

Installazione di vRealize Automation

21 luglio 2021

vRealize Automation 7.6

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

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

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

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

Copyright © 2014-2021 VMware, Inc. Tutti i diritti sono riservati. [Informazioni sul copyright e sui marchi](#)

Sommario

Installazione di vRealize Automation	7
Informazioni aggiornate	8
1 Cenni generali sull'installazione	9
Informazioni sull'installazione	9
Novità di questa installazione	10
Componenti dell'installazione	10
Appliance vRealize Automation	10
Infrastructure as a Service (IaaS)	11
Tipo di distribuzione	14
Distribuzioni minime	14
Distribuzioni distribuite	15
Scelta del metodo d'installazione	18
2 Preparazione per l'installazione	19
Preparazione generale	19
Account e password	20
Nomi host e indirizzi IP	22
Latenza e larghezza di banda	23
Appliance vRealize Automation	24
Porte dell'appliance vRealize Automation	24
Server Windows IaaS	26
Porte dei server IaaS Windows	28
Server Web IaaS	29
Host del servizio di gestione di IaaS	30
Host SQL Server di IaaS	31
Host Distributed Execution Manager di IaaS	32
DEM Worker con Amazon Web Services	32
DEM Worker con Openstack o PowerVC	32
DEM Worker con Red Hat Enterprise Virtualization	33
DEM Worker con SCVMM	33
Certificati	35
Requisiti dei certificati di vRealize Automation	36
Estrazione di certificati e chiavi private	37
3 Distribuzione dell'appliance vRealize Automation	39
Informazioni sulla distribuzione dell'appliance	39

Distribuzione di vRealize Automation appliance	39
Aggiunta di controller NIC prima di eseguire il programma di installazione	43

4 Installazione con l'installazione guidata 45

Utilizzo dell'installazione guidata per le distribuzioni minime	45
Avvio dell'installazione guidata per una distribuzione minima	45
Installazione dell'agente di gestione	46
Completamento dell'installazione guidata	48
Utilizzo dell'installazione guidata per le distribuzioni enterprise	48
Avvio dell'installazione guidata per una distribuzione enterprise	49
Installazione dell'agente di gestione	49
Completamento dell'installazione guidata	51

5 Le interfacce di installazione standard 53

Utilizzo delle interfacce standard per le distribuzioni minime	53
Elenco di controllo di una distribuzione minima	54
Configurazione dell'appliance vRealize Automation	54
Installazione dei componenti IaaS	58
Utilizzo delle interfacce standard per le distribuzioni distribuite	65
Elenco di controllo di una distribuzione distribuita	65
Disattivazione dei controlli di integrità del bilanciamento del carico	67
Requisiti di attendibilità dei certificati in una distribuzione distribuita	67
Configurazione del componente Web, del servizio di gestione e di attendibilità dei certificati dell'host DEM	69
Fogli di lavoro per l'installazione	70
Configurazione del bilanciamento del carico	73
Configurazione di appliance per vRealize Automation	73
Installazione dei componenti di IaaS in una configurazione distribuita	80
Installazione degli agenti	110
Impostare i criteri di esecuzione di PowerShell su RemoteSigned	110
Scelta dello scenario d'installazione degli agenti	111
Posizione d'installazione dell'agente e requisiti	112
Installazione e configurazione dell'agente proxy per vSphere	112
Installazione dell'agente proxy per Hyper-V o XenServer	118
Installazione dell'agente VDI per XenDesktop	123
Installazione dell'agente EPI per Citrix	127
Installazione dell'agente EPI per Visual Basic Scripting	131
Installazione dell'agente WMI per le richieste WMI remote	134

6 Installazione invisibile all'utente 138

Informazioni sull'installazione invisibile all'utente	138
Esecuzione di un'installazione invisibile all'utente	139

Esecuzione di una installazione invisibile all'utente dell'agente di gestione	139
File di risposte dell'installazione invisibile all'utente	141
La riga di comando di installazione	142
Informazioni di base sulla riga di comando dell'installazione	142
Installazione dei nomi di comando	143
L'API di installazione	143
Conversione tra proprietà invisibili utente e JSON	145
7 Attività post-installazione	146
Non modificare il fuso orario	146
Configurare la crittografia conforme al FIPS	147
Attivazione del failover automatico del servizio di gestione	147
Informazioni sul failover automatico del servizio di gestione	148
Failover automatico del database PostgreSQL	149
Sostituzione di certificati autofirmati con certificati forniti da un'autorità	150
Modifica di nomi host e indirizzi IP	150
Modifica del nome host dell'appliance	150
Modifica dell'indirizzo IP dell'appliance	151
Regolazione del database SQL per un nome host modificato	153
Modifica dell'indirizzo IP di un server IaaS	153
Modifica del nome host di un server IaaS	154
Impostazione dell'URL di login su un nome personalizzato	157
Rimozione di un nodo dell'appliance vRealize Automation	157
Installazione dell'agente di vRealize Log Insight	157
Modifica della porta del proxy di VMware Remote Console	158
Ripristino del nome di dominio completo originale di un appliance	158
Configurazione di AAG (AlwaysOn Availability Group) SQL	159
Aggiunta di controller NIC dopo l'installazione di vRealize Automation	160
Configurazione di route statiche	161
Gestione delle patch di accesso	162
Configurazione dell'accesso per il tenant predefinito	163
8 Risoluzione dei problemi d'installazione	165
Rollback di un'installazione non riuscita	165
Rollback di un'installazione minima	165
Rollback di un'installazione distribuita	166
Creazione di un bundle di supporto	167
Risoluzione dei problemi correlati all'installazione generale	168
Installazione o aggiornamento non riuscito con un errore di timeout del bilanciamento del carico	168
Gli orari dei server non sono sincronizzati	169

Quando si utilizza Internet Explorer 9 o 10 su Windows 7 possono presentarsi pagine vuote	169
Impossibile stabilire una relazione basata sulla fiducia per il canale sicuro SSL/TLS	170
Connessione alla rete attraverso un server proxy	171
Passaggi di console per la configurazione del contenuto iniziale	171
Impossibile eseguire il downgrade delle licenze di vRealize Automation	172
Risoluzione dei problemi dell'appliance vRealize Automation	173
Download non riuscito dei programmi d'installazione	173
Il file Encryption.key ha autorizzazioni errate	174
Identity Manager di Gestione directory non si avvia dopo il riavvio di Horizon Workspace	174
Errate assegnazioni del ruolo dell'appliance dopo failover	176
Errori dopo la promozione di nodi di replica e master	177
Registrazioni dei servizi componenti non corrette	177
L'aggiunta di una NIC causa errori nell'interfaccia di gestione	180
Impossibile promuovere un'appliance virtuale secondaria al livello master	180
Il tempo di conservazione del registro della sincronizzazione di Active Directory è troppo breve	181
RabbitMQ non è in grado di risolvere i nomi host	181
Risoluzione dei problemi relativi ai componenti IaaS	183
Le connessioni di Distributed Transaction Coordinator vengono rifiutate	183
I server IaaS sono disconnessi	183
Il programma di correzione dei prerequisiti non può installare le funzionalità di .NET	184
Convalida dei certificati del server per IaaS	185
Errore di credenziali quando si esegue il programma d'installazione di IaaS	186
Visualizzazione di un avviso di salvataggio impostazioni durante l'installazione di IaaS	186
Installazione del server del sito Web e dei Distributed Execution Manager non riuscita	187
L'autenticazione di IaaS non riesce durante l'installazione dei componenti di gestione modelli e Web di IaaS	187
Installazione di Model Manager Data e componenti Web non riuscita	188
I server Windows IaaS non supportano FIPS	189
L'aggiunta di un endpoint XaaS causa un errore interno	190
Disinstallazione di un agente proxy non riuscita	190
Le richieste delle macchine non riescono quando le transazioni remote sono disabilitate	191
Errore di comunicazione nel servizio di gestione	192
Il comportamento della personalizzazione email è cambiato	193
Risoluzione degli errori di accesso	193
I tentativi di accedere come amministratore di IaaS con credenziali in formato UPN errate terminano con esito negativo senza fornire dettagli	194
Accesso con alta disponibilità non riuscito	194
Il proxy impedisce l'accesso agli utenti di VMware Identity Manager	195

Installazione di vRealize Automation

In questa guida all'*installazione di vRealize Automation* sono riportate le istruzioni per l'installazione tramite procedura guidata, manuale e invisibile all'utente per VMware vRealize™ Automation.

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

Destinatari

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

Informazioni aggiornate

Nella seguente tabella sono elencate le modifiche relative all'*installazione di vRealize Automation* per questa release del prodotto.

Revisione	Descrizione
XX TBD 202X	<ul style="list-style-type: none">■ Aggiornato Installazione dell'agente di gestione di vRealize Automation.■ Aggiornato Attivazione del failover automatico del servizio di gestione.■ Aggiornato Registrazioni dei servizi componenti di vRealize Automation non corrette.
12 AGO 2020	Aggiornato Estrazione di certificati e chiavi private .
14 FEB 2020	<ul style="list-style-type: none">■ Aggiornato Server Windows IaaS.■ Aggiornato Host del servizio di gestione di IaaS.■ Aggiornato Host SQL Server di IaaS.■ Aggiornato Non modificare il fuso orario di vRealize Automation.■ Aggiornato Gestione delle patch di accesso.■ Aggiunto Le connessioni di Distributed Transaction Coordinator vengono rifiutate.■ Aggiornato Le richieste delle macchine non riescono quando le transazioni remote sono disabilitate.
24 OTT 2019	Aggiunto promemoria del connettore a Aggiunta di un'altra appliance vRealize Automation al cluster .
9 SET 2019	<ul style="list-style-type: none">■ Aggiornato Appliance vRealize Automation.■ Aggiunto Non modificare il fuso orario di vRealize Automation.
14 GIU 2019	<ul style="list-style-type: none">■ Aggiornate le impostazioni dei criteri di gruppo in Account e password.■ Aggiornate le impostazioni internazionali dell'inglese in Server Windows IaaS.■ Aggiunto I server IaaS sono disconnessi.
30 MAG 2019	<ul style="list-style-type: none">■ Aggiunte le impostazioni dei criteri di gruppo in Account e password.■ Rimosso PowerShell 2 e aggiunte le impostazioni internazionali dell'inglese in Server Windows IaaS.
7 MAG 2019	Corretti un paio di collegamenti ipertestuali.
11 APR 2019	Release del documento iniziale.

