

Gestione 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 © 2015-2021 VMware, Inc. Tutti i diritti sono riservati. [Informazioni sul copyright e sui marchi](#)

Sommario

1	Gestione e personalizzazione di componenti e opzioni di vRealize Automation	5
	Trasmettere un messaggio a tutti gli utenti	5
	Creazione di un elenco di elementi consentiti di URL per il portlet della bacheca messaggi	7
	Avvio e arresto di vRealize Automation	8
	Avvio di vRealize Automation	8
	Riavvio di vRealize Automation	9
	Arresto di vRealize Automation	11
	Aggiornamento dei certificati di vRealize Automation	12
	Estrazione di certificati e chiavi private	14
	Sostituzione di certificati nell'appliance vRealize Automation	14
	Sostituzione del certificato Infrastructure as a Service	17
	Sostituzione del certificato del servizio di gestione di IaaS	19
	Aggiornamento del vRealize Orchestrator incorporato per considerare attendibili i certificati vRealize Automation	21
	Aggiornamento del vRealize Orchestrator esterno per considerare attendibili i certificati vRealize Automation	24
	Aggiornamento del certificato del sito di gestione di vRealize Automation Appliance	24
	Sostituzione del certificato di un agente di gestione	29
	Modifica del metodo di polling per i certificati	32
	Gestione del database dell'appliance Postgres vRealize Automation	33
	Configurazione del database dell'appliance	34
	Scenari di failover automatico del database di un'appliance con tre nodi	36
	Scenario: esecuzione di un failover manuale del database dell'appliance	39
	Scenario: esecuzione di un failover di manutenzione del database	40
	Ripristino manuale del database dell'appliance da un errore irreversibile	42
	Backup e ripristino nelle installazioni di vRealize Automation	44
	Programma CEIP (Customer Experience Improvement Program)	44
	Partecipare o abbandonare il programma CEIP (Customer Experience Improvement Program) per vRealize Automation	44
	Configurazione del giorno e dell'ora per la raccolta dati	45
	Regolazione delle impostazioni di sistema	45
	Modificare l'icona Tutti i servizi nel catalogo dei servizi	46
	Personalizzazione delle impostazioni di rollover dei dati	47
	Selezione delle impostazioni nel file di configurazione del servizio di gestione	50
	Monitoraggio di vRealize Automation	55
	Monitoraggio dei workflow e visualizzazione dei registri	55
	Monitoraggio di registri eventi e servizi	56

Utilizzo della registrazione di controllo di vRealize Automation	58
Visualizzazione delle informazioni sugli host per i cluster nelle distribuzioni distribuite	60
Monitoraggio dell'integrità di vRealize Automation	62
Configurazione di prove di sistema per vRealize Automation	63
Configurazione di prove di tenant per vRealize Automation	65
Configurazione di prove per vRealize Orchestrator	67
Suite di prove personalizzate	68
Visualizzazione dei risultati della suite di test del servizio di integrità di vRealize Automation	70
Risoluzione dei problemi del servizio di integrità	71
Monitoraggio delle risorse dell'ambiente vRealize Automation tramite SNMP	72
Monitoraggio e gestione delle risorse	72
Scelta di uno scenario di monitoraggio delle risorse	73
Terminologia sull'utilizzo delle risorse	73
Connessione a una macchina cloud	74
Riduzione dell'utilizzo delle prenotazioni per termine naturale	77
Rimozione delle autorizzazioni da un percorso di storage	77
Raccolta dati	78
Il controllo allocazione eseguito da vSwap per gli endpoint vCenter Server	82
Rimozione di posizioni di data center	83
Monitoraggio dei contenitori	83
Importazione di massa, aggiornamento e migrazione di macchine virtuali	84
Importazione di una macchina virtuale in un ambiente vRealize Automation	85
Aggiornamento di una macchina virtuale in un ambiente vRealize Automation	89
Migrazione di una macchina virtuale in un ambiente vRealize Automation differente	92

Gestione e personalizzazione di componenti e opzioni di vRealize Automation

1

È possibile gestire le macchine con provisioning eseguito e altri aspetti della distribuzione di vRealize Automation.

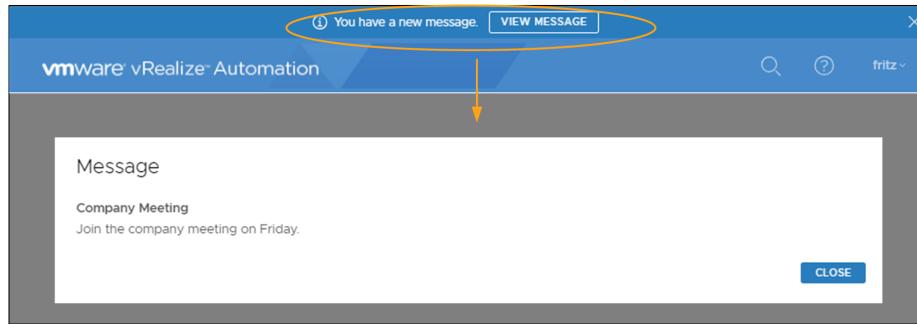
Questo capitolo include i seguenti argomenti:

- [Trasmettere un messaggio a tutti gli utenti](#)
- [Avvio e arresto di vRealize Automation](#)
- [Aggiornamento dei certificati di vRealize Automation](#)
- [Gestione del database dell'appliance Postgres vRealize Automation](#)
- [Backup e ripristino nelle installazioni di vRealize Automation](#)
- [Programma CEIP \(Customer Experience Improvement Program\)](#)
- [Regolazione delle impostazioni di sistema](#)
- [Monitoraggio di vRealize Automation](#)
- [Monitoraggio dell'integrità di vRealize Automation](#)
- [Monitoraggio delle risorse dell'ambiente vRealize Automation tramite SNMP](#)
- [Monitoraggio e gestione delle risorse](#)
- [Monitoraggio dei contenitori](#)
- [Importazione di massa, aggiornamento e migrazione di macchine virtuali](#)

Trasmettere un messaggio a tutti gli utenti

In qualità di amministratore tenant, è possibile trasmettere un messaggio a tutti gli utenti. La notifica di messaggio viene visualizzata nella parte superiore della pagina del browser. Per visualizzare il messaggio, gli utenti dovranno fare clic sulla notifica.

Come utente, è possibile accedere il messaggio dal banner o dal menu a discesa dell'utente sull'interfaccia.



La bacheca messaggi consente di trasmettere un messaggio di testo o una pagina Web. In alcune pagine Web gli utenti possono accedere alla bacheca messaggi attraverso il sito Web.

La bacheca messaggi ha le seguenti limitazioni.

Tabella 1-1. Limitazioni della bacheca messaggi

Opzione	Limiti
Limitazioni relative ai messaggi URL	<ul style="list-style-type: none"> ■ L'URL di destinazione deve essere incluso nell'elenco degli elementi consentiti della bacheca messaggi. Vedere Creazione di un elenco di elementi consentiti di URL per il portlet della bacheca messaggi. ■ È possibile pubblicare solo il contenuto che è ospitato in un sito https. ■ Non è possibile utilizzare certificati autofirmati. L'opzione di accettare il certificato non viene visualizzata nella bacheca messaggi. ■ L'URL della bacheca messaggi è incorporato in un iframe. Alcuni siti Web non funzionano in iframe e generano un messaggio di errore. Una causa di errore è la presenza di X-Frame-Options DENY o di SAMEORIGIN nell'intestazione del sito Web target. Se il proprio sito Web target viene controllato, è possibile impostare l'intestazione X-Frame-Options su X-Frame-Options: ALLOW-FROM https://<vRealizeAutomationApplianceURL>. ■ Alcuni siti Web comprendono una pagina di reindirizzamento a un livello superiore che potrebbe aggiornare l'intera pagina vRealize Automation. Questo tipo di sito Web non funziona nella bacheca messaggi. L'aggiornamento viene eliminato e nella bacheca messaggi viene visualizzato il messaggio Caricamento in corso.... ■ Se si visualizza una pagina HTML interna, la pagina non può avere l'host vRealize Automation come URL.
Limitazioni dei messaggi personalizzati	<ul style="list-style-type: none"> ■ Per garantire la sicurezza, il messaggio personalizzato consente il markup semplice, ma non supporta il codice HTML. Ad esempio non è possibile utilizzare <href> per creare un collegamento a un sito Web. È necessario utilizzare l'opzione del messaggio URL.

Prerequisiti

Accedere a vRealize Automation come **amministratore tenant**.

Procedura

- 1 Fare clic sulla scheda **Amministrazione**.
- 2 Selezionare **Notifiche Bacheca messaggi**
- 3 Nel menu a discesa **Tipo** selezionare il tipo di messaggio.

Opzione	Descrizione
Nessuno	Rimuove la notifica di messaggio.
Messaggio personalizzato	Immettere un messaggio di testo normale.
URL	<p>Immettere l'URL della pagina.</p> <p>L'URL deve essere incluso nell'elenco degli elementi consentiti della bacheca messaggi. Vedere Creazione di un elenco di elementi consentiti di URL per il portlet della bacheca messaggi.</p> <p>Per effettuare l'accesso dell'utente a un sito Web, più comunemente il proprio sito Web interno, in base all'ID utente vRealize Automation, selezionare Includi ID utente. L'URL che verrà passato al sito Web simile a <code>http://company.com/internal/message?userID=richard_dawson@company.com</code>. Questo metodo consente al sito Web di utilizzare la proprietà JavaScript <code>window.location.search</code> per fornire l'ID dell'utente corrente per il sito Web.</p>

- 4 Fare clic su **OK**.

Risultati

Il messaggio viene trasmesso come banner a tutti gli utenti tenant.

Per modificare o rimuovere il messaggio, è necessario essere connessi come amministratore tenant. Per modificare il messaggio, ripetere la stessa procedura. Per rimuovere il messaggio, selezionare Nessuno come Tipo e fare clic su **OK**.

Creazione di un elenco di elementi consentiti di URL per il portlet della bacheca messaggi

In qualità di amministratore della sicurezza, l'utente configura un elenco di URL che possono essere utilizzati nella bacheca messaggi. Questo elenco di elementi consentiti garantisce maggiore sicurezza.

Prerequisiti

Accedere a vRealize Automation come **amministratore della sicurezza**.

Procedura

- 1 Selezionare **Amministrazione > Whitelist bacheca messaggi**.
- 2 Fare clic su **Nuovo**.

3 Aggiungere un URL e fare clic su **OK**.

Le voci degli URL possono includere i seguenti contenuti:

- Indirizzo IP o nome di dominio completo di un sito. Ad esempio, <https://docs.vmware.com>.
- Include https.
- Può includere le porte consentite. Se non viene specificata alcuna porta, le porte consentite sono 80 e 443.

4 Ripetere per ogni voce aggiuntiva.**Risultati**

Un amministratore tenant non può aggiungere un URL alla bacheca messaggi a meno che l'URL non sia incluso nell'elenco.

Operazioni successive

Verificare che sia possibile aggiungere e trasmettere alla bacheca messaggi un URL incluso nell'elenco di elementi consentiti. Vedere [Trasmettere un messaggio a tutti gli utenti](#).

Avvio e arresto di vRealize Automation

Gli amministratori di sistema avviano e arrestano vRealize Automation in maniera controllata per preservare l'integrità dei dati e del sistema.

L'uso dell'avvio e dell'arresto controllato consente anche di risolvere problemi di prestazioni e nel comportamento dei prodotti, che possono causare un avvio iniziale non corretto. Utilizzare la procedura di riavvio solo quando alcuni componenti della distribuzione terminano con errore.

Avvio di vRealize Automation

Quando si avvia vRealize Automation dopo che è stato spento per qualsiasi motivo previsto o imprevisto, è necessario avviare i componenti in un ordine specifico.

Se si gestiscono i componenti della distribuzione in vCenter Server, è possibile avviare i sistemi operativi guest da lì.

Prerequisiti

Verificare che i bilanciamenti del carico utilizzati dalla distribuzione siano in esecuzione.

Procedura

- 1** Se si utilizza un database PostgreSQL autonomo legacy, avviare questo server.
- 2** In qualsiasi ordine, avviare i MS SQL Server vRealize Automation standalone.
- 3** In una distribuzione che utilizza bilanciamenti del carico con controlli di integrità, disattivare tutti i controlli di integrità eccetto i ping.
- 4** Avviare l'appliance vRealize Automation principale.

- 5** Nell'interfaccia di gestione dell'appliance vRealize Automation principale, verificare nella scheda **Cluster** se il sistema è in modalità sincrona o asincrona. La distribuzione di una singola appliance è sempre asincrona.

- Se la distribuzione è sincrona, avviare le appliance vRealize Automation rimanenti.
- Se la distribuzione è asincrona, passare all'interfaccia di gestione dell'appliance vRealize Automation principale e attendere che il servizio di gestione delle licenze sia in esecuzione e REGISTRATO.

In seguito, avviare le appliance vRealize Automation rimanenti.

- 6** Dopo l'avvio di tutte le appliance, utilizzare le interfacce di gestione per verificare che i servizi siano in esecuzione e REGISTRATI.

L'avvio delle appliance potrebbe richiedere 15 minuti o più.

- 7** Avviare tutti i nodi Web di IaaS e attendere 5 minuti.

- 8** Avviare il nodo primario del servizio di gestione e attendere da 2 a 5 minuti.

- 9** In una distribuzione distribuita con più nodi del servizio di gestione, avviare i nodi del servizio di gestione secondario e attendere da 2 a 5 minuti.

Sulle macchine secondarie, non avviare o eseguire il servizio di Windows, a meno che sia stata implementata la configurazione per il failover automatico del servizio di gestione.

- 10** In qualsiasi ordine, avviare DEM Orchestrator, i DEM Worker e tutti gli agenti proxy vRealize Automation.

Non è necessario attendere che un avvio venga completato prima di eseguirne un altro.

- 11** Se è stato necessario disattivare i controlli di integrità del bilanciamento del carico, riattivarli.

- 12** Verificare che i servizi avviati siano in esecuzione e REGISTRATI.

- a In un browser, accedere all'interfaccia di gestione dell'appliance vRealize Automation principale.

<https://vrealize-automation-appliance-FQDN:5480>

- b Fare clic sulla scheda **Servizi**.

- c Monitorare lo stato di avvio del servizio facendo clic su **Aggiorna**.

Risultati

Quando tutti i servizi sono REGISTRATI, la distribuzione è pronta.

Riavvio di vRealize Automation

Il riavvio dei componenti vRealize Automation potrebbe aiutare a risolvere i problemi. È necessario riavviare i componenti in un ordine specifico.

Se si gestiscono i componenti della distribuzione in vCenter Server, è possibile riavviare i sistemi operativi guest da lì.

Se non è possibile eseguire il riavvio, provare a eseguire le istruzioni in [Arresto di vRealize Automation](#) e [Avvio di vRealize Automation](#).

Prerequisiti

- Verificare che tutti i servizi di bilanciamento del carico utilizzati nella distribuzione siano in esecuzione.

Procedura

- 1 Verificare che il database dell'appliance vRealize Automation sia impostato in modalità asincrona. Se necessario, utilizzare l'interfaccia di gestione per passare alla modalità asincrona.

È possibile tornare alla modalità sincrona dopo aver completato l'intera procedura. Vedere [Gestione del database dell'appliance Postgres vRealize Automation](#) per ulteriori informazioni.

- 2 Riavviare l'appliance vRealize Automation principale e attendere il completamento dell'avvio.
- 3 Utilizzare l'interfaccia di gestione dell'appliance vRealize Automation principale per verificare che il servizio di gestione delle licenze sia in esecuzione e REGISTRATO.
- 4 Riavviare contemporaneamente le appliance vRealize Automation rimanenti.
- 5 Attendere il riavvio delle appliance e utilizzare le interfacce di gestione per verificare che i servizi siano in esecuzione e REGISTRATI.

Il riavvio delle appliance potrebbe richiedere 15 minuti o più.

- 6 Riavviare il nodo Web primario e attendere il completamento della procedura.
- 7 Se si esegue una distribuzione distribuita con più nodi Web, riavviare i nodi Web secondari e attendere il completamento della procedura.
- 8 Riavviare i nodi del servizio di gestione e attendere il completamento della procedura.

Se si sta eseguendo il failover automatico del servizio di gestione e si desidera mantenere comunque i nodi attivi e passivi, riavviare nell'ordine seguente:

- a Arrestare i nodi passivi del servizio di gestione senza riavviarli.
 - b Riavviare completamente il nodo del servizio di gestione attivo.
 - c Avviare i nodi passivi del servizio di gestione.
- 9 In qualsiasi ordine, riavviare DEM Orchestrator, i DEM Worker e tutti gli agenti proxy vRealize Automation. Attendere il completamento di tutte le procedure di avvio.

Non è necessario attendere che un riavvio venga completato prima di eseguirne un altro.

10 Verificare che i servizi riavviati siano in esecuzione e REGISTRATI.

- a In un browser, accedere all'interfaccia di gestione dell'appliance vRealize Automation principale.

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

- b Fare clic sulla scheda **Servizi**.
- c Monitorare lo stato di avvio del servizio facendo clic su **Aggiorna**.

Risultati

Quando tutti i servizi sono REGISTRATI, la distribuzione è pronta.

Arresto di vRealize Automation

Per garantire l'integrità dei dati, è necessario arrestare vRealize Automation seguendo un ordine specifico.

