endpoint dell'agente proxy target deve corrispondere al nome dell'endpoint dell'agente proxy di origine per gli agenti proxy vSphere, Hyper-V, Citrix XenServer e Test.
- Non creare un endpoint per gli agenti proxy vSphere, Hyper-V, Citrix XenServer o Test nell'ambiente target.
- Esaminare i numeri di versione dei componenti di vRealize Automation nell'appliance vRealize Automation target.
  - a Accedere alla gestione dell'appliance vRealize Automation target come **root** utilizzando la password immessa durante la distribuzione dell'appliance vRealize Automation target.
  - b Selezionare **Impostazioni vRA > Cluster**.
  - c Espandere i record Nome host/nodo facendo clic sul triangolo.

Verificare che i numeri di versione dei componenti di vRealize Automation IaaS corrispondano.
- Verificare che la versione del componente Microsoft SQL Server target per il database IaaS target di vRealize Automation sia 2012, 2014 o 2016.
- Verificare che la porta 22 sia aperta tra gli ambienti vRealize Automation di origine e destinazione. Tale porta è necessaria per stabilire connessioni SSH (Secure Shell) tra le appliance virtuali di origine e target.
- Verificare che vCenter dell'endpoint disponga di risorse sufficienti per completare la migrazione.
- Verificare che l'ora del sistema dell'ambiente di vRealize Automation target sia sincronizzata tra Cafe e i componenti IaaS.
- Verificare che nel nodo del server IaaS nell'ambiente target sia installato almeno Java SE Runtime Environment (JRE) 8, a 64 bit, aggiornamento 161 o successivo. Dopo avere installato JRE, assicurarsi che la variabile di ambiente JAVA\_HOME punti alla versione di Java installata in ogni nodo IaaS. Modificare il percorso se necessario.

- Verificare che in ogni nodo IaaS sia installato PowerShell 3.0 o versione successiva.
- Verificare che gli ambienti vRealize Automation di origine e target siano in esecuzione.
- Verificare che nell'ambiente vRealize Automation di origine non siano in corso attività utente o di provisioning.
- Verificare che eventuali software antivirus o di protezione in esecuzione nei nodi IaaS nell'ambiente vRealize Automation di destinazione che potrebbe interagire con il sistema operativo e i relativi componenti sia correttamente configurato o disabilitato.
- Verificare che il servizio Web di IaaS e Model Manager non debbano essere riavviati a causa di aggiornamenti dell'installazione di Windows in sospeso. Gli aggiornamenti in sospeso possono impedire l'inizio della migrazione o terminare il servizio di pubblicazione sul World Wide Web.

### **Operazioni successive**

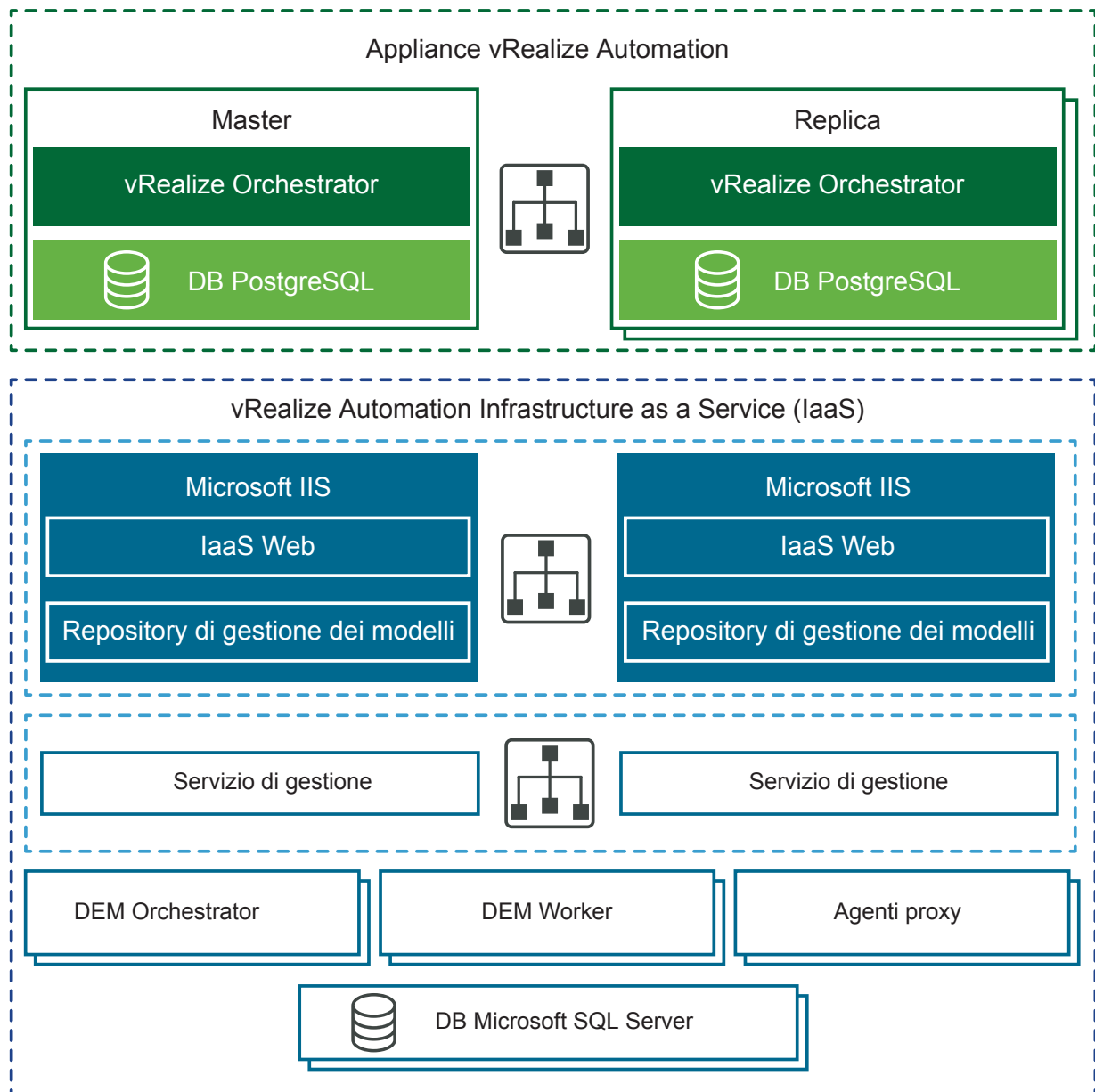
[Attività precedenti alla migrazione.](#)

### **Prerequisiti per la migrazione in un ambiente ad alta disponibilità**

Per garantire la corretta migrazione in un ambiente ad alta disponibilità, esaminare i requisiti riportati di seguito.

Gli ambienti ad alta disponibilità possono essere di dimensioni diverse. Una distribuzione distribuita di base può migliorare vRealize Automation semplicemente ospitando componenti IaaS su server Windows separati. Molti ambienti ad alta disponibilità si spingono anche oltre, con appliance e server ridondanti, uniti al bilanciamento del carico per una maggiore capacità. Le distribuzioni distribuite di grandi dimensioni offrono maggiore scalabilità, alta disponibilità e disaster recovery.

**Figura 1-18. Ambiente ad alta disponibilità vRealize Automation**





## Prerequisiti

- Verificare che sia presente una nuova installazione target di vRealize Automation con un'appliance virtuale master e di replica configurata per l'alta disponibilità. Vedere [Considerazioni sulla configurazione dell'alta disponibilità di vRealize Automation](#).
- Verificare che tutte le appliance virtuali vRealize Automation utilizzino la stessa password per l'utente root.
- Installare gli agenti proxy rilevanti nell'ambiente target in base ai requisiti riportati di seguito.
  - Il nome dell'agente proxy target deve corrispondere al nome dell'agente proxy di origine per gli agenti proxy vSphere, Hyper-V, Citrix XenServer e Test.

---

**Nota** Per ottenere un nome di agente, completare i passaggi descritti di seguito.

- 1 Nell'host IaaS, accedere a Windows come utente locale con privilegi di **amministratore**.
  - 2 Utilizzare Esplora risorse per passare alla directory di installazione dell'agente.
  - 3 Aprire il file VRMAgent.exe.config.
  - 4 Nel tag serviceConfiguration cercare il valore dell'attributo agentName.
- 

- Il nome dell'endpoint dell'agente proxy target deve corrispondere al nome dell'endpoint dell'agente proxy di origine per gli agenti proxy vSphere, Hyper-V, Citrix XenServer e Test.
- Non creare un endpoint per gli agenti proxy vSphere, Hyper-V, Citrix XenServer o Test nell'ambiente target.
- Controllare i numeri di versione dei componenti di vRealize Automation nell'appliance vRealize Automation target.
  - a Nell'ambiente vRealize Automation di destinazione, avviare un browser e passare alla console di gestione dell'appliance vRealize Automation all'indirizzo `https:// vra-va-hostname.domain.name:5480`.
  - b Accedere con il nome utente root e la password immessa durante la distribuzione dell'appliance.
  - c Selezionare **Impostazioni vRA > Cluster**.
  - d Per espandere i record Nome host/nodo in modo da visualizzare i componenti, fare clic sul pulsante Espandi.

Verificare che i numeri di versione dei componenti di vRealize Automation corrispondano in tutti i nodi dell'appliance virtuale.

Verificare che i numeri di versione dei componenti di vRealize Automation IaaS corrispondano in tutti i nodi IaaS.
- Consultare l'articolo della Knowledge Base [51531](#).
- Eseguire questi passaggi per indirizzare il traffico solo al nodo master.
  - a Disabilitare tutti i nodi ridondanti.

- b Rimuovere i controlli di integrità per questi elementi in base alla documentazione del bilanciamento del carico:
  - Appliance virtuale vRealize Automation
  - Sito Web di IaaS
  - Servizio di gestione di IaaS
- Verificare che la versione del componente Microsoft SQL Server target per il database IaaS target di vRealize Automation sia 2012, 2014 o 2016.
- Verificare che la porta 22 sia aperta tra gli ambienti vRealize Automation di origine e destinazione. Tale porta è necessaria per stabilire connessioni SSH (Secure Shell) tra le appliance virtuali di origine e target.
- Verificare che vCenter dell'endpoint disponga di risorse sufficienti per completare la migrazione.
- Assicurarsi di aver modificato le impostazioni di timeout del bilanciamento del carico dal valore predefinito ad almeno 10 minuti.
- Verificare che l'ora del sistema dell'ambiente di vRealize Automation target sia sincronizzata tra Cafe e i componenti IaaS.
- Verificare che i nodi IaaS Web Service e Model Manager nell'ambiente di destinazione dispongano dell'istanza di Java Runtime Environment corretta. È necessario che sia installato Java SE Runtime Environment (JRE) 8, a 64 bit, aggiornamento 161 o versioni successive. Assicurarsi che la variabile di sistema JAVA\_HOME punti alla versione di Java installata in ciascun nodo IaaS. Modificare il percorso se necessario.
- Verificare che in ogni nodo IaaS sia installato almeno PowerShell 3.0 o versione successiva.
- Verificare che gli ambienti vRealize Automation di origine e target siano in esecuzione.
- Verificare che nell'ambiente vRealize Automation di origine non siano in corso attività utente o di provisioning.
- Verificare che eventuali software antivirus o di protezione in esecuzione nei nodi IaaS nell'ambiente vRealize Automation di destinazione che potrebbe interagire con il sistema operativo e i relativi componenti sia correttamente configurato o disabilitato.
- Verificare che il servizio Web di IaaS e Model Manager non debbano essere riavviati a causa di aggiornamenti dell'installazione di Windows in sospeso. Gli aggiornamenti in sospeso possono impedire l'inizio della migrazione o terminare il servizio di pubblicazione sul World Wide Web.

## Operazioni successive

[Attività precedenti alla migrazione.](#)

## Attività precedenti alla migrazione

Prima di eseguire la migrazione, è necessario completare diverse attività preliminari.

Le attività precedenti alla migrazione eseguite prima di migrare i dati dell'ambiente vRealize Automation di origine all'ambiente vRealize Automation target variano in base all'ambiente di origine.

## Esame delle modifiche introdotte dalla migrazione da vRealize Automation 6.2.x a 7.x

vRealize Automation 7 e versione successiva introduce diverse modifiche funzionali durante e dopo il processo di aggiornamento. Esaminare queste modifiche prima di aggiornare la distribuzione vRealize Automation 6.2.x all'ultima versione.

Per informazioni sulle differenze tra vRealize Automation 6.2.x e 7.x, vedere [Considerazioni sull'aggiornamento a questa versione di vRealize Automation](#) in *Aggiornamento di vRealize Automation 6.2.5 alla versione 7.4*.

---

**Nota** Lo strumento di assistenza all'aggiornamento di vRealize per i test in ambiente di produzione analizza l'ambiente di vRealize Automation 6.2.x per rilevare eventuali configurazioni di funzionalità che possono provocare problemi di aggiornamento e verifica che l'ambiente sia pronto per l'aggiornamento. Lo strumento può essere scaricato dalla pagina di download del prodotto di [VMware vRealize Production Test Tool](#).

---

Dopo la migrazione da vRealize Automation 6.2.x alla versione più recente, gli elementi del catalogo che utilizzano queste definizioni di proprietà vengono visualizzati all'interno del catalogo dei servizi, ma non sono disponibili per la richiesta.

- Tipi di controllo: casella di controllo o collegamento.
- Attributi: relazione, espressioni regolari o layout delle proprietà.

In vRealize Automation 7.x, le definizioni delle proprietà non utilizzano più questi elementi. È necessario ricreare la definizione della proprietà o configurarla in modo che utilizzi un'azione di script di vRealize Orchestrator anziché i tipi di controllo o gli attributi incorporati. Per ulteriori informazioni, vedere [Gli elementi del catalogo vengono visualizzati nel catalogo dei servizi dopo la migrazione, ma non sono disponibili per la richiesta](#).

## Applicazione di patch dell'agente software

Prima di effettuare la migrazione da vRealize Automation 7.1 o 7.3 alla versione 7.4, è necessario applicare un hotfix all'appliance di origine per poter aggiornare gli agenti software a TLS 1.2.

Il protocollo TLS (Transport Layer Security) garantisce l'integrità dei dati tra il browser e vRealize Automation. Questo hotfix consente l'aggiornamento degli agenti software a TLS 1.2 nell'ambiente di origine. L'aggiornamento garantisce il massimo livello di sicurezza ed è obbligatorio per vRealize Automation 7.1 o 7.3. È disponibile un hotfix per ciascuna versione.

### Prerequisiti

Ambiente di origine di vRealize Automation 7.1 o 7.3 in esecuzione.

### Procedura

- ◆ Applicare questo hotfix all'appliance vRealize Automation 7.1 o 7.3 di origine prima di eseguire la migrazione alla versione 7.4. Vedere l'[articolo 52897 della Knowledge Base](#).

### Operazioni successive

[Modifica dell'impostazione DoDeletes nell'agente di vSphere su False](#).

## Modifica dell'impostazione DoDeletes nell'agente di vSphere su False

Se si effettua la migrazione da un ambiente vRealize Automation 6.2.x, è necessario modificare il valore DoDeletes da **true** a **false** nell'agente di vSphere di destinazione prima della migrazione.

### Prerequisiti

Completare i prerequisiti per la migrazione.

### Procedura

- 1 Cambiare il valore DoDeletes su **false**.

Questo impedisce l'eliminazione delle macchine virtuali dall'ambiente di origine. Gli ambienti di origine e di destinazione sono eseguiti in parallelo. Si possono verificare discrepanze di lease dopo la convalida della migrazione della produzione.

- 2 Impostare il valore DoDeletes su **true** dopo la convalida della migrazione della produzione e l'arresto dell'ambiente di origine.
- 3 Eseguire i passaggi della procedura [Configurazione dell'agente di vSphere](#) per impostare DoDeletes su **false**.

### Operazioni successive

[Preparazione alla migrazione di macchine virtuali vRealize Automation.](#)

## Controllo dei modelli nell'ambiente di origine di vRealize Automation 6.x

Prima di effettuare la migrazione da vRealize Automation 6.x alla versione 7.4, è necessario controllare i modelli della macchina virtuale in uso per verificare che la quantità di memoria minima impostata in ogni modello sia di almeno 4 MB.

Se nell'ambiente di origine di vRealize Automation 6.x è presente un modello di macchina virtuale con una quantità di memoria inferiore a 4 MB, la migrazione non riesce. Per verificare se nell'ambiente di origine 6.x sono presenti blueprint con una quantità di memoria inferiore a 4 MB, eseguire la seguente procedura.

### Prerequisiti

Si effettua la migrazione da vRealize Automation 6.x alla versione 7.4.

### Procedura

- 1 Accedere all'appliance vRealize Automation principale tramite SSH come **root**.  
Se vRealize Orchestrator è esterno, accedere alla macchina host di Orchestrator.
- 2 Passare alla cartella di dati PostgreSQL sull'host primario nel percorso `/var/vmware/vpostgres/current/pgdata/`.