Cenni generali sull'installazione di vRealize Automation

1

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.

Questo capitolo include i seguenti argomenti:

- [Informazioni sull'installazione di vRealize Automation](#)
- [Novità di questa installazione di vRealize Automation](#)
- [Componenti d'installazione di vRealize Automation](#)
- [Tipo di distribuzione](#)
- [Scelta del metodo d'installazione](#)

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 possibile installare vRealize Automation anche utilizzando Lifecycle Manager. Per ulteriori informazioni, consultare la [guida all'installazione, all'aggiornamento e alla gestione di vRealize Suite Lifecycle Manager](#).

vRealize Suite Lifecycle Manager automatizza l'installazione, la configurazione, l'aggiornamento, l'applicazione di patch, la gestione della configurazione, la correzione dello scostamento e il controllo dell'integrità da un unico pannello di controllo. Fare clic qui per installare [vRealize Suite Lifecycle Manager](#). Lifecycle Manager fornisce ai responsabili IT le risorse di amministrazione del cloud che consentono loro di concentrarsi sulle operazioni aziendali importanti, migliorando time-to-value, affidabilità e coerenza.

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.

- Quando si accede dopo l'installazione, l'interfaccia di amministrazione dell'appliance vRealize Automation viene aperta in una nuova pagina di riepilogo con le informazioni di sistema, lo stato e le statistiche di utilizzo.
- La scheda Cluster dell'interfaccia di amministrazione dell'appliance vRealize Automation può ora segnalare un assortimento di statistiche di integrità.

Per modificare i report predefiniti del cluster, modificare il file seguente nell'appliance vRealize Automation.

```
/etc/vcac/validation.properties
```

Alcune impostazioni dei file influiscono anche sullo stato della pagina di riepilogo.

- Questa versione corregge i problemi segnalati come descritto in dettaglio nelle note di rilascio.

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 AutomationaaS 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.

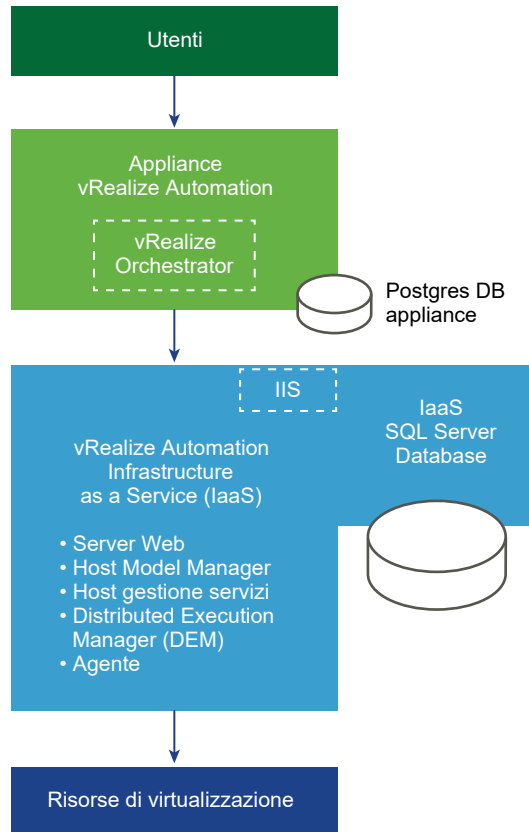
Tipo di distribuzione

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 1-1. Distribuzione minima di vRealize Automation

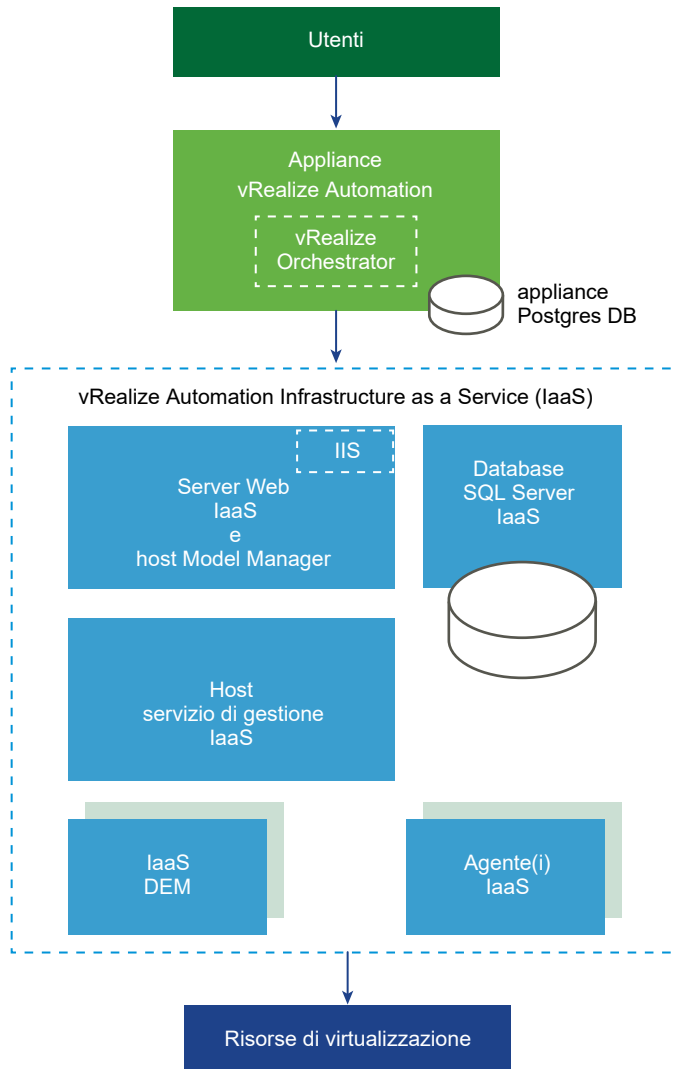


Non è possibile convertire una distribuzione minima in una distribuzione enterprise. Per ampliare una distribuzione, iniziare con una distribuzione enterprise di piccole dimensioni e aggiungervi componenti. Non è possibile iniziare con una distribuzione minima.

Distribuzioni di vRealize Automation distribuite

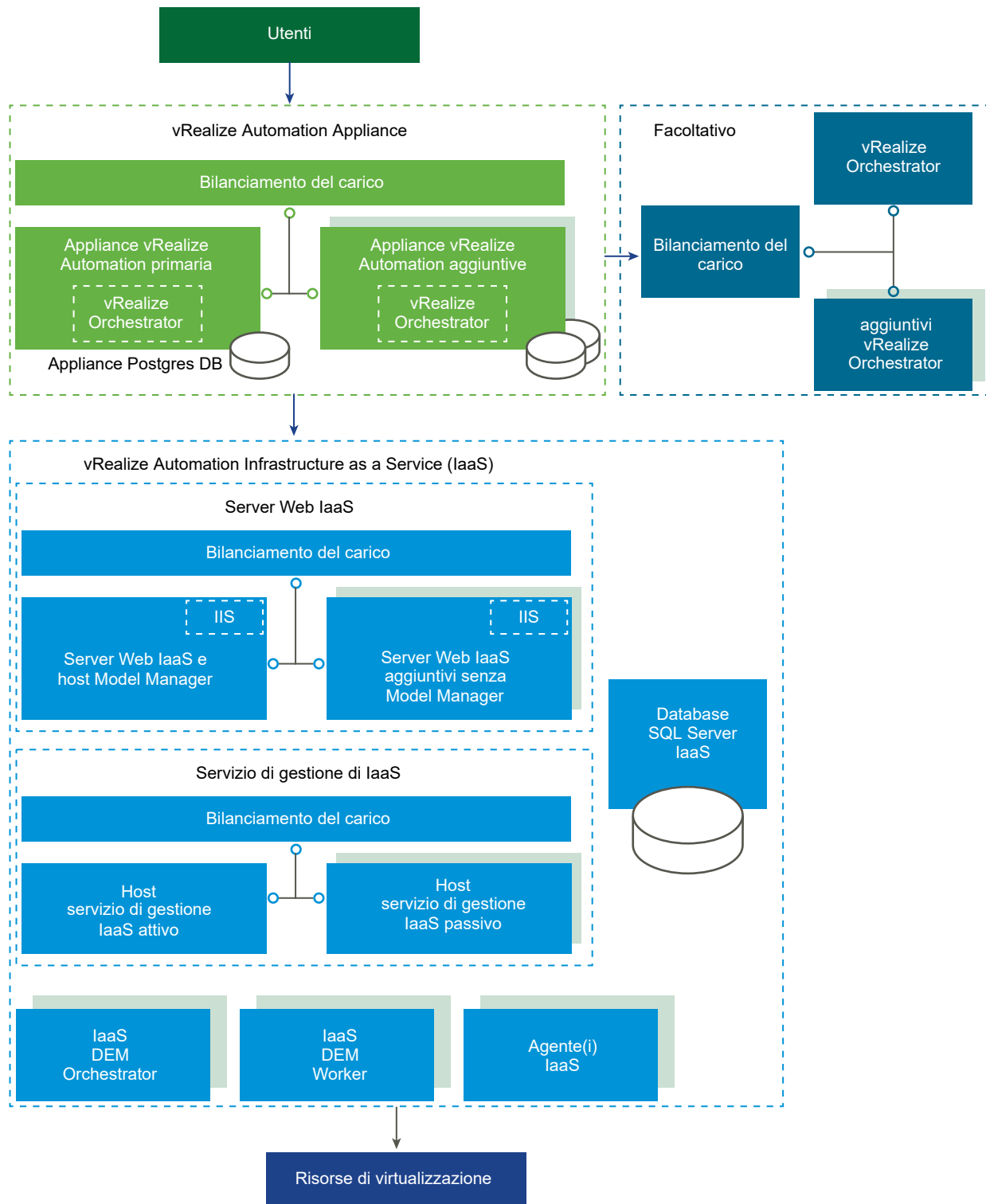
Le dimensioni delle distribuzioni enterprise distribuite possono essere varie. Una distribuzione distribuita di base può migliorare vRealize Automation semplicemente ospitando componenti IaaS in server Windows, come mostrato nell'illustrazione seguente.