Se si gestiscono i componenti della distribuzione in vCenter Server, è possibile arrestare i sistemi operativi guest da lì.

Procedura

- 1** In qualsiasi ordine, arrestare DEM Orchestrator, i DEM Worker e tutti gli agenti proxy vRealize Automation. Attendere il completamento della procedura.
- 2** Arrestare i nodi del servizio di gestione e attendere il completamento della procedura.
- 3** Nelle distribuzioni distribuite con più nodi Web, arrestare i nodi Web secondari e attendere il completamento della procedura.
- 4** Arrestare il nodo Web primario e attendere il completamento della procedura.
- 5** Nelle distribuzioni distribuite con più appliance vRealize Automation in modalità sincrona, utilizzare l'interfaccia di gestione dell'appliance vRealize Automation per passare alla modalità asincrona.
- 6** Nelle distribuzioni distribuite con più appliance vRealize Automation, arrestare le appliance secondarie e attendere il completamento della procedura.
- 7** Arrestare l'appliance vRealize Automation primaria e attendere il completamento della procedura.

L'appliance vRealize Automation primaria è quella che contiene il database dell'appliance principale o scrivibile. Prendere nota dell'appliance è primaria in modo da poter iniziare il backup nell'ordine corretto.

- 8** In qualsiasi ordine, arrestare tutti i MS SQL Server vRealize Automation standalone e attendere il completamento della procedura.
- 9** Se si utilizza un database PostgreSQL autonomo legacy, arrestare anche questo server.

Aggiornamento dei certificati di vRealize Automation

L'amministratore di sistema può aggiornare o sostituire certificati per i componenti di vRealize Automation.

vRealize Automation contiene tre componenti principali che utilizzano certificati SSL per la protezione delle comunicazioni reciproche.

- Appliance vRealize Automation
- Componente sito Web di IaaS
- Componente servizio di gestione di IaaS

In aggiunta, la distribuzione può avere certificati per il sito Web dell'interfaccia di gestione di Appliance vRealize Automation. Ogni macchina IaaS esegue inoltre un agente di gestione che utilizza un certificato.

Nota vRealize Automation utilizza diversi prodotti di terze parti, come ad esempio Rabbit MQ, per supportare varie funzionalità. Alcuni di questi prodotti utilizzano i propri certificati autofirmati che persistono anche se i certificati primari di vRealize Automation vengono sostituiti con certificati forniti da un'autorità di certificazione. A causa di tale situazione, gli utenti non possono controllare effettivamente l'uso del certificato su porte specifiche, come ad esempio la 5671 che viene utilizzata da RabbitMQ per le comunicazioni interne.

Con un'unica eccezione, i cambiamenti che avvengono sui componenti successivi nell'elenco non influenzano quelli precedenti. L'eccezione è che un certificato aggiornato per componenti di IaaS deve essere registrato con l'appliance vRealize Automation.

In genere, i certificati autofirmati vengono generati e applicati a questi componenti durante l'installazione del prodotto. Potrebbe essere necessario sostituire un certificato per passare da certificati autofirmati a certificati forniti da un'autorità di certificazione o in occasione della scadenza di un certificato. Quando si sostituisce un certificato per un componente di vRealize Automation, le relazioni basate sulla fiducia per altri componenti di vRealize Automation vengono aggiornate automaticamente.

Ad esempio, in un sistema distribuito con istanze multiple di una Appliance vRealize Automation, se si aggiorna un certificato per una Appliance vRealize Automation, tutti gli altri certificati correlati vengono aggiornati automaticamente.

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.

L'interfaccia di gestione dell'appliance vRealize Automation fornisce le opzioni per l'aggiornamento o la sostituzione dei certificati.

In una distribuzione in cluster, è necessario avviare le modifiche dall'interfaccia del nodo principale.

- **Genera certificato:** vRealize Automation genera un certificato autofirmato.
- **Importa certificato:** consente di usare il proprio certificato.
- **Fornisci identificazione personale certificato:** consente di fornire un'identificazione personale del certificato per utilizzare un certificato già presente nell'archivio certificati nei server Windows IaaS.

Con questa opzione il certificato non verrà trasmesso dall'appliance vRealize Automation ai server Windows IaaS. L'opzione consente agli utenti di distribuire i certificati esistenti già presenti nei server Windows IaaS senza caricare i certificati nell'interfaccia di gestione dell'appliance vRealize Automation.

- **Mantieni esistente:** consente di continuare a utilizzare il certificato corrente.

I certificati per il sito Web dell'interfaccia di gestione dell'appliance vRealize Automation non hanno requisiti di registrazione.

Nota Se il certificato utilizza una passphrase per la crittografia e questa non viene inserita all'atto della sostituzione del certificato sull'appliance, la sostituzione del certificato non viene eseguita e compare il messaggio `Unable to load private key`.

Modelli di macchine virtuali

Dopo aver modificato i certificati dell'appliance vRealize Automation o del server Windows IaaS, è necessario aggiornare gli agenti guest e software di vRealize Automation nei modelli di macchine virtuali in modo che i modelli funzionino di nuovo in vRealize Automation. Se non si aggiornano gli agenti, le richieste di distribuzione che coinvolgono componenti software non riescono con un errore simile all'esempio seguente.

```
The following component requests failed: Linux. Request failed: Machine VM-001:
InstallSoftwareWorkflow. Install software work item timeout.
```

vRealize Orchestrator

Dopo aver modificato i certificati vRealize Automation, è necessario aggiornare vRealize Orchestrator in modo che consideri attendibili i nuovi certificati.

Il componente vRealize Orchestrator associato alla distribuzione vRealize Automation ha certificati propri e inoltre deve considerare attendibili i certificati vRealize Automation. Per impostazione predefinita, il componente vRealize Orchestrator è incorporato in vRealize Automation, anche se alcuni utenti scelgono di utilizzare un vRealize Orchestrator esterno. In entrambi i casi, consultare la documentazione di vRealize Orchestrator per informazioni sull'aggiornamento dei certificati vRealize Orchestrator.

Se si esegue una distribuzione di vRealize Orchestrator con più nodi dietro un bilanciamento del carico, tutti i nodi di vRealize Orchestrator devono utilizzare lo stesso certificato.

Ulteriori informazioni

Per ulteriori informazioni sulla risoluzione dei problemi relativi ai certificati, sul supporto e sui requisiti di attendibilità per i certificati, vedere l'[articolo 2106583 della Knowledge Base di VMware](#).

Estrazione di certificati e chiavi private

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

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

Tabella 1-2. Esempi di comandi e valori dei certificati (openssl)

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

Sostituzione di certificati nell'appliance vRealize Automation

L'amministratore di sistema può aggiornare o sostituire un certificato autofirmato con uno attendibile emesso da un'autorità di certificazione. È possibile utilizzare certificati SAN (Subject Alternative Name, nome alternativo del soggetto), certificati con caratteri jolly o qualsiasi altro metodo di certificazione multiuso appropriato per l'ambiente esistente, purché soddisfi i requisiti di attendibilità.

Quando si aggiorna o si sostituisce il certificato dell'appliance vRealize Automation, la relazione di attendibilità con gli altri componenti correlati viene reinizializzata automaticamente. Vedere [Aggiornamento dei certificati di vRealize Automation](#) per ulteriori informazioni sull'aggiornamento dei certificati.

Procedura

- 1 Accedere come root all'interfaccia di gestione dell'appliance vRealize Automation.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Selezionare **vRA > Certificati**.
- 3 Selezionare il componente vRealize Automation per il quale si sta aggiornando il certificato.
- 4 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	<ol style="list-style-type: none"> a Il valore visualizzato nella casella di testo Nome comune è il nome host visualizzato nella parte superiore della pagina. Se sono disponibili istanze aggiuntive 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.

5 Fare clic su **Salva impostazioni**.

Un aggiornamento del certificato dell'appliance vRealize Automation richiede i servizi vRealize Automation per il corretto riavvio. Il riavvio potrebbe richiedere da 15 minuti a un'ora in base al numero di appliance vRealize Automation presenti nell'ambiente.

Dopo il riavvio, nella pagina vengono visualizzati i dettagli del certificato per tutte le istanze applicabili dell'appliance vRealize Automation.

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

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

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

Completata l'operazione, deselezionare la casella di controllo per disattivare SSH.

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

Completata l'operazione, deselezionare la casella di controllo per disattivare SSH.

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

7 Assicurarsi che sia possibile accedere alla console di vRealize Automation.

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

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

- b Se richiesto, continuare ignorando gli avvisi sul certificato.

- c Accedere con il nome utente **administrator@vsphere.local** e la password specificata quando è stata configurata Gestione directory.

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

8 Se si utilizza un bilanciamento del carico, configurare e abilitare tutti i controlli di integrità applicabili.

Risultati

Il certificato viene aggiornato.

Sostituzione del certificato Infrastructure as a Service

Per garantire la sicurezza in un ambiente con una distribuzione distribuita, l'amministratore di sistema può sostituire un certificato scaduto o un certificato autofirmato con uno emesso da un'autorità di certificazione.

È possibile utilizzare un certificato Subject Alternative Name (SAN) su più macchine. I certificati utilizzati per i componenti di IaaS (sito Web e servizio di gestione) devono essere emessi con valori SAN che includono i nomi di dominio completi (FQDN) di tutti gli host Windows su cui è installato il componente corrispondente e con il nome di dominio completo del bilanciamento del carico per lo stesso componente.

Procedura

- 1** Accedere come root all'interfaccia di gestione dell'appliance vRealize Automation.

<https://vrealize-automation-appliance-FQDN:5480>

- 2** Selezionare **vRA > Certificati**.

- 3** Fare clic su **Web IaaS** nel menu **Tipo di componente**.

- 4** Passare al pannello **Certificato Web IaaS**.

- 5** Selezionare l'opzione di certificato sostitutivo dal menu **Azione certificato**.

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

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

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	Descrizione
Mantieni esistente	Lasciare invariata la configurazione SSL corrente. Scegliere questa opzione per annullare le modifiche.
Genera certificato	<ol style="list-style-type: none"> a Il valore visualizzato nella casella di testo Nome comune è il nome host visualizzato nella parte superiore della pagina. Se sono disponibili istanze aggiuntive 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.
Importazione	<ol style="list-style-type: none"> a Copiare i valori del certificato dalla stringa BEGIN PRIVATE KEY alla stringa END PRIVATE KEY, inclusi intestazione e piè di pagina, quindi incollarli nella casella di testo Chiave privata RSA. b Copiare i valori del certificato dalla stringa BEGIN CERTIFICATE alla stringa END CERTIFICATE, inclusi intestazione e piè di pagina, quindi incollarli nella casella di testo Catena di certificati. Per valori di certificati multipli, includere un'intestazione BEGIN CERTIFICATE e un piè di pagina END CERTIFICATE per ciascun certificato. <p>Nota In caso di certificati concatenati, possono essere disponibili attributi aggiuntivi.</p> <ol style="list-style-type: none"> c (Facoltativo) Se il certificato utilizza una passphrase per crittografare la chiave del certificato, copiare la passphrase e incollarla nella casella di testo Passphrase.
Fornisci identificazione personale certificato	Utilizzare questa opzione se si desidera fornire un'identificazione personale certificato per impiegare un certificato già distribuito nell'archivio certificati sui server IaaS. Con questa opzione il certificato non verrà trasmesso dall'appliance virtuale ai server IaaS. L'opzione consente agli utenti di distribuire certificati esistenti su server IaaS senza caricarli nell'interfaccia di gestione.

6 Fare clic su **Salva impostazioni**.

Un aggiornamento del certificato del server Windows di IaaS richiede i servizi vRealize Automation per il corretto riavvio. Il riavvio potrebbe richiedere da 15 minuti a un'ora in base al numero di appliance vRealize Automation presenti nell'ambiente.

Dopo il riavvio, il certificato viene visualizzato nella pagina.

Sostituzione del certificato del servizio di gestione di IaaS

Per garantire la sicurezza in un ambiente con una distribuzione distribuita, un amministratore di sistema può sostituire un certificato scaduto o un certificato autofirmato con uno emesso da un'autorità di certificazione.

È possibile utilizzare un certificato Subject Alternative Name (SAN) su più macchine. I certificati utilizzati per i componenti di IaaS (sito Web e servizio di gestione) devono essere emessi con valori SAN che includono i nomi di dominio completi (FQDN) di tutti gli host Windows su cui è installato il componente corrispondente e con il nome di dominio completo del bilanciamento del carico per lo stesso componente.

Il servizio di gestione di IaaS e il servizio Web di IaaS condividono un unico certificato.

Procedura

- 1 Aprire un browser Web e passare all'URL dell'interfaccia di gestione dell'appliance vRealize Automation.
- 2 Accedere con il nome utente **root** e la password specificata per la distribuzione della Appliance vRealize Automation.
- 3 Selezionare **vRA > Certificati**.
- 4 Fare clic su **Servizio di gestione** dal menu **Tipo di componente**.
- 5 Selezionare il tipo di certificato dal menu **Azione certificato**.

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

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

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	Descrizione
Mantieni esistente	Lasciare invariata la configurazione SSL corrente. Scegliere questa opzione per annullare le modifiche.
Genera certificato	<ol style="list-style-type: none"> a Il valore visualizzato nella casella di testo Nome comune è il nome host visualizzato nella parte superiore della pagina. Se sono disponibili istanze aggiuntive 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.
Importazione	<ol style="list-style-type: none"> a Copiare i valori del certificato dalla stringa BEGIN PRIVATE KEY alla stringa END PRIVATE KEY, inclusi intestazione e piè di pagina, quindi incollarli nella casella di testo Chiave privata RSA. b Copiare i valori del certificato dalla stringa BEGIN CERTIFICATE alla stringa END CERTIFICATE, inclusi intestazione e piè di pagina, quindi incollarli nella casella di testo Catena di certificati. Per valori di certificati multipli, includere un'intestazione BEGIN CERTIFICATE e un piè di pagina END CERTIFICATE per ciascun certificato. <p>Nota In caso di certificati concatenati, possono essere disponibili attributi aggiuntivi.</p> <ol style="list-style-type: none"> c (Facoltativo) Se il certificato utilizza una passphrase per crittografare la chiave del certificato, copiare la passphrase e incollarla nella casella di testo Passphrase.
Fornisci identificazione personale certificato	Utilizzare questa opzione se si desidera fornire un'identificazione personale certificato per impiegare un certificato già distribuito nell'archivio certificati sui server IaaS. Con questa opzione il certificato non verrà trasmesso dall'appliance virtuale ai server IaaS. L'opzione consente agli utenti di distribuire certificati esistenti su server IaaS senza caricarli nell'interfaccia di gestione.

6 Fare clic su **Salva impostazioni**.

Dopo qualche minuto il certificato viene visualizzato nella pagina.

- 7 Se la rete o il bilanciamento del carico lo richiedono, copiare il certificato importato o appena creato nel bilanciamento del carico.
- 8 Aprire un browser e passare a `https://managerServiceAddress/vmpsProvision/` da un server che esegue un DEM Worker o un agente.

Se si utilizza un bilanciamento del carico, il nome host deve essere il nome di dominio completo del bilanciamento del carico.
- 9 Se richiesto, continuare ignorando gli avvisi sul certificato.
- 10 Verificare che il nuovo certificato sia fornito e che sia attendibile.
- 11 Se si utilizza un bilanciamento del carico, configurare e abilitare tutti i controlli di integrità applicabili.

Aggiornamento del vRealize Orchestrator incorporato per considerare attendibili i certificati vRealize Automation

Se si aggiorna o si modificano i certificati di Appliance vRealize Automation o IaaS, è necessario aggiornare vRealize Orchestrator modo che consideri attendibile i certificati nuovi o aggiornati.

Questa procedura si applica a tutte le distribuzioni vRealize Automation che utilizzano un'istanza di vRealize Orchestrator incorporata. Se si utilizza un'istanza di vRealize Orchestrator esterna, vedere [Aggiornamento del vRealize Orchestrator esterno per considerare attendibili i certificati vRealize Automation](#).

Nota La procedura reimposta l'autenticazione di tenant e gruppo alle impostazioni predefinite. Se la configurazione di autenticazione è stata personalizzata, prendere nota delle modifiche in modo da poterle riconfigurare dopo aver completato la procedura.

Consultare la documentazione di vRealize Orchestrator per informazioni sull'aggiornamento e la sostituzione dei certificati vRealize Orchestrator.

In una configurazione di cluster, è necessario completare questa procedura nel nodo dell'appliance vRealize Automation principale, quindi eseguire un `join-cluster` sull'elemento principale da ogni nodo dell'appliance vRealize Automation di replica.

Nota In un cluster, arrestare il servizio `vco-configurator` su tutti i nodi di replica finché non viene completata la procedura per evitare la sincronizzazione automatica indesiderata di Control Center.

Se si sostituiscono o si aggiornano i certificati di vRealize Automation senza aver completato la procedura, è possibile che il Control Center di vRealize Orchestrator sia inaccessibile e che vengano visualizzati messaggi di errore nei file di registro `vco-server` e `vco-configurator`.

Possono verificarsi problemi con l'aggiornamento dei certificati anche se vRealize Orchestrator è configurato per l'autenticazione in un altro tenant e gruppo anziché vRealize Automation. Per informazioni, vedere l'articolo della Knowledge Base di VMware [Catena di certificati non attendibili di eccezione dopo la sostituzione del certificato vRA \(2147612\)](#).