- 3 Eseguire questo script per controllare se sono presenti blueprint con una quantità di memoria specificata inferiore a 4 MB.

```
select * from [vCAC].[dbo].[VirtualMachineTemplate] where IsHidden = 0 and
MemoryMB < 4;
```

dove vCAC è il nome del database.

- 4 Se lo script rileva blueprint con una quantità di memoria specificata inferiore a 4 MB, eseguire questo script per aggiornare tale valore impostandolo su almeno 4 MB.

```
update [vCAC].[dbo].[VirtualMachineTemplate] set MemoryMB = 4 where IsHidden = 0
and MemoryMB < 4;
```

dove vCAC è il nome del database.

### Operazioni successive

[Preparazione alla migrazione di macchine virtuali vRealize Automation.](#)

### Preparazione alla migrazione di macchine virtuali vRealize Automation

Le problematiche note relative alla migrazione di macchine virtuali vRealize Automation 6.2.x possono causare problemi dopo la migrazione.

È necessario esaminare l'[articolo della Knowledge Base 000051531](#) ed eseguire eventuali correzioni rilevanti agli ambienti prima della migrazione.

### Operazioni successive

[Raccolta di informazioni necessarie per la migrazione.](#)

### Raccolta di informazioni necessarie per la migrazione

Per registrare le informazioni necessarie per la migrazione dagli ambienti di origine e di destinazione, fare riferimento alle tabelle riportate di seguito.

#### Prerequisiti

Verificare i prerequisiti per il proprio ambiente.

- [Prerequisiti per la migrazione in un ambiente minimo.](#)
- [Prerequisiti per la migrazione in un ambiente ad alta disponibilità.](#)

**Tabella 1-81. Appliance vRealize Automation di origine**

Opzione	Descrizione	Valore
Nome host	Accedere alla gestione dell'appliance vRealize Automation di origine. Individuare il nome host nella scheda <b>Sistema</b> . Il nome host deve corrispondere a un nome di dominio completo (FQDN).	
Nome utente radice	root	

**Tabella 1-81. Appliance vRealize Automation di origine (Continua)**

Opzione	Descrizione	Valore
Password root	Password root immessa durante la distribuzione dell'appliance Appliance vRealize Automation di origine.	
Posizione pacchetto migrazione	Percorso di una directory esistente nell'appliance vRealize Automation 6.2.x o 7.x di origine in cui viene creato il pacchetto di migrazione. La directory deve avere uno spazio libero disponibile pari a due volte la dimensione del database di vRealize Automation. La posizione predefinita è /storage.	

**Tabella 1-82. Appliance vRealize Automation target**

Opzione	Descrizione	Valore
Nome utente radice	root	
Password root	La password root immessa durante la distribuzione dell'appliance vRealize Automation di destinazione.	
Tenant predefinito	vsphere.local	
Nome utente amministratore	administrator	
Password amministratore	Password dell'utente administrator@vsphere.local immessa durante la distribuzione dell'ambiente vRealize Automation target.	

**Tabella 1-83. Database IaaS target**

Opzione	Descrizione	Valore
Server di database	Posizione dell'istanza di Microsoft SQL Server in cui si trova il database clonato. Se si utilizza un'istanza denominata e una porta non predefinita, specificarle nel formato SERVER,PORT\INSTANCE-NAME.	
Nome database clonato	Il nome del database Microsoft SQL IaaS di origine di vRealize Automation 6.2.x/7.x clonato per la migrazione.	
Modalità di autenticazione	Selezionare Windows o SQL Server. Se si seleziona SQL Server, è necessario immettere un nome di accesso e una password.	
Nome login	Nome di accesso per l'utente dell'istanza di SQL Server che dispone del ruolo db_owner per il database Microsoft SQL IaaS clonato.	
Password	Password dell'utente di SQL Server.	

**Tabella 1-83. Database IaaS target (Continua)**

Opzione	Descrizione	Valore
Chiave di crittografia originale	La chiave di crittografia originale recuperata dall'ambiente di origine. Vedere <a href="#">Ottenere la chiave di crittografia dell'ambiente vRealize Automation di origine</a> .	
Nuova passphrase	Serie di parole utilizzate per generare una nuova chiave di crittografia. Questa passphrase viene utilizzata durante ogni installazione di un nuovo componente IaaS nell'ambiente vRealize Automation target.	

**Operazioni successive**

[Ottenere la chiave di crittografia dell'ambiente vRealize Automation di origine](#).

**Ottenere la chiave di crittografia dell'ambiente vRealize Automation di origine**

Durante la procedura di migrazione è necessario immettere la chiave di crittografia dell'ambiente vRealize Automation di origine.

**Prerequisiti**

Assicurarsi di disporre dei privilegi di amministratore sulla macchina virtuale host del servizio di gestione attivo nell'ambiente di origine.

**Procedura**

- 1 Aprire un prompt dei comandi come amministratore nella macchina virtuale che ospita il servizio di gestione attivo ed eseguire il comando seguente.

```
"C:\Program Files
(x86)\VMware\VCAC\Server\ConfigTool\EncryptionKeyTool\DynamicOps.Tools.Encryption
KeyTool.exe" key-read -c "C:\Program Files
(x86)\VMware\VCAC\Server\ManagerService.exe.config" -v
```

Se la directory di installazione non si trova nella posizione predefinita, C:\Program Files (x86)\VMware\VCAC, modificare il percorso includendo la directory di installazione effettiva.

- 2 Salvare la chiave visualizzata dopo l'esecuzione del comando.

La chiave è una lunga stringa di caratteri simile a quella illustrata di seguito:

```
NRH+f/BlnCB6yvasLS3sxespgdkcFWAEuyV0g4lfryg=.
```

**Operazioni successive**

- Se si sta eseguendo la migrazione da un ambiente vRealize Automation 6.2.x: [Aggiunta di ciascun tenant dall'ambiente vRealize Automation di origine all'ambiente di destinazione](#).
- Se si sta eseguendo la migrazione da un ambiente vRealize Automation 7.x: [Creazione di un elenco di amministratori Tenant e IaaS dell'ambiente vRealize Automation 6.2.x di origine](#).

## Creazione di un elenco di amministratori Tenant e IaaS dell'ambiente vRealize Automation 6.2.x di origine

Prima di eseguire la migrazione di un ambiente vRealize Automation 6.2.x, è necessario creare un elenco degli amministratori tenant e IaaS per ogni tenant.

Eseguire la procedura seguente per ogni tenant dalla console di vRealize Automation di origine.

---

**Nota** Se si effettua la migrazione da un ambiente vRealize Automation 7.x, non è necessario eseguire questa procedura.

---

### Prerequisiti

Accedere alla console di vRealize Automation di origine come **amministratore** con la password immessa durante la distribuzione dell'appliance vRealize Automation di origine.

---

**Nota** Per un ambiente ad alta disponibilità, aprire la console utilizzando il nome di dominio completo del bilanciamento del carico dell'appliance virtuale di origine, ovvero `https://vra-va-lb-hostname.domain.name/vcac`.

---

### Procedura

- 1 Selezionare **Amministrazione > Tenant**.
- 2 Fare clic su un nome di tenant.
- 3 Fare clic su **Amministratori**.
- 4 Creare un elenco dei nomi utente di tutti gli amministratori tenant e IaaS.
- 5 Fare clic su **Annulla**.

### Operazioni successive

[Aggiunta di ciascun tenant dall'ambiente vRealize Automation di origine all'ambiente di destinazione.](#)

### Aggiunta di ciascun tenant dall'ambiente vRealize Automation di origine all'ambiente di destinazione

È necessario aggiungere tenant all'ambiente di destinazione utilizzando il nome di ciascun tenant nell'ambiente di origine.

Per una migrazione corretta, è obbligatorio che ciascun tenant nell'ambiente di origine venga creato nell'ambiente di destinazione. È anche necessario utilizzare un URL di accesso specifico del tenant per ciascun tenant che viene aggiunto utilizzando il nome dell'URL del tenant dall'ambiente di origine. Se nell'ambiente di origine sono presenti tenant inutilizzati di cui non si desidera effettuare la migrazione, eliminarli dall'ambiente di origine prima della migrazione.

---

**Nota** La convalida della migrazione assicura che il sistema di destinazione disponga almeno degli stessi tenant configurati nell'ambiente di origine, come richiesto dai prerequisiti. Consente di eseguire confronto tra tenant non in base ai relativi nomi, bensì in base ai nomi degli URL dei tenant, per i quali si fa distinzione tra maiuscole e minuscole.

---



Eseguire questa procedura per ciascun tenant dell'ambiente di origine.

- Quando si esegue la migrazione da un ambiente vRealize Automation 6.2.x, si migrano gli archivi identità e i tenant SSO2 esistenti dall'ambiente di origine nel VMware Identity Manager dell'ambiente di destinazione.
- Quando si effettua la migrazione da un ambiente vRealize Automation 7.x, si migrano gli archivi identità e i tenant esistenti di VMware Identity Manager dall'ambiente di origine nel VMware Identity Manager dell'ambiente di destinazione.

#### Prerequisiti

- [Raccolta di informazioni necessarie per la migrazione.](#)
- Accedere alla console di vRealize Automation target come **amministratore** con la password immessa durante la distribuzione dell'appliance vRealize Automation target.

---

**Nota** Per un ambiente ad alta disponibilità, aprire la console utilizzando il nome di dominio completo del bilanciamento del carico dell'appliance virtuale target, ovvero `https://vra-va-lb-hostname.domain.name/vcac`.

---

#### Procedura

1 Selezionare **Amministrazione > Tenant**.

2 Fare clic sull'icona **Nuovo** (+).

3 Nella casella di testo **Nome** immettere un nome di tenant corrispondente al nome di un tenant dell'ambiente di origine.

Ad esempio, se il nome del tenant dell'ambiente di origine è DEVTenant, immettere **DEVTenant**.

4 (Facoltativo) Immettere una descrizione nella casella di testo **Descrizione**.

5 Nella casella di testo **Nome URL** immettere un nome di URL del tenant corrispondente al nome dell'URL di un tenant nell'ambiente di origine.

Il nome dell'URL viene utilizzato per aggiungere un identificatore specifico del tenant all'URL della console di vRealize Automation.

Ad esempio, se il nome dell'URL per DEVTenant nell'ambiente di origine è dev, immettere **dev** per creare l'URL `https://vrealize-appliance-hostname.domain.name/vcac/org/dev`.

6 (Facoltativo) Inserire un indirizzo email nella casella di testo **Email di contatto**.

7 Fare clic su **Invia e Avanti**.

#### Operazioni successive

[Creazione di un amministratore per ciascun tenant aggiunto.](#)

## Creazione di un amministratore per ciascun tenant aggiunto

È necessario creare un amministratore per ciascun tenant aggiunto all'ambiente di destinazione. È possibile creare un amministratore creando un account utente locale e assegnando privilegi di amministratore del tenant all'account utente locale.

Eseguire questa procedura per ciascun tenant dell'ambiente di destinazione.

### Prerequisiti

- [Aggiunta di ciascun tenant dall'ambiente vRealize Automation di origine all'ambiente di destinazione.](#)
- Accedere alla console di vRealize Automation target come **amministratore** con la password immessa durante la distribuzione dell'appliance vRealize Automation target.

---

**Nota** Per un ambiente ad alta disponibilità, aprire la console utilizzando il nome di dominio completo del bilanciamento del carico dell'appliance virtuale target, ovvero `https://vra-vb-lb-hostname.domain.name/vcac`.

---

### Procedura

- 1 Selezionare **Amministrazione > Tenant**.
- 2 Fare clic su un tenant aggiunto.  
Ad esempio, per DEVTenant, fare clic su **DEVTenant**.
- 3 Fare clic su **Utenti locali**.
- 4 Fare clic sull'icona **Nuovo** (+).
- 5 In **Dettagli utente** immettere le informazioni richieste per creare un account utente locale a cui assegnare il ruolo di amministratore tenant.  
Il nome utente locale deve essere univoco per la directory locale predefinita vsphere.local.
- 6 Fare clic su **OK**.
- 7 Fare clic su **Amministratori**.
- 8 Immettere il nome utente locale nella casella di ricerca **Amministratori tenant** e premere Invio.
- 9 Nei risultati della ricerca, fare clic sul nome appropriato per aggiungere l'utente all'elenco di amministratori tenant.
- 10 Fare clic su **Fine**.
- 11 Uscire dalla console.

### Operazioni successive

- Per una distribuzione minima: [Sincronizzazione di utenti e gruppi per un collegamento di Active Directory prima della migrazione in un ambiente minimo.](#)
- Per una distribuzione ad alta disponibilità: [Sincronizzazione di utenti e gruppi per un collegamento di Active Directory prima della migrazione in un ambiente ad alta disponibilità.](#)

## Sincronizzazione di utenti e gruppi per un collegamento di Active Directory prima della migrazione in un ambiente minimo

Prima di importare utenti e gruppi in una distribuzione minima di vRealize Automation, è necessario connettersi vRealize Automation target al collegamento di Active Directory.

Eseguire questa procedura per ogni tenant. Se un tenant include più Active Directory, eseguire questa procedura per ogni Active Directory utilizzato.

### Prerequisiti

- [Creazione di un amministratore per ciascun tenant aggiunto.](#)
- Verificare di disporre dei privilegi di accesso ad Active Directory.
- Accedere a vRealize Automation come **amministratore tenant**.

### Procedura

- 1 Selezionare **Amministrazione > Gestione directory > Directory**.
- 2 Fare clic sull'icona **Aggiungi directory** (+) e selezionare **Aggiungi Active Directory su LDAP/IWA**.
- 3 Immettere le impostazioni dell'account di Active Directory.

#### ◆ Per le istanze di Active Directory non native

Opzione	Input di esempio
<b>Nome directory</b>	Immettere un nome di directory univoco. Selezionare <b>Active Directory su LDAP</b> quando si utilizza un'istanza di Active Directory non nativa.
<b>Questa directory supporta la posizione servizio DNS</b>	Deselezionare questa opzione.
<b>DN di base</b>	Immettere il DN (Distinguished Name) del punto di inizio per le ricerche nel server della directory. Ad esempio, <b>cn=users,dc=rainpole,dc=local</b> .
<b>DN di binding</b>	Immettere il DN (Distinguished Name) completo, incluso il CN (Common Name), di un account utente di Active Directory che disponga di privilegi per la ricerca degli utenti. Ad esempio, <b>cn=config_admin_infra,cn=users,dc=rainpole,dc=local</b> .
<b>Password DN di binding</b>	Immettere la password di Active Directory per l'account che può eseguire la ricerca di utenti e fare clic su <b>Prova connessione</b> per verificare la connessione alla directory configurata.

#### ◆ Per le istanze di Active Directory native

Opzione	Input di esempio
<b>Nome directory</b>	Immettere un nome di directory univoco. Selezionare <b>Active Directory (autenticazione integrata di Windows)</b> quando si utilizza un'istanza di Active Directory nativa.
<b>Nome di dominio</b>	Immettere il nome del dominio da unire.

Opzione	Input di esempio
<b>Nome utente amministratore di dominio</b>	Immettere il nome utente dell'amministratore del dominio.
<b>Password amministratore di dominio</b>	Immettere la password dell'amministratore del dominio.
<b>UPN utente di binding</b>	Utilizzare il formato di indirizzo email per immettere il nome dell'utente autorizzato ad eseguire l'autenticazione nel dominio.
<b>Password DN di binding</b>	Immettere la password dell'account di binding di Active Directory per l'account che può effettuare la ricerca di utenti.

4 Fare clic su **Salva e avanti**.

La pagina **Seleziona domini** mostra un elenco di domini.

5 Accettare l'impostazione del dominio predefinito e fare clic su **Avanti**.

6 Verificare che i nomi di attributo siano mappati agli attributi di Active Directory corretti e fare clic su **Avanti**.

7 Selezionare i gruppi e gli utenti da sincronizzare.

a Fare clic sull'icona **Nuovo** (+).

b Immettere il dominio dell'utente e fare clic su **Trova gruppi**.

Ad esempio, inserire **dc=vcac,dc=local**.

c Per selezionare i gruppi da sincronizzare, fare clic su **Seleziona**, quindi su **Avanti**.

d Nella pagina di **selezione degli utenti** selezionare gli utenti da sincronizzare e fare clic su **Avanti**.

Aggiungere solo gli utenti e i gruppi necessari per l'utilizzo di vRealize Automation. Non selezionare **Sincronizza gruppi nidificati** a meno che a tutti i gruppi nella nidificazione sia richiesto di utilizzare vRealize Automation.

8 Verificare gli utenti e i gruppi che si stanno sincronizzando con la directory e fare clic su **Sincronizza directory**.

La sincronizzazione della directory richiede un po' di tempo e viene eseguita in background.