Figura 1-2. 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 1-3. 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

2

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.

Questo capitolo include i seguenti argomenti:

- [Preparazione generale](#)
- [Account e password](#)
- [Nomi host e indirizzi IP](#)
- [Latenza e larghezza di banda](#)
- [Appliance vRealize Automation](#)
- [Server Windows IaaS](#)
- [Server Web IaaS](#)
- [Host del servizio di gestione di IaaS](#)
- [Host SQL Server di IaaS](#)
- [Host Distributed Execution Manager di IaaS](#)
- [Certificati](#)

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 del 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.

- Se il sito utilizza impostazioni di protezione dei criteri di gruppo, verificare le seguenti impostazioni per l'account. Eseguire l'editor dei criteri di gruppo gpedit.msc e cercare in **Configurazione computer > Impostazioni di Windows > Impostazioni sicurezza > Criteri locali > Assegnazione diritti utente**.
 - Nega accesso locale: non aggiunge l'account.
 - Consenti accesso locale: aggiunge l'account.
 - Nega accesso al computer dalla rete: non aggiunge l'account.
 - Accedi al computer dalla rete: aggiunge l'account.

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 risolversi 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.

- 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.

L'appliance esegue SUSE Linux Enterprise 11 a 64 bit. VMware non supporta modifiche o personalizzazioni dell'appliance. Non aggiungere, rimuovere o aggiornare pacchetti o script personalizzati, incluso il software antivirus.

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 2-1. 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"> ■ 4 CPU ■ 18 GB di memoria ■ 140 GB di spazio su disco 	<ul style="list-style-type: none"> ■ 4 CPU ■ 22 GB di memoria ■ 140 GB di spazio su disco

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 2-2. 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.

Tabella 2-2. Porte in ingresso (continua)

Porta	Protocollo	Commenti
4369, 5671, 5672, 25672	TCP	Messaggistica RabbitMQ.
5480	TCP	Consente di accedere all'interfaccia di gestione dell'appliance virtuale. 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.
8494	TCP	Sincronizzazione del cluster servizi contenitore
9300-9400	TCP	Accesso ai controlli di Identity Manager.
54328	UDP	
40002, 40003	TCP	sincronizzazione del cluster vIDM
8090, 8092	TCP	Utilizzato dal servizio di integrità per la connessione tra nodi di vRA

Tabella 2-3. 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.

Tabella 2-3. Porte in uscita (continua)

Porta	Protocollo	Commenti
		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 predefinita visualizzata, ma è possibile configurarla.
8281	TCP	Facoltativi. Per la comunicazione con un'istanza di vRealize Orchestrator esterna.
8494	TCP	Sincronizzazione del cluster servizi contenitore
9300-9400	TCP	Accesso ai controlli di Identity Manager.
54328	UDP	
40002, 40003	TCP	sincronizzazione del cluster vIDM

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.

Importante L'installazione disabilita Windows Firewall. Se i criteri del sito richiedono Windows Firewall, riabilitarlo dopo l'installazione e aprire le porte del server Windows IaaS una alla volta. Vedere [Porte dei server IaaS Windows](#).

- 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.

- I server Windows IaaS e l'host del database SQL Server devono essere in grado di risolversi a vicenda mediante il nome NETBIOS. Se necessario, aggiungere i nomi NETBIOS al file `/etc/hosts` in ogni server Windows IaaS e nell'host del database SQL Server, quindi riavviare le macchine.
- 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 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.
- Per qualsiasi distribuzione di dimensioni superiori a quelle minime, impostare i server Windows IaaS nelle impostazioni internazionali dell'inglese.
- 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 2-4. 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 2-5. Porte in uscita

Porta	Protocollo	Componente	Commenti
53	TCP, UDP	Tutto	DNS.
67, 68, 546, 547	TCP, UDP	Tutto	DHCP
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

Tabella 2-5. Porte in uscita (continua)

Porta	Protocollo	Componente	Commenti
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 201 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 2-6. Internet Information Services IaaS

Componente IIS	Impostazione
Ruoli di Internet Information Services (IIS)	<ul style="list-style-type: none"> ■ Autenticazione Windows ■ Contenuto statico ■ Documento predefinito ■ ASP.NET 3.5 e ASP.NET 4.5 ■ Estensioni ISAPI ■ Filtro ISAPI
Ruoli del servizio Attivazione processo Windows di IIS	<ul style="list-style-type: none"> ■ API di configurazione ■ Ambiente di rete ■ Modello di processo ■ Attivazione WCF (solo varianti di Windows 2008) ■ Attivazione HTTP ■ Attivazione non HTTP (solo varianti di Windows 2008) <p>(Varianti di Windows 2012: passare a Funzionalità > Funzionalità di .Net Framework 3.5 > Attivazione non HTTP)</p>
Impostazioni di autenticazione IIS	<p>Configurare le seguenti impostazioni non predefinite.</p> <ul style="list-style-type: none"> ■ Autenticazione Windows attivata ■ Autenticazione anonima disabilitata <p>Non modificare le seguenti impostazioni predefinite.</p> <ul style="list-style-type: none"> ■ Provider negoziazione attivata ■ Provider NTLM attivata ■ Modalità kernel autenticazione Windows attivata ■ Protezione estesa autenticazione Windows disattivata ■ Per i certificati che utilizzano SHA512, è necessario disabilitare TLS1.2 sulle varianti di Windows 2012

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.

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](#).

I requisiti sono gli stessi, indipendentemente dal fatto che l'host del servizio di gestione sia primario o di backup.

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.

Lo stesso comportamento si applica anche a SQL Server 2017.

- AAG (AlwaysOn Availability Group) è supportato solo con SQL Server 2016 Enterprise o SQL Server 2017 Enterprise. Quando si utilizza AAG, specificare il nome di dominio completo del listener AAG come host dell'istanza SQL Server. Quando si crea AAG, impostare DTC_Support = Per_DB. L'impostazione di questo valore dopo la creazione di AAG non funzionerà.
- Se ospitato insieme ai componenti di IaaS, è necessario configurare Java.
 - Installare l'aggiornamento 201 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 capacità massime* nella Guida di vRealize Automation *Architettura di riferimento*.
- 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 2-7. 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 su come preparare l'ambiente SCVMM, vedere *Configurazione di vRealize Automation*.

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 2-8. Implementazioni dei certificati

Componente	Distribuzione minima (non di produzione)	Distribuzione distribuita (pronta per la produzione)
Appliance vRealize Automation	Generare un certificato autofirmato durante la configurazione dell'appliance.	Per ciascun cluster di appliance, è possibile utilizzare un certificato proveniente da un'autorità di certificazione interna o esterna. Vengono supportati certificati multiuso e certificati wildcard.
Componenti 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 per le appliance virtuali devono essere in formato PEM.

Se l'autorità di certificazione ha fornito un certificato in formato PFX, utilizzare OpenSSL per convertire PFX in PEM.

```
openssl pkcs12 -in path-to-pfx -out desired-path-to-pem -nodes
```

Ad esempio:

```
openssl pkcs12 -in C:\vra-cert.pfx -out C:\vra-cert.pem -nodes
```

Potrebbe essere necessario immettere una passphrase se il certificato PFX ne include una.

Distribuzione dell'appliance vRealize Automation

3

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

Questo capitolo include i seguenti argomenti:

- [Informazioni sulla distribuzione dell'appliance vRealize Automation](#)
- [Distribuzione di vRealize Automation appliance](#)
- [Aggiunta di controller NIC prima di eseguire il programma di installazione](#)

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 3-1. Proprietà di esempio dell'appliance virtuale

▼ Application	3 settings
Enable SSH service in the appliance	This will be used as an initial status of the SSH service in the appliance. You can change it later from the appliance Web console. <input checked="" type="checkbox"/>
Hostname	The host name for this virtual machine. Provide the fully qualified domain name if you use a static IP. Leave blank to try to reverse look up the IP address if you use DHCP. va1.mycompany.com
Initial root password	This will be used as an initial password for the root user account. You can change the password later (by using the passwd command or from the appliance Web console). Enter password: <input type="password"/> Confirm password: <input type="password"/>
▼ Networking Properties	6 settings
Default Gateway	The default gateway address for this VM. Leave blank if DHCP is desired. 12.34.56.79
Domain Name	The domain name of this VM. Leave blank if DHCP is desired. mycompany.com
Domain Name Servers	The domain name server IP Addresses for this VM (comma separated). Leave blank if DHCP is desired. 12.34.56.80, 12.34.56.81
Domain Search Path	The domain search path (comma or space separated domain names) for this VM. Leave blank if DHCP is desired. mycompany.com
Network 1 IP Address	The IP address for this interface. Leave blank if DHCP is desired. 12.34.56.78
Network 1 Netmask	The netmask or prefix for this interface. Leave blank if DHCP is desired. 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-addressnetmaskgateway-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 [Capitolo 5 Le interfacce di installazione standard di vRealize Automation](#).