Le sintassi del comando `trust` illustrate qui hanno uno scopo puramente rappresentativo e non sono definitive. Benché siano appropriate per la maggior parte delle distribuzioni tipiche, in alcune situazioni potrebbe essere necessario sperimentare comandi diversi.

- Se si specifica `--certificate`, è necessario fornire il percorso di un file di certificato valido in formato PEM.
- Se si specifica `--uri`, è necessario fornire l'URI da cui il comando può recuperare un certificato attendibile.
- Specificando l'opzione `--registry-certificate` si indica che il certificato richiesto deve essere considerato come certificato per il registro componenti e il certificato attendibile viene aggiunto all'archivio di attendibilità con un alias specifico utilizzato dal certificato del registro componenti.

È anche possibile gestire i certificati utilizzando i workflow SSL Trust Manager in vRealize Orchestrator. Per informazioni, vedere l'argomento *Gestione dei certificati di Orchestrator* nella [documentazione di vRealize Orchestrator](#).

Procedura

- 1 Arrestare il server di vRealize Orchestrator e i servizi del Control Center.

```
service vco-server stop
service vco-configurator stop
```

- 2 Reimpostare il provider di autenticazione di vRealize Orchestrator eseguendo il comando seguente.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh reset-authentication
ls -l /etc/vco/app-server/
mv /etc/vco/app-server/vco-registration-id /etc/vco/app-server/vco-registration-id.old
vcac-vami vco-service-reconfigure
```

- 3 Verificare il certificato attendibile per l'archivio di attendibilità di vRealize Orchestrator tramite l'utilità dell'interfaccia della riga di comando che si trova in `/var/lib/vco/tools/configuration-cli/bin` con il seguente comando.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh list-trust
```

- Cercare il certificato con il seguente alias: `vco.cafe.component-registry.ssl.certificate`. Questo deve essere il certificato di vRealize Automation che l'istanza di vRealize Orchestrator utilizza come provider di autenticazione.
- Questo certificato deve corrispondere al certificato di vRealize Automation appena configurato. Se non corrisponde, può essere modificato come segue:

- 1 Copiare il file PEM del certificato dell'appliance firmato di vRealize Automation nella cartella `/tmp` nell'appliance.

- 2 Eseguire il comando seguente aggiungendo il percorso del certificato appropriato.

```
./vro-configure.sh trust --certificate path-to-the-certificate-file-in-PEM-format--registry-certificate
```

Di seguito è disponibile un esempio di comando.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh trust --certificate /var/tmp/test.pem --registry-certificate
```

- 4 Potrebbe essere necessario eseguire i seguenti comandi per considerare attendibile il certificato.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh trust --uri https://vra.domain.com  
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh trust --registry-certificate --uri https://vra.domain.com
```

- 5 Assicurarsi che il certificato di vRealize Automation si trovi a questo punto nell'archivio di attendibilità di vRealize Orchestrator utilizzando il comando seguente.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh list-trust
```

- 6 Avviare i servizi del server vRealize Orchestrator e del Control Center.

```
service vco-server start  
service vco-configurator start
```

Operazioni successive

È possibile verificare che l'attendibilità sia stata aggiornata in un sistema di cluster.

- 1 Accedere come root all'interfaccia di gestione dell'appliance virtuale.
- 2 Selezionare la pagina Servizi.
- 3 Assicurarsi che non siano presenti servizi vco duplicati.

Se sono presenti servizi vco duplicati, fare clic su **Annulla registrazione** per rimuovere i servizi che non hanno stato Registered.

- 4 Assicurarsi che vco-configurator sia avviato in tutti i nodi dell'appliance virtuale.
- 5 Accedere al centro di controllo di vRealize Orchestrator e passare alla pagina Convalida configurazione per convalidare la configurazione.
- 6 Passare alla pagina Provider di autenticazione e verificare che le impostazioni di autenticazione siano corrette.

In questa pagina è possibile anche testare le credenziali di accesso.

Aggiornamento del vRealize Orchestrator esterno per considerare attendibili i certificati vRealize Automation

Se si aggiorna o si modificano i certificati di Appliance vRealize Automation o IaaS, è necessario aggiornare vRealize Orchestrator modo che consideri attendibile i certificati nuovi o aggiornati.

Questa procedura si applica alle distribuzioni vRealize Automation che utilizzano un'istanza di vRealize Orchestrator esterna.

Nota La procedura reimposta l'autenticazione di tenant e gruppo alle impostazioni predefinite. Se la configurazione di autenticazione è stata personalizzata, prendere nota delle modifiche in modo da poterle riconfigurare dopo aver completato la procedura.

Consultare la documentazione di vRealize Orchestrator per informazioni sull'aggiornamento e la sostituzione dei certificati vRealize Orchestrator.

Se si sostituisce o aggiornano i certificati vRealize Automation senza aver completato la procedura, il Control Center di vRealize Orchestrator potrebbe essere inaccessibile e possono comparire errori nei file di registro vco-server e vco-configurator.

Possono verificarsi problemi con l'aggiornamento dei certificati anche se vRealize Orchestrator è configurato per l'autenticazione in un altro tenant e gruppo anziché vRealize Automation. Consultare l'[articolo 2147612 della Knowledge Base](#).

Procedura

- 1 Arrestare il server di vRealize Orchestrator e i servizi del Control Center.

```
service vco-configurator stop
```
- 2 Reimpostare il provider di autenticazione di vRealize Orchestrator.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh reset-authentication
```
- 3 Avviare il servizio del Control Center di vRealize Orchestrator.

```
service vco-configurator start
```
- 4 Accedere al Control Center utilizzando le credenziali di root dell'interfaccia di gestione dell'appliance virtuale.
- 5 Annullare la registrazione e registrare nuovamente il provider di autenticazione.

Aggiornamento del certificato del sito di gestione di vRealize Automation Appliance

L'amministratore di sistema può sostituire il certificato SSL del servizio del sito di gestione quando scade o sostituire il certificato autofirmato con uno emesso da un'autorità di certificazione. La protezione del servizio del sito di gestione avviene sulla porta 5480.

L'appliance vRealize Automation utilizza lighttpd per eseguire il proprio sito di gestione. Quando si sostituisce un certificato del sito di gestione è necessario anche configurare tutti gli agenti di gestione affinché riconoscano il nuovo certificato.

Se si esegue una distribuzione distribuita, è possibile aggiornare gli agenti di gestione manualmente o automaticamente. Se si esegue una distribuzione minima, l'agente di gestione dovrà essere aggiornato manualmente.

Vedere [Aggiornamento manuale del riconoscimento certificati dell'agente di gestione](#) per ulteriori informazioni.

Procedura

1 Individuare l'identificatore dell'agente di gestione

L'identificatore dell'agente di gestione è utilizzato quando si crea e si registra un nuovo certificato server del sito di gestione.

2 Sostituzione del certificato del sito di gestione di vRealize Automation Appliance

Se il certificato SSL del servizio del sito di gestione scade, oppure se è stato utilizzato un certificato autofirmato e i criteri del sito ne richiedono uno diverso, è possibile sostituire il certificato.

3 Aggiornamento del riconoscimento certificati dell'agente di gestione

Dopo aver sostituito un certificato del sito di gestione dell'appliance vRealize Automation, è necessario aggiornare tutti gli agenti di gestione affinché riconoscano il nuovo certificato e ristabiliscano le comunicazioni attendibili tra il sito di gestione dell'appliance virtuale e gli agenti di gestione negli host di IaaS.

Individuare l'identificatore dell'agente di gestione

L'identificatore dell'agente di gestione è utilizzato quando si crea e si registra un nuovo certificato server del sito di gestione.

Procedura

- 1 Aprire il file di configurazione dell'agente di gestione localizzato in `<vra-installation-dir>\Management Agent\VMware.IaaS.Management.Agent.exe.config`.

- 2 Prendere nota del valore dell'attributo id dell'elemento agentConfiguration.

```
<agentConfiguration id="0E22046B-9D71-4A2B-BB5D-70817F901B27">
```

Sostituzione del certificato del sito di gestione di vRealize Automation Appliance

Se il certificato SSL del servizio del sito di gestione scade, oppure se è stato utilizzato un certificato autofirmato e i criteri del sito ne richiedono uno diverso, è possibile sostituire il certificato.

È possibile riutilizzare il certificato utilizzato dal servizio di vRealize Automation nella porta 443 oppure usarne uno diverso. Se si richiede un nuovo certificato emesso dall'autorità di certificazione per aggiornare un certificato esistente, è consigliabile riutilizzare il nome comune del certificato esistente.

Nota L'appliance vRealize Automation utilizza lighttpd per eseguire il proprio sito di gestione. La protezione del servizio del sito di gestione avviene sulla porta 5480.

Prerequisiti

- Il certificato deve essere in formato PEM.
- Il certificato deve includere entrambi gli elementi seguenti, nell'ordine specificato, in un file:
 - a Chiave privata RSA
 - b Catena di certificati
- La chiave privata non può essere crittografata.
- La posizione e il nome del file predefiniti sono `/opt/vmware/etc/lighttpd/server.pem`.

Vedere [Estrazione di certificati e chiavi private](#) per ulteriori informazioni sull'esportazione di certificato e chiave privata da un keystore Java in un file PEM.

Procedura

- 1 Accedere utilizzando la console dell'appliance o SSH.
- 2 Eseguire il backup del file del certificato corrente.

```
cp /opt/vmware/etc/lighttpd/server.pem /opt/vmware/etc/lighttpd/server.pem-bak
```

- 3 Copiare il nuovo certificato nell'appliance sostituendo il contenuto del file `/opt/vmware/etc/lighttpd/server.pem` con le informazioni del nuovo certificato.
- 4 Eseguire il comando seguente per riavviare il server lighttpd.

```
service vami-lighttpd restart
```
- 5 Eseguire il comando seguente per riavviare il servizio haproxy.

```
service haproxy restart
```
- 6 Accedere alla console di gestione e verificare che il certificato sia stato sostituito. Potrebbe essere necessario chiudere e riaprire il browser.

Operazioni successive

Aggiornare tutti gli agenti di gestione per riconoscere il nuovo certificato.

Per distribuzioni distribuite, è possibile aggiornare manualmente o automaticamente gli agenti di gestione. Nelle installazioni minime è necessario aggiornare gli agenti manualmente.

- Per informazioni sull'aggiornamento automatico, vedere [Aggiornamento automatico degli agenti di gestione in un ambiente distribuito per il riconoscimento di un certificato del sito di gestione di vRealize Automation Appliance](#).
- Per informazioni sull'aggiornamento manuale, vedere [Aggiornamento manuale del riconoscimento certificati dell'agente di gestione](#).

Aggiornamento del riconoscimento certificati dell'agente di gestione

Dopo aver sostituito un certificato del sito di gestione dell'appliance vRealize Automation, è necessario aggiornare tutti gli agenti di gestione affinché riconoscano il nuovo certificato e ristabiliscano le comunicazioni attendibili tra il sito di gestione dell'appliance virtuale e gli agenti di gestione negli host di IaaS.

Ogni host di IaaS esegue un agente di gestione e ogni agente di gestione deve essere aggiornato. Le distribuzioni minime devono essere aggiornate manualmente, mentre le distribuzioni distribuite possono essere aggiornate manualmente o utilizzando un processo automatizzato.

■ [Aggiornamento manuale del riconoscimento certificati dell'agente di gestione](#)

Dopo aver sostituito un certificato del sito di gestione dell'appliance vRealize Automation, è necessario aggiornare manualmente gli agenti di gestione affinché riconoscano il nuovo certificato per ristabilire le comunicazioni attendibili tra il sito di gestione dell'appliance virtuale e gli agenti di gestione negli host di IaaS.

■ [Aggiornamento automatico degli agenti di gestione in un ambiente distribuito per il riconoscimento di un certificato del sito di gestione di vRealize Automation Appliance](#)

Dopo aver aggiornato il certificato del sito di gestione in una distribuzione ad alta disponibilità, è inoltre necessario aggiornare la configurazione dell'agente di gestione in modo che riconosca il nuovo certificato e ristabilisca la comunicazione attendibile.

Aggiornamento manuale del riconoscimento certificati dell'agente di gestione

Dopo aver sostituito un certificato del sito di gestione dell'appliance vRealize Automation, è necessario aggiornare manualmente gli agenti di gestione affinché riconoscano il nuovo certificato per ristabilire le comunicazioni attendibili tra il sito di gestione dell'appliance virtuale e gli agenti di gestione negli host di IaaS.

Eseguire questi passaggi per ciascun agente di gestione della distribuzione dopo aver sostituito un certificato per il sito di gestione dell'appliance vRealize Automation.

Per distribuzioni distribuite, è possibile aggiornare manualmente o automaticamente gli agenti di gestione. Per informazioni sull'aggiornamento automatico, vedere [Aggiornamento automatico degli agenti di gestione in un ambiente distribuito per il riconoscimento di un certificato del sito di gestione di vRealize Automation Appliance](#).

Prerequisiti

Ottenere le identificazioni personali SHA1 del nuovo certificato del sito di gestione dell'appliance vRealize Automation.

Procedura

- 1 Arrestare il servizio Management Agent di VMware vCloud Automation Center.
- 2 Individuare il file di configurazione dell'agente di gestione memorizzato in `[vcac_installation_folder]\Management Agent\VMware.IaaS.Management.Agent.exe.Config`, di solito `C:\Programmi (x86)\VMware\VCAC\Management Agent\VMware.IaaS.Management.Agent.exe.Config`.
- 3 Aprire il file per la modifica e individuare l'impostazione di configurazione dell'endpoint per il vecchio certificato del sito di gestione, identificabile dall'indirizzo dell'endpoint.

Ad esempio:

```
<agentConfiguration id="C816CFBC-4830-4FD2-8951-C17429CEA291" pollingInterval="00:03:00">
  <managementEndpoints>
    <endpoint address="https://vra-va.local:5480"
thumbprint="D1542471C30A9CE694A512C5F0F19E45E6FA32E6" />
  </managementEndpoints>
</agentConfiguration>
```

- 4 Sostituire l'indicatore digitale corrente con l'indicatore digitale SHA1 del nuovo certificato.

Ad esempio:

```
<agentConfiguration id="C816CFBC-4830-4FD2-8951-C17429CEA291" pollingInterval="00:03:00">
  <managementEndpoints>
    <endpoint address="https://vra-va.local:5480"
thumbprint="8598B073359BAE7597F04D988AD2F083259F1201" />
  </managementEndpoints>
</agentConfiguration>
```

- 5 Avviare il servizio Management Agent di VMware vCloud Automation Center.
- 6 Accedere al sito di gestione dell'appliance virtuale e selezionare la scheda **Cluster**.
- 7 Consultare la tabella Informazioni sulla distribuzione distribuita per verificare se il server di IaaS ha contattato di recente l'appliance virtuale. In caso affermativo, l'aggiornamento è stato completato correttamente.

Aggiornamento automatico degli agenti di gestione in un ambiente distribuito per il riconoscimento di un certificato del sito di gestione di vRealize Automation Appliance

Dopo aver aggiornato il certificato del sito di gestione in una distribuzione ad alta disponibilità, è inoltre necessario aggiornare la configurazione dell'agente di gestione in modo che riconosca il nuovo certificato e ristabilisca la comunicazione attendibile.

Le informazioni sul certificato del sito di gestione dell'appliance vRealize Automation per sistemi distribuiti possono essere aggiornate manualmente o automaticamente. Per informazioni sull'aggiornamento manuale degli agenti di gestione, vedere [Aggiornamento manuale del riconoscimento certificati dell'agente di gestione](#).

Attenersi alla seguente procedura per aggiornare automaticamente le informazioni sul certificato.

Procedura

- 1 Quando gli agenti di gestione sono in esecuzione, sostituire il certificato in un singolo sito di gestione dell'appliance vRealize Automation della distribuzione.
- 2 Attendere quindici minuti in modo che l'agente di gestione esegua la sincronizzazione con il nuovo certificato del sito di gestione dell'appliance vRealize Automation.
- 3 Sostituire i certificati negli altri siti di gestione dell'appliance vRealize Automation della distribuzione.

Gli agenti di gestione vengono aggiornati automaticamente con le informazioni del nuovo certificato.

Sostituzione del certificato di un agente di gestione

L'amministratore di sistema può sostituire il certificato dell'agente di gestione quando scade o sostituire il certificato autofirmato con uno emesso da un'autorità di certificazione.

Ogni host IaaS esegue il proprio agente di gestione. Ripetere questa procedura su ogni nodo IaaS di cui si desidera aggiornare l'agente di gestione.

Prerequisiti

- Prima di rimuovere il record, copiare l'identificatore dell'agente di gestione riportato nella colonna ID nodo. L'identificatore sarà utilizzato nella creazione del nuovo certificato dell'agente di gestione e quando lo si registrerà.
- Quando si richiede un nuovo certificato, assicurarsi che l'attributo Nome comune (CN) nel campo dell'oggetto del nuovo certificato sia immesso nel seguente formato:

```
VMware Management Agent 00000000-0000-0000-0000-000000000000
```

Utilizzare la stringa VMware Management Agent seguita da uno spazio e dal GUID dell'agente di gestione nel formato numerico mostrato.