### Operazioni successive

[Esecuzione della raccolta dati di Inventario rete e sicurezza di NSX nell'ambiente vRealize Automation di origine](#)

### Sincronizzazione di utenti e gruppi per un collegamento di Active Directory prima della migrazione in un ambiente ad alta disponibilità

Prima di importare utenti e gruppi in un ambiente vRealize Automation ad alta disponibilità, è necessario connettersi al collegamento di Active Directory.

- Eseguire i passaggi 1- 8 per ogni tenant. Se un tenant include più Active Directory, eseguire questa procedura per ogni Active Directory utilizzato.
- Ripetere i passaggi 9–10 per ogni provider di identità associato a un tenant.

## Prerequisiti

- Creazione di un amministratore per ciascun tenant aggiunto.
- Verificare di disporre dei privilegi di accesso ad Active Directory.
- Accedere a vRealize Automation come **amministratore tenant**.

## Procedura

- 1 Selezionare **Amministrazione > Gestione directory > Directory**.
- 2 Fare clic sull'icona **Aggiungi directory** (+) e selezionare **Aggiungi Active Directory su LDAP/IWA**.
- 3 Immettere le impostazioni dell'account di Active Directory.
  - ◆ Per le istanze di Active Directory non native

Opzione	Input di esempio
<b>Nome directory</b>	Immettere un nome di directory univoco. Selezionare <b>Active Directory su LDAP</b> quando si utilizza un'istanza di Active Directory non nativa.
<b>Questa directory supporta la posizione servizio DNS</b>	Deselezionare questa opzione.
<b>DN di base</b>	Immettere il DN (Distinguished Name) del punto di inizio per le ricerche nel server della directory. Ad esempio, <b>cn=users,dc=rainpole,dc=local</b> .
<b>DN di binding</b>	Immettere il DN (Distinguished Name) completo, incluso il CN (Common Name), di un account utente di Active Directory che disponga di privilegi per la ricerca degli utenti. Ad esempio, <b>cn=config_admin infra,cn=users,dc=rainpole,dc=local</b> .
<b>Password DN di binding</b>	Immettere la password di Active Directory per l'account che può eseguire la ricerca di utenti e fare clic su <b>Prova connessione</b> per verificare la connessione alla directory configurata.

- ◆ Per le istanze di Active Directory native

Opzione	Input di esempio
<b>Nome directory</b>	Immettere un nome di directory univoco. Selezionare <b>Active Directory (autenticazione integrata di Windows)</b> quando si utilizza un'istanza di Active Directory nativa.
<b>Nome di dominio</b>	Immettere il nome del dominio da unire.
<b>Nome utente amministratore di dominio</b>	Immettere il nome utente dell'amministratore del dominio.
<b>Password amministratore di dominio</b>	Immettere la password dell'account dell'amministratore del dominio
<b>UPN utente di binding</b>	Utilizzare il formato di indirizzo email per immettere il nome dell'utente autorizzato ad eseguire l'autenticazione nel dominio.
<b>Password DN di binding</b>	Immettere la password dell'account di binding di Active Directory per l'account che può effettuare la ricerca di utenti.

4 Fare clic su **Salva e avanti**.

Viene visualizzata la pagina **Seleziona domini** con l'elenco dei domini.

5 Accettare l'impostazione del dominio predefinito e fare clic su **Avanti**.

6 Verificare che i nomi di attributo siano mappati agli attributi di Active Directory corretti e fare clic su **Avanti**.

7 Selezionare i gruppi e gli utenti da sincronizzare.

a Fare clic sull'icona **Nuovo** .

b Immettere il dominio dell'utente e fare clic su **Trova gruppi**.

Ad esempio, inserire **dc=vcac,dc=local**.

c Per selezionare i gruppi da sincronizzare, fare clic su **Seleziona**, quindi su **Avanti**.

d Nella pagina di **selezione degli utenti**, selezionare gli utenti da sincronizzare e fare clic su **Avanti**.

Aggiungere solo gli utenti e i gruppi necessari per l'utilizzo di vRealize Automation. Non selezionare **Sincronizza gruppi nidificati** a meno che a tutti i gruppi nella nidificazione sia richiesto di utilizzare vRealize Automation.

8 Verificare gli utenti e i gruppi che si stanno sincronizzando con la directory e fare clic su **Sincronizza directory**.

La sincronizzazione della directory richiede un po' di tempo e viene eseguita in background.

9 Selezionare **Amministrazione > Gestione directory > Provider di identità** e fare clic sul nuovo provider di identità.

Ad esempio, **WorkspaceIDP\_\_1**.

10 Nella pagina del provider di identità selezionato aggiungere un connettore per ogni nodo.

a Seguire le istruzioni per aggiungere un connettore.

b Aggiornare il valore della proprietà **IdP Hostname** in modo che punti al nome di dominio completo del bilanciamento del carico di vRealize Automation.

c Fare clic su **Salva**.

## Operazioni successive

[Esecuzione della raccolta dati di Inventario rete e sicurezza di NSX nell'ambiente vRealize Automation di origine.](#)

## Esecuzione della raccolta dati di Inventario rete e sicurezza di NSX nell'ambiente vRealize Automation di origine

Prima di effettuare la migrazione, è necessario eseguire la raccolta dati di Inventario rete e sicurezza di NSX nell'ambiente vRealize Automation di origine.

La raccolta dati è necessaria per assicurare il funzionamento dell'azione di riconfigurazione del bilanciamento del carico in vRealize Automation 7.4 quando si esegue la migrazione dalle distribuzioni 7.1, 7.2 o 7.3.

---

**Nota** Non è necessario eseguire la raccolta dei dati nell'ambiente di origine quando si esegue la migrazione da vRealize Automation 6.2.x. vRealize Automation 6.2.x non supporta l'azione di riconfigurazione del bilanciamento del carico.

---

#### Procedura

- ◆ Prima di effettuare la migrazione a vRealize Automation 7.4, eseguire la raccolta dati di Inventario rete e sicurezza di NSX nell'ambiente vRealize Automation di origine. Vedere l'[argomento relativo all'avvio manuale della raccolta dati dell'endpoint](#) in *Gestione di vRealize Automation*.

#### Operazioni successive

[Clonazione manuale del database Microsoft SQL IaaS di origine di vRealize Automation.](#)

#### Clonazione manuale del database Microsoft SQL IaaS di origine di vRealize Automation

Prima della migrazione, è necessario eseguire il backup del database Microsoft SQL di IaaS nell'ambiente di origine di vRealize Automation e ripristinarlo in un nuovo database vuoto creato nell'ambiente vRealize Automation di destinazione.

#### Prerequisiti

- [Esecuzione della raccolta dati di Inventario rete e sicurezza di NSX nell'ambiente vRealize Automation di origine.](#)
- Ottenere informazioni sul backup e il ripristino di un database SQL Server. Cercare gli articoli disponibili in [Microsoft Developer Network](#) sulla creazione di un backup completo del database SQL Server e sul ripristino di un database SQL Server su una nuova posizione.

#### Procedura

- ◆ Creare un backup completo del database Microsoft SQL IaaS di origine di vRealize Automation 6.2.x o 7.x. Il backup viene utilizzato per ripristinare il database SQL in un nuovo database vuoto creato nell'ambiente di destinazione.

#### Operazioni successive

[Snapshot dell'ambiente target di vRealize Automation.](#)

#### Snapshot dell'ambiente target di vRealize Automation

Creare uno snapshot di ogni macchina virtuale vRealize Automation target. Se la migrazione non riesce, è possibile riprovare utilizzando gli snapshot delle macchine virtuali.

Per ulteriori informazioni, vedere la documentazione di vSphere.

#### Prerequisiti

[Clonazione manuale del database Microsoft SQL IaaS di origine di vRealize Automation.](#)

## Operazioni successive

Eseguire una delle seguenti procedure:

- [Migrazione dei dati di origine di vRealize Automation in un ambiente vRealize Automation 7.4 minimo.](#)
- [Migrazione dei dati di origine di vRealize Automation in un ambiente di vRealize Automation 7.4 ad alta disponibilità.](#)

## Procedure di migrazione

La procedura di migrazione dei dati dell'ambiente vRealize Automation di origine varia a seconda che i dati vengano migrati in un ambiente minimo o in un ambiente ad alta disponibilità.

### Migrazione dei dati di origine di vRealize Automation in un ambiente vRealize Automation 7.4 minimo

È possibile effettuare la migrazione dei dati dell'ambiente vRealize Automation corrente in una nuova installazione di vRealize Automation 7.4.

Tutti i tenant nel sistema di origine devono essere ricreati nella destinazione ed essere sottoposti alla procedura di migrazione dell'archivio identità. Per ulteriori informazioni, vedere [Migrazione degli archivi identità in VMware Identity Manager](#).

#### Prerequisiti

- [Raccolta di informazioni necessarie per la migrazione.](#)
- [Ottenere la chiave di crittografia dell'ambiente vRealize Automation di origine.](#)
- [Aggiunta di ciascun tenant dall'ambiente vRealize Automation di origine all'ambiente di destinazione.](#)
- [Creazione di un amministratore per ciascun tenant aggiunto.](#)
- [Sincronizzazione di utenti e gruppi per un collegamento di Active Directory prima della migrazione in un ambiente minimo.](#)
- [Clonazione manuale del database Microsoft SQL IaaS di origine di vRealize Automation.](#)
- [Snapshot dell'ambiente target di vRealize Automation.](#)
- Accedere alla gestione dell'appliance vRealize Automation target come **root** utilizzando la password immessa durante la distribuzione dell'appliance vRealize Automation target.

#### Procedura

- 1 Selezionare **Impostazioni vRA > Migrazione**.
- 2 Immettere le informazioni per l'appliance vRealize Automation di origine.

Opzione	Descrizione
Nome host	Il nome host dell'appliance vRealize Automation di origine.
Nome utente radice	root



Opzione	Descrizione
<b>Password root</b>	La password root immessa durante la distribuzione dell'appliance vRealize Automation.
<b>Posizione pacchetto migrazione</b>	Percorso di una directory esistente nell'appliance vRealize Automation 6.2.x o 7.x di origine in cui viene creato il pacchetto di migrazione.

### 3 Immettere le informazioni per l'appliance vRealize Automation di destinazione.

Opzione	Descrizione
<b>Nome utente radice</b>	<b>root</b>
<b>Password root</b>	La password root immessa durante la distribuzione dell'appliance vRealize Automation di destinazione.
<b>Tenant predefinito</b>	vsphere.local Non è possibile modificare questo campo.
<b>Nome utente amministratore</b>	administrator Non è possibile modificare questo campo.
<b>Password amministratore</b>	Password dell'utente administrator@vsphere.local immessa durante la distribuzione dell'ambiente vRealize Automation target.

### 4 Immettere le informazioni relative al server di database IaaS di destinazione.

Opzione	Descrizione
<b>Server di database</b>	Posizione dell'istanza di Microsoft SQL Server in cui si trova il database Microsoft SQL IaaS vRealize Automation. Se si utilizza l'istanza denominata e la porta non predefinita, specificarle nel formato <i>SERVER,PORT\INSTANCE-NAME</i> . Se si configura l'istanza di Microsoft SQL Server di destinazione per l'uso della funzione AlwaysOn Availability Group (AAG), è necessario immettere il nome dell'istanza SQL Server di destinazione come listener AAG, senza una porta o un nome dell'istanza.
<b>Nome database clonato</b>	Nome del database di origine Microsoft SQL IaaS di vRealize Automation 6.2.x o 7.x di cui è stato eseguito il backup nell'origine e il ripristino nell'ambiente target.
<b>Modalità di autenticazione</b>	<ul style="list-style-type: none"> <li>■ <b>Windows</b> Se si utilizza la modalità di autenticazione di Windows, l'utente del servizio IaaS deve disporre del ruolo db_owner di SQL Server. Le stesse autorizzazioni si applicano quando si utilizza la modalità di autenticazione di SQL Server.</li> <li>■ <b>SQL Server</b> <b>SQL Server</b> apre le caselle di testo <b>Nome login</b> e <b>Password</b>.</li> </ul>
<b>Nome login</b>	Nome di login dell'utente SQL Server con il ruolo db_owner per il database Microsoft SQL IaaS clonato.
<b>Password</b>	Password dell'utente SQL Server con il ruolo db_owner per il database Microsoft SQL IaaS clonato.
<b>Chiave di crittografia originale</b>	La chiave di crittografia originale recuperata dall'ambiente di origine. Vedere <a href="#">Ottenere la chiave di crittografia dell'ambiente vRealize Automation di origine</a> .
<b>Nuova passphrase</b>	Serie di parole utilizzate per generare una nuova chiave di crittografia. Questa passphrase viene utilizzata durante ogni installazione di un nuovo componente IaaS nell'ambiente vRealize Automation target.

## 5 Fare clic su **Convalida**.

Nella pagina è visualizzato l'avanzamento della convalida.

- Se tutti gli elementi vengono convalidati, andare al passaggio 8.
- Se non riesce la convalida di un elemento, ispezionare il messaggio di errore e il file di registro di convalida nei nodi IaaS. Per i percorsi del file di registro, vedere [Posizioni dei registri di migrazione](#). Fare clic su **Modifica impostazioni** e modificare l'elemento che crea il problema. Andare al passaggio 7.

## 6 Fare clic su **Migra**.

Nella pagina è visualizzato l'avanzamento della migrazione.

- Se la migrazione va a buon fine, la pagina visualizza tutte le attività di migrazione come completate.
- Se la migrazione non va a buon fine, ispezionare i file di registro della migrazione nell'appliance virtuale e nei nodi IaaS. Per i percorsi del file di registro, vedere [Posizioni dei registri di migrazione](#).

Terminare questi passaggi prima di riavviare la migrazione.

- a Ripristinare l'ambiente vRealize Automation di destinazione allo stato catturato durante lo snapshot precedente la migrazione.
- b Ripristinare il database Microsoft SQL IaaS di destinazione utilizzando il backup del database IaaS di origine.

### Operazioni successive

[Attività di post-migrazione.](#)

## Migrazione dei dati di origine di vRealize Automation in un ambiente di vRealize Automation 7.4 ad alta disponibilità

È possibile migrare l'ambiente di vRealize Automation corrente in una nuova installazione di vRealize Automation 7.4 configurata come ambiente ad alta disponibilità.

Tutti i tenant nel sistema di origine devono essere ricreati nella destinazione ed essere sottoposti alla procedura di migrazione dell'archivio identità. Per ulteriori informazioni, vedere [Migrazione degli archivi identità in VMware Identity Manager](#).

### Prerequisiti

- [Raccolta di informazioni necessarie per la migrazione.](#)
- [Ottenere la chiave di crittografia dell'ambiente vRealize Automation di origine.](#)
- [Aggiunta di ciascun tenant dall'ambiente vRealize Automation di origine all'ambiente di destinazione.](#)
- [Creazione di un amministratore per ciascun tenant aggiunto.](#)
- [Sincronizzazione di utenti e gruppi per un collegamento di Active Directory prima della migrazione in un ambiente ad alta disponibilità.](#)

- [Clonazione manuale del database Microsoft SQL IaaS di origine di vRealize Automation.](#)
- [Snapshot dell'ambiente target di vRealize Automation.](#)
- Accedere alla gestione dell'appliance vRealize Automation target come **root** utilizzando la password immessa durante la distribuzione dell'appliance vRealize Automation target.

## Procedura

- 1 Selezionare **Impostazioni vRA > Migrazione**.
- 2 Immettere le informazioni per l'appliance vRealize Automation di origine.

Opzione	Descrizione
<b>Nome host</b>	Il nome host dell'appliance vRealize Automation di origine.
<b>Nome utente radice</b>	<b>root</b>
<b>Password root</b>	La password root immessa durante la distribuzione dell'appliance vRealize Automation di origine.

- 3 Immettere le informazioni relative alla posizione del pacchetto di migrazione nell'appliance vRealize Automation di origine.

Opzione	Descrizione
<b>Posizione pacchetto migrazione</b>	Percorso di una directory esistente nell'appliance vRealize Automation 6.2.x o 7.x di origine in cui viene creato il pacchetto di migrazione.

- 4 Immettere le informazioni per l'appliance vRealize Automation di destinazione.

Opzione	Descrizione
<b>Nome utente radice</b>	<b>root</b>
<b>Password root</b>	La password root immessa durante la distribuzione dell'appliance vRealize Automation di destinazione.
<b>Tenant predefinito</b>	vsphere.local
<b>Nome utente amministratore</b>	administrator
<b>Password amministratore</b>	Password dell'utente administrator@vsphere.local immessa durante la distribuzione dell'ambiente vRealize Automation target.

- 5 Immettere le informazioni relative al server di database IaaS di destinazione.