Questo capitolo include i seguenti argomenti:

- [Utilizzo dell'installazione guidata per le distribuzioni minime](#)
- [Utilizzo dell'installazione guidata per le distribuzioni enterprise](#)

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 [Capitolo 2 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`

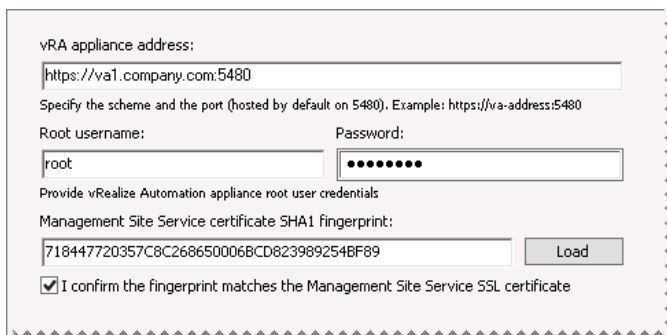
- 3 Copiare l'impronta digitale per poterla verificare successivamente. Ad esempio:
71:84:47:72:03:57:C8:C2:68:65:00:06:BC:D8:23:98:92:54:BF:89
- 4 Accedere al server Windows IaaS utilizzando un account che disponga di diritti di amministratore.
- 5 Aprire un browser Web nell'URL del programma di installazione 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 4-1. 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.

Risultati

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 [Capitolo 6 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 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 attiva.

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 [Capitolo 2 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 loro appliance vRealize Automation primaria.

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 Automation primaria, 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 una o più 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 primaria 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 con l'URL del programma di installazione dell'appliance vRealize Automation primaria.

```
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 primaria:

- a Immettere l'indirizzo HTTPS dell'appliance primaria, includendo il nome di dominio completo e il numero di porta :5480.
- b Immettere le credenziali dell'account root dell'appliance primaria.
- 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 4-2. 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.**Risultati**

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 [Capitolo 6 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 configurare l'accesso al tenant predefinito per altri utenti, vedere [Configurazione dell'accesso per il tenant predefinito](#).

Le interfacce di installazione standard di vRealize Automation

5

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 [Capitolo 4 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.

Questo capitolo include i seguenti argomenti:

- [Utilizzo delle interfacce standard per le distribuzioni minime](#)
- [Utilizzo delle interfacce standard per le distribuzioni distribuite](#)
- [Installazione degli agenti di vRealize Automation](#)

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 5-1. Elenco di controllo di una distribuzione minima

Attività	Dettagli
<input type="checkbox"/> Pianificare i prerequisiti d'installazione di ambiente e indirizzo.	Capitolo 2 Preparazione per l'installazione di vRealize Automation
<input type="checkbox"/> Creare un'appliance vRealize Automation non configurata.	Distribuzione di vRealize Automation appliance
<input type="checkbox"/> Configurare manualmente l'appliance vRealize Automation.	Configurazione dell'appliance vRealize Automation
<input type="checkbox"/> Installare i componenti IaaS su un singolo server Windows.	Installazione dei componenti IaaS
<input type="checkbox"/> Installare agenti aggiuntivi, se necessario.	Installazione degli agenti di vRealize Automation
<input type="checkbox"/> Eseguire le attività post-installazione, come la configurazione del tenant predefinito.	Configurazione dell'accesso per il tenant predefinito

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
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.

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 **vRA > Impostazioni host**.

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

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

5 Selezionare l'azione appropriata nel 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
Mantieni esistente	Lasciare invariata la configurazione SSL corrente. Selezionare questa opzione per annullare le modifiche.
Genera certificato	<ul style="list-style-type: none"> a Il valore visualizzato nella casella di testo Nome comune è il nome host visualizzato nella parte superiore della pagina. Se sono disponibili istanze aggiuntive dell'appliance vRealize Automation, i rispettivi nomi di dominio completi vengono inclusi nell'attributo SAN del certificato. b Immettere il nome dell'organizzazione, come ad esempio quello della propria azienda, nella casella di testo Organizzazione. c Immettere l'unità organizzativa, ad esempio il nome o la posizione del proprio reparto, nella casella di testo Unità organizzativa. d Immettere il codice di paese ISO 3166 a due lettere, ad esempio IT, nella casella di testo Paese.

Opzione	Azione
Genera richiesta di firma	<ul style="list-style-type: none"> a Selezionare Genera richiesta di firma. b Verificare le voci nelle caselle di testo Organizzazione, Unità organizzativa, Prefisso internazionale e Nome comune. Queste voci vengono populate dal certificato esistente. Se necessario, è possibile modificare queste voci. c Fare clic su Genera CSR per generare una richiesta di firma del certificato, quindi fare clic sul collegamento Scarica qui la richiesta CSR generata 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. d Una volta ricevuto il certificato preparato, fare clic su Importa e seguire le istruzioni per importare un certificato in vRealize Automation.
Importazione	<ul style="list-style-type: none"> a Copiare i valori del certificato dalla stringa BEGIN PRIVATE KEY alla stringa END PRIVATE KEY, inclusi intestazione e piè di pagina, quindi incollarli nella casella di testo Chiave privata RSA. b Copiare i valori del certificato dalla stringa BEGIN CERTIFICATE alla stringa END CERTIFICATE, inclusi intestazione e piè di pagina, quindi incollarli nella casella di testo Catena di certificati. Per valori di certificati multipli, includere un'intestazione BEGIN CERTIFICATE e un piè di pagina END CERTIFICATE per ciascun certificato. <hr/> <p>Nota In caso di certificati concatenati, possono essere disponibili attributi aggiuntivi.</p> <hr/> <ul style="list-style-type: none"> c (Facoltativo) Se il certificato utilizza una passphrase per crittografare la chiave del certificato, copiare la passphrase e incollarla nella casella di testo Passphrase.

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

Risultati

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 AutomationIaaS

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 AutomationIaaS

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 all'interfaccia di gestione dell'appliance vRealize Automation 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 Avanti .
Errori non critici	Fare clic su Bypass .
Errori critici	Se si ignorano gli errori critici, l'installazione non riuscirà. Se vengono visualizzati avvisi, selezionare l'avviso nel riquadro di sinistra e seguire le istruzioni visualizzate a destra. Risolvere tutti gli errori critici e fare clic su Controlla di nuovo per verificare.

- 2 Fare clic su **Avanti**.

Risultati

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**.

Risultati

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 5-2. Elenco di controllo di una distribuzione distribuita

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

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 *Uso del plug-in 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.

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

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 segue in gran parte l'architettura di vRealize Automation in tre livelli.

- Appliance vRealize Automation
- Componenti Web di IaaS
- Componenti del servizio di gestione di IaaS

In una distribuzione distribuita, ogni macchina in un determinato livello condivide un certificato. Ad esempio, ogni appliance vRealize Automation condivide un certificato comune e ogni host del servizio di gestione condivide un certificato comune.

Quando i componenti Web e del servizio di gestione sono ospitati nella stessa macchina, un certificato è sufficiente per entrambi i livelli.

Certificati generati dal sistema

A partire dalla versione 7.0, se non si forniscono i propri certificati, l'installazione guidata di vRealize Automation può generare automaticamente certificati autofirmati e posizzarli negli archivi attendibili appropriati nei componenti distribuiti che li richiedono.

Se è necessario aggiornare i certificati autofirmati generati dal sistema con certificati forniti dall'utente o dall'autorità di certificazione, vedere *Gestione di vRealize Automation*.

Utilizzo dei propri certificati

Quando si esegue il programma di installazione manuale standard, si forniscono i propri certificati autofirmati generati o i certificati dell'autorità di certificazione (CA).

Quando si forniscono o si generano i propri certificati utilizzando OpenSSL o un altro metodo, è possibile usare certificati con carattere jolly o SAN (Subject Alternative Name).

I certificati IaaS devono essere certificati multiuso. Quando si forniscono certificati, è necessario ottenere un certificato multiuso che includa i componenti IaaS nel cluster, quindi copiare tale certificato nell'archivio attendibile per ciascun componente.

Bilanciamento del carico

Per la disponibilità elevata e il failover, è possibile aggiungere bilanciamenti del carico davanti ai componenti distribuiti di vRealize Automation. VMware consiglia una configurazione pass-through per i bilanciamenti del carico di vRealize Automation. In una configurazione pass-through, i bilanciamenti del carico passano le richieste ai componenti senza decrittografia. Le appliance vRealize Automation e gli host IaaS eseguono quindi la decrittografia necessaria.

Se si utilizzano i bilanciamenti del carico, nell'indirizzo attendibile dei certificati multiuso del cluster è necessario includere il nome di dominio completo (FQDN) del bilanciamento del carico.

Per ulteriori informazioni sull'uso e la configurazione dei bilanciamenti del carico, vedere *Bilanciamento del carico di vRealize Automation*.

Requisiti di attendibilità dei certificati

La tabella seguente riepiloga i requisiti di registrazione attendibile per i diversi certificati importati.

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

Attendibilità dei certificati e programma di installazione standard

Ogni volta che si esegue o si riesegue il programma di installazione manuale standard per creare componenti IaaS, è necessario configurare l'attendibilità dei certificati in tali componenti IaaS. Ad esempio, è possibile utilizzare il programma di installazione standard per eseguire la scalabilità orizzontale di una distribuzione esistente.

- Host del servizio di gestione e Web di IaaS

Importare i file `web.pfx` e `ms.pfx` nelle seguenti posizioni.