Procedura

- 1 Arrestare il servizio dell'agente di gestione dallo snap-in Servizi di Windows.
 - a Da una macchina Windows scegliere **Start**.
 - b Nella casella Cerca del pulsante Start di Windows, immettere **services.msc** e premere Invio.
 - c Fare clic con il pulsante destro del mouse sul servizio **dell'agente di gestione di VMware vCloud Automation Center** e fare clic su **Arresta** per arrestare il servizio.
- 2 Rimuovere il certificato corrente dalla macchina. Per informazioni sulla gestione dei certificati su Windows Server 2008 R2, fare riferimento all'articolo della Knowledge Base di Microsoft all'indirizzo <http://technet.microsoft.com/en-us/library/cc772354.aspx> o all'articolo wiki di Microsoft all'indirizzo <http://social.technet.microsoft.com/wiki/contents/articles/2167.how-to-use-the-certificates-console.aspx>.
 - a Aprire Microsoft Management Console immettendo il comando **mmc.exe**.
 - b Premere Ctrl + M per aggiungere un nuovo snap-in alla console o scegliere l'opzione dal menu a discesa File.
 - c Selezionare **Certificati** e fare clic su **Aggiungi**.
 - d Selezionare **Account del computer** e fare clic su **Avanti**.
 - e Selezionare **Computer locale: (il computer su cui è in esecuzione la console)**.
 - f Fare clic su **OK**.
 - g Espandere **Certificati (computer locale)** sul lato sinistro della console.
 - h Espandere **Personale** e selezionare la cartella Certificati.
 - i Selezionare il certificato dell'agente di gestione corrente e fare clic su **Elimina**.
 - j Fare clic su **Sì** per confermare l'eliminazione.
- 3 Importare il certificato appena generato nell'archivio **computer.personal** locale o non importare nulla se si desidera che il sistema generi automaticamente un nuovo certificato autofirmato.

- 4 Registrare il certificato dell'agente di gestione nel sito di gestione dell'appliance vRealize Automation.

- a Aprire il prompt dei comandi come utente amministratore e passare alla directory Cafe sulla macchina su cui è installato l'agente di gestione in `<vra-installation-dir>\Management Agent\Tools\Cafe`, di solito `C:\Programmi (x86)\VMware\vCAC\Management Agent\Tools\Cafe`.
- b Immettere il comando `Vcac-Config.exe RegisterNode`, includendo le opzioni per registrare l'identificatore dell'agente di gestione e il certificato in un unico passaggio. Inserire l'identificatore dell'agente di gestione annotato prima come valore dell'opzione `-nd`.

Tabella 1-3. Opzioni e argomenti richiesti per il comando Vcac-Config.exe RegisterNode

[illegible]

L'esempio seguente mostra il formato del comando:

```
Vcac-Config.exe RegisterNode -v -vamih "vra-vam-hostname.domain.name:5480"  
-cu "root" -cp "password" -hn "machine-hostname.domain.name"  
-nd "00000000-0000-0000-0000-000000000000"  
-tp "00000000000000000000000000000000000000000000000000000000"
```

5 Riavviare l'agente di gestione.

Esempio: comando per la registrazione di un certificato di un agente di gestione

```
Vcac-Config.exe RegisterNode -v -vamih "vra-va.eng.mycompany:5480" -cu "root" -cp
"secret" -hn "iaas.eng.mycompany" -nd "C816CFBX-4830-4FD2-8951-C17429CEA291" -tp
"70928851D5B72B206E4B1CF9F6ED953EE1103DED"
```

Modifica del metodo di polling per i certificati

Se sono presenti virgole nella sezione OU del certificato laaS, è possibile che si verifichino errori del WebSocket STOMP nei file di registro del servizio di gestione. Inoltre, il provisioning della macchina virtuale potrebbe non riuscire. È possibile rimuovere le virgole o modificare il metodo di polling da WebSocket a HTTP.

Per modificare il metodo di polling, effettuare i passaggi seguenti.

Procedura

- 1** Aprire il seguente file in un editor di testo.

C:\\Program Files (x86)\\VMware\\vCAC\\Server\\Manager Service.exe.config.

- 2** Aggiungere le seguenti righe nella sezione `<appSettings>`.

```
<add key="Extensibility.Client.RetrievalMethod" value="Polling"/>
<add key="Extensibility.Client.PollingInterval" value="2000"/>
<add key="Extensibility.Client.PollingMaxEvents" value="128"/>
```

- ### 3 Salvare e chiudere Manager Service.exe.config.

- 4** Riavviare il servizio di gestione.

Risultati

Per ulteriori informazioni sul servizio di gestione, vedere *Installazione di vRealize Automation*.

Gestione del database dell'appliance Postgres vRealize Automation

vRealize Automation richiede il database dell'appliance per il funzionamento del sistema. È possibile gestire il database dell'appliance tramite l'interfaccia VAMI (Virtual Appliance Management Interface) dell'appliance vRealize Automation.

Nota Queste informazioni si applicano solo a distribuzioni che utilizzano un database dell'appliance incorporato. Non si applica a distribuzioni che utilizzano un database Postgres esterno.

È possibile configurare il database come un nodo singolo o a più nodi per favorire la disponibilità elevata tramite failover. Il programma di installazione di vRealize Automation include un nodo di database su ciascuna installazione dell'Appliance vRealize Automation. Pertanto se vengono installate tre istanze di un'Appliance vRealize Automation, saranno disponibili tre nodi di database. Il failover automatico viene implementato nelle distribuzioni applicabili. Il database dell'appliance non richiede alcuna manutenzione a meno che non venga modificata la configurazione di una macchina oppure, se si usa una configurazione in cluster, non venga promosso un nodo diverso come nodo primario.

Nota la configurazione cluster del database viene impostata automaticamente quando si unisce un'appliance virtuale al cluster mediante l'operazione Unisci cluster. Il cluster del database non dipende direttamente dal cluster dell'appliance virtuale. È ad esempio possibile che una macchina virtuale unita a un cluster funzioni in modo normale anche se il database dell'appliance incorporata non è stato avviato o ha generato un errore.

Per la disponibilità elevata, vRealize Automation utilizza il modello di replica primario PostgreSQL per supportare la replica dei dati. Questo significa che tutti i nodi di database operano in un cluster con un nodo principale, definito anche nodo primario, e diversi nodi di replica, noti come repliche. Il nodo primario gestisce tutte le richieste di database e i nodi di replica trasmettono e riproducono le transazioni dal nodo primario in locale.

Una configurazione in cluster contiene un nodo primario e uno o più nodi di replica. Il nodo primario è il nodo dell'appliance vRealize Automation con il database primario che supporta la funzionalità del sistema. I nodi di replica contengono copie del database che possono essere inserite nel servizio se il nodo primario non riesce.

Esistono numerose opzioni di database dell'appliance ad alta disponibilità. La scelta della modalità di replica è l'opzione di configurazione del database più importante. La modalità di replica determina in che modo la distribuzione di vRealize Automation gestisce l'integrità dei dati e, per le configurazioni a disponibilità elevata, in che modo esegue il failover in caso di errore del nodo primario. Esistono due modalità di replica: sincrona e asincrona.

Entrambe le modalità supportano il failover del database, ma ciascuna di esse presenta vantaggi e svantaggi. Per supportare il failover del database ad alta disponibilità, la modalità asincrona richiede due nodi, mentre la modalità sincrona ne richiede tre. La modalità sincrona richiama anche il failover automatico.

Modalità di replica	Vantaggi	Svantaggi
Sincrona	<ul style="list-style-type: none"> ■ Riduce al minio la possibilità di perdita di dati. ■ Richiama il failover automatico. 	<ul style="list-style-type: none"> ■ Può influire sulle prestazioni del sistema. ■ Richiede tre nodi.
Asincrona	<ul style="list-style-type: none"> ■ Richiede solo due nodi. ■ Influisce sulle prestazioni del sistema meno della modalità sincrona. 	Non è così solida come la modalità sincrona nell'impedire la perdita di dati.

vRealize Automation supporta entrambe le modalità, ma funziona in modalità asincrona per impostazione predefinita e offre disponibilità elevata solo se sono presenti almeno due nodi del database dell'appliance. La scheda **Cluster** dell'interfaccia VAMI (Virtual Appliance Management Interface) consente di passare da una modalità di sincronizzazione all'altra e aggiungere nodi di database in base alle necessità.

Quando viene utilizzato in modalità sincrona, vRealize Automation richiama il failover automatico.

Se si inizia con un nodo in una configurazione non ad alta disponibilità, è possibile aggiungere tutti i nodi necessari in un secondo momento per migliorare l'alta disponibilità. Se si dispone dell'hardware appropriato e si necessita della massima protezione dalla perdita dei dati, è consigliabile configurare la propria distribuzione in modo che funzioni in modalità sincrona.

Failover del database dell'appliance

In una configurazione a disponibilità elevata, il nodo primario trasmette costantemente le transazioni ai server di replica. Se il nodo primario non funziona, la replica attiva e funzionante è pronta per procedere con le richieste di sola lettura. Quando viene promosso il nuovo nodo primario, manualmente o automaticamente, tutte le richieste future vengono indirizzate a tale nodo.

Configurazione del database dell'appliance

Dalla pagina del database Virtual Appliance Management Interface, è possibile monitorare e aggiornare la configurazione del database dell'appliance. Inoltre consente di cambiare la designazione del nodo primario e la modalità di sincronizzazione utilizzata dal database.

Il database dell'appliance viene installato e configurato nel corso dell'installazione e della configurazione del sistema vRealize Automation, ma è possibile monitorare e cambiare la configurazione dalla scheda **Database** dell'interfaccia Virtual Appliance Management Interface.

La casella di testo **Stato connessione** indica se il database è connesso al sistema vRealize Automation e correttamente funzionante.

Se il database dell'appliance utilizza più nodi per supportare il failover, nella tabella nella parte inferiore della pagina vengono elencati i nodi e il rispettivo stato e viene indicato qual è il nodo primario. La casella di testo **Modalità di replica** mostra la modalità operativa (sincrona o asincrona) correntemente configurata per il sistema. Utilizzare questa pagina per aggiornare la configurazione del database dell'appliance.

La colonna Stato di sincronizzazione* nella tabella dei nodi di database mostra il metodo di sincronizzazione per il cluster. Questa colonna è associata alla colonna Stato per mostrare lo stato dei nodi del cluster. I potenziali stati variano in base alla replica utilizzata, sincrona o asincrona.

Tabella 1-4. Stato di sincronizzazione per le modalità di replica del database dell'appliance

Modalità	Messaggio dello stato di sincronizzazione
Replica sincrona	Nodo primario - nessuno stato
	Nodo di replica - sincronizzazione
	Altri nodi - potenziali
Replica asincrona	Nodo primario - nessuno stato
	Altri nodi - potenziali

La colonna Valido indica se le repliche sono sincronizzate con il nodo primario. Il nodo primario è sempre valido.

La colonna Priorità mostra la posizione dei nodi della replica in relazione al nodo primario. Il nodo primario non ha un valore di priorità. Quando si promuove una replica per convertirla nel nodo primario, selezionare il nodo con il valore di priorità più basso.

Quando viene utilizzato in modalità sincrona, vRealize Automation richiama il failover automatico. In caso di errore del nodo primario, il nodo di replica successivo disponibile diventerà automaticamente il nuovo nodo primario. L'operazione di failover richiede da 10 a 30 secondi in una distribuzione tipica di vRealize Automation.

Prerequisiti

- Installare e configurare vRealize Automation in base alle istruzioni relative disponibili in *Installazione di vRealize Automation*.
- Accedere alla gestione dell'appliance di vRealize Automation come **root** utilizzando la password immessa durante la distribuzione dell'appliance vRealize Automation.
- Configurare un adeguato cluster di database dell'appliance Postgres incorporata come parte della propria vRealize Automation distribuzione.

Procedura

- 1 In Virtual Appliance Management Interface, selezionare **Impostazioni vRA > Database**.
- 2 Se il database utilizza più nodi, esaminare la tabella nella parte inferiore della pagina e verificare che il sistema funzioni correttamente.
 - Accertarsi che siano elencati tutti i nodi.
 - Verificare che il nodo primario designato sia quello giusto.

Nota Non fare clic su **Modalità di sincronizzazione** per cambiare la modalità di sincronizzazione del database se non si è certi che i dati sono al sicuro. Il cambio di modalità di sincronizzazione senza preparazione può comportare la perdita di dati.

- 3 Per promuovere uno dei nodi come nodo primario, fare clic su **Promuovi** nella colonna appropriata.
- 4 Fare clic su **Salva impostazioni** per salvare la configurazione se sono state apportate modifiche.

Scenari di failover automatico del database di un'appliance con tre nodi

Esistono diversi scenari di failover della disponibilità elevata del database dell'appliance e il comportamento di vRealize Automation cambia in base alla configurazione del database dell'appliance e al numero di nodi in cui si verifica un errore.

Scenari di errore di un nodo singolo

Se in uno dei tre nodi si verifica un errore, vRealize Automation avvierà un failover automatico. Non è possibile eseguire alcuna operazione di failover automatico aggiuntiva finché non vengono ripristinati tutte e tre i nodi.

La seguente tabella descrive il comportamento e le azioni correlate a un errore del nodo primario in una distribuzione a disponibilità elevata.

Tabella 1-5. Nel nodo primario si verifica un errore

Comportamento previsto	<ul style="list-style-type: none"> ■ Il nodo di replica di sincronizzazione configurato diventa il nodo primario e riprende automaticamente la funzionalità del database dell'appliance. ■ La replica di sincronizzazione potenziale diventa il nodo di standby della sincronizzazione. ■ La distribuzione vRealize Automation opera in modalità di sola lettura finché il failover automatico non viene completato.
Ulteriori operazioni	<ul style="list-style-type: none"> ■ Quando il nodo primario precedente viene ripristinato, viene reimpostato automaticamente come replica dalla logica di ripristino dell'agente di failover. Non è necessario eseguire alcuna operazione manuale. ■ Se il nodo primario precedente non può essere ripristinato, impostare manualmente la modalità asincrona del database dell'appliance.

La seguente tabella descrive il comportamento e le azioni correlate a un errore del nodo di replica della sincronizzazione in una distribuzione a disponibilità elevata.

Tabella 1-6. La replica della sincronizzazione non riesce

Comportamento previsto	<ul style="list-style-type: none"> ■ Nella distribuzione vRealize Automation non si verifica alcun periodo di inattività. Si verificherà un ritardo di un paio di secondi per le richieste del database finché la replica potenziale non diventerà la nuova replica della sincronizzazione. Il database dell'appliance esegue questa operazione automaticamente.
Ulteriori operazioni	<ul style="list-style-type: none"> ■ Quando la replica della sincronizzazione precedente ritorna online, diventa automaticamente una replica potenziale. Non è necessario eseguire alcuna operazione manuale. ■ Se la replica della sincronizzazione precedente non può essere recuperata, impostare manualmente la modalità asincrona del database dell'appliance.

La seguente tabella descrive il comportamento e le azioni correlate a un errore del nodo primario in una distribuzione a disponibilità elevata.

Tabella 1-7. La replica potenziale non riesce

Comportamento previsto	Nessun periodo di inattività della distribuzione.
Ulteriori operazioni	<ul style="list-style-type: none"> ■ Quando la replica potenziale precedente ritorna online, diventa automaticamente una replica potenziale. Non è necessario eseguire alcuna operazione manuale. ■ Se la replica potenziale precedente non può essere recuperata, impostare la modalità asincrona del database dell'appliance.

Scenari di errore di due nodi

Se si verifica un problema in due dei tre nodi contemporaneamente, vRealize Automation passa alla modalità di sola lettura finché non viene eseguita una riparazione manuale.

La seguente tabella descrive il comportamento e le azioni correlate a un errore di un nodo primario e di un nodo di replica potenziale in una distribuzione a disponibilità elevata.

Tabella 1-8. Si verifica un errore del nodo primario e della replica potenziale

Comportamento previsto	<ul style="list-style-type: none"> ■ La replica della sincronizzazione non viene promossa automaticamente a nodo primario. vRealize Automation funziona in modalità di sola lettura perché è in grado di elaborare solo transazioni di sola lettura finché non viene eseguita una promozione manuale.
Ulteriori operazioni	<ul style="list-style-type: none"> ■ È necessario eseguire la promozione manuale. Impostare la modalità asincrona del database dell'appliance. ■ Quando il nodo primario e la replica potenziale vengono ripristinati, impostarli manualmente in modo che vengano sincronizzati con il nuovo nodo primario. A questo punto, è possibile reimpostare la modalità sincrona di vRealize Automation. ■ Quando due dei tre nodi non sono attivi contemporaneamente, vRealize Automation passa alla modalità di sola lettura finché non viene eseguita una riparazione manuale. Se è disponibile un solo nodo del database, impostare la modalità asincrona della distribuzione.

La seguente tabella descrive il comportamento e le azioni correlate a un errore del nodo di sincronizzazione e del nodo potenziale in una distribuzione a disponibilità elevata.