Opzione	Descrizione
<b>Server di database</b>	La posizione dell'istanza di Microsoft SQL Server in cui si trova il database Microsoft SQL IaaS di vRealize Automation ripristinato. Se si utilizza l'istanza denominata e la porta non predefinita, specificarle nel formato <b>SERVER,PORT\INSTANCE-NAME</b> . Se si configura l'istanza di Microsoft SQL Server di destinazione per l'uso della funzione AlwaysOn Availability Group (AAG), è necessario immettere il nome dell'istanza SQL Server di destinazione come listener AAG, senza una porta o un nome dell'istanza.
<b>Nome database clonato</b>	Nome del database di origine Microsoft SQL IaaS di vRealize Automation 6.2.x o 7.x di cui è stato eseguito il backup nell'origine e il ripristino nell'ambiente target.

Opzione	Descrizione
<b>Modalità di autenticazione</b>	<ul style="list-style-type: none"> <li>■ <b>Windows</b> Se si utilizza la modalità di autenticazione di Windows, l'utente del servizio IaaS deve disporre del ruolo db_owner di SQL Server. Le stesse autorizzazioni si applicano quando si utilizza la modalità di autenticazione di SQL Server.</li> <li>■ <b>SQL Server</b> <b>SQL Server</b> apre le caselle di testo <b>Nome login</b> e <b>Password</b>.</li> </ul>
<b>Nome login</b>	Nome di login dell'utente SQL Server con il ruolo db_owner per il database Microsoft SQL IaaS clonato.
<b>Password</b>	Password dell'utente SQL Server con il ruolo db_owner per il database Microsoft SQL IaaS clonato.
<b>Chiave di crittografia originale</b>	La chiave di crittografia originale recuperata dall'ambiente di origine. Vedere <a href="#">Ottenere la chiave di crittografia dell'ambiente vRealize Automation di origine</a> .
<b>Nuova passphrase</b>	Serie di parole utilizzate per generare una nuova chiave di crittografia. Questa passphrase viene utilizzata durante ogni installazione di un nuovo componente IaaS nell'ambiente vRealize Automation target.

## 6 Fare clic su **Convalida**.

Nella pagina è visualizzato l'avanzamento della convalida.

- Se tutti gli elementi vengono convalidati, andare al passaggio 8.
- Se non riesce la convalida di un elemento, ispezionare il messaggio di errore e il file di registro di convalida nei nodi IaaS. Per i percorsi del file di registro, vedere [Posizioni dei registri di migrazione](#). Fare clic su **Modifica impostazioni** e modificare l'elemento che crea il problema. Andare al passaggio 7.

## 7 Fare clic su **Migra**.

Nella pagina è visualizzato l'avanzamento della migrazione.

- Se la migrazione va a buon fine, la pagina visualizza tutte le attività di migrazione come completate.
- Se la migrazione non va a buon fine, ispezionare i file di registro della migrazione nell'appliance virtuale e nei nodi IaaS. Per i percorsi del file di registro, vedere [Posizioni dei registri di migrazione](#).

Terminare questi passaggi prima di riavviare la migrazione.

- Ripristinare l'ambiente vRealize Automation di destinazione allo stato catturato durante lo snapshot precedente la migrazione.
- Ripristinare il database Microsoft SQL IaaS target utilizzando il backup del database IaaS di origine.

## Operazioni successive

[Attività di post-migrazione](#).

## Attività di post-migrazione

Dopo aver eseguito la migrazione vRealize Automation, eseguire le attività successive alla migrazione in base alla propria situazione.

---

**Nota** Dopo aver eseguito la migrazione degli archivi identità, gli utenti di vRealize Code Stream devono riassegnare manualmente i ruoli di vRealize Code Stream.

---

### Aggiunta di amministratori tenant e IaaS dall'ambiente vRealize Automation 6.2.x di origine

È necessario eliminare e ripristinare gli amministratori tenant di vRealize Automation 6.2.x in ciascun tenant dopo la migrazione.

Eseguire la procedura seguente per ciascun tenant nella console vRealize Automation di destinazione.

---

**Nota** Se si effettua la migrazione da un ambiente vRealize Automation 7.x, non è necessario eseguire questa procedura.

---

#### Prerequisiti

- Migrazione riuscita all'ultima versione di vRealize Automation.
- Accedere alla console di vRealize Automation target come **amministratore** con la password immessa durante la distribuzione dell'appliance vRealize Automation target.

#### Procedura

- 1 Selezionare **Amministrazione > Tenant**.
- 2 Fare clic su un nome di tenant.
- 3 Fare clic su **Amministratori**.
- 4 Creare un elenco che includa nome e nome utente di tutti gli amministratori tenant.
- 5 Puntare su ciascun amministratore e fare clic sull'icona di eliminazione (Elimina) finché non vengono eliminati tutti gli amministratori.
- 6 Fare clic su **Fine**.
- 7 Nella pagina Tenant fare clic nuovamente sul nome del tenant.
- 8 Fare clic su **Amministratori**.
- 9 Immettere nella casella di ricerca appropriata il nome di ciascun utente eliminato e premere Invio.
- 10 Fare clic sul nome dell'utente appropriato dai risultati della ricerca per aggiungere nuovamente l'utente come amministratore.

Al termine, l'elenco degli amministratori tenant sarà uguale all'elenco degli amministratori eliminati.

- 11 Fare clic su **Fine**.

### Esecuzione di Prova connessione e verifica degli endpoint migrati

La migrazione a vRealize Automation 7.4 apporta modifiche agli endpoint nell'ambiente target.

Dopo aver effettuato la migrazione a vRealize Automation 7.4, è necessario utilizzare l'azione **Prova connessione** per tutti gli endpoint applicabili. Potrebbe anche essere necessario apportare modifiche ad alcuni endpoint migrati. Per ulteriori informazioni, vedere [Considerazioni sull'utilizzo degli endpoint aggiornati o migrati](#).

L'impostazione di sicurezza predefinita per gli endpoint aggiornati o migrati prevede che i certificati non attendibili non vengano accettati.

Dopo l'aggiornamento o la migrazione da un'installazione precedente di vRealize Automation, se venivano utilizzati certificati non attendibili, è necessario eseguire la procedura che segue per tutti gli endpoint vSphere e NSX per consentire la convalida dei certificati. In caso contrario, le operazioni sugli endpoint non riusciranno e verranno restituiti errori di certificato. Per ulteriori informazioni, vedere gli articoli della Knowledge Base di VMware *Endpoint communication is broken after upgrade to vRA 7.3* (2150230) all'indirizzo <http://kb.vmware.com/kb/2150230> e *How to download and install vCenter Server root certificates to avoid Web Browser certificate warnings* (2108294) all'indirizzo <http://kb.vmware.com/kb/2108294>.

- 1 Dopo l'aggiornamento o la migrazione, accedere alla macchina dell'agente vRealize Automation vSphere e riavviare gli agenti vSphere utilizzando la scheda **Servizi**.

La migrazione potrebbe non riavviare tutti gli agenti, pertanto è necessario riavviarli manualmente se richiesto.

- 2 Attendere il completamento di almeno un report di ping. Questa operazione richiede uno o due minuti.
- 3 Dopo che gli agenti vSphere avranno avviato la raccolta dati, accedere a vRealize Automation come amministratore IaaS.
- 4 Fare clic su **Infrastruttura > Endpoint > Endpoint**.
- 5 Modificare un endpoint vSphere e fare clic su **Prova connessione**.
- 6 Se viene visualizzato un prompt sul certificato, fare clic su **OK** per accettare il certificato.  
  
In caso contrario, è possibile che al momento il certificato sia correttamente archiviato presso un'autorità root attendibile del servizio di hosting della macchina Windows per l'endpoint, ad esempio come macchina agente proxy o come macchina DEM.
- 7 Fare clic su **OK** per accettare il certificato e salvare l'endpoint.
- 8 Ripetere questa procedura per ogni endpoint vSphere.
- 9 Ripetere questa procedura per ogni endpoint NSX.

Se l'azione **Prova connessione** riesce ma alcune operazioni di provisioning o di raccolta dati hanno esito negativo, è possibile installare lo stesso certificato in tutte le macchine agente che servono l'endpoint e su tutte le macchine DEM. In alternativa, è possibile disinstallare il certificato dalle macchine esistenti e ripetere la procedura precedente per l'endpoint in cui si verifica l'errore.

## Esecuzione della raccolta dati di Inventario rete e sicurezza NSX nell'ambiente vRealize Automation 7.4 target

Dopo aver completato la migrazione, è necessario eseguire la raccolta dati di Inventario Rete e sicurezza NSX nell'ambiente vRealize Automation 7.4 target.

La raccolta dati è necessaria per assicurare il funzionamento dell'azione di riconfigurazione del bilanciamento del carico in vRealize Automation 7.4 per le distribuzioni 7.1, 7.2 e 7.3.

---

**Nota** Non è necessario eseguire la raccolta dati se è stata eseguita la migrazione di vRealize Automation 6.2.x alla versione 7.4.

---

### Prerequisiti

- [Esecuzione della raccolta dati di Inventario rete e sicurezza di NSX nell'ambiente vRealize Automation di origine](#) .
- Effettuare la migrazione a vRealize Automation 7.4 correttamente.

### Procedura

- ◆ Prima di effettuare la migrazione a vRealize Automation 7.4, eseguire la raccolta dati di Inventario rete e sicurezza di NSX nell'ambiente vRealize Automation target. Vedere [l'argomento relativo all'avvio manuale della raccolta dati dell'endpoint](#) in *Gestione di vRealize Automation*.

## Riconfigurazione dei bilanciamenti del carico dopo la migrazione in un ambiente ad alta disponibilità

Al termine della migrazione in un ambiente ad alta disponibilità, è necessario eseguire queste attività per ogni servizio di bilanciamento del carico.

### Prerequisiti

[Migrazione dei dati di origine di vRealize Automation in un ambiente di vRealize Automation 7.4 ad alta disponibilità](#).

### Procedura

- 1 Ripristinare le impostazioni originali per il controllo dell'integrità in modo che i nodi di replica possano accettare il traffico in entrata, configurando i servizi di bilanciamento del carico per gli elementi elencati di seguito.
  - Appliance vRealize Automation.
  - Server Web IaaS che ospita il servizio di gestione dei modelli.
  - Manager Service.
- 2 Ripristinare il valore predefinito per le impostazioni di timeout dei servizi di bilanciamento del carico.

## Migrazione di un server Orchestrator esterno in vRealize Automation 7.4

È possibile effettuare la migrazione del server Orchestrator esterno esistente in un'istanza di vRealize Orchestrator incorporata in vRealize Automation.

È possibile distribuire vRealize Orchestrator come istanza esterna del server e configurare vRealize Automation per il funzionamento con tale istanza esterna oppure configurare e utilizzare il server vRealize Orchestrator incluso in Appliance vRealize Automation.

VMware consiglia di effettuare la migrazione del server vRealize Orchestrator esterno nel server Orchestrator integrato in vRealize Automation. La migrazione da un server Orchestrator esterno a uno incorporato offre i seguenti vantaggi:

- Riduce il costo totale di proprietà.
- Semplifica il modello di distribuzione.
- Migliora l'efficienza operativa.

**Nota** È consigliabile utilizzare il server vRealize Orchestrator esterno nei casi seguenti:

- Più tenant nell'ambiente di vRealize Automation.
- Ambiente diffuso geograficamente.
- Gestione del carico di lavoro.
- Uso di plug-in specifici, ad esempio versioni del plug-in Site Recovery Manager precedenti alla 6.5.

## Migration Scenarios

The procedure of migrating an external vRealize Orchestrator instance to a vRealize Orchestrator instance embedded in vRealize Automation varies depending on the setup that you have. Several migration scenarios exist based on whether the external Orchestrator server is Windows-based or a virtual appliance, using the embedded database or an external one, and other conditions. You can combine the migration process with an upgrade of vRealize Orchestrator, vRealize Automation, or both. In this case, the migration procedure depends on the source versions of the products.

## Migration Scenario Matrix

You can choose a migration scenario based on the source deployment.

vRealize Orchestrator Deployment	vRealize Automation Deployment	Migration Scenario
vRealize Orchestrator 6.0.3 Virtual Appliance	vRealize Automation 6.2.3	<a href="#">Migrazione di un'appliance virtuale vRealize Orchestrator 6.x esterna in vRealize Automation 7.4</a>
vRealize Orchestrator 6.0.4 on Windows	vRealize Automation 6.2.4	<a href="#">Migrazione di un server vRealize Orchestrator 6.x esterno su Windows in vRealize Automation 7.4</a>
vRealize Orchestrator 6.0.4 Virtual Appliance	vRealize Automation 6.2.4	<a href="#">Migrazione di un'appliance virtuale vRealize Orchestrator 6.x esterna in vRealize Automation 7.4</a>
vRealize Orchestrator 6.0.5 Virtual Appliance	vRealize Automation 6.2.5	<a href="#">Migrazione di un'appliance virtuale vRealize Orchestrator 6.x esterna in vRealize Automation 7.4</a>
vRealize Orchestrator 7.0 Virtual Appliance with an external Oracle Database 12 c	vRealize Automation 7.0 or IaaS	<a href="#">Migrate an External vRealize Orchestrator 7.x to vRealize Automation 7.2</a>



vRealize Orchestrator Deployment	vRealize Automation Deployment	Migration Scenario
vRealize Orchestrator 7.0.1 Virtual Appliance with an external PostgreSQL 9.3.9 database	vRealize Automation 7.0.1 or IaaS	<a href="#">Migrate an External vRealize Orchestrator 7.x to vRealize Automation 7.2</a>
vRealize Orchestrator 7.1 Virtual Appliance	vRealize Automation 7.1	<a href="#">Migrate an External vRealize Orchestrator 7.x to vRealize Automation 7.2</a>
vRealize Orchestrator 7.2 Virtual Appliance	vRealize Automation 7.2	<a href="#">Migrate an External vRealize Orchestrator 7.x to vRealize Automation 7.2</a>
vRealize Orchestrator 7.3 Virtual Appliance	vRealize Automation 7.3	<a href="#">Migrazione di un server vRealize Orchestrator 7.x esterno in vRealize Automation 7.4</a>
vRealize Orchestrator 6.0.3 on Windows	vRealize Automation 6.2.3	<a href="#">Migrazione della configurazione di Orchestrator da Windows all'appliance virtuale</a>

### Migrazione della configurazione di Orchestrator da Windows all'appliance virtuale

È possibile eseguire la migrazione della configurazione autonoma Windows di Orchestrator 5.5.x e 6.x in Orchestrator Appliance.

#### Prerequisiti

- Distribuire e configurare un nodo Orchestrator nella versione target. Vedere [Configurazione di un server Orchestrator autonomo](#).
- Se l'Orchestrator di origine utilizza un certificato di firma pacchetto SHA1, accertarsi di rigenerare il certificato utilizzando un algoritmo di firma più complesso. L'algoritmo di firma consigliato è SHA2.
- Interrompere il servizio del server Orchestrator nelle istanze di Orchestrator di origine e di destinazione.
- Eseguire una copia di backup del database del server Orchestrator di origine, incluso lo schema di database.

**Nota** Se si intende utilizzare l'ambiente Orchestrator di origine fino al completamento della configurazione del nuovo ambiente, creare una copia del database di origine. In caso contrario, è possibile configurare il database Orchestrator target per utilizzare lo stesso database, ma l'ambiente Orchestrator di origine non funzionerà in quanto lo schema di database viene aggiornato alla versione del database Orchestrator target.

#### Procedura

- 1 Scaricare lo strumento di migrazione dal server Orchestrator di destinazione.
  - a Accedere a Control Center come **root**.
  - b Aprire la pagina **Esporta/Importa configurazione** e fare clic sulla scheda **Importa configurazione**.
  - c Scaricare lo strumento di migrazione come specificato nella descrizione nella pagina o scaricarlo direttamente da [https://orchestrator\\_server\\_IP\\_or\\_DNS\\_name:8283/vco-controlcenter/api/server/migration-tool](https://orchestrator_server_IP_or_DNS_name:8283/vco-controlcenter/api/server/migration-tool).

## 2 Esportare la configurazione di Orchestrator dal server Orchestrator di origine.

- a Estrarre l'archivio scaricato nella cartella di installazione di Orchestrator.  
Il percorso predefinito della cartella di installazione di Orchestrator in un'installazione basata su Windows è C:\Program Files\VMware\Orchestrator.
- b Impostare la variabile di ambiente PATH in modo che punti alla cartella bin di Java JRE installato con Orchestrator.
- c Utilizzare il prompt dei comandi di Windows per passare alla cartella bin nella cartella di installazione di Orchestrator.

Per impostazione predefinita, il percorso della cartella bin è C:\Program Files\VMware\Orchestrator\migration-cli\bin.

- d Eseguire il comando export dalla riga di comando.

```
C:\Program Files\VMware\Orchestrator\migration-cli\bin\vro-migrate.bat export
```

Questo comando combina i file di configurazione e i plug-in di VMware vRealize Orchestrator in un archivio di esportazione.

Viene creato un archivio con nome file orchestrator-config-export-orchestrator\_ip\_address-date\_hour nella stessa cartella della cartella migration-cli.