```
Host Computer/Certificates/Personal certificate store
Host Computer/Certificates/Trusted People certificate store
```

- Host di DEM Orchestrator, DEM Worker e agente proxy di IaaS

Importare i file `web.pfx` e `ms.pfx` nelle seguenti posizioni.

```
Host Computer/Certificates/Trusted People certificate store
```

Nell'archivio certificati Persone attendibili, non è necessario importare la chiave privata insieme al certificato. Il processo di installazione automatica installa solo il certificato nell'archivio certificati Persone attendibili.

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 5-3. 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 (https://appliance-FQDN:5480)	root (predefinito)	root
Password interfaccia di gestione		admin123

Tabella 5-3. Appliance vRealize Automation (continua)

Variabile	Valore personale	Esempio
Tenant predefinito	vsphere.local (predefinito)	vsphere.local
Nome utente tenant predefinito	administrator@vsphere.local (predefinito)	administrator@vsphere.local
Password tenant predefinita		login123

Tabella 5-4. 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

Tabella 5-4. Server Windows IaaS (continua)

Variabile	Valore personale	Esempio
Indirizzo IP del bilanciamento del carico dell'host del servizio di gestione IaaS Solo per riferimento; non inserire indirizzi IP		123.234.203
Per i servizi IaaS, account di dominio con diritti di amministratore sugli host		SUPPORT\provisioner
Password account		login123

Tabella 5-5. 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 5-6. 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 il white paper tecnico *Guida alla configurazione del 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
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.

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 all'interno di una distribuzione vRealize Automation.

- 4 Selezionare **vRA > Impostazioni host**.

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

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

- 5 Selezionare l'azione appropriata nel 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
Mantieni esistente	Lasciare invariata la configurazione SSL corrente. Selezionare questa opzione per annullare le modifiche.
Genera certificato	<ul style="list-style-type: none"> a Il valore visualizzato nella casella di testo Nome comune è il nome host visualizzato nella parte superiore della pagina. Se sono disponibili istanze aggiuntive dell'appliance vRealize Automation, i rispettivi nomi di dominio completi vengono inclusi nell'attributo SAN del certificato. b Immettere il nome dell'organizzazione, come ad esempio quello della propria azienda, nella casella di testo Organizzazione. c Immettere l'unità organizzativa, ad esempio il nome o la posizione del proprio reparto, nella casella di testo Unità organizzativa. d Immettere il codice di paese ISO 3166 a due lettere, ad esempio IT, nella casella di testo Paese.

Opzione	Azione
Genera richiesta di firma	<ul style="list-style-type: none"> a Selezionare Genera richiesta di firma. b Verificare le voci nelle caselle di testo Organizzazione, Unità organizzativa, Prefisso internazionale e Nome comune. Queste voci vengono populate dal certificato esistente. Se necessario, è possibile modificare queste voci. c Fare clic su Genera CSR per generare una richiesta di firma del certificato, quindi fare clic sul collegamento Scarica qui la richiesta CSR generata 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. d Una volta ricevuto il certificato preparato, fare clic su Importa e seguire le istruzioni per importare un certificato in vRealize Automation.
Importazione	<ul style="list-style-type: none"> a Copiare i valori del certificato dalla stringa BEGIN PRIVATE KEY alla stringa END PRIVATE KEY, inclusi intestazione e piè di pagina, quindi incollarli nella casella di testo Chiave privata RSA. b Copiare i valori del certificato dalla stringa BEGIN CERTIFICATE alla stringa END CERTIFICATE, inclusi intestazione e piè di pagina, quindi incollarli nella casella di testo Catena di certificati. Per valori di certificati multipli, includere un'intestazione BEGIN CERTIFICATE e un piè di pagina END CERTIFICATE per ciascun certificato. <hr/> <p>Nota In caso di certificati concatenati, possono essere disponibili attributi aggiuntivi.</p> <hr/> <ul style="list-style-type: none"> c (Facoltativo) Se il certificato utilizza una passphrase per crittografare la chiave del certificato, copiare la passphrase e incollarla nella casella di testo Passphrase.

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

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

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

a Se non è già stato fatto, accedere all'interfaccia di gestione dell'appliance vRealize Automation come utente root.

`https://vrealize-automation-appliance-FQDN:5480`

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

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

11 Fare clic su Messaggistica. Vengono visualizzate le impostazioni di configurazione e lo stato della messaggistica per l'appliance. Non cambiare queste impostazioni.**12 Fare clic sulla scheda Telemetria** per scegliere se partecipare al programma CEIP (Customer Experience Improvement Program) di VMware.

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

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

13 Fare clic su Salva impostazioni.**14 Assicurarsi che sia possibile accedere 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.

Active Directory: 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. Dopo aver aggiunto un'altra appliance, ricordarsi di configurare un secondo connettore che corrisponda all'appliance aggiunta. Il secondo connettore si connette al provider di identità e punta alla stessa istanza di Active Directory. In questo modo, se la prima appliance non riesce, la seconda assume la gestione dell'autenticazione utente.

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 **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.

Risultati

Se un'operazione di unione di cluster richiede molto tempo e alla fine va in timeout, vedere [l'articolo 58708 della Knowledge Base di VMware](#).

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 AutomationIaaS

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 AutomationIaaS](#).

Scaricare il programma di installazione di vRealize AutomationIaaS

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 laaS.

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 laaS 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 5-7. Scelta di uno scenario di database laaS

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

Creazione manuale del database laaS

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 laaS](#).
- Aprire in un browser Web l'URL del programma di installazione dell'appliance vRealize Automation, quindi scaricare gli script di installazione del database laaS.

<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 5-8. Valori del database

Variabile	Valore
<i>db_server</i>	Specifica l'istanza di SQL Server nel formato <code>dbhostname[,port number]\SQL instance</code> . 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 <code>localhost</code> .
<i>db_name</i>	Nome del database. Il valore predefinito è <code>vra</code> . I nomi dei database non possono contenere più di 128 caratteri ASCII.
<i>db_dir</i>	Percorso della directory dei dati per il database (escludere la barra finale).
<i>log_dir</i>	Percorso della directory dei registri per il database (escludere la barra finale).
<i>service_user</i>	Nome utente utilizzato per l'esecuzione del servizio di gestione.
<i>Web_user</i>	Nome utente utilizzato per l'esecuzione dei servizi Web.
<i>version_string</i>	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 <code>6.1.0.1200</code> .

Risultati

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 laaS 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 laaS](#).
- Aprire in un browser Web l'URL del programma di installazione dell'appliance vRealize Automation, quindi scaricare gli script di installazione del database laaS.

<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 5-9. 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 laaS. 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 AutomationIaaS](#).

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 all'interfaccia di gestione dell'appliance vRealize Automation 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 **Use Windows identity**. Immettere le credenziali SQL nelle caselle di testo di utente e password.

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

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

18 Fare clic su **Installa**.

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

20 Fare clic su **Fine**.

Risultati

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.

Risultati

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 all'interfaccia di gestione dell'appliance vRealize Automation 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-revoce 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 Fare 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
Senza bilanciamento del carico	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.
Con bilanciamento del carico	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
Nessun errore	Fare clic su Avanti .
Errori non critici	Fare clic su Bypass .
Errori critici	Se si ignorano gli errori critici, l'installazione non riuscirà. Se vengono visualizzati avvisi, selezionare l'avviso nel riquadro di sinistra e seguire le istruzioni visualizzate a destra. Risolvere tutti gli errori critici e fare clic su Controlla di nuovo per verificare.

- 13** 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
Se sono già stati installati componenti in questo ambiente	Immettere la passphrase precedentemente creata nelle caselle di testo Passphrase e Conferma .
Se questa è la prima installazione	Immettere una passphrase nelle caselle di testo Passphrase e Conferma . È necessario utilizzare questa passphrase ogni volta che si installa un nuovo componente.

Conservare la passphrase in un luogo sicuro per uso futuro.

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

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

- 16** Fare clic su **Avanti**.

- 17** Fare clic su **Installa**.

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

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* nella guida *Gestione di vRealize Automation*.
- 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 all'interfaccia di gestione dell'appliance vRealize Automation 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
Senza bilanciamento del carico	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.
Con bilanciamento del carico	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
Nessun errore	Fare clic su Avanti .
Errori non critici	Fare clic su Bypass .
Errori critici	Se si ignorano gli errori critici, l'installazione non riuscirà. Se vengono visualizzati avvisi, selezionare l'avviso nel riquadro di sinistra e seguire le istruzioni visualizzate a destra. Risolvere tutti gli errori critici e fare clic su Controlla di nuovo per verificare.

- 22 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
Se sono già stati installati componenti in questo ambiente	Immettere la passphrase precedentemente creata nelle caselle di testo Passphrase e Conferma .
Se questa è la prima installazione	Immettere una passphrase nelle caselle di testo Passphrase e Conferma . È necessario utilizzare questa passphrase ogni volta che si installa un nuovo componente.

Conservare la passphrase in un luogo sicuro per uso futuro.

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

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

- 25** Fare clic su **Avanti**.

- 26** Fare clic su **Installa**.

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

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 all'interfaccia di gestione dell'appliance vRealize Automation 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
Senza bilanciamento del carico	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.
Con bilanciamento del carico	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.
- Se è stato importato un certificato dopo aver iniziato l'installazione, fare clic su **Aggiorna** per aggiornare l'elenco.
 - Selezionare il certificato da utilizzare da **Certificati disponibili**.
 - 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 Passphrase e Conferma .
Se questa è la prima installazione	Immettere una passphrase nelle caselle di testo Passphrase e Conferma . È necessario utilizzare questa passphrase ogni volta che si installa un nuovo componente.

Conservare la passphrase in un luogo sicuro per uso futuro.

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