Tabella 1-9. Le replica della sincronizzazione e la replica potenziale non riescono

Comportamento previsto	<ul style="list-style-type: none"> ■ vRealize Automation funziona in modalità di sola lettura perché è in grado di elaborare solo transazioni di sola lettura finché non viene eseguita una riparazione manuale.
Ulteriori operazioni	<ul style="list-style-type: none"> ■ È necessario eseguire la promozione manuale. Impostare la modalità asincrona del database dell'appliance. ■ Quando la replica della sincronizzazione e la replica potenziale vengono recuperate, devono essere reimpostate manualmente in modo che vengano sincronizzate con il nodo primario. A questo punto, è possibile reimpostare la modalità sincrona di vRealize Automation. ■ Quando due dei tre nodi non sono attivi contemporaneamente, vRealize Automation passa alla modalità di sola lettura finché non viene eseguita una riparazione manuale. Se è disponibile un solo nodo del database, impostare la modalità asincrona della distribuzione.

Problemi relativi ai collegamenti tra nodi

Se si verifica un problema in un collegamento tra nodi in una distribuzione, l'agente di failover automatico tenta di ripristinare la configurazione.

La seguente tabella descrive il comportamento e le azioni correlate a un errore di collegamento tra due siti in una distribuzione a disponibilità elevata con la configurazione specificata quando tutti nodi rimangono operativi e online.

Sito A: nodo primario e replica potenziale

Sito B: replica della sincronizzazione

Tabella 1-10. Problema di collegamento tra due siti quando tutti i nodi rimangono operativi e online

Comportamento previsto	Nessun periodo di inattività per la distribuzione vRealize Automation. La replica potenziale divente automaticamente la replica della sincronizzazione.
Ulteriori operazioni	Non è necessario eseguire alcuna operazione manuale.

La seguente tabella descrive il comportamento e le azioni correlate a un errore di collegamento tra due siti in una distribuzione a disponibilità elevata con la configurazione specificata quando tutti nodi rimangono operativi e online.

Sito A: nodo primario

Sito B: replica della sincronizzazione e replica potenziale

Tabella 1-11. Problema di collegamento tra due siti quando tutti i nodi rimangono operativi e online - Configurazione alternativa

Comportamento previsto	La replica della sincronizzazione diventa il nodo primario e riprende automaticamente la funzionalità del database dell'appliance. L'agente di failover automatico promuove la replica potenziale in modo che diventi la nuova replica della sincronizzazione. La distribuzione vRealize Automation opera in modalità di sola lettura fino al completamento della promozione.
Ulteriori operazioni	Non è necessario eseguire alcuna operazione manuale. Quando viene ripristinato il collegamento, l'agente di failover automatico reimposta il nodo primario precedente come replica.

Scenario: esecuzione di un failover manuale del database dell'appliance vRealize Automation

Quando si verifica un problema relativo al database Postgres dell'appliance vRealize Automation, è necessario eseguire il failover manuale di un nodo di replica dell'appliance vRealize Automation nel cluster.

Quando il database Postgres nel nodo primario dell'appliance vRealize Automation restituisce un errore o smette di funzionare, eseguire i passaggi seguenti.

Nota Se un nodo passa allo stato di non integrità, non tentare di utilizzare la relativa interfaccia di gestione dell'appliance virtuale per alcuna operazione, incluso il failover.

Prerequisiti

- Configurare un cluster di nodi dell'appliance vRealize Automation. Ciascun nodo ospita una copia incorporata di database dell'appliance Postgres.

Procedura

- 1 Rimuovere l'indirizzo IP del nodo primario dal bilanciamento del carico esterno.
- 2 Accedere come root all'interfaccia di gestione dell'appliance vRealize Automation.
`https://vrealize-automation-appliance-FQDN:5480`
- 3 Selezionare **Cluster**.
- 4 Dall'elenco di nodi del database, individuare il nodo di replica con la priorità più bassa.
I nodi di replica vengono visualizzati in ordine di priorità crescente.
- 5 Fare clic su **Promuovi** e attendere il completamento dell'operazione.
Al termine, il nodo di replica viene elencato come nuovo nodo primario.
- 6 Risolvere i problemi relativi al nodo primario precedente e aggiungerlo di nuovo al cluster:
 - a Isolare il nodo primario precedente.

Disconnettere il nodo dalla rete corrente, ovvero quella che effettua il routing ai nodi rimanenti dell'appliance vRealize Automation. Selezionare un altro NIC per la gestione oppure gestirlo direttamente dalla console di gestione della macchina virtuale.

- b Recuperare il nodo primario precedente.

Accendere il nodo oppure risolvere l'errore in altro modo. Ad esempio, se la macchina virtuale non risponde, è possibile reimpostarla.

- c Da una sessione di console come root, arrestare il servizio vpostgres.

```
service vpostgres stop
```

- d Aggiungere di nuovo il nodo primario precedente alla rete originale, ovvero quella che effettua il routing agli altri nodi dell'appliance vRealize Automation.

- e Da una sessione di console come root, riavviare il servizio haproxy.

```
service haproxy restart
```

- f Accedere all'interfaccia di gestione del nuovo nodo primario dell'appliance vRealize Automation come utente root.

- g Selezionare **Cluster**.

- h Individuare il nodo primario precedente e fare clic su **Reimposta**.

- i Una volta completata correttamente la reimpostazione, riavviare il nodo primario precedente.

- j Con il nodo primario precedente acceso, verificare che i seguenti servizi siano in esecuzione.

```
haproxy horizon-workspace rabbitmq-server vami-lighttpd vcac-server vco-server
```

- k Aggiungere di nuovo il nodo primario precedente al bilanciamento del carico esterno.

Nota Se un nodo primario che è stato abbassato di livello a replica è ancora elencato come primario, potrebbe essere necessario aggiungerlo di nuovo manualmente al cluster per risolvere il problema.

Scenario: esecuzione di un failover di manutenzione del database

In qualità di amministratore del sistema vRealize Automation, è necessario eseguire un'operazione di failover di manutenzione del database dell'appliance.

In questo scenario si presuppone che il nodo primario corrente stia funzionando correttamente. Esistono due passaggi di manutenzione del failover del database: manutenzione del nodo primario e manutenzione di un nodo di replica. Dopo aver sostituito un nodo primario in modo da trasformarlo in una replica, è consigliabile eseguire un'operazione di manutenzione su tale nodo in modo che possa diventare di nuovo il nodo primario in caso di necessità.

Nota Non arrestare o riavviare il servizio HAProxy nella macchina host pertinente durante l'esecuzione di un failover di manutenzione.

Prerequisiti

- vRealize Automation è installato e configurato in base alle istruzioni appropriate contenute in *Installazione di vRealize Automation*.
- Accedere alla gestione dell'appliance di vRealize Automation come **root** utilizzando la password immessa durante la distribuzione dell'appliance vRealize Automation.
- Installare e configurare un cluster del database dell'appliance Postgres incorporata appropriato.
- Se il database utilizza la modalità di replica sincrona, verificare che il cluster contenga tre nodi attivi.

Procedura

- 1 Rimuovere l'indirizzo IP del nodo primario dal bilanciamento del carico esterno.
- 2 Isolare il nodo primario.
 Disconnettere il nodo dalla rete corrente. Questa dovrebbe essere la rete che esegue il routing ai nodi Appliance vRealize Automation rimanenti.
- 3 Selezionare un'altra NIC per la gestione oppure gestirla direttamente dall'interfaccia di gestione dell'appliance virtuale.
- 4 Selezionare **Cluster** nell'interfaccia VAMI.
- 5 Selezionare il nodo di replica con la priorità più bassa per promuoverlo a nodo primario e fare clic su **Promuovi**.
 I nodi di replica vengono visualizzati in ordine di priorità crescente.
 Il nodo primario precedente viene abbassato allo stato di replica e il nuovo nodo primario viene promosso.
- 6 Eseguire le operazioni di manutenzione della replica appropriate.
- 7 Al termine della manutenzione, verificare che l'appliance virtuale stia funzionando con la connettività di rete e che il relativo servizio HAProxy sia in esecuzione.
 - a Accedere alla console di gestione di vRealize Automation come **root**.
 - b Assicurarsi che il nodo di replica possa essere sottoposto a ping, nonché risolto in base al nome e che disponga di uno stato recente nella scheda **Cluster** dell'interfaccia VAMI.

8 Fare clic su **Reimposta** per il nodo di replica.

Questa operazione comporta la reimpostazione del database in modo da configurarlo per la replica nel nodo primario corrente, nonché la risincronizzazione del nodo di replica con la configurazione HAProxy più recente del nodo primario.

- 9 Dopo aver completato correttamente la reimpostazione, reimpostare l'indirizzo IP del nodo dell'appliance virtuale di replica sul pool esterno di indirizzi IP di bilanciamento del carico dell'appliance virtuale.
- 10 Assicurarsi che il nodo di replica sia integro nella tabella del database e che possa essere sottoposto a ping e risolto mediante nome.

Operazioni successive

Risolvere i problemi relativi al nodo primario precedente e aggiungerlo al cluster.

Ripristino manuale del database dell'appliance da un errore irreversibile

Se il database dell'appliance ha un problema e nessuno dei nodi del database è in funzione o tutti i nodi di replica sono fuori sincronizzazione nel momento in cui si verifica l'errore dell'elemento principale, utilizzare la seguente procedura per tentare di ripristinare il database.

Questa procedura si applica nelle situazioni in cui nessuno dei nodi del database è operativo in un cluster che è in esecuzione in modalità asincrona. In una situazione di questo tipo, in genere vengono mostrati errori simili al seguente nella pagina dell'interfaccia di gestione dell'appliance virtuale quando si tenta di caricare o aggiornare la pagina:

```
Error initializing the database service: Could not open JDBC Connection for transaction; nested exception is org.postgresql.util.PSQLException: The connection attempt failed.
```

Procedura

- 1 Provare a ripristinare il database utilizzando l'interfaccia di gestione dell'appliance virtuale da uno dei nodi del database.
 - a Se possibile, aprire la pagina **Cluster** dell'interfaccia VAMI del nodo con lo stato più recente. In genere, questo nodo è quello che era il nodo principale prima dell'errore del database.
 - b Se l'apertura dell'interfaccia di gestione dell'appliance virtuale per il nodo principale non riesce, provare ad aprire l'interfaccia per altri nodi di replica.
 - c Se è possibile trovare un nodo di database con un'interfaccia di gestione dell'appliance virtuale funzionante, provare a ripristinarlo eseguendo un failover manuale.

Vedere [Scenario: esecuzione di un failover manuale del database dell'appliance vRealize Automation](#).

- 2 Se la procedura al passaggio 1 non riesce, avviare una sessione della shell e provare a stabilire il nodo con lo stato più recente. Avviare una sessione della shell per tutti i nodi del cluster disponibili e provare ad avviare i relativi database eseguendo il seguente comando della shell: `service vpostgres start`
- 3 Attenersi alla seguente procedura per ogni nodo che dispone di un database locale in esecuzione per determinare il nodo con lo stato più recente.
 - a Eseguire il comando seguente per determinare il nodo con lo stato più recente. Se il comando restituisce `f`, è quello il nodo con lo stato più recente ed è possibile continuare dal passaggio 4.

```
su - postgres
psql vcac
vcac=# select pg_is_in_recovery();
pg_is_in_recovery
```

- Se questo comando restituisce `f`, questo nodo presenta lo stato più recente.
- Se il nodo restituisce `t`, eseguire il comando seguente nel nodo:

```
SELECT pg_last_xlog_receive_location() as receive_loc, pg_last_xlog_replay_location() as
replay_loc, extract(epoch from pg_last_xact_replay_timestamp()) as replay_timestamp;
```

Questo comando dovrebbe restituire un risultato simile al seguente.

```
vcac=# SELECT pg_last_xlog_receive_location() as receive_loc, pg_last_xlog_replay_location()
as replay_loc, extract(epoch from pg_last_xact_replay_timestamp()) as replay_timestamp;
 receive_loc | replay_loc | replay_timestamp
-----+-----+-----
 0/20000000 | 0/203228A0 | 1491577215.68858
(1 row)
```

- 4 Confrontare i risultati per ciascun nodo per determinare quale dispone dello stato più recente. Selezionare il nodo con il valore più grande nella colonna `receive_loc`. Se i valori sono uguali, selezionare il nodo con il valore più grande nella colonna `replay_loc` e, se i valori sono ancora uguali, selezionare il nodo con il valore più grande in `replay_timestamp`.
- 5 Eseguire il comando seguente nel nodo con lo stato più recente: `vcac-vami psql-promote-master -force`
- 6 Aprire il file `/etc/haproxy/conf.d/10-psql.cfg` in un editor di testo e aggiornare la riga seguente.

```
server masterserver sc-rdops-vm06-dhcp-170-156.eng.vmware.com:5432 check on-marked-up shutdown-
backup-sessions
```

Il nome di dominio completo del nodo corrente dev'essere simile al seguente:

```
server masterserver current-node-fqdn:5432 check on-marked-up shutdown-backup-sessions
```

- 7 Salvare il file.
- 8 Eseguire il comando `service haproxy restart`.
- 9 Aprire la pagina **Cluster** dell'interfaccia VAMI per il nodo più recente.

Questo nodo dovrebbe risultare il nodo principale e gli altri nodi repliche non valide. Inoltre viene abilitato il pulsante **Reimposta** per le repliche.

- 10 Fare clic su **Reimposta** per ciascuna replica in successione fino al ripristino dello stato del cluster.

Backup e ripristino nelle installazioni di vRealize Automation

Per ridurre al minimo il downtime del sistema e la perdita di dati in caso di guasti, gli amministratori eseguono regolarmente il backup dell'intera installazione di vRealize Automation. In caso di guasti al sistema, è possibile recuperare l'installazione ripristinando l'ultimo backup sicuramente funzionante e reinstallando alcuni componenti.

Per eseguire il backup e il ripristino di vRealize Automation, vedere gli argomenti seguenti nella documentazione relativa a [vRealize Suite](#):

- Preparazioni per il backup di vRealize Automation
- Ripristino del sistema di vRealize Automation

Programma CEIP (Customer Experience Improvement Program)

Questo prodotto partecipa al programma CEIP (Customer Experience Improvement Program) di VMware. Il programma CEIP fornisce a VMware informazioni che consentono a VMware di migliorare i propri prodotti e servizi, risolvere problemi e fornire best practice per la distribuzione e l'uso dei prodotti. È possibile partecipare e rimuovere la partecipazione al programma CEIP per vRealize Automation in qualsiasi momento.

I dettagli relativi ai dati raccolti mediante 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>.

Partecipare o abbandonare il programma CEIP (Customer Experience Improvement Program) per vRealize Automation

È possibile partecipare o abbandonare il programma CEIP (Customer Experience Improvement Program) per vRealize Automation in qualsiasi momento.

vRealize Automation offre l'opportunità di partecipare al programma CEIP (Customer Experience Improvement Program) quando inizialmente si installa e configura il prodotto. Dopo l'installazione, è possibile partecipare o abbandonare il programma CEIP procedendo come segue.

Procedura

- 1 Accedere come root all'interfaccia di gestione dell'appliance vRealize Automation.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Fare clic sulla scheda **Telemetria**.
- 3 Selezionare o deselezionare l'opzione **Partecipa al programma CEIP (Customer Experience Improvement Program) di VMware**.

Quando questa opzione è selezionata, il programma viene attivato e i dati vengono inviati a `https://vmware.com`.
- 4 Fare clic su **Salva impostazioni**.

Configurazione del giorno e dell'ora per la raccolta dati

È possibile impostare data e ora nel momento in cui il programma CEIP (Customer Experience Improvement Program) invia i dati a VMware.

Procedura

- 1 Accedere a una sessione della console nell'appliance vRealize Automation come utente root.
- 2 Aprire il seguente file in un editor di testo.
`/etc/telemetry/telemetry-collector-vami.properties`
- 3 Modificare le proprietà per il giorno della settimana (dow) e per le ore del giorno (hod).

Proprietà	Descrizione
<code>frequency.dow=<giorno della settimana></code>	Giorno in cui avviene la raccolta dati.
<code>frequency.hod=<ora del giorno></code>	Ora locale del giorno in cui viene effettuata la raccolta dei dati. I valori possibili sono 0-23.

- 4 Salvare e chiudere `telemetry-collector-vami.properties`.
- 5 Per applicare le impostazioni, inserire il seguente comando.
`vcac-config telemetry-config-update --update-info`

Le modifiche vengono applicate a tutti i nodi della distribuzione.

Regolazione delle impostazioni di sistema

In qualità di amministratore del sistema, è possibile registrare e personalizzare i modelli email IaaS. È anche possibile gestire le impostazioni visualizzate come predefinite per ogni tenant, ad esempio i server email che devono gestire le notifiche. Gli amministratori tenant possono scegliere se sovrascrivere tali impostazioni predefinite, qualora i tenant richiedano impostazioni diverse.

Modificare l'icona Tutti i servizi nel catalogo dei servizi

È possibile modificare l'icona predefinita nel catalogo dei servizi per visualizzare un'immagine personalizzata. Quando si modifica l'icona, questa cambia per tutti i tenant. Non è possibile configurare icone specifiche per i tenant del catalogo.

I comandi sono forniti per Linux o Mac e Windows, in modo che sia possibile eseguire i comandi cURL in uno qualsiasi di questi sistemi operativi.

Prerequisiti

- Convertire l'immagine a una stringa con codifica base64.
- cURL deve essere installato sulla macchina in cui vengono eseguiti i comandi.
- È necessario disporre delle credenziali di un utente vRealize Automation con il ruolo di amministratore del sistema.