## 3 Importare la configurazione nell'istanza di Orchestrator target.

- a Accedere a Control Center come **root**.
- b Aprire **Esporta/Importa configurazione** in Control Center e fare clic sulla scheda **Importa configurazione**.
- c Cercare e selezionare il file .ZIP esportato dall'istanza di Orchestrator di origine.
- d Immettere la password utilizzata in fase di esportazione della configurazione.  
Lasciare il campo vuoto se l'esportazione della configurazione è stata effettuata senza password.
- e Selezionare il tipo di importazione.

- f Se si sta importando la configurazione in un server Orchestrator esterno, scegliere se importare le impostazioni del database.

---

**Nota** Se i server Orchestrator di origine e target non sono configurati per l'utilizzo dello stesso database esterno, lasciare deselezionata la casella di controllo **Esegui migrazione impostazioni database** per evitare l'aggiornamento dello schema del database alla versione più recente. In caso contrario, l'ambiente Orchestrator di origine smetterebbe di funzionare.

È necessario configurare il database che il server Orchestrator target utilizzerà prima della migrazione.

---

- g Fare clic su **IMPORTA** per completare la migrazione.

Viene visualizzato un messaggio che conferma il completamento dell'importazione della configurazione. Il servizio del server Orchestrator dell'istanza di Orchestrator target viene riavviato automaticamente.

- 4 Se l'istanza di vRealize Orchestrator target utilizza come provider di autenticazione un server diverso da quello utilizzato dall'istanza di Orchestrator di origine, importare nell'archivio attendibile del server Orchestrator target il certificato SSL del provider di autenticazione per il cui utilizzo è stato configurato.
  - a Nella pagina **Certificati** in Control Center fare clic su **Importa da URL**.
  - b Specificare l'URL dell'istanza di vRealize Automation o vSphere.

Un messaggio indica che la migrazione è stata completata correttamente. Il servizio del server Orchestrator viene riavviato automaticamente.

#### Operazioni successive

Verificare che Orchestrator sia configurato correttamente nella pagina **Convalida configurazione** in Control Center.

#### Migrazione di un server vRealize Orchestrator 6.x esterno su Windows in vRealize Automation 7.4

Dopo aver aggiornato vRealize Automation dalla versione 6.x alla versione 7.4, è possibile effettuare la migrazione del server Orchestrator 6.x esterno esistente installato su Windows nel server Orchestrator integrato in vRealize Automation 7.4.

---

**Nota** Se è presente un ambiente vRealize Automation distribuito con più nodi di Appliance vRealize Automation, eseguire la procedura di migrazione solo nel nodo di vRealize Automation primario.

---

#### Prerequisiti

- Aggiornare o migrare vRealize Automation alla versione 7.4. Per ulteriori informazioni, vedere *Aggiornamento di vRealize Automation in Installazione o Aggiornamento di vRealize Automation*.
- Se l'Orchestrator di origine utilizza un certificato di firma pacchetto SHA1, accertarsi di rigenerare il certificato utilizzando un algoritmo di firma più complesso. L'algoritmo di firma consigliato è SHA2.

- Arrestare il servizio del server Orchestrator esterno.
- Eseguire il backup del database del server Orchestrator esterno, incluso lo schema di database.

## Procedura

- 1 Scaricare lo strumento di migrazione dal server Orchestrator di destinazione.
  - a Accedere all'Appliance vRealize Automation su SSH come **root**.
  - b Scaricare l'archivio `migration-tool.zip` che si trova nella directory `/var/lib/vco/downloads`.
- 2 Esportare la configurazione di Orchestrator dal server Orchestrator di origine.
  - a Impostare la variabile di ambiente `PATH` in modo che punti alla cartella `bin` di Java JRE installato con Orchestrator.
  - b Caricare lo strumento di migrazione nel server Windows in cui è installato il server Orchestrator esterno.
  - c Estrarre l'archivio scaricato nella cartella di installazione di Orchestrator.  
Il percorso predefinito della cartella di installazione di Orchestrator in un'installazione basata su Windows è `C:\Program Files\VMware\Orchestrator`.
  - d Eseguire il prompt dei comandi di Windows come amministratore e passare alla cartella `bin` nella cartella di installazione di Orchestrator.  
Per impostazione predefinita, il percorso della cartella `bin` è `C:\Program Files\VMware\Orchestrator\migration-cli\bin`.
  - e Eseguire il comando `export` dalla riga di comando.

```
C:\Program Files\VMware\Orchestrator\migration-cli\bin\vro-migrate.bat export
```

Questo comando combina i file di configurazione e i plug-in di VMware vRealize Orchestrator in un archivio di esportazione.

L'archivio viene creato nella stessa cartella `migration-cli`.

- 3 Effettuare la migrazione della configurazione esportata nel server Orchestrator integrato in vRealize Automation 7.4.
  - a In Appliance vRealize Automation, arrestare il servizio del server Orchestrator e il servizio Control Center del server vRealize Orchestrator integrato.
 

```
service vco-server stop && service vco-configurator stop
```
  - b Caricare il file di configurazione esportato nella directory `/usr/lib/vco/tools/configuration-cli/bin` in Appliance vRealize Automation.

- c Modificare la proprietà del file di configurazione del server Orchestrator esportato.

```
chown vco:vco orchestrator-config-export-orchestrator_ip_address-date_hour.zip
```

- d Importare il file di configurazione del server Orchestrator nel server vRealize Orchestrator integrato eseguendo lo script vro-configure con il comando import.

```
./vro-configure.sh import --type embedded --path orchestrator-config-export-orchestrator_appliance_ip-date_hour.zip
```

- e Rimuovere tutti i certificati dal keystore del database.

```
./vro-configuration.sh untrust --reset-db
```

- 4 Migrare il database nel database PostgreSQL interno mediante l'esecuzione dello script vro-configure con il comando db-migrate.

```
./vro-configure.sh db-migrate --sourceJdbcUrl JDBC_connection_URL --sourceDbUsername database_user --sourceDbPassword database_user_password
```

**Nota** Racchiudere tra apici le password contenenti caratteri speciali.

Il valore di *JDBC\_connection\_URL* dipende dal tipo di database utilizzato.

PostgreSQL: *jdbc:postgresql://host:port/database\_name*

MSSQL: *jdbc:jtds:sqlserver://host:port/database\_name\*; if using SQL authentication and MSSQL: *jdbc:jtds:sqlserver://host:port/database\_name\;domain=domain\;useNTLMv2=TRUE* if using Windows authentication.

Oracle: *jdbc:oracle:thin:@host:port:database\_name*

Le informazioni di accesso del database predefinite sono:

<i>database_name</i>	vmware
<i>database_user</i>	vmware
<i>database_user_password</i>	vmware

La migrazione di un server vRealize Orchestrator 6.x esterno installato su Windows in un'istanza di vRealize Orchestrator incorporata in vRealize Automation 7.4 è stata eseguita correttamente.

### Operazioni successive

Configurare il server vRealize Orchestrator integrato. Vedere [Configurazione del server vRealize Orchestrator integrato](#).

## Migrazione di un'appliance virtuale vRealize Orchestrator 6.x esterna in vRealize Automation 7.4

Una volta aggiornato vRealize Automation dalla versione 6.x alla versione 7.4, è possibile effettuare la migrazione dell'appliance virtuale Orchestrator 6.x esterna nel server Orchestrator integrato in vRealize Automation 7.4.

**Nota** Se è presente un ambiente vRealize Automation distribuito con più nodi di Appliance vRealize Automation, eseguire la procedura di migrazione solo nel nodo di vRealize Automation primario.

### Prerequisiti

- Aggiornare o migrare vRealize Automation alla versione 7.4. Per ulteriori informazioni, vedere *Aggiornamento di vRealize Automation in Installazione o Aggiornamento di vRealize Automation*.
- Se l'Orchestrator di origine utilizza un certificato di firma pacchetto SHA1, accertarsi di rigenerare il certificato utilizzando un algoritmo di firma più complesso. L'algoritmo di firma consigliato è SHA2.
- Arrestare il servizio del server Orchestrator esterno.
- Eseguire il backup del database del server Orchestrator esterno, incluso lo schema di database.

### Procedura

- 1 Scaricare lo strumento di migrazione dal server Orchestrator di destinazione al server Orchestrator di origine.

- a Accedere all'appliance virtuale vRealize Orchestrator 6.x su SSH come **root**.
- b Nella directory `/var/lib/vco`, eseguire il comando `scp` per scaricare l'archivio `migration-tool.zip`.

```
scp root@vra-va-hostname.domain.name:/var/lib/vco/downloads/migration-tool.zip ./
```

- c Eseguire il comando `unzip` per estrarre l'archivio dello strumento di migrazione.

```
unzip migration-tool.zip
```

- 2 Esportare la configurazione di Orchestrator dal server Orchestrator di origine.

- a Nella directory `/var/lib/vco/migration-cli/bin`, eseguire il comando `export`.

```
./vro-migrate.sh export
```

Questo comando combina i file di configurazione e i plug-in di VMware vRealize Orchestrator in un archivio di esportazione.

Viene creato un archivio con nome di file `orchestrator-config-export-orchestrator_ip_address-date_hour.zip` nella cartella `/var/lib/vco`.

### 3 Effettuare la migrazione della configurazione esportata nel server Orchestrator integrato in vRealize Automation 7.4.

- a Accedere all'Appliance vRealize Automation su SSH come **root**.
- b Arrestare il servizio del server Orchestrator e il servizio Control Center del server vRealize Orchestrator integrato.

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

- c Nella directory `/usr/lib/vco/tools/configuration-cli/bin`, eseguire il comando `scp` per scaricare l'archivio di configurazione esportato.

```
scp root@orchestrator_ip_or_DNS_name:/var/lib/vco/orchestrator-config-export-orchestrator_ip_address-date_hour.zip ./
```

- d Modificare la proprietà del file di configurazione del server Orchestrator esportato.

```
chown vco:vco orchestrator-config-export-orchestrator_ip_address-date_hour.zip
```

- e Importare il file di configurazione del server Orchestrator nel server vRealize Orchestrator integrato eseguendo lo script `vro-configure` con il comando `import`.

```
./vro-configure.sh import --type embedded --path orchestrator-config-export-orchestrator_appliance_ip-date_hour.zip
```

### 4 Se il server Orchestrator esterno da cui si desidera effettuare la migrazione utilizza il database PostgreSQL integrato, modificare i suoi file di configurazione del database.

- a Nel file `/var/vmware/vpostgres/current/pgdata/postgresql.conf`, rimuovere il commento per la riga `listen_addresses`.
- b Impostare i valori di `listen_addresses` su un carattere jolly (\*).

```
listen_addresses = '*'
```

- c Aggiungere una riga al file `/var/vmware/vpostgres/current/pgdata/pg_hba.conf`.

```
host all all vra-va-ip-address/32 md5
```

---

**Nota** Il file `pg_hba.conf` richiede l'uso di un formato di prefisso CIDR al posto di un indirizzo IP e di una subnet mask.

---

- d Riavviare il servizio del server PostgreSQL.

```
service vpostgres restart
```

- 5 Migrare il database nel database PostgreSQL interno mediante l'esecuzione dello script vro-configure con il comando db-migrate.

```
./vro-configure.sh db-migrate --sourceJdbcUrl JDBC_connection_URL --sourceDbUsername database_user
--sourceDbPassword database_user_password
```

**Nota** Racchiudere tra apici le password contenenti caratteri speciali.

Il valore di *JDBC\_connection\_URL* dipende dal tipo di database utilizzato.

PostgreSQL: `jdbc:postgresql://host:port/database_name`

MSSQL: `jdbc:jtds:sqlserver://host:port/database_name\;` if using SQL authentication and MSSQL:  
`jdbc:jtds:sqlserver://host:port/database_name\;domain=domain\;useNTLMv2=TRUE` if using Windows authentication.

Oracle: `jdbc:oracle:thin:@host:port:database_name`

Le informazioni di accesso del database predefinite sono:

<i>database_name</i>	vmware
<i>database_user</i>	vmware
<i>database_user_password</i>	vmware

- 6 Rimuovere tutti i certificati dal keystore del database.

```
./vro-configure.sh untrust --reset-db
```

- 7 Reinstallare i plug-in di Orchestrator.
  - a Accedere a Control Center come **root**.
  - b Fare clic su **Risoluzione dei problemi**.
  - c Fare clic su **Forza reinstallazione plug-in**.
- 8 Avviare il servizio del server di Orchestrator.
- 9 Ripristinare la configurazione predefinita dei file `postgresql.conf` e `pg_hba.conf`.
  - a Riavviare il servizio del server PostgreSQL.

La migrazione di un'appliance virtuale vRealize Orchestrator 6.x esterna in un'istanza di vRealize Orchestrator incorporata in vRealize Automation 7.4 è stata eseguita correttamente.

#### Operazioni successive

Configurare il server vRealize Orchestrator integrato. Vedere [Configurazione del server vRealize Orchestrator integrato](#).



## Migrazione di un server vRealize Orchestrator 7.x esterno in vRealize Automation 7.4

È possibile esportare la configurazione dall'istanza del server Orchestrator esterno esistente e importarla nel server Orchestrator integrato in vRealize Automation.

**Nota** Se sono presenti più nodi di Appliance vRealize Automation, eseguire la procedura di migrazione solo nel nodo vRealize Automation primario.

### Prerequisiti

- Aggiornare o migrare vRealize Automation alla versione 7.4. Per ulteriori informazioni, vedere *Aggiornamento di vRealize Automation in Installazione o Aggiornamento di vRealize Automation*.
- Arrestare il servizio del server Orchestrator esterno.
- Eseguire il backup del database del server Orchestrator esterno, incluso lo schema di database.

### Procedura

- 1 Esportare la configurazione dal server Orchestrator esterno.
  - a Accedere al servizio Control Center del server Orchestrator esterno come **root** o come **amministratore** a seconda della versione di origine.
  - b Arrestare il servizio del server Orchestrator dalla pagina **Opzioni di avvio** per impedire modifiche indesiderate al database.
  - c Passare alla pagina **Esporta/Importa configurazione**.
  - d Nella pagina **Esporta configurazione**, selezionare **Esporta configurazione server, Plug-in bundle** ed **Esporta configurazioni plug-in**.
- 2 Effettuare la migrazione della configurazione esportata nell'istanza del server Orchestrator incorporato.
  - a Caricare il file di configurazione di Orchestrator incorporato nella directory `/usr/lib/vco/tools/configuration-cli/bin` di Appliance vRealize Automation.
  - b Accedere all'Appliance vRealize Automation su SSH come **root**.
  - c Arrestare il servizio del server Orchestrator e il servizio Control Center del server vRealize Orchestrator integrato.

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

- d Importare il file di configurazione del server Orchestrator nel server vRealize Orchestrator integrato eseguendo lo script `vro-configure` con il comando `import`.

```
./vro-configure.sh import --type embedded --path orchestrator-config-export-orchestrator_appliance_ip-date_hour.zip
```

- 3 Se il server Orchestrator esterno da cui si desidera effettuare la migrazione utilizza il database PostgreSQL integrato, modificare i suoi file di configurazione del database.

- Nel file `/var/vmware/vpostgres/current/pgdata/postgresql.conf`, rimuovere il commento per la riga `listen_addresses`.
- Impostare i valori di `listen_addresses` su un carattere jolly (\*).

```
listen_addresses = '*'
```

- Aggiungere una riga al file `/var/vmware/vpostgres/current/pgdata/pg_hba.conf`.

```
host all all vra-va-ip-address/32 md5
```

**Nota** Il file `pg_hba.conf` richiede l'uso di un formato di prefisso CIDR al posto di un indirizzo IP e di una subnet mask.

- Riavviare il servizio del server PostgreSQL.

```
service vpostgres restart
```

- 4 Migrare il database nel database PostgreSQL interno mediante l'esecuzione dello script `vro-configure` con il comando `db-migrate`.

```
./vro-configure.sh db-migrate --sourceJdbcUrl JDBC_connection_URL --sourceDbUsername database_user  
--sourceDbPassword database_user_password
```

**Nota** Racchiudere tra apici le password contenenti caratteri speciali.

Il valore di `JDBC_connection_URL` dipende dal tipo di database utilizzato.

PostgreSQL: `jdbc:postgresql://host:port/database_name`

MSSQL: `jdbc:jtds:sqlserver://host:port/database_name\;` if using SQL authentication and MSSQL: `jdbc:jtds:sqlserver://host:port/database_name\;domain=domain\;useNTLMv2=TRUE` if using Windows authentication.