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

- 23** Fare clic su **Avanti**.

- 24** Fare clic su **Installa**.

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

- 26** Fare clic su **Fine**.

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* nella guida *Gestione di vRealize Automation*.
- 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 all'interfaccia di gestione dell'appliance vRealize Automation 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
Senza bilanciamento del carico	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.
Con bilanciamento del carico	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 Passphrase e Conferma .
Se questa è la prima installazione	Immettere una passphrase nelle caselle di testo Passphrase e Conferma . È necessario utilizzare questa passphrase ogni volta che si installa un nuovo componente.

Conservare la passphrase in un luogo sicuro per uso futuro.

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

Si tratta delle informazioni relative a server di database IaaS, nome e autenticazione create precedentemente.
- 24** Fare clic su **Avanti**.
- 25** Fare clic su **Installa**.
- 26** Al termine dell'installazione, deselezionare **Configurazione iniziale guidata** e fare clic su **Avanti**.
- 27** Fare clic su **Fine**.

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](#).

Prima di installare un nuovo DEMWorker, esportare il certificato dall'appliance virtuale di installazione di vRA e importarlo nel percorso di storage del certificato radice attendibile per la macchina locale.

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 all'interfaccia di gestione dell'appliance vRealize Automation 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
Worker	Il Worker si occupa di eseguire i workflow.
Orchestrator	L'Orchestrator supervisiona le attività del DEM Worker, inclusa la pianificazione e la pre-elaborazione dei workflow, e monitora lo stato online del DEM Worker.

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

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
Senza bilanciamento del carico	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.
Con bilanciamento del carico	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.

Risultati

Per ulteriori informazioni, vedere [DEM Worker con SCVMM](#).

Informazioni aggiuntive sulla preparazione dell'ambiente SCVMM e la creazione di un endpoint SCVMM sono disponibili in *Configurazione di vRealize Automation*.

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**.

Risultati

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 5-10. Scelta dello scenario per un agente

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

Posizione d'installazione dell'agente e requisiti

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

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

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

Installazione e configurazione dell'agente proxy per vSphere

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

Requisiti dell'agente di vSphere

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

Credenziali

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

Il privilegio VApp.Import consente di distribuire una macchina vSphere utilizzando le impostazioni importate da un OVF. Informazioni dettagliate sul privilegio vSphere sono disponibili nella [documentazione di vSphere SDK](#). Se si intende utilizzare un endpoint vSphere per distribuire macchine virtuali da modelli OVF, verificare che le proprie credenziali includano il privilegio VApp.Import di vSphere nell'istanza di vCenter Server associata all'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 5-11. Autorizzazioni richieste per consentire all'agente di vSphere di gestire l'istanza di vCenter Server

Valore attributo	Autorizzazione
Datastore	Spazio allocato
	Sfoglia datastore

Tabella 5-11. Autorizzazioni richieste per consentire all'agente di vSphere di gestire l'istanza di vCenter Server (continua)

Valore attributo		Autorizzazione
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
vApp		Importazione
		Configurazione dell'applicazione vApp
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

Tabella 5-11. Autorizzazioni richieste per consentire all'agente di vSphere di gestire l'istanza di vCenter Server (continua)

Valore attributo	Autorizzazione
	Avanzate
	Cambia numero CPU
	Cambia risorsa
	Estendi disco virtuale
	Traccia cambiamenti disco
	Memoria
	Modifica impostazioni dispositivo
	Rinomina
	Imposta annotazione (versione 5.0 e successive)
	Impostazioni
	Posizionamento file di swap
Provisioning	Personalizza
	Clona modello
	Clona macchina virtuale
	Distribuisci modello
	Leggi specifiche di personalizzazione
Stato	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 all'interfaccia di gestione dell'appliance vRealize Automation 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
Agente ridondante	Installare gli agenti ridondanti su server diversi. Denominare e configurare gli agenti ridondanti in modo identico.
Agente autonomo	Assegnare un nome univoco all'agente.

13 Configurare una connessione all'host del servizio di gestione di IaaS.

Opzione	Descrizione
Senza bilanciamento del carico	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.
Con bilanciamento del carico	Specificare il nome di dominio completo e il numero di porta della macchina su cui è stato installato il componente servizio di gestione, <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
Senza bilanciamento del carico	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.
Con bilanciamento del carico	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
true	(Predefinito) Le macchine virtuali eliminate in vRealize Automation da vCenter Server vengono cancellate.
false	Le macchine virtuali eliminate in vRealize Automation vengono spostate nella directory 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 all'interfaccia di gestione dell'appliance vRealize Automation 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
Agente ridondante	Installare gli agenti ridondanti su server diversi. Denominare e configurare gli agenti ridondanti in modo identico.
Agente autonomo	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
Senza bilanciamento del carico	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.
Con bilanciamento del carico	Specificare il nome di dominio completo e il numero di porta della macchina su cui è stato installato il componente servizio di gestione, <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
Senza bilanciamento del carico	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.
Con bilanciamento del carico	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 AutomationIaaS](#).

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 all'interfaccia di gestione dell'appliance vRealize Automation 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
Agente ridondante	Installare gli agenti ridondanti su server diversi. Denominare e configurare gli agenti ridondanti in modo identico.
Agente autonomo	Assegnare un nome univoco all'agente.

- 14 Configurare una connessione all'host del servizio di gestione di IaaS.

Opzione	Descrizione
Senza bilanciamento del carico	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.
Con bilanciamento del carico	Specificare il nome di dominio completo e il numero di porta della macchina su cui è stato installato il componente servizio di gestione, <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
Senza bilanciamento del carico	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.
Con bilanciamento del carico	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 AutomationIaaS.](#)

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 all'interfaccia di gestione dell'appliance vRealize Automation 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
Agente ridondante	Installare gli agenti ridondanti su server diversi. Denominare e configurare gli agenti ridondanti in modo identico.
Agente autonomo	Assegnare un nome univoco all'agente.

13 Configurare una connessione all'host del servizio di gestione di IaaS.

Opzione	Descrizione
Senza bilanciamento del carico	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.
Con bilanciamento del carico	Specificare il nome di dominio completo e il numero di porta della macchina su cui è stato installato il componente servizio di gestione, <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
Senza bilanciamento del carico	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.
Con bilanciamento del carico	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 5-12. Agenti EPI per Visual Basic Scripting

Requisito	Descrizione
Credenziali	Le credenziali con cui sarà eseguito l'agente devono consentire l'accesso amministrativo all'host d'installazione.
Microsoft PowerShell	Prima dell'installazione dell'agente è necessario installare Microsoft PowerShell sull'host d'installazione: la versione richiesta dipende dal sistema operativo dell'host d'installazione e potrebbe essere stata installata insieme al sistema operativo. Per ulteriori informazioni, visitare http://support.microsoft.com .
Criteri di esecuzione di MS PowerShell	<p>I criteri di esecuzione di MS PowerShell devono essere impostati su RemoteSigned o Unrestricted.</p> <p>Per informazioni sui criteri di esecuzione di PowerShell, eseguire uno dei seguenti comandi al prompt dei comandi della PowerShell:</p> <pre>help about_signing help Set-ExecutionPolicy</pre>

Installazione dell'agente per Visual Basic Scripting

Gli agenti della PowerShell di External Provisioning Integration (EPI) consentono di integrare sistemi esterni nel processo di provisioning delle macchine. Utilizzare un agente EPI per eseguire script Visual Basic e attuare operazioni aggiuntive durante il processo di provisioning.

Prerequisiti

- 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 AutomationIaaS](#).

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 all'interfaccia di gestione dell'appliance vRealize Automation 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
Agente ridondante	Installare gli agenti ridondanti su server diversi. Denominare e configurare gli agenti ridondanti in modo identico.
Agente autonomo	Assegnare un nome univoco all'agente.

13 Configurare una connessione all'host del servizio di gestione di IaaS.

Opzione	Descrizione
Senza bilanciamento del carico	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.
Con bilanciamento del carico	Specificare il nome di dominio completo e il numero di porta della macchina su cui è stato installato il componente servizio di gestione, <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
Senza bilanciamento del carico	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.
Con bilanciamento del carico	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 AutomationIaaS](#).

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 all'interfaccia di gestione dell'appliance vRealize Automation 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
Agente ridondante	Installare gli agenti ridondanti su server diversi. Denominare e configurare gli agenti ridondanti in modo identico.
Agente autonomo	Assegnare un nome univoco all'agente.

13 Configurare una connessione all'host del servizio di gestione di IaaS.

Opzione	Descrizione
Senza bilanciamento del carico	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.
Con bilanciamento del carico	Specificare il nome di dominio completo e il numero di porta della macchina su cui è stato installato il componente servizio di gestione, <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
Senza bilanciamento del carico	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.
Con bilanciamento del carico	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

6

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

Questo capitolo include i seguenti argomenti:

- [Informazioni sull'installazione di vRealize Automation invisibile all'utente](#)
- [Esecuzione di un'installazione di vRealize Automation invisibile all'utente](#)
- [Esecuzione di un'installazione dell'agente di gestione di vRealize Automation invisibile all'utente](#)
- [File di risposte dell'installazione di vRealize Automation invisibile all'utente](#)
- [La riga di comando di installazione di vRealize Automation](#)
- [L'API di installazione di vRealize Automation](#)
- [Conversione tra proprietà invisibili all'utente di vRealize Automation e JSON](#)

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
```

Risultati

È anche possibile visualizzare la guida relativa allo script.

```
/usr/lib/vcac/tools/install/convert-properties --help
```

Attività post-installazione di vRealize Automation

7

Dopo aver installato vRealize Automation, è necessario prestare attenzione ad alcune attività post-installazione.