Procedura

- 1 Impostare la variabile VCAC nella sessione terminale per i comandi cURL.

Sistema operativo	Comando
Linux/Mac	<code>export VCAC=<VA URL></code>
Windows	<code>set VCAC=<VA URL></code>

- 2 Recuperare il token di autenticazione per l'utente amministratore del sistema.

Sistema operativo	Comando
Linux/Mac	<code>curl https://\$VCAC/identity/api/tokens --insecure -H "Accept: application/json" -H 'Content-Type: application/json' --data '{"username": "<Catalog Administrator User>", "password": "<password>", "tenant": "vsphere.local"}'</code>
Windows	<code>curl https://%VCAC%/identity/api/tokens --insecure -H "Accept:application/json" -H "Content-Type:application/json" --data "{\"username\":\"<Catalog Administrator User>\", \"password\":\"<password>\", \"tenant\":\"vsphere.local\"}"</code>

Viene generato un token di autenticazione.

- 3 Impostare la variabile del token di autenticazione sostituendo <Auth Token> con la stringa del token generata nel passaggio precedente.

Sistema operativo	Comando
Linux/Mac	<code>export AUTH="Bearer <Auth Token>"</code>
Windows	<code>set AUTH=Bearer <Auth Token></code>

4 Aggiungere la stringa codificata base64 per l'immagine.

Sistema operativo	Comando
Linux/Mac	<pre>curl https://\$VCAC/catalog-service/api/icons --insecure -H "Accept: application/json" -H 'Content-Type: application/json' -H "Authorization: \$AUTH" --data '{"id":"cafe_default_icon_genericAllServices","fileName":"<filename>","contentType":"image/png","image":"<IMAGE DATA as base64 string>"}'</pre>
Windows	<pre>curl https://%VCAC%/catalog-service/api/icons --insecure -H "Accept: application/json" -H "Content-Type: application/json" -H "Authorization: %AUTH%" --data "{\"id\":\"cafe_default_icon_genericAllServices\", \"fileName\":\"<filename>\", \"contentType\":\"image/png\", \"image\":\"<IMAGE DATA as base64 string>\"}"</pre>

Risultati

La nuova icona dei servizi viene visualizzata nel catalogo dei servizi dopo circa cinque minuti.

Se si desidera ripristinare l'icona predefinita, è possibile eseguire questo comando dopo i passaggi 1-3.

Sistema operativo	Comando
Linux/Mac	<pre>curl https://\$VCAC/catalog-service/api/icons/cafe_default_icon_genericAllServices --insecure -H "Authorization: \$AUTH" --request DELETE</pre>
Windows	<pre>curl https://%VCAC%/catalog-service/api/icons/cafe_default_icon_genericAllServices --insecure -H "Authorization: %AUTH%" --request DELETE</pre>

Personalizzazione delle impostazioni di rollover dei dati

È possibile configurare le impostazioni di rollover dei dati di vRealize Automation per controllare il modo in cui i dati legacy vengono conservati, archiviati o eliminati dal sistema.

La funzionalità di rollover dei dati consente di attivare il rollover, impostare il numero massimo di giorni per cui i dati devono essere conservati da vRealize Automation nel database SQL Server di IaaS prima che vengano archiviati o eliminati, nonché eseguire altri controlli del rollover dei dati.

Per impostazione predefinita, la funzionalità di rollover dei dati è disattivata.

Configurare le impostazioni di rollover dei dati nella pagina **Impostazioni globali** di vRealize Automation. Quando questa funzionalità è attivata, i dati vengono sottoposti a query e rimozione dalle seguenti tabelle del database SQL Server:

- UserLog
- Audit
- CategoryLog
- VirtualMachineHistory
- VirtualMachineHistoryProp

- AuditLogItems
- AuditLogItemsProperties
- TrackingLogItems
- WorkflowHistoryInstances
- WorkflowHistoryResults

Se l'opzione `DataRolloverIsArchiveEnabled` è impostata su `True`, vengono create versioni di archiviazione delle tabelle nello schema `dbo`. Ad esempio, la versione di archiviazione di `UserLog` sarebbe `UserLogArchive` e quella di `VirtualMachineHistory` sarebbe `VirtualMachineHistoryArchive`.

Se la funzionalità è attivata, il rollover dei dati viene eseguito una volta al giorno all'ora predefinita (03:00) a seconda della configurazione dell'ora locale dell'appliance vRealize Automation. Utilizzando l'impostazione `DataRollover MaximumAgeInDays`, è possibile impostare il numero massimo di giorni per cui si desidera che i dati vengano conservati. Si noti che in genere questo processo viene eseguito rapidamente entro un intervallo di tempo che varia da pochi minuti a un'ora. Tuttavia, quando questa funzionalità viene attivata per la prima volta, è possibile che il processo debba archiviare/eliminare una grande quantità di dati e quindi richiedere molto più tempo per il completamento. Questo processo è progettato per l'esecuzione fino al completamento. Viene eseguito rapidamente in blocchi di lavoro transazionali di piccole dimensioni per non causare problemi di concomitanza. Si noti che questo processo può essere interrotto normalmente come descritto di seguito.

Nota È possibile interrompere il processo `DataRollover` impostando l'opzione `DataRollover Status` dell'esecuzione su `Disattivata` o `Attivata`. Ciò consente di interrompere normalmente il processo in esecuzione, senza perdere dati. Tutti i dati archiviati o eliminati fino al punto di interruzione del processo vengono salvati.

Se l'opzione `DataRollover IsArchiveEnabled` è impostata su `True`, i dati precedenti al numero di giorni specificato nell'impostazione `DataRollover MaximumAgeInDays` vengono spostati nelle tabelle di archiviazione. Se l'opzione `DataRollover IsArchiveEnabled` è impostata su `False`, i dati vengono invece eliminati definitivamente, senza essere archiviati. I dati eliminati non possono essere ripristinati.

Procedura

- 1 Accedere alla console di vRealize Automation come **amministratore di sistema**.
- 2 Selezionare **Infrastruttura > Amministrazione > Impostazioni globali**.

- 3 Nella pagina **Impostazioni globali**, individuare la sezione **Rollover dati** della tabella, quindi verificare e configurare le impostazioni.

Impostazione	Descrizione
DataRollover BatchSize	Il valore predefinito di questa impostazione è 2000 e probabilmente non è necessario modificarlo. Tuttavia, se questo valore influisce negativamente sulle prestazioni, è possibile impostare un valore di BatchSize inferiore. Un valore di BatchSize superiore potrebbe consentire di svolgere il lavoro più rapidamente, ma effettuerebbe una pressione maggiore sulle elaborazioni simultanee. L'intervallo valido è da 100 a 20000.
DataRollover IsArchiveEnabled	Specifica se spostare i dati di rollover nelle tabelle di archiviazione una volta trascorso il limite massimo di giorni. Per impostazione predefinita, questo valore è impostato su True. Se lo si imposta su False, tutti i dati precedenti al valore specificato nell'impostazione DataRollover MaximumAgeInDays vengono eliminati definitivamente.
DataRollover MaximumAgeInDays	Specifica per quanti giorni i dati vengono conservati nel database prima che vengano archiviati o eliminati definitivamente. Per impostazione predefinita, questo valore è impostato su 90 giorni.
DataRollover Status	Specifica se attivare o meno il rollover dei dati. Per impostazione predefinita, questo valore è impostato su Disabled (Disattivato). Per attivare il rollover dei dati, impostare questo valore su Enabled (Attivato).
DataRollover VirtualMachineHistory BatchSize	Specifica la dimensione del batch nella tabella VirtualMachineHistory in un intervallo che va da 1 a 5 record. Il valore predefinito è 1.
DataRollover UpdateStatistics	L'impostazione UpdateStatistics è disattivata per impostazione predefinita, ma è consigliabile attivarla (impostandola su 1) poiché le statistiche aggiornate sono utili per le prestazioni delle query. Ciò comporta che la stored procedure [dbo].[usp_DataRollover] esegua il comando di aggiornamento delle statistiche nelle tabelle dopo l'esecuzione del processo di archiviazione.

- 4 Per modificare un'impostazione, fare clic sull'icona **Modifica** (✎) nella prima colonna della tabella.

L'area **Valore** per l'impostazione applicabile diventa modificabile.

- 5 Per salvare le modifiche, fare clic sull'icona **Salva** (✔) nella prima colonna della tabella.

Selezione delle impostazioni nel file di configurazione del servizio di gestione

È possibile utilizzare il file di configurazione di Servizio di gestione (`managerService.exe.config`) per configurare le impostazioni comuni per le distribuzioni della macchina.

Generalmente, il file `managerService.exe.config` si trova nella directory `%System-Drive%\Program Files x86\VMware\VCAC\Server`. È sempre consigliabile creare una copia del file prima di modificarlo.

È possibile utilizzare le impostazioni del file `managerService.exe.config` indicate di seguito per controllare vari aspetti delle distribuzioni della macchina. Sono mostrati i valori predefiniti.

- `<add key="ProcessLeaseWorkflowTimerCallbackIntervalMilliseconds" value="3600000"/>`
- `<add key="BulkRequestWorkflowTimerCallbackMilliseconds" value="10000"/>`
- `<add key="MachineRequestTimerCallbackMilliseconds" value="10000"/>`
- `<add key="MachineWorkflowCreationTimerCallbackMilliseconds" value="10000"/>`
- `<add key="RepositoryConnectionMaxRetryCount" value="100"/>`
- `<add key="MachineCatalogRegistrationRetryTimerCallbackMilliseconds" value="120000"/>`
- `<add key="MachineCatalogUnregistrationRetryTimerCallbackMilliseconds" value="120000"/>`
- `<add key="MachineCatalogUpdateMaxRetryCount" value="15"/>`

Impostazione dei limiti di simultaneità a uso intensivo di risorse

Per risparmiare risorse, vRealize Automation limita il numero di istanze di provisioning e raccolta dati di macchine contemporaneamente in esecuzione. È possibile cambiare i limiti.

Configurazione del provisioning simultaneo di macchine

Richieste multiple simultanee del provisioning di macchine possono avere un impatto significativo sulle prestazioni di vRealize Automation. È possibile operare alcune modifiche ai limiti definiti sugli agenti proxy e nelle attività dei workflow per variare le prestazioni.

In base alle esigenze dei proprietari delle macchine del sito, il server di vRealize Automation potrebbe ricevere richieste simultanee multiple di provisioning di macchine. Questa circostanza può presentarsi nelle seguenti situazioni:

- Un singolo utente invia una richiesta di macchine multiple
- Molti utenti richiedono contemporaneamente macchine
- Uno o più manager di gruppo approvano in rapida successione richieste di macchine multiple che erano in sospeso

Il tempo richiesto a vRealize Automation per eseguire il provisioning di una macchina in genere aumenta in presenza di un numero elevato di richieste simultanee. L'aumento del tempo di provisioning dipende da tre importanti fattori:

- L'effetto sulle prestazioni delle attività dei workflow di vRealize Automation simultanee che impiegano intensivamente le risorse, incluse l'attività di SetupOS (per macchine create all'interno della piattaforma di virtualizzazione, come nel provisioning basato su WIM) e l'attività Clona (per macchine clonate all'interno della piattaforma di virtualizzazione).
- La soglia configurata in vRealize Automation che limita il numero di attività di provisioning a uso intensivo di risorse, tipicamente lunghe, che possono essere eseguite simultaneamente. L'impostazione predefinita è otto. Le attività simultanee successive al raggiungimento del limite vengono messe in coda.
- Eventuali limiti all'interno della piattaforma di virtualizzazione o nell'account del servizio cloud rispetto al numero di elementi di lavoro di vRealize Automation (a uso intensivo di risorse o meno) che possono essere eseguiti simultaneamente. Ad esempio, il limite predefinito in vCenter Server è quattro, gli elementi di lavoro successivi al raggiungimento del limite vengono messi in coda.

Per impostazione predefinita, vRealize Automation limita le attività simultanee di provisioning virtuale per gli hypervisor che utilizzano agenti proxy a otto per endpoint. Ciò garantisce che la piattaforma di virtualizzazione gestita da un particolare agente non riceva mai una mole elementi di lavoro a uso intensivo di risorse tale da evitare l'esecuzione di altri elementi. Prima di cambiare il limite, pianificare un test attento su quali sarebbero gli effetti del nuovo limite. La determinazione del limite migliore per il proprio sito potrebbe richiedere l'analisi dell'esecuzione degli elementi di lavoro all'interno della piattaforma di virtualizzazione e dell'esecuzione delle attività dei workflow all'interno di vRealize Automation.

Se si aumenta il limite di vRealize Automation per agente configurato, potrebbe essere necessario effettuare regolazioni di configurazione aggiuntive in vRealize Automation, nei modi seguenti:

- Gli intervalli di timeout di esecuzione predefiniti per le attività di workflow di SetupOS e Clona sono di due ore per ognuno. Se il tempo richiesto per eseguire una di queste attività supera il limite, l'attività viene annullata e il provisioning ha esito negativo. Per prevenire questo problema, aumentare uno solo o entrambi questi intervalli di timeout di esecuzione.
- Gli intervalli di timeout di consegna predefiniti per le attività di workflow di SetupOS e Clona sono di 20 ore per ognuno. Una volta che una di queste attività è iniziata, se la macchina risultante dall'attività non viene fornita in provisioning entro 20 ore, l'attività viene annullata e il provisioning ha esito negativo. Pertanto, se il limite è stato aumentato fino al punto in cui talvolta si verifica questa situazione, è consigliabile aumentare uno solo o entrambi questi intervalli di timeout di consegna.

Configurazione di raccolte dati simultanee

Per impostazione predefinita, vRealize Automation limita le attività di raccolta dati simultanee. Se si cambia questo limite, è possibile evitare timeout non necessari cambiando gli intervalli di timeout di esecuzione predefiniti per i diversi tipi di raccolta dati.

vRealize Automation raccoglie regolarmente dati dalle risorse di elaborazione di virtualizzazione conosciute attraverso i suoi agenti proxy, nonché dagli account dei servizi cloud e dalle macchine fisiche attraverso gli endpoint a loro associati. A seconda del numero di risorse di elaborazione di virtualizzazione, di agenti e di endpoint nel sito, potrebbero verificarsi frequentemente operazioni di raccolta dati simultanee.

Il giorno e l'ora di esecuzione della raccolta dati dipende dal numero di oggetti sugli endpoint che includono macchine virtuali, datastore, modelli e risorse di elaborazione. Sono molte le condizioni che possono causare l'aumento significativo del tempo necessario a eseguire una singola raccolta dati. Come con il provisioning delle macchine, la simultaneità incrementa il tempo richiesto per completare la raccolta dati.

Per impostazione predefinita, le attività di raccolta dati simultanee sono limitate a due per agente, mentre quelle successive al raggiungimento del limite vengono messe in coda. Questa configurazione garantisce il completamento relativamente veloce di ogni raccolta dati e rende molto improbabile un impatto negativo delle attività di raccolta dati simultanee sulle prestazioni di IaaS.

In base alle risorse e alle circostanze specifiche del sito, però, può essere possibile aumentare il limite configurato e mantenere al tempo stesso prestazioni sufficientemente veloci per trarre beneficio dalla simultaneità della raccolta dati proxy. Sebbene l'incremento del limite possa far aumentare il tempo richiesto da una singola raccolta dati, questo svantaggio potrebbe essere giustificato e superato dalla capacità di raccogliere più informazioni da più risorse di elaborazione e macchine nello stesso momento.

Se si aumenta il limite per agente configurato, potrebbe essere necessario regolare gli intervalli di timeout di esecuzione predefiniti per i diversi tipi di raccolta dati che utilizzano un agente proxy: inventario, prestazioni, stato e WMI. Se il tempo richiesto per eseguire una di queste attività supera gli intervalli di timeout configurati, l'attività viene annullata e riavviata. Per evitare l'annullamento dell'attività, aumentare uno solo o più di questi intervalli di timeout di esecuzione.

Regolazione di limiti di simultaneità e intervalli di timeout

È possibile cambiare i limiti per agente sul provisioning simultaneo, le attività di raccolta dati e gli intervalli di timeout predefiniti.

Quando si inserisce un valore di tempo per queste variabili, utilizzare il formato hh:mm:ss (hh=ore, mm=minuti e ss=secondi).

Prerequisiti

Accedere come amministratore al server che esegue il servizio di gestione IaaS. Per installazioni distribuite, questo è il server su cui è installato il servizio di gestione.

Procedura

- 1 Aprire il file `ManagerService.exe.config` in un editor. Il file si trova nella directory d'installazione del server di vRealize Automation, che di solito è `%SystemDrive%\Programmi (x86)\VMware\VCAC\Server`.
- 2 Individuare la sezione denominata `workflowTimeoutConfigurationSection`.
- 3 Aggiornare le variabili seguenti secondo necessità.