Oracle: `jdbc:oracle:thin:@host:port:database_name`

Le informazioni di accesso del database predefinite sono:

<code>database_name</code>	vmware
<code>database_user</code>	vmware
<code>database_user_password</code>	vmware

- 5 Rimuovere tutti i certificati dal keystore del database.

```
./vro-configuration.sh untrust --reset-db
```

- 6 Reinstallare i plug-in di Orchestrator.
  - a Accedere a Control Center come **root**.
  - b Fare clic su **Risoluzione dei problemi**.
  - c Fare clic su **Forza reinstallazione plug-in**.
- 7 Avviare il servizio del server di Orchestrator.
- 8 Ripristinare la configurazione predefinita dei file `postgresql.conf` e `pg_hba.conf`.
  - a Riavviare il servizio del server PostgreSQL.

È stata effettuata correttamente la migrazione di un'istanza del server Orchestrator esterno a un'istanza di vRealize Orchestrator incorporata in vRealize Automation.

#### Operazioni successive

Configurare il server vRealize Orchestrator integrato. Vedere [Configurazione del server vRealize Orchestrator integrato](#).

#### Configurazione del server vRealize Orchestrator integrato

Dopo aver esportato una configurazione di vRealize Orchestrator esterna e averla importata in vRealize Automation, configurare il server vRealize Orchestrator integrato in vRealize Automation.

#### Prerequisiti

Migrazione della configurazione dal server vRealize Orchestrator esterno a quello interno.

#### Procedura

- 1 Accedere come utente root a una sessione del prompt dei comandi nell'appliance vRealize Automation.
- 2 Avviare i servizi per il server e il centro di controllo di vRealize Orchestrator:

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

- 3 Accedere come utente root al centro di controllo di vRealize Orchestrator integrato.

<https://vrealize-automation-appliance-FQDN:8283/vco-controlcenter/config>

---

**Nota** Se la versione dell'istanza esterna di vRealize Orchestrator è uguale a quella dell'istanza interna, è possibile ignorare il passaggio successivo.

---

- 4 Nel centro di controllo fare clic su **Convalida configurazione** e verificare che vRealize Orchestrator sia configurato correttamente.

- 5 Nel centro di controllo fare clic su **Certificati**, fare clic su **Certificato di firma del pacchetto** e generare un nuovo certificato di firma del pacchetto.
- 6 Nel centro di controllo fare clic su **Configura provider autenticazione**.  
Per le opzioni **Tenant predefinito** e **Gruppo di amministratori** vengono impostati i valori predefiniti `vsphere.local` e `vsphere.local\vcoadmins`. Modificare le impostazioni predefinite impostando i valori appropriati per il proprio ambiente.
- 7 Nell'interfaccia di gestione dell'appliance vRealize Automation verificare che vco-server sia REGISTRATO in **Servizi**.
- 8 Selezionare i servizi vco del server vRealize Orchestrator esterno e fare clic su **Annulla registrazione**.

#### Operazioni successive

- Importare i certificati considerati attendibili nel server vRealize Orchestrator esterno, nell'archivio di attendibilità del server vRealize Orchestrator integrato. Per ulteriori informazioni, vedere [Gestione dei certificati di Orchestrator](#).
- Unire i nodi di replica di vRealize Automation al cluster di vRealize Automation per sincronizzare la configurazione di vRealize Orchestrator.

Per ulteriori informazioni, vedere la *sezione relativa alla riconfigurazione del server vRealize Orchestrator integrato di destinazione per il supporto dell'alta disponibilità* in *Installazione o aggiornamento di vRealize Automation*.

---

**Nota** Le istanze di vRealize Orchestrator vengono incluse automaticamente nel cluster e sono disponibili per l'utilizzo.

---

- Riavviare il servizio vco-configurator in tutti i nodi del cluster.
- Aggiornare l'endpoint di vRealize Orchestrator in modo che punti al server vRealize Orchestrator integrato di cui è stata eseguita la migrazione.
- Aggiungere l'host vRealize Automation e l'host IaaS all'inventario del plug-in vRealize Automation, eseguendo i workflow per l'aggiunta di un host vRA e l'aggiunta dell'host IaaS di un host vRA.

#### Aggiornamento del vRealize Orchestrator incorporato per considerare attendibili i certificati vRealize Automation

Se si aggiorna o si modificano i certificati di Appliance vRealize Automation o IaaS, è necessario aggiornare vRealize Orchestrator modo che consideri attendibile i certificati nuovi o aggiornati.

Questa procedura si applica a tutte le distribuzioni vRealize Automation che utilizzano un'istanza di vRealize Orchestrator incorporata. Se si utilizza un'istanza di vRealize Orchestrator esterna, vedere [l'argomento che illustra come aggiornare un'istanza di vRealize Orchestrator esterna in modo che consideri attendibili i certificati di vRealize Automation](#).

---

**Nota** La procedura reimposta l'autenticazione di tenant e gruppo alle impostazioni predefinite. Se la configurazione di autenticazione è stata personalizzata, prendere nota delle modifiche in modo da poterle riconfigurare dopo aver completato la procedura.

---

Consultare la documentazione di vRealize Orchestrator per informazioni sull'aggiornamento e la sostituzione dei certificati vRealize Orchestrator.

Se si sostituisce o aggiornano i certificati vRealize Automation senza aver completato la procedura, il Control Center di vRealize Orchestrator potrebbe essere inaccessibile e possono comparire errori nei file di registro vco-server e vco-configurator.

Possono verificarsi problemi con l'aggiornamento dei certificati anche se vRealize Orchestrator è configurato per l'autenticazione in un altro tenant e gruppo anziché vRealize Automation. Vedere <https://kb.vmware.com/kb/2147612>.

## Procedura

- 1 Arrestare il server di vRealize Orchestrator e i servizi del Control Center.

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

- 2 Reimpostare il provider di autenticazione di vRealize Orchestrator.
  - a Eseguire il comando `/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh reset-authentication`.
  - b Eliminare `/etc/vco/app-server/vco-registration-id`.
  - c Avviare `vcac-vami vco-service-reconfigure`.
- 3 Avviare i servizi del server vRealize Orchestrator e del Control Center.

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

## Differenze di Control Center tra server Orchestrator esterni e incorporati

Alcune delle voci di menu disponibili in Control Center per un server vRealize Orchestrator esterno non sono incluse nella vista di Control Center predefinita di un'istanza di Orchestrator incorporata.

In un server Orchestrator incorporato, alcune opzioni di Control Center sono nascoste per impostazione predefinita.

Voce di menu	Dettagli
<b>Gestione licenze</b>	Il server Orchestrator incorporato è preconfigurato per l'utilizzo di vRealize Automation come provider di licenze.
<b>Esporta/Importa configurazione</b>	La configurazione del server Orchestrator incorporato è inclusa nei componenti di vRealize Automation esportati.
<b>Consente di configurare database</b>	Il server Orchestrator incorporato utilizza il database usato da vRealize Automation.
<b>Programma per il miglioramento dell'esperienza del cliente (CEIP)</b>	È possibile partecipare al programma CEIP dall'interfaccia di gestione dell'appliance vRealize Automation. Vedere <i>Programma per il miglioramento dell'esperienza del cliente</i> in <i>Gestione di vRealize Automation</i> .

Altre opzioni nascoste dalla vista di Control Center predefinita sono la casella di testo **Indirizzo host** e il pulsante **ANNULLA REGISTRAZIONE** nella pagina **Configura provider di autenticazione**.

**Nota** Per vedere l'intera serie di opzioni di Control Center in vRealize Orchestrator integrato in vRealize Automation, è necessario accedere alla pagina di gestione avanzata di Orchestrator all'indirizzo [https://vra-va-hostname.domain.name\\_or\\_load\\_balancer\\_address:8283/vco-controlcenter/#!/?advanced](https://vra-va-hostname.domain.name_or_load_balancer_address:8283/vco-controlcenter/#!/?advanced) e premere il pulsante F5 sulla tastiera per aggiornare la pagina.

## Riconfigurazione dell'endpoint vRealize Automation nel componente vRealize Orchestrator target

Per riconfigurare l'endpoint vRealize Automation nel componente vRealize Orchestrator target incorporato, utilizzare la procedura descritta di seguito.

### Prerequisiti

- Migrazione riuscita all'ultima versione di vRealize Automation.
- Connettersi al componente vRealize Orchestrator target utilizzando il client vRealize Orchestrator. Per ulteriori informazioni, vedere *Utilizzo del client VMware vRealize Orchestrator* nella [documentazione di vRealize Orchestrator](#).

### Procedura

- 1 Selezionare **Progettazione** dal menu a discesa in alto.
- 2 Fare clic su **Inventario**.
- 3 Espandere **vRealize Automation**.

- 4 Se è stata effettuata la migrazione da un ambiente minimo, identificare gli endpoint contenenti il nome di dominio completo (FQDN) dell'host dell'appliance vRealize Automation di origine. Se è stata effettuata la migrazione da un ambiente ad alta disponibilità, identificare gli endpoint contenenti il nome di dominio completo (FQDN) del bilanciamento del carico dell'appliance di origine.

Se si individuano endpoint contenenti il nome di dominio completo, procedere come segue.	Se non si individuano endpoint contenenti il nome di dominio completo, procedere come segue.
<ol style="list-style-type: none"> <li>1 Fare clic su <b>Workflow</b>.</li> <li>2 Fare clic sul pulsante Espandi per selezionare <b>Libreria &gt; vRealize Automation &gt; Configurazione</b>.</li> <li>3 Eseguire uno dei passaggi seguenti. <ul style="list-style-type: none"> <li>■ Se è stata effettuata la migrazione da un ambiente minimo, eseguire il workflow di <b>rimozione di un host vRA</b> per ogni endpoint contenente il nome di dominio completo (FQDN) dell'host dell'appliance vRealize Automation di origine.</li> <li>■ Se è stata effettuata la migrazione da un ambiente ad alta disponibilità, eseguire il workflow di <b>rimozione di un host vRA</b> per ogni endpoint contenente il nome di dominio completo (FQDN) dell'host del bilanciamento del carico dell'appliance di origine.</li> </ul> </li> </ol>	<ol style="list-style-type: none"> <li>1 Fare clic su <b>Risorse</b>.</li> <li>2 Fare clic sull'icona di aggiornamento sulla barra degli strumenti.</li> <li>3 Fare clic sul pulsante Espandi per selezionare <b>Libreria &gt; vCACCAFE &gt; Configurazione</b>.</li> <li>4 Eseguire uno dei passaggi seguenti. <ul style="list-style-type: none"> <li>■ Se è stata effettuata la migrazione da un ambiente minimo, eliminare tutte le risorse con una proprietà URL contenente il nome di dominio completo dell'host dell'appliance vRealize Automation di origine.</li> <li>■ Se è stata effettuata la migrazione da un ambiente ad alta disponibilità, eliminare tutte le risorse con una proprietà URL contenente il nome di dominio completo del bilanciamento del carico dell'appliance vRealize Automation di origine.</li> </ul> </li> </ol>

- 5 Fare clic su **Workflow**.
- 6 Fare clic sul pulsante Espandi per selezionare **Libreria > vRealize Automation > Configurazione**.
- 7 Per aggiungere l'host dell'appliance vRealize Automation target o, se è stata effettuata la migrazione in una distribuzione ad alta disponibilità, dell'host con bilanciamento del carico, eseguire il workflow di **aggiunta di un host vRA mediante il registro componenti**.

### Riconfigurazione dell'endpoint dell'infrastruttura vRealize Automation nel componente vRealize Orchestrator target

Per riconfigurare l'endpoint dell'infrastruttura vRealize Automation nel server vRealize Orchestrator target incorporato, utilizzare la procedura seguente.

#### Prerequisiti

- Migrazione riuscita all'ultima versione di vRealize Automation.
- Connettersi al componente vRealize Orchestrator target utilizzando il client vRealize Orchestrator. Per ulteriori informazioni, vedere *Utilizzo del client VMware vRealize Orchestrator* nella [documentazione di vRealize Orchestrator](#).

#### Procedura

- 1 Selezionare **Progettazione** dal menu a discesa in alto.
- 2 Fare clic su **Inventario**.
- 3 Espandere **Infrastruttura vRealize Automation**.

- 4 Se è stata effettuata la migrazione da un ambiente minimo, identificare gli endpoint contenenti il nome di dominio completo dell'host dell'infrastruttura vRealize Automation di origine. Se è stata effettuata la migrazione da un ambiente ad alta disponibilità, identificare gli endpoint contenenti il nome di dominio completo (FQDN) del bilanciamento del carico dell'appliance di origine.

Se si individuano endpoint contenenti il nome di dominio completo, procedere come segue.	Se non si individuano endpoint contenenti il nome di dominio completo, procedere come segue.
<ol style="list-style-type: none"> <li>1 Fare clic su <b>Workflow</b>.</li> <li>2 Fare clic sul pulsante Espandi per selezionare <b>Libreria &gt; vRealize Automation &gt; Amministrazione infrastruttura &gt; Configurazione</b>.</li> <li>3 Eseguire uno dei passaggi seguenti. <ul style="list-style-type: none"> <li>■ Se è stata effettuata la migrazione da un ambiente minimo, eseguire il workflow di <b>rimozione di un host IaaS</b> per ogni endpoint contenente il nome di dominio completo (FQDN) dell'host dell'infrastruttura vRealize Automation di origine.</li> <li>■ Se è stata effettuata la migrazione da un ambiente ad alta disponibilità, eseguire il workflow di <b>rimozione di un host IaaS</b> per ogni endpoint contenente il nome di dominio completo (FQDN) del bilanciamento del carico dell'host dell'infrastruttura vRealize Automation di origine.</li> </ul> </li> </ol>	<ol style="list-style-type: none"> <li>1 Fare clic su <b>Risorse</b>.</li> <li>2 Fare clic sull'icona di aggiornamento sulla barra degli strumenti.</li> <li>3 Fare clic sul pulsante Espandi per selezionare <b>Libreria &gt; vCAC &gt; Configurazione</b>.</li> <li>4 Eseguire uno dei passaggi seguenti. <ul style="list-style-type: none"> <li>■ Se è stata effettuata la migrazione da un ambiente minimo, eliminare tutte le risorse con una proprietà host contenente il nome di dominio completo dell'host dell'infrastruttura vRealize Automation di origine.</li> <li>■ Se è stata effettuata la migrazione da un ambiente ad alta disponibilità, eliminare tutte le risorse con una proprietà host contenente il nome di dominio completo del bilanciamento del carico dell'host dell'infrastruttura vRealize Automation di origine.</li> </ul> </li> </ol>

- 5 Fare clic su **Workflow**.
- 6 Fare clic sul pulsante Espandi per selezionare **Libreria > vRealize Automation > Configurazione**.
- 7 Per aggiungere l'host dell'infrastruttura vRealize Automation target o, se è stata effettuata la migrazione in una distribuzione ad alta disponibilità, l'host con bilanciamento del carico, eseguire il workflow di **aggiunta dell'host IaaS di un host vRA**.

### Installazione di una personalizzazione di vRealize Orchestrator

È possibile eseguire un workflow per installare gli stub dei workflow di cambiamento dello stato personalizzati e i workflow di funzionamento del menu di vRealize Orchestrator.

Per informazioni, vedere [Installazione di una personalizzazione di vRealize Orchestrator](#).

### Prerequisiti

Migrazione riuscita all'ultima versione di vRealize Automation.

### Riconfigurazione dell'endpoint dell'infrastruttura vRealize Orchestrator incorporata nel componente vRealize Automation target

Quando si esegue la migrazione da un ambiente vRealize Automation 6.2.x, è necessario aggiornare l'URL dell'endpoint dell'infrastruttura che punta al server vRealize Orchestrator target incorporato.

### Prerequisiti

- Effettuare la migrazione a vRealize Automation 7.4 correttamente.



- Accedere alla console di vRealize Automation di destinazione.
  - a Aprire la console di vRealize Automation utilizzando il nome di dominio completo dell'appliance virtuale di destinazione: `https://vra-va-hostname.domain.name/vcac`.  
  
Per un ambiente ad alta disponibilità, aprire la console utilizzando il nome di dominio completo del bilanciamento del carico dell'appliance virtuale di destinazione: `https://vra-va-lb-hostname.domain.name/vcac`.
  - b Accedere come utente amministratore laaS.

#### Procedura

- 1 Selezionare **Infrastruttura > Endpoint > Endpoint**.
- 2 Nella pagina Endpoint selezionare l'endpoint vRealize Orchestrator e fare clic su **Modifica**.
- 3 Nella casella di testo Indirizzo modificare l'URL dell'endpoint vRealize Orchestrator.
  - Se è stata effettuata la migrazione a un ambiente minimo, sostituire l'URL dell'endpoint vRealize Orchestrator con `https://vra-va-hostname.domain.name:443/vco`.
  - Se è stata effettuata la migrazione a un ambiente ad alta disponibilità, sostituire l'URL dell'endpoint vRealize Orchestrator con `https://vra-va-lb-hostname.domain.name:443/vco`.
- 4 Fare clic su **OK**.
- 5 Eseguire manualmente una raccolta dati sull'endpoint vRealize Orchestrator.
  - a Nella pagina Endpoint, selezionare l'endpoint vRealize Orchestrator.
  - b Selezionare **Azioni > Raccolta dati**.