Questo capitolo include i seguenti argomenti:

- [Non modificare il fuso orario di vRealize Automation](#)
- [Configurazione della crittografia conforme al Federal Information Processing Standard](#)
- [Attivazione del failover automatico del servizio di gestione](#)
- [Failover automatico del database PostgreSQL di vRealize Automation](#)
- [Sostituzione di certificati autofirmati con certificati forniti da un'autorità](#)
- [Modifica di nomi host e indirizzi IP](#)
- [Rimozione di un nodo dell'appliance vRealize Automation](#)
- [Installazione dell'agente di vRealize Log Insight su server IaaS](#)
- [Modifica della porta del proxy di VMware Remote Console](#)
- [Ripristino del nome di dominio completo originale di un appliance vRealize Automation](#)
- [Configurazione di AAG \(AlwaysOn Availability Group\) SQL](#)
- [Aggiunta di controller NIC dopo l'installazione di vRealize Automation](#)
- [Configurazione di route statiche](#)
- [Gestione delle patch di accesso](#)
- [Configurazione dell'accesso per il tenant predefinito](#)

Non modificare il fuso orario di vRealize Automation

Anche se l'interfaccia di gestione dell'appliance vRealize Automation offre un'opzione per cambiarlo, lasciare sempre il fuso orario di vRealize Automation impostato su Etc/UTC.

L'utilizzo di un fuso orario diverso da Etc/UTC causa errori insoliti, ad esempio migrazioni non riuscite e bundle di registri che non contengono voci di tutti i nodi di vRealize Automation.

L'opzione dell'interfaccia di gestione dell'appliance vRealize Automation che è necessario evitare è in **Sistema > Fuso orario**.

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 **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.

Risultati

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.

In una configurazione con più nodi, è sufficiente eseguire i passaggi una sola volta in qualsiasi nodo dell'appliance vRealize Automation.

Procedura

- 1 Accedere come utente root a una sessione della console nell'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
```

Risultati

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 *Aggiornamento da vRealize Automation 7.1 o 7.2 a 7.3*.

Per informazioni su come effettuare il bilanciamento del carico degli host del servizio di gestione, vedere [Bilanciamento del carico di vRealize Automation](#).

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 nella scheda Cluster dell'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 informazioni sull'esecuzione di un failover manuale, vedere *Gestione di 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 *Gestione 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 *Gestione di vRealize Automation*.
- 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 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.

Risultati

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**.

The screenshot shows the 'vApp Options' tab in the vRealize Automation interface. The 'IP allocation' section is expanded, showing the 'IP allocation scheme' set to 'OVF environment' (checked) and 'IP protocol' set to 'Both'. The 'OVF settings' section is also expanded, showing 'OVF environment transport' set to 'ISO image' (checked), 'VMware Tools' checked, and 'Installation boot' set to 'Enable'. The 'Installation boot' section also includes a delay in seconds to wait for the VM to power off, set to 0.

- 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.
 - Stato della connessione al database in **Cluster**
 - Stato di RabbitMQ in **vRA > Messaggistica**
 - Stato di Xenon in **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 sull'aggiornamento dei certificati, vedere *Gestione 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 7-1. 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
Nodo con componente Model Manager installato	<i>install-folder</i> \Server\Model Manager Data	Repoutil.exe.config
	<i>install-folder</i> \Server\Model Manager Data\Cafe	Vcac-Config.exe.config
Nodi del servizio di gestione	<i>install-folder</i> \Server	ManagerService.exe.config
Nodi di DEM Orchestrator	<i>install-folder</i> \Distributed Execution Manager\dem	DynamicOps.DEM.exe.config

Tabella 7-1. File da aggiornare quando si modifica il nome host di un nodo Web (continua)

Server di IaaS	Percorso	File
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 7-2. 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 7-3. 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 **vRA > Impostazioni host**, modificare **Nome host** impostando il CNAME desiderato.

Rimozione di un nodo dell'appliance vRealize Automation

Durante la gestione di un ambiente HA, potrebbe essere necessario rimuovere un nodo dell'appliance vRealize Automation con errore dal cluster.

Per rimuovere un nodo, seguire le linee guida riportate nell'[articolo 2149866 della knowledge base di VMware](#).

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 *guida all'amministrazione dell'agente 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.

Risultati

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 vRealize Automation.
- 2 Se si tratta di un ambiente HA, eseguire i passaggi relativi alla configurazione di Gestione directory per HA in *Configurazione di vRealize Automation*.
- 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 **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 **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 7-4. 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.
- Fare clic con il pulsante destro del mouse sul server IaaS e selezionare **Modifica impostazioni**.
 - 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

- Accedere come root alla riga di comando dell'appliance vRealize Automation.
- 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.

Poiché i problemi possono verificarsi pressoché in tempo reale, le patch, i prerequisiti e le istruzioni di installazione sono reperibili sul sito Web [Knowledge Base di VMware](#). Ad esempio, l'[articolo 70911 di VMware Knowledge Base](#) viene monitorato e aggiornato con le informazioni più recenti sulla patch per vRealize Automation 7.6.

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

Procedura

- 1 Accedere come root all'interfaccia di gestione dell'appliance vRealize Automation.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Fare clic su **vRA > Patch**.

- 3 In Gestione patch, fare clic sull'opzione desiderata e seguire le istruzioni visualizzate.

Opzione	Descrizione
Nuova patch	Installare una nuova patch scaricata.
Patch installate	Aggiungere le patch installate più di recente ai nodi del cluster appena aggiunti.
Rollback	Rimuovere le patch installate più di recente ed eseguire il rollback di vRealize Automation al livello di patch precedente.
Cronologia	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
```

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

- Accedere a vRealize Automation come amministratore di sistema del tenant predefinito.
 - Passare all'interfaccia del prodotto vRealize Automation.
`https://vrealize-automation-FQDN/vcac`
 - Accedere con il nome utente **administrator** e la password definita per questo utente quando è stato configurato SSO.
- Selezionare **Amministrazione > Tenant**.
- Fare clic sul nome del tenant predefinito **vsphere.local**.
- Fare clic sulla scheda **Utenti locali**.
- 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.
 - Fare clic su Aggiungi (+).
 - 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 di vRealize Automation*.
- Gli amministratori IaaS preparano le risorse esterne per il provisioning. Vedere *Configurazione di vRealize Automation*.
- Se durante l'installazione è stata configurata la creazione del contenuto iniziale, l'amministratore della configurazione può richiedere l'elemento di catalogo Contenuto iniziale per popolare rapidamente un'implementazione di prototipazione.

Risoluzione dei problemi d'installazione di vRealize Automation

8

Nella risoluzione dei problemi di vRealize Automation sono descritte le procedure che consentono di risolvere i problemi che si possono verificare durante l'installazione o la configurazione di vRealize Automation.

Questo capitolo include i seguenti argomenti:

- [Rollback di un'installazione non riuscita](#)
- [Creazione di un bundle di supporto di vRealize Automation](#)
- [Risoluzione dei problemi correlati all'installazione generale](#)
- [Risoluzione dei problemi dell'appliance vRealize Automation](#)
- [Risoluzione dei problemi relativi ai componenti IaaS](#)
- [Risoluzione degli errori di accesso](#)

Rollback di un'installazione non riuscita

Quando un'installazione non riesce e viene ripristinata con il rollback, è necessario che l'amministratore di sistema verifichi che tutti i file richiesti siano stati disinstallati prima di avviare un'altra installazione. Alcuni file devono essere disinstallati manualmente.

Rollback di un'installazione minima

L'amministratore di sistema deve rimuovere manualmente alcuni file e ripristinare il database per disinstallare completamente un'installazione di IaaS vRealize Automation non riuscita.

Procedura

- 1 Se sono presenti i seguenti componenti, disinstallarli utilizzando il programma d'installazione di Windows.
 - Agenti di vRealize Automation
 - DEM Worker di vRealize Automation

- DEM Orchestrator di vRealize Automation
- Server di vRealize Automation
- vRealize Automation WAPI

Nota se viene visualizzato il messaggio seguente, riavviare la macchina e attenersi alla seguente procedura: Errore durante l'apertura del file di registro. Verificare che il file di registro specificato sia presente e che sia scrivibile.

Nota se il sistema Windows è stato ripristinato o se è stato disinstallato IaaS, è necessario eseguire il comando `iisreset` prima di reinstallare IaaS di vRealize Automation.

- 2 Riportare il database allo stato in cui era prima che venisse avviata l'installazione. Il metodo utilizzato dipende dalla modalità d'installazione originale del database.
- 3 In IIS (Gestione Internet Information Services) selezionare il Sito Web predefinito (o il proprio sito personalizzato) e fare clic su **Binding**. Rimuovere il binding https (predefinito sulla porta 443).
- 4 Verificare che Applications Repository, vRealize Automation e WAPI siano stati eliminati e che anche i pool di applicazioni RepositoryAppPool, vCACAppPool, WapiAppPool siano stati eliminati.