Parametro	Descrizione
<i>MaxOutstandingResourceIntensive WorkItems</i>	Limite di provisioning simultanei (il valore predefinito è 8)
<i>CloneExecutionTimeout</i>	Intervallo di timeout esecuzione provisioning virtuale
<i>SetupOSExecutionTimeout</i>	Intervallo di timeout esecuzione provisioning virtuale
<i>CloneTimeout</i>	Intervallo di timeout consegna clone provisioning virtuale
<i>SetupOSTimeout</i>	Intervallo di timeout consegna configurazione sistema operativo provisioning virtuale
<i>CloudInitializeProvisioning</i>	Intervallo di timeout inizializzazione provisioning cloud
<i>MaxOutstandingDataCollectionWorkItems</i>	Limite di raccolta dati simultanei
<i>InventoryTimeout</i>	Intervallo di timeout esecuzione raccolta dati inventario
<i>PerformanceTimeout</i>	Intervallo di timeout esecuzione raccolta dati prestazioni
<i>StateTimeout</i>	Intervallo di timeout esecuzione raccolta dati di stato

- 4 Salvare e chiudere il file.
- 5 Selezionare **Start > Strumenti di amministrazione > Servizi**.
- 6 Arrestare e riavviare il servizio vRealize Automation.
- 7 (Facoltativo) Se vRealize Automation è in esecuzione in modalità alta disponibilità, tutte le modifiche apportate al file `ManagerService.exe.config` dopo l'installazione devono essere eseguite sia sui server primari che su quelli di failover.

Regolazione della frequenza di esecuzione dei callback delle macchine

È possibile cambiare la frequenza di diverse procedure di callback, inclusa la frequenza con cui viene eseguita la procedura di callback di vRealize Automation per i lease della macchina cambiati.

vRealize Automation utilizza un intervallo di tempo configurato per eseguire procedure di callback differenti sul servizio Model Manager, come ad esempio `ProcessLeaseWorkflowTimerCallbackIntervalMiliSeconds` che cerca le macchine di cui sono cambiati i lease. È possibile cambiare questi intervalli di tempo per eseguire controlli più o meno frequentemente.

Quando si inserisce un valore di tempo per queste variabili, specificare un valore espresso in millisecondi. Ad esempio, 10000 millisecondi = 10 secondi e 3600000 millisecondi = 60 minuti = 1 ora.

Prerequisiti

Accedere come amministratore al server che esegue il servizio di gestione IaaS. Per installazioni distribuite, questo è il server su cui è installato il servizio di gestione.

Procedura

- 1 Aprire il file `ManagerService.exe.config` in un editor. Il file si trova nella directory d'installazione del server di vRealize Automation, che di solito è `%SystemDrive%\Programmi (x86)\VMware\VCAC\Server`.
- 2 Aggiornare le variabili seguenti come desiderato.

Parametro	Descrizione
<i>RepositoryWorkflowTimerCallbackMiliSeconds</i>	Controlla l'attività del servizio repository o del servizio Web di Model Manager. Il valore predefinito è 10000.
<i>ProcessLeaseWorkflowTimerCallbackIntervalMiliSeconds</i>	Controlla i lease scaduti delle macchine. Il valore predefinito è 3600000.
<i>BulkRequestWorkflowTimerCallbackMiliSeconds</i>	Controlla le richieste di massa. Il valore predefinito è 10000.
<i>MachineRequestTimerCallbackMiliSeconds</i>	Controlla le richieste della macchina. Il valore predefinito è 10000.
<i>MachineWorkflowCreationTimerCallbackMiliSeconds</i>	Controlla le nuove macchine. Il valore predefinito è 10000.

- 3 Salvare e chiudere il file.
- 4 Selezionare **Start > Strumenti di amministrazione > Servizi**.
- 5 Arrestare e riavviare il servizio vCloud Automation Center.
- 6 (Facoltativo) Se vRealize Automation è in esecuzione in modalità alta disponibilità, tutte le modifiche apportate al file `ManagerService.exe.config` dopo l'installazione devono essere eseguite sia sui server primari che su quelli di failover.

Regolazione delle impostazioni del registro di IaaS

È possibile configurare vRealize Automation per registrare solo le informazioni che si desidera includere nel registro del servizio di gestione.

Se vRealize Automation è in esecuzione in modalità alta disponibilità e si apportano modifiche al file `ManagerService.exe.config` dopo l'installazione, è necessario effettuare le modifiche sui server vRealize Automation primario e di failover.

Procedura

- 1 Accedere al server vRealize Automation utilizzando credenziali con accesso amministrativo.

- 2 Modificare il file `ManagerService.exe.config` in `%SystemDrive%\Programmi x86\VMware\vCAC\Server` o nell'eventuale diversa directory d'installazione del server vRealize Automation.
- 3 Modificare le chiavi `RepositoryLogSeverity` e `RepositoryLogCategory` per configurare quali tipi di eventi dovranno essere registrati nei file di registro.

Opzione	Descrizione
RepositoryLogSeverity	<p>Specificare un livello di severità al di sotto del quale gli eventi saranno ignorati.</p> <ul style="list-style-type: none"> ■ <i>Error</i> registra solo gli errori recuperabili e di entità superiore ■ <i>Warning</i> registra solo gli avvisi non critici e di entità superiore ■ <i>Information</i> registra solo i messaggi informativi e di entità superiore ■ <i>Verbose</i> registra un'analisi debug e può pregiudicare le prestazioni <p>Ad esempio <code><add key="RepositoryLogSeverity" value="Warning" /></code>.</p>
RepositoryLogCategory	<p>Specificare una categoria per registrare tutti gli eventi a essa relativi, indipendentemente dalla severità. Ad esempio, <code><add key="RepositoryLogCategory" value="MissingMachines,UnregisteredMachines,AcceptMachineRequest,RejectMachineRequest" /></code> registra tutti gli eventi per le macchine mancanti o non registrate, nonché tutte le richieste di macchine accettate o rifiutate.</p>

- 4 Salvare e chiudere il file.
- 5 Scegliere **Start > Strumenti di amministrazione > Servizi** e riavviare il servizio vCloud Automation Center.

Risultati

È possibile scoprire come influiscono sulla registrazione le modifiche apportate visualizzando il file di registro del servizio di gestione che si trova in `%SystemDrive%\Programmi (x86)\VMware\vCAC\Server\Logs` sulla macchina dove è installato il servizio di gestione o nella directory d'installazione del server di vRealize Automation, se questo è stato installato in una posizione differente.

Monitoraggio di vRealize Automation

A seconda del proprio ruolo, è possibile monitorare i workflow o i servizi, visualizzare registri di eventi o di controllo o raccogliere registri per tutti gli host in una distribuzione distribuita.

Monitoraggio dei workflow e visualizzazione dei registri

Il base al proprio ruolo, è possibile monitorare i workflow e visualizzare i registri delle attività.

Tabella 1-12. Opzioni di monitoraggio e visualizzazione dei registri

Obiettivo	Ruolo	Sequenza menu e descrizione
Visualizzare informazioni sulle azioni che si sono verificate, come il tipo di azione, data e ora dell'azione e così via.	Amministratore di IaaS	Visualizzare le informazioni predefinite dei registri o controllare il contenuto da visualizzare utilizzando le opzioni di colonne e filtri. Selezionare Infrastruttura > Monitoraggio > Registro di controllo . Il registro di controllo fornisce i dettagli sullo stato delle macchine virtuali gestite e sulle attività eseguite su queste macchine durante la riconfigurazione. Il registro include informazioni sul provisioning delle macchine, su NSX e sulle azioni di recupero e riconfigurazione.
Visualizzare lo stato dei workflow pianificati e disponibili di Distributed Execution Manager e altri.	Amministratore di IaaS	Visualizzare lo stato dei workflow e, facoltativamente, aprire un workflow specifico per visualizzarne i dettagli. Selezionare Infrastruttura > Monitoraggio > Stato DEM .
Visualizzare e opzionalmente esportare i dati dei registri.	Amministratore di IaaS	Visualizzare le informazioni predefinite dei registri o controllare il contenuto da visualizzare utilizzando le opzioni di colonne e filtri. Selezionare Infrastruttura > Monitoraggio > Registro .
Visualizzare lo stato e la cronologia dei workflow di Distributed Execution Manager eseguiti e altri.	Amministratore di IaaS	Visualizzare la cronologia dei workflow e, facoltativamente, aprire un workflow specifico per visualizzarne i dettagli di esecuzione. Selezionare Infrastruttura > Monitoraggio > Cronologia workflow .
Visualizzare un elenco di eventi che includa tipo di evento, data e ora, ID utente, ecc. e, facoltativamente, visualizzare una pagina dei dettagli dell'evento.	Amministratore di sistema	Visualizzare un elenco di eventi e dei rispettivi attributi associati, come data e ora di esecuzione, descrizione dell'evento, nome del tenant, tipo e ID del target e altre caratteristiche. Selezionare Amministrazione > Eventi > Registri eventi .
Consente di monitorare lo stato delle richieste e visualizza i relativi dettagli.	Amministratore tenant o manager del gruppo di business	Visualizzare lo stato delle richieste di proprietà o per cui si è responsabili. Fare clic su Richieste .
Visualizzare le informazioni su eventi recenti.	Amministratore di IaaS o di tenant	Visualizzare gli eventi recenti per l'utente attualmente connesso. Selezionare Infrastruttura > Eventi recenti .

Monitoraggio di registri eventi e servizi

È possibile monitorare i registri eventi e i servizi di vRealize Automation per determinarne lo stato corrente e gli stati precedenti.

Il periodo di conservazione predefinito per i registri eventi è 90 giorni. È possibile modificare il periodo dal file `/etc/vcac/vcac.properties`.

Per informazioni sulla cancellazione dei registri mediante la personalizzazione delle impostazioni di rollover dei dati, vedere *Configurazione di vRealize Automation*.

Servizi di vRealize Automation

Un amministratore di sistema può visualizzare lo stato dei servizi di vRealize Automation dal Registro eventi sulla console dell'amministratore di sistema.

Per eseguire singoli componenti di prodotto sono necessari sottoinsiemi di servizi. È ad esempio necessario che i servizi di identità e i servizi principali dell'interfaccia utente siano in esecuzione per poter configurare un tenant.

Nelle tabelle riportate di seguito sono indicati i servizi associati alle varie aree della funzionalità vRealize Automation.

Tabella 1-13. Gruppo di servizi di identità

Servizio	Descrizione
management-service	Gruppo di servizi di identità
sts-service	Appliance Single-Sign-On
authorization	Servizio di autorizzazione
authentication	Autenticazione
eventlog-service	Servizio registro eventi
licensing-service	Servizio di gestione licenze

Tabella 1-14. Servizi interfaccia utente principali

Servizio	Descrizione
shel-ui-app	Servizio della shell
branding-service	Servizio di branding
plugin-service	Servizio (plug-in) di estendibilità
portal-service	Servizio del portale

Per eseguire il componente IaaS sono richiesti tutti i servizi elencati di seguito.

Tabella 1-15. Gruppo catalogo dei servizi (servizi di governance)

Servizio	Descrizione
notification-service	Servizio di notifica
workitem-service	Servizio elementi di lavoro
approval-service	Servizio di approvazione
catalog-service	Catalogo dei servizi

Tabella 1-16. Gruppo di servizi IaaS

Servizio	Descrizione
iaas-proxy-provider	Proxy IaaS
iaas-server	Macchina Windows di IaaS

Tabella 1-17. XaaS

Servizio	Descrizione
vco	vRealize Orchestrator
advanced-designer-service	Blueprint e azioni risorsa di XaaS

Utilizzo della registrazione di controllo di vRealize Automation

vRealize Automation offre la registrazione di controllo per supportare la raccolta e conservazione degli eventi di sistema importanti.

Attualmente, vRealize Automation supporta la registrazione di controllo come estensione della registrazione degli eventi. Questa funzionalità fornisce le informazioni di controllo di base e le impostazioni di conservazione sono configurabili solo utilizzando le chiamate appropriate al servizio del gestore eventi della REST API di vRealize Automation. La registrazione di controllo è attualmente disponibile per gli amministratori tenant e per gli amministratori di sistema che possono accedere ai tenant. Essa fornisce funzionalità di ricerca e filtro per gli eventi.

Per impostazione predefinita, vRealize Automation supporta la registrazione di controllo per gli eventi di creazione, aggiornamento ed eliminazione di sottoscrizione al workflow, endpoint e gruppi di strutture. vRealize Automation supporta anche la personalizzazione della registrazione di controllo per una varietà di eventi di IaaS.

La registrazione di controllo di vRealize Automation è disattivata per impostazione predefinita. È possibile attivarla o disattivarla utilizzando la casella di controllo **Abilitato** nella sezione dell'integrazione del registro di controllo nella pagina **vRA > Registri** dell'interfaccia di gestione dell'appliance virtuale.

Le informazioni del registro di controllo vengono visualizzate nella pagina standard dei registri eventi. Come amministratore tenant, selezionare **Amministrazione > Registri eventi** per visualizzare questa pagina. Gli eventi di controllo sono identificati nella tabella dei registri eventi con l'indicazione Controllo nel campo Tipo di evento. In ogni voce sono riportati una descrizione dell'evento per ciascun evento e tenant, data e ora, utente e nome del servizio correlato.

L'abilitazione della registrazione di controllo per altri eventi di IaaS richiede un file di configurazione personalizzato e l'esecuzione dei comandi appropriati sulla macchina host di IaaS. Rivolgersi ai Professional Services di VMware per assistenza.

È possibile configurare vRealize Automation per esportare gli eventi in un server syslog esterno, nello specifico VMware Log Insight.

Configurazione di vRealize Automation per la registrazione di controllo di Log Insight

È possibile configurare vRealize Automation per l'esportazione degli eventi di controllo in VMware Log Insight, in modo da semplificare la visualizzazione degli eventi di controllo.

La registrazione di controllo è disattivata per impostazione predefinita, ed è necessario abilitarla per generare e visualizzare gli eventi di registrazione di controllo.

Se utilizzato, SSL viene configurato nell'istanza di Appliance vRealize Automation in cui si trova l'agente Log Insight e riguarda la connessione al server Log Insight Syslog. Per utilizzare SSL, è necessario configurare i certificati e la connettività appropriati tra vRealize Automation e il server Log Insight installato nella distribuzione.

Prerequisiti

vRealize Automation utilizza l'agente di Log Insight installato per impostazione predefinita in una distribuzione di vRealize Automation per leggere le voci di registro per la visualizzazione in Log Insight.

Procedura

- 1 Accedere all'interfaccia di gestione dell'appliance virtuale come amministratore di sistema.
- 2 Selezionare **vRA > Registri**.
- 3 Verificare che sia selezionata la casella di controllo **Abilitato** per la registrazione di controllo sotto l'intestazione Integrazione registro di controllo.
- 4 Immettere il nome della macchina **Host** per il server di Log Insight sotto l'intestazione Configurazione agente di Log Insight.
 - a Immettere il nome della macchina **Host** dell'agente di Log Insight.
 - b Immettere la **Porta** da utilizzare per la comunicazione con l'agente di Log Insight.
 - c Selezionare il protocollo di comunicazione appropriato.
 - d Utilizzare la casella di controllo **SSL abilitato** per indicare se SSL verrà utilizzato per la comunicazione tra l'agente e il server Log Insight.

Se si sceglie di non utilizzare SSL, è possibile ignorare le altre impostazioni nella pagina. Se si utilizza SSL, è necessario configurare queste impostazioni.

- 5 Se si utilizza SSL, effettuare le selezioni appropriate nella sezione dei certificati radice attendibili SSL.

Per impostazione predefinita, l'istanza di Appliance vRealize Automation utilizza un certificato autofirmato. Se si desidera utilizzare un certificato radice attendibile, è necessario importarlo.

- a Selezionare la casella di controllo appropriata per indicare se si desidera utilizzare un nuovo certificato o un certificato esistente.

Per ulteriori informazioni, vedere le note nella pagina di configurazione della registrazione di vRealize Automation nell'interfaccia di gestione dell'appliance virtuale.

- 6 Fare clic su **Salva impostazioni**.
- 7 Effettuare le selezioni opportune nella sezione relativa ai certificati del server SSL.
- 8 Utilizzare la sezione relativa alla configurazione del comportamento dell'agente per configurare la modalità di funzionamento dell'agente con i file di registro.

Risultati

Gli eventi dei registri di controllo di vRealize Automation sono visibili dall'interfaccia di Log Insight.

Visualizzazione delle informazioni sugli host per i cluster nelle distribuzioni distribuite

Dalla console di gestione dell'appliance vRealize Automation è possibile raccogliere registri per tutti i nodi in cluster di una distribuzione distribuita.

È anche possibile visualizzare informazioni per ogni host nella distribuzione. La scheda **Cluster** della console di gestione di vRealize Automation contiene la tabella Informazioni distribuzione distribuita che riporta le seguenti informazioni:

- L'elenco di tutti i nodi presenti nella distribuzione
- Il nome host per il nodo. Il nome dell'host viene mostrato in forma di nome completo.
- Il tempo trascorso dall'ultima volta che l'host ha risposto alla console di gestione. I nodi dei componenti IaaS segnalano la disponibilità ogni tre minuti, mentre i nodi delle appliance virtuali ogni nove minuti.
- Il tipo di componente di vRealize Automation. Specifica se il nodo è un'appliance virtuale o un server IaaS.

Figura 1-1. tabella Informazioni distribuzione distribuita

	Host / Node Name	Version	Last Connected	Type	State*	Valid*
▶	cava-n-80-175.eng.vmware.com	7.5.0.378	7 minutes ago	MASTER	Up	<button>Delete</button>
▶	cava-n-85-043.eng.vmware.com	7.5.0.14528	14 seconds ago	IaaS		<button>Delete</button>

È possibile utilizzare questa tabella per monitorare l'attività nella distribuzione. Ad esempio, se la colonna Ultima connessione indica che un host non si è connesso di recente, l'informazione può essere indice di un problema con il server host.