Verificare la corretta esecuzione della raccolta dati.

#### Riconfigurazione dell'endpoint di Azure nell'ambiente vRealize Automation target

Dopo la migrazione, è necessario riconfigurare l'endpoint di Microsoft Azure.

Eseguire questa procedura per ogni endpoint di Azure.

#### Prerequisiti

- Effettuare la migrazione alla versione più recente di vRealize Automation 7.4 correttamente.
- Accedere alla console di vRealize Automation di destinazione.
  - a Aprire la console di vRealize Automation utilizzando il nome di dominio completo dell'appliance virtuale di destinazione: `https://vra-va-hostname.domain.name/vcac`.  
  
Per un ambiente ad alta disponibilità, aprire la console utilizzando il nome di dominio completo del bilanciamento del carico dell'appliance virtuale di destinazione: `https://vra-va-lb-hostname.domain.name/vcac`.
  - b Accedere come utente amministratore laaS.

## Procedura

- 1 Selezionare **Amministrazione > Configurazione vRO > Endpoint**.
- 2 Selezionare un endpoint di Azure.
- 3 Fare clic su **Modifica**.
- 4 Fare clic su **Dettagli**.
- 5 Nella casella di testo **Segreto client** immettere il segreto client originale.
- 6 Fare clic su **Fine**.
- 7 Ripetere per ogni endpoint di Azure.

## Migrazione di vRealize Automation 6.2.x Automation Application Services alla versione 7.4

È possibile utilizzare lo strumento VMware vRealize Application Services Migration Tool per eseguire la migrazione dei blueprint dei servizi applicativi e dei profili di distribuzione esistenti da VMware vRealize Application Services 6.2.x a vRealize Automation 7.4.

### Prerequisiti

Migrazione riuscita all'ultima versione di vRealize Automation.

### Procedura

- ◆ Per scaricare lo strumento VMware vRealize Application Services Migration Tool, completare i passaggi descritti di seguito.
  - a Fare clic su [Scarica VMware vRealize Automation](#).
  - b Selezionare **Driver e strumenti > VMware vRealize Application Services Migration Tool**.

## Eliminazione del database Microsoft SQL IaaS di vRealize Automation di destinazione originale

È possibile eliminare il database IaaS originale una volta completata la migrazione.

### Prerequisiti

Migrazione riuscita all'ultima versione di vRealize Automation.

L'ambiente di cui è stata eseguita la migrazione non utilizza il database Microsoft SQL IaaS di vRealize Automation originale creato durante l'installazione dell'ambiente di vRealize Automation target. È possibile eliminare senza problemi questo database IaaS dal server Microsoft SQL una volta completata la migrazione.

## Aggiornamento dei contenuti del menu Posizione dei data center dopo la migrazione

Dopo la migrazione, è necessario aggiungere le posizioni personalizzate mancanti dei data center al menu a discesa **Posizione**.

Al termine della migrazione alla versione più recente di vRealize Automation, viene ripristinato l'elenco predefinito delle posizioni dei data center nel menu a discesa **Posizione** nella pagina Risorse di elaborazione. Anche se mancano le posizioni personalizzate dei data center, la migrazione di tutte le configurazioni delle risorse di elaborazione viene eseguita correttamente, senza influire sulla proprietà `Vrm.DataCenter.Location`. È ancora possibile aggiungere posizioni dei data center personalizzate nel menu **Posizione**.

### Prerequisiti

Effettuare la migrazione alla versione più recente di vRealize Automation.

### Procedura

- ◆ Aggiungere le posizioni dei data center mancanti nel menu a discesa **Posizione**. Vedere [Scenario: aggiunta di posizioni di data center per distribuzioni tra le regioni](#).

### Aggiornamento degli agenti software a TLS 1.2

Dopo la migrazione di vRealize Automation 7.1, 7.2, 7.3 o 7.3.1 alla versione 7.4, è necessario eseguire varie attività per aggiornare gli agenti software dell'ambiente di origine a Transport Layer Security (TLS) 1.2.

A partire da vRealize Automation 7.4, TLS 1.2 è l'unico protocollo TLS supportato per la comunicazione dati tra vRealize Automation e il browser. Dopo la migrazione, è necessario aggiornare i modelli di macchina virtuale esistenti dell'ambiente di origine vRealize Automation 7.1 o 7.3, nonché tutte le macchine virtuali esistenti.

### Aggiornamento di modelli di macchine virtuali dell'ambiente di origine

Una volta completata la migrazione alla versione 7.4, è necessario aggiornare i modelli di vRealize Automation 7.1, 7.2, 7.3 e 7.3.1 esistenti in modo che gli agenti software utilizzino il protocollo TLS 1.2.

L'agente guest e il codice bootstrap dell'agente devono essere aggiornati nei modelli dell'ambiente di origine. Se si utilizza l'opzione di un clone collegato, potrebbe essere necessario rimappare i modelli alle nuove macchine virtuali create e ai relativi snapshot.

Per aggiornare i modelli, completare le seguenti attività.

- 1 Accedere a vSphere.
- 2 Convertire ogni modello da vRealize Automation 7.1, 7.2, 7.3 o 7.3.1 a una macchina virtuale e accendere la macchina.
- 3 Importare il programma di installazione del software appropriato ed eseguire il programma di installazione del software in ogni macchina virtuale.
- 4 Convertire nuovamente ogni macchina virtuale in un modello.

Per individuare i programmi di installazione del software per Linux o Windows, utilizzare la seguente procedura.

## Prerequisiti

- [Applicazione di patch dell'agente software](#) se è stata effettuata la migrazione da vRealize Automation 7.1 o 7.3 alla versione 7.4.
- Migrazione corretta di vRealize Automation 7.1, 7.2, 7.3 o 7.3.1 alla versione 7.4.

## Procedura

- 1 Avviare un browser e aprire la pagina iniziale dell'appliance vRealize Automation 7.4 utilizzando il nome di dominio completo dell'appliance virtuale: `https://vra-virtual-hostname.domain.name`.
- 2 Fare clic sulla **pagina degli agenti guest e software**.
- 3 Seguire le istruzioni per i programmi di installazione del software di Linux o Windows.

## Operazioni successive

[Identificazione delle macchine virtuali che richiedono l'aggiornamento dell'agente software.](#)

### Identificazione delle macchine virtuali che richiedono l'aggiornamento dell'agente software

È possibile utilizzare il servizio di integrità nella console di vRealize Automation per identificare le macchine virtuali che richiedono un aggiornamento dell'agente software a TLS 1.2.

In alcuni casi, la patch applicata al proprio ambiente di origine vRealize Automation non esegue l'aggiornamento di tutte le macchine virtuali. È possibile utilizzare il servizio di integrità per identificare le macchine virtuali che richiedono un aggiornamento dell'agente software a TLS 1.2. Tutti gli agenti software nell'ambiente di destinazione devono essere aggiornati per poter eseguire le procedure di post-provisioning.

## Prerequisiti

- [Applicazione di patch dell'agente software](#) se è stata effettuata la migrazione da vRealize Automation 7.1 o 7.3 alla versione 7.4.
- Se è stata effettuata la migrazione di vRealize Automation 7.1, 7.2, 7.3 o 7.3.1 alla versione 7.4.
- Si è connessi a vRealize Automation 7.4 nell'appliance virtuale primaria.

## Procedura

- 1 Fare clic su **Amministrazione > Integrità**.
- 2 Fare clic su **Nuova configurazione**.
- 3 Nella pagina dei dettagli della configurazione, fornire le informazioni richieste.

Opzione	Commento
Nome	Immettere <b>SW Agent verification</b> .
Descrizione	Aggiungere una descrizione facoltativa, ad esempio <b>Locate software agents for upgrade to TLS 1.2</b> .
Prodotto	Selezionare vRealize Automation 7.4.0.
Pianificazione	Selezionare Nessuna.

- 4 Fare clic su **Avanti**.
- 5 Nella pagina di selezione delle suite di prove, selezionare **Prove di sistema per vRealize Automation** e **Prove del tenant per vRealize Automation**.
- 6 Fare clic su **Avanti**.
- 7 Nella pagina dei parametri di configurazione, fornire le informazioni richieste.

**Tabella 1-84. Appliance virtuale vRealize Automation**

Opzione	Descrizione
Indirizzo server Web pubblico	<ul style="list-style-type: none"> <li>■ Per una distribuzione minima, l'URL di base per l'host dell'appliance vRealize Automation. Ad esempio, <code>https://va-host.domain/</code>.</li> <li>■ Per una distribuzione ad alta disponibilità, l'URL di base per il servizio di bilanciamento del carico di vRealize Automation. Ad esempio, <code>https://load-balancer-host.domain/</code>.</li> </ul>
Indirizzo console SSH	Nome di dominio completo dell'appliance vRealize Automation. Ad esempio, <code>va-host.domain</code> .
Utente console SSH	<b>root</b>
Password console SSH	Password root.
Tempo di risposta massimo del servizio (ms)	Accettare il valore predefinito: 2000

**Tabella 1-85. Tenant di sistema vRealize Automation**

Opzione	Descrizione
Amministratore tenant di sistema	administrator
Password tenant di sistema	Password per l'amministratore.

**Tabella 1-86. Monitoraggio dello spazio su disco di vRealize Automation**

Opzione	Descrizione
Percentuale soglia di avviso	Accettare il valore predefinito: 75
Percentuale soglia critica	Accettare il valore predefinito: 90

**Tabella 1-87. Tenant vRealize Automation**

Opzione	Descrizione
Tenant in prova	Tenant selezionato per la prova.
Nome utente amministratore della struttura	<p>Nome dell'utente amministratore della struttura Ad esempio, <code>admin@va-host.local</code>.</p> <p><b>Nota</b> L'amministratore della struttura deve anche disporre di un ruolo di amministratore tenant e di amministratore IaaS nell'ordine per tutte le prove da eseguire.</p>
Password amministratore struttura	Password per l'amministratore della struttura.

- 8 Fare clic su **Avanti**.

- 9 Nella pagina Riepilogo, esaminare le informazioni e fare clic su **Fine**.

La configurazione di verifica dell'agente software è terminata.

- 10 Nella scheda della verifica dell'agente SW, fare clic su **Esegui**.

- 11 Una volta completata la prova, fare clic al centro della scheda di verifica dell'agente SW.

- 12 Nella pagina dei risultati della verifica dell'agente SW, scorrere i risultati delle prove e individuare la prova Check Software Agent Version nella colonna Nome. Se il risultato della prova è Non riuscita, fare clic sul collegamento **Causa** nella colonna Causa per visualizzare le macchine virtuali il cui agente software è obsoleto.

### Operazioni successive

Se sono presenti macchine virtuali con un agente software obsoleto, vedere [Aggiornamento degli agenti software in vSphere](#).

### Aggiornamento degli agenti software in vSphere

È possibile aggiornare qualsiasi agente software obsoleto in vSphere a TLS 1.2 dopo la migrazione utilizzando la console di gestione dell'appliance di vRealize Automation.

Questa procedura aggiorna gli agenti software obsoleti nelle macchine virtuali dall'ambiente di origine a TLS 1.2 ed è necessaria per la migrazione a vRealize Automation 7.4.

### Prerequisiti

- [Applicazione di patch dell'agente software](#) se è stata effettuata la migrazione da vRealize Automation 7.1 o 7.3 alla versione 7.4.
- Migrazione corretta di vRealize Automation 7.1, 7.2, 7.3 o 7.3.1 alla versione 7.4.
- È stato utilizzato il servizio di integrità per identificare le appliance virtuali con agenti software obsoleti.

### Procedura

- 1 Nell'appliance vRealize Automation primaria, accedere alla gestione dell'appliance di vRealize Automation come **root** utilizzando la password immessa durante la distribuzione dell'appliance vRealize Automation.

Per un ambiente ad alta disponibilità, aprire la console di gestione dell'appliance nell'appliance master.

- 2 Fare clic su **Impostazioni vRA > Agenti SW**.

- 3 Fare clic su **Attiva/Disattiva TLS 1.0, 1.1**.

Lo stato di TLS v1.0, v1.1 è Abilitato.

- 4 Per le credenziali del tenant, immettere le informazioni richieste per l'appliance vRealize Automation di origine.

Opzione	Descrizione
Nome tenant	Nome del tenant nell'appliance vRealize Automation di origine.  <b>Nota</b> All'utente del tenant è necessario assegnare il ruolo Architetto del software.
Username	Nome utente dell'amministratore tenant nell'appliance vRealize Automation di origine.
Password	Password dell'amministratore tenant.

- 5 Fare clic su **Prova connessione**.

Se viene stabilita una connessione, viene visualizzato un messaggio che indica che l'operazione è riuscita.

- 6 Per l'appliance di origine, immettere l'indirizzo IP o il nome di dominio completo dell'appliance vRealize Automation di origine.

L'appliance di origine e l'appliance target devono entrambe utilizzare le stesse credenziali del tenant.

- 7 Fare clic su **Elenca batch**.

Viene visualizzata una tabella che include i batch.

- 8 Fare clic su **Mostra**.

Viene visualizzata una tabella con l'elenco delle macchine virtuali con agenti software obsoleti.

- 9 Aggiornare l'agente software per le macchine virtuali con stato Aggiornabile.

- Per aggiornare l'agente software in una singola macchina virtuale, fare clic su **Mostra** per un gruppo di macchine virtuali, identificare la macchina virtuale che si desidera aggiornare e fare clic su **Esegui** per avviare il processo di aggiornamento.
- Per aggiornare l'agente software per un batch di macchine virtuali, identificare il gruppo che si desidera aggiornare e fare clic su **Esegui** per avviare il processo di aggiornamento.

Se sono presenti più di 200 macchine virtuali da aggiornare, è possibile controllare la velocità del processo di aggiornamento batch inserendo i valori per questi parametri.

Opzione	Descrizione
Dimensioni batch	Il numero di macchine virtuali selezionato per l'aggiornamento batch. È possibile modificare questo numero per regolare la velocità di aggiornamento.
Profondità coda	Numero di aggiornamenti paralleli eseguiti contemporaneamente. Ad esempio, 20. È possibile modificare questo numero per regolare la velocità di aggiornamento.

Opzione	Descrizione
Errori batch	Numero di errori REST che causano il rallentamento dell'aggiornamento batch. Se ad esempio si desidera arrestare l'aggiornamento batch corrente dopo 5 errori per migliorare la stabilità dell'aggiornamento, inserire 5 nel campo di testo.
Operazioni batch non riuscite	Numero di aggiornamenti dell'agente software non riusciti che causano il rallentamento dell'elaborazione batch. Se ad esempio si desidera arrestare l'aggiornamento batch corrente dopo 5 errori per migliorare la stabilità dell'aggiornamento, inserire 5 nel campo di testo.
Polling batch	Frequenza con cui viene eseguito il polling nel processo di aggiornamento per controllarne l'avanzamento. È possibile modificare questo numero per regolare la velocità di aggiornamento.

Se il processo di aggiornamento è troppo lento o produce troppi aggiornamenti non riusciti, è possibile modificare questi parametri per migliorare le prestazioni dell'aggiornamento.

**Nota** Se si fa clic su **Aggiorna**, l'elenco dei batch viene cancellato. Ciò non influisce sul processo di aggiornamento. L'operazione aggiorna anche le informazioni relative al fatto che TLS 1.2 sia o meno impostato. Se si fa clic su **Aggiorna**, viene inoltre eseguito un controllo dell'integrità dei servizi di vRealize Automation. Se i servizi non sono in esecuzione, il sistema visualizza un messaggio di errore e disattiva tutti gli altri pulsanti di azione.

## 10 Fare clic su **Attiva/Disattiva TLS 1.0, 1.1**.

Lo stato di TLS v1.0, v1.1 è Disabilitato.

## Aggiornamento degli agenti software su Amazon Web Service o Azure

È possibile aggiornare manualmente agenti software obsoleti in Amazon Web Service (AWS) o Azure.

- È necessario aggiornare le proprietà del tunnel specificate nella prenotazione del server vRealize Automation migrato.

### Prerequisiti

- [Applicazione di patch dell'agente software](#) se è stata effettuata la migrazione da vRealize Automation 7.1 o 7.3 alla versione 7.4.
- Migrazione corretta di vRealize Automation 7.1, 7.2, 7.3 o 7.3.1 alla versione 7.4.
- È presente un tunnel software e l'indirizzo IP della macchina virtuale del tunnel è noto.