Risultati

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.

Risultati

Tabella 8-1. Rollback dei punti di errore

Punto di errore	Azione
Installazione del servizio di gestione	Se presente, disinstallare vCloud Automation Center Server.
Installazione di DEM Orchestrator	Se presente, disinstallare il DEM Orchestrator
Installazione di DEM Worker	Se presenti, disinstallare tutti i DEM Worker
Installazione di un agente	Se presenti, disinstallare tutti gli agenti di vRealize Automation

Creazione di un bundle di supporto 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 Accedere come root all'interfaccia di gestione dell'appliance vRealize Automation.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Fare clic su **vRA > Registri**.
- 3 Fare clic su **Crea bundle di supporto**.
- 4 Fare clic su **Download** e salvare il file del bundle di supporto nel sistema.

Risultati

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.

Riga di comando: per generare un bundle di supporto dalla riga di comando dell'appliance vRealize Automation come root, è possibile eseguire `vcac-support` o `vcac-config log-bundle`.

In alternativa, è possibile eseguire il comando `log-bundle` completo, come illustrato nell'esempio seguente. Vedere [Informazioni di base sulla riga di comando dell'installazione di vRealize Automation](#) per informazioni generali sull'esecuzione di `vra-command`.

```
# vra-command execute --node cafe.node.497772175.21500 log-bundle --requestor va-1.mycompany.com

Parent command with id='981e3028-c99b-5c92-1bae-7d2bf5b6aaaa' was created.
Waiting for all child commands to complete...
...
Command execution result:
Command id: 3d64d122-0af1-28dd-b5a5-d932b78b3678
  Type: log-bundle
  Node id: cafe.node.497772175.21500
  Node host: va-1.mycompany.com
  Result: The command was successfully executed.
  Result description: {"path": "/opt/vmware/var/support-bundle/log/
va-1.mycompany.com_cafe.node.497772175.21500-VA.zip"}

Status: COMPLETED
```

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.

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**).

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

- 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.

Soluzione

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.

Prerequisiti

Procurarsi i nomi, numeri di porta e credenziali per il server proxy dall'amministratore del sito.

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

- 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.

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.

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

- 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/workflowexecutor.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.

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.

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

- 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. È necessario utilizzare l'interfaccia di gestione su un altro nodo per promuovere tale nodo come nuovo master, che ripristina l'accesso in scrittura al database vRealize Automation.

In seguito, è necessario riportare il vecchio nodo master online, ma nella scheda Cluster della relativa interfaccia di gestione il nodo è ancora visualizzato come nodo master anche se non lo è. Eventuali tentativi di utilizzare l'interfaccia di gestione di un qualsiasi nodo 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 l'interfaccia di gestione del nuovo nodo master. Cercare il vecchio nodo visualizzato come `invalid` nella scheda Cluster, quindi fare clic sul relativo 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 l'interfaccia 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.
- Il servizio SQL potrebbe non essere in esecuzione.

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.

Le connessioni di Distributed Transaction Coordinator vengono rifiutate

Le impostazioni di Microsoft Remote Procedure Call (RPC) possono influire sul servizio DTC (Distributed Transaction Coordinator) in vRealize Automation.

Problema

Vengono visualizzati messaggi di errore che indicano che le connessioni DTC tra i server Windows IaaS o il server del database SQL vRealize Automation sono state rifiutate.

Causa

Un'impostazione della connessione RPC limita l'accesso e deve essere disabilitata.

Soluzione

In tutti i server Windows IaaS e nel server del database SQL vRealize Automation, rimuovere la seguente chiave del Registro di sistema o impostarla su zero.

HKLM\SOFTWARE\Policies\Microsoft\Windows NT\RPC\RestrictRemoteClients

I server IaaS sono disconnessi

Se si verificano problemi relativi al contatore delle prestazioni di Windows, è possibile che i server IaaS vengano segnalati come disconnessi.

Problema

Dopo l'installazione o l'aggiornamento dell'agente di gestione, il server IaaS invia ping all'appliance vRealize Automation. Il problema si verifica quando i ping non riescono, causando uno stato Non connesso per il server IaaS nella scheda Cluster dell'interfaccia di gestione dell'appliance vRealize Automation.

Nel server IaaS, viene visualizzato un errore simile al seguente nel file dell'agente di gestione All.log.

```
[UTC:2019-05-25 16:09:37 Local:2019-05-25 18:09:37] [Error]: [sub-thread-Id="4" context="" token=""]
System.InvalidOperationException: Category does not exist.
at System.Diagnostics.PerformanceCounterLib.CounterExists(String machine, String category, String
counter)
at System.Diagnostics.PerformanceCounter.InitializeImpl()
at System.Diagnostics.PerformanceCounter.NextSample()
at System.Diagnostics.PerformanceCounter.NextValue()
at VMware.IaaS.Component.Metrics.MetricsUtility.CalculateMachineProcessorMeasure(Int32
samplePeriodMilliseconds)
```

```

at VMware.IaaS.Management.Agent.ManagementEndpointService.CollectEnvironmentInfo()
at VMware.IaaS.Management.Agent.ManagementEndpointService.<PingAsync>d__0.MoveNext()
--- End of stack trace from previous location where exception was thrown ---
at System.Runtime.CompilerServices.TaskAwaiter.ThrowForNonSuccess(Task task)
at System.Runtime.CompilerServices.TaskAwaiter.HandleNonSuccessAndDebuggerNotification(Task task)
at System.Runtime.CompilerServices.ConfiguredTaskAwaitable`1.ConfiguredTaskAwaiter.GetResult()
at VMware.IaaS.Management.Agent.ManagementAgent.<<PingManagementEndpointAsync>b__1f>d__23.MoveNext()
--- End of stack trace from previous location where exception was thrown ---
at System.Runtime.CompilerServices.TaskAwaiter.ThrowForNonSuccess(Task task)
at System.Runtime.CompilerServices.TaskAwaiter.HandleNonSuccessAndDebuggerNotification(Task task)
at VMware.IaaS.Management.Agent.ManagementAgent.<ExecutePeriodicAction>d__8.MoveNext()

```

Causa

Esiste un problema noto per cui i contatori delle prestazioni di Windows si danneggiano nel tempo causando l'errore.

Soluzione

Rigenerare tutti i contatori delle prestazioni, inclusi i contatori estendibili e di terze parti.

- 1 Nel server IaaS, aprire un prompt dei comandi come Amministratore.
- 2 Rigenerare i contatori:


```
cd C:\Windows\system32

lodctr /R

cd C:\Windows\syswow64

lodctr /R
```
- 3 Sincronizzare nuovamente i contatori con Strumentazione gestione Windows (WMI):


```
WINMGMT.EXE /RESYNCPERF
```
- 4 Arrestare e riavviare i registri di prestazioni e il servizio Avvisi.
- 5 Arrestare e riavviare il servizio Strumentazione gestione Windows.

Operazioni successive

Se i passaggi precedenti non risolvono il problema, vedere l'[articolo 300956 del supporto tecnico Microsoft](#) o l'[articolo 2554336 del supporto tecnico Microsoft](#). Gli articoli descrivono come reimpostare manualmente i record del registro associato. È consigliabile eseguire prima il backup del registro.

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 msixexec non validi.

Causa

La password dell'account del servizio IaaS contiene un carattere virgolette doppie.

Soluzione

- 1 Assicurarsi che la password dell'account del servizio IaaS non contenga le virgolette doppie.
- 2 Se la password contiene virgolette doppie, creare una nuova password.
- 3 Riavviare l'installazione.

L'autenticazione di IaaS non riesce durante l'installazione dei componenti di gestione modelli e Web di IaaS

Quando si esegue il Controllo prerequisiti, viene visualizzato un messaggio che attesta l'esito negativo del controllo dell'autenticazione di IIS.

Problema

Il messaggio attesta che l'autenticazione non è attivata, ma la casella di controllo dell'autenticazione di IIS è selezionata.

Soluzione

- 1 Deselezionare la casella di controllo dell'autenticazione Windows.
- 2 Fare clic su **Salva**.
- 3 Selezionare la casella di controllo dell'autenticazione Windows.
- 4 Fare clic su **Salva**.
- 5 Rieseguire il Controllo prerequisiti.

Installazione di Model Manager Data e componenti Web non riuscita

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, passare a **Start > Strumenti di amministrazione > Servizi componenti**.

Nota assicurarsi che tutti i server Windows abbiano un SID univoco per la configurazione di MSDTC.

- 2 Aprire tutti i nodi per individuare il DTC locale o il DTC in cluster se si utilizza un sistema in cluster.

Passare a **Servizi componenti > Computer > Computer locale > Distributed Transaction Coordinator**.

- 3 Fare clic con il pulsante destro del mouse sul DTC locale o in cluster e scegliere **Proprietà**.
- 4 Fare clic sulla scheda Sicurezza.
- 5 Selezionare l'opzione **Accesso di rete DTC**.
- 6 Selezionare le opzioni **Consenti client remoti** e **Consenti amministrazione remota**.

- 7 Selezionare le opzioni **Consenti connessioni in ingresso** e **Consenti connessioni in uscita**.
- 8 Immettere o selezionare NT AUTHORITY\Network Service nel campo **Account** del riquadro Account di accesso DTC.
- 9 Fare clic su **OK**.
- 10 Rimuovere le macchine bloccate nello stato Clone Workflow.
 - a Accedere 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.

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.

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

- ◆ 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.

Prerequisiti

Configurare vRealize Automation per accedere alla rete tramite un server proxy. Vedere [Connessione alla rete attraverso un server proxy](#).

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

- 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`