### Procedura

- 1 Creare un file di nodo per ogni nodo da aggiornare.

```
/usr/lib/vcac/server/webapps/ROOT/software/initializeUpdateSoftwareAgents.py -a <
$DestinationVRAServer> -t <$Tenant> -tu <$TenantUser> -S <$SourceVRAServer>
```



## 2 Creare un file di piano per aggiornare l'agente software in una macchina virtuale Windows o Linux.

- Modificare il file params di migrazione in `/var/log/vcac/agentupdate/{tenant}/{subtenant-UUID}` in modo che contenga il valore dell'indirizzo IP privato corrispondente all'endpoint di AWS o Azure.

```
"key": "ipAddress",

    "value": {

        "type": "string",

        "value": "<$PrivateIp:$PrivatePort>"

    }
}
```

- Utilizzare questo comando per aggiornare una macchina Linux.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer>
-t <$Tenant> -S <$SourceVRAServer> -tu <$TenantUser> -CL Software.LinuxAgentUpdate74 --
source_cloud_provider azure
```

- Utilizzare questo comando per aggiornare una macchina Windows.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer>
-t <$Tenant> -S <$SourceVRAServer> -tu <$TenantUser> -CW Software.WindowsAgentUpdate74 --
source_cloud_provider azure
```

- Questo comando esegue il file di piano.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer>
-t <$Tenant> -tu <$TenantUser> --plan_file /usr/lib/vcac/server/webapps/ROOT/software/plan
```

- 3 Utilizzare questo comando per aggiornare l'agente software utilizzando il file di nodo del passaggio 1 e il file di piano del passaggio 2.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer> -t <$tenant> -tu <$TenantUser> --component_windows Software.WindowsAgentUpdate74 --component_linux Software.LinuxAgentUpdate74 --plan_file /usr/lib/vcac/server/webapps/ROOT/software/plan --plan_index 0 --node_file /usr/lib/vcac/server/webapps/ROOT/software/node --source_cloud_provider azure --action plan_batch -S <$SourceVRAServer>
```

In alternativa, è possibile utilizzare questo comando per eseguire un nodo alla volta a partire dal file di nodo, fornendo un indice dei nodi.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer> -t <$tenant> -tu <$TenantUser> --component_windows Software.WindowsAgentUpdate74 --component_linux Software.LinuxAgentUpdate74 --plan_file /usr/lib/vcac/server/webapps/ROOT/software/plan --plan_index 0 --node_file /usr/lib/vcac/server/webapps/ROOT/software/node --source_cloud_provider azure --action execute_node -S <$SourceVRAServer> --node_index <0 through n-1>
```

Quando si esegue questa procedura, è possibile accodare i registri dell'appliance virtuale vRealize Automation e dalla macchina host per vedere il processo di aggiornamento dell'agente server.

Dopo l'aggiornamento, il processo di aggiornamento importa uno script di aggiornamento del software per Windows o Linux nell'appliance virtuale vRealize Automation 7.4. È possibile accedere all'host dell'appliance virtuale vRealize Automation per assicurarsi che il componente software sia stato importato correttamente. Dopo l'importazione del componente, un aggiornamento software viene inviato al servizio EBS (Event Broker Service) precedente per l'inoltro degli script di aggiornamento software alle macchine virtuali identificate. Quando l'aggiornamento viene completato e i nuovi agenti software diventano operativi, effettuano il binding alla nuova appliance virtuale di vRealize Automation inviando una richiesta di ping.

---

**Nota** File di registro utili

---

- Output di Catalina per vRealize Automation di origine: /var/log/vcac/catalina.out. In questo file sono contenute le richieste di aggiornamento create all'esecuzione delle migrazioni degli agenti. Questa attività corrisponde all'esecuzione di una richiesta di provisioning del software.
- Output di Catalina per vRealize Automation di destinazione: /var/log/vcac/catalina.out. In questo file sono contenute le richieste di ping delle macchine virtuali migrate per includere numeri di versione 7.4.0-SNAPSHOT. È possibile registrarle insieme confrontando i nomi degli argomenti EBS, ad esempio sw-agent-UUID.
- Cartella di aggiornamento dell'agente nel file di registro dell'aggiornamento master della macchina vRealize Automation di destinazione: /var/log/vmware/vcac/agentupdate/updateSoftwareAgents.log. È possibile accodare questo file per vedere quale operazione di aggiornamento è in corso.
- Registri singoli disponibili nelle cartelle del tenant: /var/log/vcac/agentupdate/{tenant}/{subtenant-UUID}. Qui sono elencati i singoli nodi come file LOT con errori ed estensioni in corso.

- Macchine virtuali migrate: `/opt/vmware-appdirector/agent/logs/darwin*.log`. È possibile controllare a campione questo percorso in cui vengono elencate le richieste di aggiornamento software ricevute e l'eventuale riavvio di `agent_bootstrap` + agente software.

### Modificare l'impostazione del dizionario delle proprietà dopo la migrazione

Dopo la migrazione da vRealize Automation 6.2.x, impostare le proprietà del tipo di controllo `Label` del dizionario delle proprietà come non sovrascrivibile nei blueprint.

Il controllo Etichetta nel dizionario delle proprietà di vRealize Automation 6.2.x non esiste in vRealize Automation 7.x. Durante la migrazione, il controllo `Label` viene convertito in un controllo di tipo `TextBox` nel dizionario delle proprietà migrato.

Dopo la migrazione, impostare le proprietà interessate come non sovrascrivibili, manualmente nel dizionario delle proprietà di vRealize Automation o utilizzando le funzionalità di esportazione e importazione.

### Convalida dell'ambiente vRealize Automation 7.4 target

È possibile verificare che tutti i dati siano stati migrati correttamente nell'ambiente vRealize Automation target.

#### Prerequisiti

- Effettuare la migrazione alla versione più recente di vRealize Automation.
- Accedere alla console di vRealize Automation di destinazione.
  - a Aprire la console di vRealize Automation utilizzando il nome di dominio completo dell'appliance virtuale di destinazione: `https://vra-vd-hostname.domain.name/vcac`.  
  
Per un ambiente ad alta disponibilità, aprire la console utilizzando il nome di dominio completo del bilanciamento del carico dell'appliance virtuale di destinazione: `https://vra-vd-lb-hostname.domain.name/vcac`.
  - b Accedere con il nome utente e la password di amministratore tenant.

#### Procedura

- 1 Selezionare **Infrastruttura > Macchine gestite** e verificare che siano presenti tutte le macchine virtuali gestite.
- 2 Fare clic su **Risorse di elaborazione**, selezionare tutti gli endpoint e fare clic su **Raccolta dati**, **Richiedi ora** e **Aggiorna** per verificare il funzionamento degli endpoint.
- 3 Fare clic su **Progettazione** e, nella pagina **Blueprint**, verificare gli elementi di ciascun blueprint.
- 4 Fare clic su **XaaS** e verificare i contenuti di **Risorse personalizzate**, **Mappature risorse**, **Blueprint XaaS** e **Azioni risorsa**.
- 5 Selezionare **Amministrazione > Gestione catalogo** e verificare i contenuti di **Servizi**, **Elementi del catalogo**, **Azioni** e **Permessi**.
- 6 Selezionare **Elementi > Distribuzioni** e verificare i dettagli delle macchine virtuali di cui è stato effettuato il provisioning.

- 7 Nella pagina Distribuzioni, selezionare una macchina virtuale spenta e di cui è stato effettuato il provisioning, quindi selezionare **Azioni > Accendi**, fare clic su **Invia** e su **OK**. Verificare che la macchina virtuale si accenda correttamente.
- 8 Fare clic su **Catalogo** e richiedere un nuovo elemento del catalogo.
- 9 Nella scheda **Generale** immettere le informazioni richieste.
- 10 Fare clic sull'icona Macchina, accettare tutte le impostazioni predefinite, fare clic su **Invia** e su **OK**.
- 11 Verificare che la richiesta venga elaborata correttamente.

## Risoluzione dei problemi relativi alla migrazione

Gli argomenti della risoluzione dei problemi relativi alla migrazione offrono soluzioni per gli eventuali problemi che si potrebbero riscontrare durante la migrazione di vRealize Automation.

### Errore causato dalla versione di PostgreSQL

Un ambiente vRealize Automation 6.2.x di origine contenente un database PostgreSQL aggiornato blocca l'accesso dell'amministratore.

#### Problema

Se un database PostgreSQL aggiornato viene utilizzato da vRealize Automation 6.2.x, un amministratore deve aggiungere una voce al file `pg_hba.conf` che consente di accedere a questo database da vRealize Automation.

#### Soluzione

- 1 Aprire il file `pg_hba.conf`.
- 2 Per concedere l'accesso a questo database, aggiungere la voce che segue.

```
host all vcac-database-user vra-va-ip trust-method
```

### Per alcune macchine virtuali non viene creata una distribuzione durante la migrazione

Per le macchine virtuali il cui stato al momento della migrazione risulta mancante non viene creata una distribuzione corrispondente nell'ambiente target.

#### Problema

Se durante la migrazione lo stato di una macchina virtuale risulta mancante nell'ambiente di origine, nell'ambiente target non viene creata una distribuzione corrispondente.

#### Soluzione

- ◆ Se dopo la migrazione lo stato di una macchina virtuale non risulta più mancante, è possibile importare la macchina virtuale nella distribuzione target utilizzando l'importazione di massa.

### Posizioni dei registri di migrazione

È possibile risolvere i problemi di convalida o migrazione visualizzando i registri relativi che tengono traccia del processo di migrazione.

**Tabella 1-88. Appliance vRealize Automation di origine**

Registro	Posizione
Registro di creazione del pacchetto	/var/log/vmware/vcac/migration-package.log

**Tabella 1-89. Appliance vRealize Automation target**

Registro	Posizione
Registro di migrazione	/var/log/vmware/vcac/migrate.log
Registro di esecuzione della migrazione	/var/log/vmware/vcac/mseq.migration.log
Registro di output dell'esecuzione della migrazione	/var/log/vmware/vcac/mseq.migration.out.log
Registro di esecuzione della convalida	/var/log/vmware/vcac/mseq.validation.log
Registro di output dell'esecuzione della convalida	/var/log/vmware/vcac/mseq.validation.out.log

**Tabella 1-90. Nodi dell'infrastruttura vRealize Automation target**

Registro	Posizione
Registro di migrazione	C:\Programmi (x86)\VMware\VCAC\InstallLogs-YYYYMMDDHHMMXX\Migrate.log
Registro di convalida	C:\Programmi(x86)\VMware\VCAC\InstallLogs-YYYYMMDDHHMMXX\Validate.log

**Gli elementi del catalogo vengono visualizzati nel catalogo dei servizi dopo la migrazione, ma non sono disponibili per la richiesta**

Gli elementi del catalogo che utilizzano determinate definizioni delle proprietà dalle versioni precedenti vengono visualizzati nel catalogo dei servizi, ma non sono disponibili per la richiesta dopo la migrazione alla versione più recente di vRealize Automation.

#### Problema

Se si effettua la migrazione dalla versione 6.2.x o da una versione precedente e si dispone di definizioni delle proprietà con questi tipi di controllo o attributi, questi elementi non saranno presenti nelle definizioni delle proprietà e tutti gli elementi del catalogo che utilizzano le definizioni non funzioneranno come prima della migrazione.

- Tipi di controllo. Casella di controllo o collegamento.
- Attributi. Relazione, espressioni regolari o layout delle proprietà.

#### Causa

In vRealize Automation 7.0 e versioni successive le definizioni delle proprietà non utilizzano più questi elementi. È necessario ricreare la definizione della proprietà o configurarla in modo che utilizzi un'azione di script di vRealize Orchestrator anziché i tipi di controllo o gli attributi incorporati.

Eseguire la migrazione del tipo di controllo o degli attributi a vRealize Automation 7.x utilizzando un'azione di script.

## Soluzione

- 1 In vRealize Orchestrator creare un'azione di script che restituisca i valori delle proprietà. L'azione deve restituire un tipo semplice. Ad esempio, stringhe di ritorno, numeri interi o altri tipi supportati. L'azione può acquisire le altre proprietà da cui dipende come parametro di input.
- 2 Nella console di vRealize Automation configurare la definizione del prodotto.
  - a Selezionare **Amministrazione > Dizionario proprietà > Definizioni proprietà**.
  - b Selezionare la definizione della proprietà e fare clic su **Modifica**.
  - c Dal menu a discesa Visualizza consiglio selezionare **Elenco a discesa**.
  - d Dal menu a discesa Valori, selezionare **Valori esterni**.
  - e Selezionare l'azione di script.
  - f Fare clic su **OK**.
  - g Configurare i parametri di input che vengono inclusi nell'azione di script. Per mantenere la relazione esistente, effettuare il binding del parametro all'altra proprietà.
  - h Fare clic su **OK**.

## Pulsanti di opzione di Raccolta dati disabilitati in vRealize Automation

Dopo la migrazione da vRealize Automation 6.2.x a 7.x, la pagina Risorse di elaborazione in vRealize Automation di destinazione contiene pulsanti di opzione disabilitati in Raccolta dati.

## Causa

Se si installa un agente nell'ambiente di origine che punta a un endpoint e si installa un agente nell'ambiente di destinazione che punta allo stesso endpoint, ma l'agente ha un nome diverso, è possibile eseguire una connessione di prova all'endpoint in qualità di amministratore nell'ambiente di destinazione. Tuttavia, se si accede a vRealize Automation nell'ambiente di destinazione come amministratore di struttura, i pulsanti di opzione della sezione Raccolta dati della pagina Risorse di elaborazione sono disabilitati.

## Soluzione

È possibile evitare questa situazione utilizzando per l'agente installato nell'ambiente di destinazione lo stesso nome dell'agente installato nell'ambiente di origine.

## Risoluzione dei problemi relativi all'aggiornamento dell'agente software

Quando si utilizza l'interfaccia di gestione dell'appliance vRealize Automation per aggiornare gli agenti software, è possibile consultare i file di registro per identificare le cause degli eventuali problemi che possono verificarsi.

## Problema

Quando si esegue l'aggiornamento degli agenti software, è possibile che si verifichino problemi. Esaminando i file di registro durante il processo di aggiornamento dell'agente software, è possibile identificare il punto in cui si è verificato un problema.

---

### Nota Registri del server

---

- Per esaminare il processo, analizzare il file `updateSoftwareAgents.log` nel server: `/storage/log/vmware/vcac/agentupdate/updateSoftwareAgents.log`.
- Analizzare il file `catlaina.out` nell'appliance di destinazione per verificare per quali agenti software l'aggiornamento viene eseguito correttamente: `/var/log/vcac/catalina.out`.

Cercare una stringa simile a "ping" restituita per 7.4.0-SNAPSHOT.

Ulteriori informazioni sono disponibili nelle seguenti posizioni.

- `/var/cache/vcac/agentupdate/{Tenant}/{UUID}/UUID.plan`
- `/var/cache/vcac/agentupdate/{Tenant}/{UUID}/UUID.log`
- `/var/cache/vcac/agentupdate/sqa/UUID/UUID.log` (per sistema operativo)

Prima di avviare un aggiornamento in batch principale, è sempre consigliabile eseguire un aggiornamento di prova dell'agente software dell'appliance virtuale. Per una panoramica del processo:

- Esaminare la prima richiesta effettuata all'appliance virtuale di destinazione per identificare le versioni degli agenti.
- Esaminare la richiesta di aggiornamento effettuata all'appliance virtuale di origine.
- Nell'appliance virtuale di destinazione, esaminare gli agenti che presentano la nuova versione 7.4.
- Tra questi eventi, esaminare il file `updateSoftwareAgents.log` in `/storage/log/vmware/vcac/agentupdate/updateSoftwareAgents.log`

---

### Nota Registri del client

---

I registri dell'agente Linux si trovano nella cartella dei registri dell'agente `appdirector`: `/opt/vmware-appdirector/agent/logs/*.log`

Nei registri potrebbero venire visualizzati errori come questi, che sono temporanei perché le code EBS funzionano a intermittenza durante il processo di aggiornamento.

```
Feb 15 2018 16:54:10.105 ERROR [EventPoller-sw-agent-0ad2418d-5b42-4231-a839-a05dd618e43e] []
com.vmware.vcac.platform.event.broker.client.rest.RestEventSubscribeHandler - Error while polling
events for subscription '{}'.
org.springframework.web.client.HttpClientErrorException: 404 Not Found
at
org.springframework.web.client.DefaultResponseErrorHandler.handleError(DefaultResponseErrorHandler
.java:91) ~[nobel-agent.jar:na]
```

at org.springframework.web.client.RestTemplate.handleResponse(RestTemplate.java:641) ~[nobel-agent.jar:na]

at org.springframework.web.client.RestTemplate.doExecute(RestTemplate.java:597) ~[nobel-agent.jar:na]

at org.springframework.web.client.RestTemplate.execute(RestTemplate.java:557) ~[nobel-agent.jar:na]

at org.springframework.web.client.RestTemplate.exchange(RestTemplate.java:503) ~[nobel-agent.jar:na]

at

com.vmware.vcac.platform.event.broker.client.rest.RestEventSubscribeHandler.pollEvents(RestEventSubscribeHandler.java:297) ~[nobel-agent.jar:na]

at com.vmware.vcac.platform.event.broker.client.rest.RestEventSubscribeHandler  
\$EventPoller.run(RestEventSubscribeHandler.java:329) ~[nobel-agent.jar:na]