Raccolta dei registri

È possibile creare un file ZIP contenente i file di registro per tutti gli host della distribuzione mediante il pulsante Crea bundle di supporto nella pagina **vRA > Registri**. Per ulteriori informazioni, vedere [Raccolta di registri per cluster e distribuzioni distribuite](#).

Rimozione di nodi dalla tabella

Quando si rimuove un host dalla distribuzione, rimuovere il nodo corrispondente dalla tabella Informazioni distribuzione distribuita per ottimizzare i tempi di raccolta registri. Fare clic sul pulsante **Elimina** per rimuovere un nodo dalla tabella.

Raccolta di registri per cluster e distribuzioni distribuite

Per supportare la risoluzione dei problemi e le attività di mantenimento dei dati, è possibile creare un file zip contenente tutti i file di registro dei server nella distribuzione.

La tabella Informazioni distribuzioni distribuite, nella scheda Cluster dell'interfaccia di gestione degli accessori virtuali, elenca i nodi a cui sono collegati i file di registro. È anche possibile eliminare i nodi da questa tabella.

Per informazioni correlate alla configurazione della distribuzione dell'appliance vRealize Automation, vedere *Installazione di vRealize Automation*.

Procedura

- 1 Accedere all'interfaccia di gestione dell'appliance virtuale come amministratore di sistema.
- 2 Fare clic su **vRA > Registri**.
- 3 Fare clic su **Crea bundle di supporto**.

I file registro vengono raccolti da tutti i nodi e copiati in un file ZIP.

Rimozione di un nodo dalla tabella Informazioni distribuzione distribuita

Eliminare un nodo quando si desidera rimuoverlo dal cluster della distribuzione o quando si sostituisce un certificato dell'agente di gestione.

La tabella Informazioni distribuzioni distribuite, nella scheda Cluster dell'interfaccia di gestione degli accessori virtuali, elenca i nodi del cluster applicabile. È possibile fare clic sul pulsante **Elimina** per qualsiasi nodo sulla tabella per rimuovere il nodo dal cluster oppure è possibile utilizzare la procedura seguente.

Procedura

- 1 Accedere all'appliance vRealize Automation con il nome utente **root** e la password specificata durante la distribuzione dell'appliance.
- 2 Fare clic sulla scheda **Cluster**.

La tabella Informazioni distribuzione distribuita mostra un elenco di nodi per la distribuzione distribuita.

- 3 Individuare l'ID del nodo da eliminare aprendo un prompt dei comandi ed eseguendo il comando seguente:

```
/usr/sbin/vcac-config cluster-config-node --action list
```

- 4 Individuare l'ID del nodo, ad esempio `cafe.node.46686239.17144`, nell'output JSON.

- 5 Aprire un prompt dei comandi e digitare un comando nel formato seguente, utilizzando l'ID del nodo ottenuto nel passaggio precedente.

```
/usr/sbin/vcac-config cluster-config-node
--action delete --id node-UID
```

Immettere, ad esempio, il comando seguente per l'ID del nodo di esempio `cafe.node.46686239.17144`:

```
/usr/sbin/vcac-config cluster-config-node --action delete --id cafe.node.46686239.17144
```

- 6 Fare clic su **Aggiorna**.

Il nodo non viene più visualizzato.

Monitoraggio dell'integrità di vRealize Automation

Il servizio di integrità di vRealize Automation valuta l'integrità funzionale di un ambiente di vRealize Automation.

Gli amministratori IaaS configurano il servizio di integrità per l'esecuzione delle suite di prove che determinano se i componenti sono registrati e le risorse necessarie sono disponibili. Questa tabella illustra le suite di prove fornite dal servizio di integrità e alcune prove di esempio per ciascuna suite.

Suite di test del servizio di integrità	Test di esempio
Test di sistema per vRealize Automation	<ul style="list-style-type: none"> ■ Test della connessione SSO/Identity VA ■ Controllo della licenza di vRealize Automation - La licenza è scaduta? ■ Controllo della password root dell'appliance virtuale di vRealize Automation - La password sta per scadere?
Test dei tenant per vRealize Automation	<ul style="list-style-type: none"> ■ Controllo dei percorsi di storage delle prenotazioni di vSphere ■ Controllo del criterio di prenotazione per le assegnazioni delle prenotazioni ■ Controllo dello stato del servizio del portale
Test per vRealize Orchestrator	<ul style="list-style-type: none"> ■ Controllo del numero di vRO attivi ■ Controllo dell'utilizzo dell'heap della memoria Java nei nodi vRO ■ Controllo dello stato del servizio del server vRO nei nodi vRO

Dopo l'esecuzione di una suite di prove in una macchina virtuale, il servizio di integrità indica il numero di prove superate e di quelle non riuscite. Per ogni prova con esito negativo, il servizio di integrità fornisce questi collegamenti:

Collegamento	Contenuto
Causa	Spiegazione del motivo per cui il test non è riuscito.
Correzione	Informazioni utilizzabili per risolvere il problema.

È possibile configurare il servizio di integrità per l'esecuzione dei test in base a una pianificazione o solo su richiesta.

È inoltre possibile utilizzare Python per creare test personalizzati. Consultare la *guida all'estendibilità del servizio integrità di vRealize Automation*.

Gli amministratori tenant con il ruolo di consumatori del servizio di integrità possono visualizzare i risultati dei test per la propria tenancy ma non possono configurare né eseguire un test.

Configurazione di prove di sistema per vRealize Automation

Un **amministratore IaaS** può configurare il servizio di integrità per eseguire prove di sistema in un'appliance virtuale vRealize Automation selezionata. Queste prove determinano se i componenti, come la licenza di vRealize Automation, sono registrati e se le risorse necessarie, come la memoria, sono disponibili nell'appliance virtuale. Quando si configurano prove di sistema, le prove vengono visualizzate nella scheda Prova della pagina Integrità.

Per configurare il servizio di integrità per l'esecuzione di prove di sistema per vRealize Automation, procedere come segue.

Prerequisiti

Accedere a vRealize Automation come **amministratore IaaS**.

Procedura

- 1 Selezionare **Amministrazione > Integrità**.
- 2 Fare clic su **Nuova configurazione**.
- 3 Nella pagina dei dettagli della configurazione, fornire le informazioni richieste.

Opzione	Descrizione
Nome	Il titolo per questa configurazione. Questo titolo viene visualizzato nella scheda Prova.
Descrizione	Descrizione della suite di prove.
Prodotto	Selezionare vRealize Automation.
Pianificazione	Selezionare la frequenza con cui viene eseguita la suite di prove.

- 4 Fare clic su **Avanti**.
- 5 Nella pagina di selezione delle suite di prova, selezionare **Prove di sistema per vRealize Automation**.

6 Fare clic su **Avanti**.

7 Nella pagina dei parametri di configurazione, fornire le informazioni richieste.

Tabella 1-18. Appliance virtuale vRealize Automation

Opzione	Descrizione
Indirizzo server Web pubblico	<ul style="list-style-type: none"> ■ Per una distribuzione minima, l'URL di base per l'host dell'appliance vRealize Automation. Ad esempio, <code>https://va-host.domain/</code>. ■ Per una distribuzione ad alta disponibilità, l'URL di base per il servizio di bilanciamento del carico di vRealize Automation. Ad esempio, <code>https://load-balancer-host.domain/</code>.
Indirizzo console SSH	Nome di dominio completo dell'appliance vRealize Automation. Ad esempio, <code>va-host.domain</code> .
Utente console SSH	root
Password console SSH	La password root.

Tabella 1-19. Tenant di sistema vRealize Automation

Opzione	Descrizione
Amministratore tenant di sistema	administrator
Password tenant di sistema	La password dell'amministratore.

Tabella 1-20. Monitoraggio dello spazio su disco di vRealize Automation

Opzione	Descrizione
Percentuale soglia di avviso	Percentuale accettabile di spazio su disco dell'appliance virtuale utilizzata prima di ottenere un errore della prova di avviso.
Percentuale soglia critica	Percentuale accettabile di spazio su disco dell'appliance virtuale utilizzata prima di ottenere un errore della prova critica.

8 Fare clic su **Avanti**.

9 Vedere le informazioni nella pagina Riepilogo.

10 Fare clic su **Fine**.

Le prove vengono eseguite in base alla pianificazione selezionata.

Operazioni successive

[Visualizzazione dei risultati della suite di test del servizio di integrità di vRealize Automation](#)

Configurazione di prove di tenant per vRealize Automation

Un **amministratore IaaS** può configurare il servizio di integrità per eseguire prove dei tenant in un'appliance virtuale vRealize Automation selezionata. Queste prove determinano se i componenti relativi al tenant, come i servizi software, sono registrati e se le risorse necessarie, come le macchine virtuali vSphere, sono disponibili nell'appliance virtuale. Quando si configurano prove dei tenant, le prove vengono visualizzate nella scheda Prova della pagina Integrità.

Per configurare il servizio di integrità per l'esecuzione di prove dei tenant per vRealize Automation, procedere come segue.

Prerequisiti

Accedere a vRealize Automation come **amministratore IaaS**.

Procedura

- 1 Selezionare **Amministrazione > Integrità**.
- 2 Fare clic su **Nuova configurazione**.
- 3 Nella pagina dei dettagli della configurazione, fornire le informazioni richieste.

Opzione	Descrizione
Nome	Il titolo per questa configurazione. Questo titolo viene visualizzato nella scheda Prova.
Descrizione	Una descrizione delle prove.
Prodotto	Selezionare vRealize Automation.
Pianificazione	Selezionare la frequenza di esecuzione delle prove.

- 4 Fare clic su **Avanti**.
- 5 Nella pagina di selezione delle suite di prova, selezionare **Prove di tenant per vRealize Automation**.
- 6 Fare clic su **Avanti**.
- 7 Nella pagina dei parametri di configurazione, fornire le informazioni richieste.

Tabella 1-21. Appliance virtuale vRealize Automation

Opzione	Descrizione
Indirizzo Web di vRealize Automation	<ul style="list-style-type: none"> ■ Per una distribuzione minima, l'URL di base per l'host dell'appliance vRealize Automation. Ad esempio, <code>https://va-host.domain/</code>. ■ Per una distribuzione ad alta disponibilità, l'URL di base per il servizio di bilanciamento del carico di vRealize Automation. Ad esempio, <code>https://load-balancer-host.domain/</code>.
Indirizzo console SSH	Nome di dominio completo dell'host SSH. Ad esempio, <code>ssh-host.domain</code> .

Tabella 1-21. Appliance virtuale vRealize Automation (continua)

Opzione	Descrizione
Utente console SSH	root
Password console SSH	Password root.
Tempo di risposta massimo del servizio (ms)	Quantità di tempo massima, espressa in millisecondi, per cui il sistema attende una risposta.

Tabella 1-22. Tenant vRealize Automation

Opzione	Descrizione
Tenant in prova	qe
Nome utente amministratore struttura	Nome dell'utente amministratore della struttura Nota L'amministratore della struttura deve anche disporre di un ruolo di amministratore tenant e di amministratore laaS nell'ordine per tutte le prove da eseguire.
Password amministratore struttura	Password per l'amministratore della struttura.

Tabella 1-23. Tenant di sistema vRealize Automation

Opzione	Descrizione
Amministratore tenant di sistema	administrator
Password tenant di sistema	Password per l'amministratore.

Tabella 1-24. Monitoraggio dello spazio su disco di vRealize Automation

Opzione	Descrizione
Percentuale soglia critica	Percentuale accettabile di spazio su disco dell'appliance virtuale utilizzata prima di ottenere un errore della prova critica.

- 8 Fare clic su **Avanti**.
- 9 Vedere le informazioni nella pagina Riepilogo.
- 10 Fare clic su **Fine**.

Le prove vengono eseguite in base alla pianificazione selezionata.

Operazioni successive

[Visualizzazione dei risultati della suite di test del servizio di integrità di vRealize Automation](#)

Configurazione di prove per vRealize Orchestrator

Un **amministratore IaaS** può configurare il servizio di integrità per eseguire prove per vRealize Orchestrator nell'host vRealize Orchestrator. Queste prove verificano che i componenti, come il servizio vro-server, siano registrati e le risorse necessarie, come un heap di memoria Java sufficiente, siano disponibili nella macchina host. Quando si configurano le prove di vRealize Orchestrator, le prove vengono visualizzate nella scheda Prova della pagina Integrità.

Prerequisiti

Accedere a vRealize Automation come **amministratore IaaS**.

Procedura

- 1 Selezionare **Amministrazione > Integrità**.
- 2 Fare clic su **Nuova configurazione**.
- 3 Nella pagina dei dettagli della configurazione, fornire le informazioni richieste.

Opzione	Descrizione
Nome	Il titolo per questa configurazione. Questo titolo viene visualizzato nella scheda Prova.
Descrizione	Una descrizione delle prove.
Prodotto	Selezionare vRealize Orchestrator.
Pianificazione	Selezionare la frequenza di esecuzione delle prove.

- 4 Fare clic su **Avanti**.
- 5 Nella pagina di selezione delle suite di prova, selezionare **Prove per vRealize Orchestrator**.
- 6 Fare clic su **Avanti**.
- 7 Nella pagina dei parametri di configurazione, fornire le informazioni richieste.

Tabella 1-25. Bilanciamento del carico/host vRealize Orchestrator

Opzione	Descrizione
Indirizzo client	<ul style="list-style-type: none"> ■ Per una distribuzione minima, si tratta del nome di dominio completo dell'host vRealize Orchestrator. Ad esempio, <i>vro-host.domain</i>. ■ Per una distribuzione ad alta disponibilità, si tratta dell'URL di base per il servizio di bilanciamento del carico di vRealize Orchestrator, https://load-balancer-host.domain/.
Nome utente client	administrator
Password client	La password dell'amministratore.
Nome utente console SSH	root

Tabella 1-25. Bilanciamento del carico/host vRealize Orchestrator (continua)

Opzione	Descrizione
Password console SSH	La password root.
Soglia utilizzo heap	Percentuale accettabile di spazio di heap utilizzata prima di ottenere un errore della prova di avviso.

Tabella 1-26. Istanze di vRealize Orchestrator dietro il bilanciamento del carico

Opzione	Descrizione
Indirizzo console SSH	Indirizzo IP o URL dell'istanza di vRealize Orchestrator dietro il bilanciamento del carico.
Nome utente console SSH	Nome utente con accesso a questa istanza.
Password console SSH	La password del nome utente.

- Fare clic su **Aggiungi** per aggiungere un'altra istanza di vRealize Orchestrator all'elenco.
- Fare clic su **Rimuovi** per rimuovere dall'elenco di istanze dietro il bilanciamento del carico un'istanza di vRealize Orchestrator selezionata.

8 Fare clic su **Avanti**.

9 Vedere le informazioni nella pagina Riepilogo.

10 Fare clic su **Fine**.

Le prove vengono eseguite in base alla pianificazione selezionata.

Operazioni successive

[Visualizzazione dei risultati della suite di test del servizio di integrità di vRealize Automation](#)

Suite di prove personalizzate

È possibile utilizzare Python per creare una suite di prove personalizzate per il servizio integrità di vRealize Automation.

La creazione di una suite di prove personalizzate consente di estendere le prove fornite per il servizio di integrità aggiungendo una suite di prove per determinare l'integrità dei componenti aggiuntivi di vRealize Automation. Per informazioni sulla creazione di una suite di prove personalizzate, vedere la *guida all'estendibilità del servizio integrità di vRealize Automation*.

Aggiunta di una suite di prove personalizzate

Affinché sia possibile eseguire la suite di prove, un **amministratore IaaS** deve aggiungerla al servizio di integrità di vRealize Automation.

Per aggiungere una suite di prove personalizzate per un asset di vRealize Automation, procedere come segue.

Prerequisiti

- Creare una wheel Python per i file della suite di prove personalizzate. Per informazioni, vedere la *Guida all'estensibilità del servizio di integrità vRealize Automation*.
- Accedere a vRealize Automation come **amministratore IaaS**.

Procedura

- 1 Fare clic su **Amministrazione > Integrità**.
- 2 In alto a destra, fare clic sull'icona a forma di ingranaggio e selezionare **Estensibilità**.
- 3 Fare clic su **Nuovo asset**.
- 4 Nella finestra di dialogo Aggiungi asset, fornire le informazioni richieste.

Opzione	Descrizione
Titolo asset	Nome e numero di versione della suite di prove che si sta eseguendo, ad esempio Infoblox 1.0.
Descrizione asset	Descrizione delle prove contenute nella wheel Python.
Versione asset	Numero di versione della suite di test.
File asset	Fare clic su Scegli file e selezionare il file della suite di prove personalizzate.

- 5 Fare clic su **Aggiungi**.

Alla tabella dell'asset viene aggiunta una nuova riga con lo stato UPLOADED. Quando lo stato passa a INSTALLED, la suite di prove è pronta per l'utilizzo. Se il processo di installazione non riesce, viene visualizzato un popup che spiega il motivo.

Nota Se la pagina non viene aggiornata, fare clic sull'icona di aggiornamento.

Operazioni successive

[Esecuzione di una suite di prove personalizzate.](#)

Esecuzione di una suite di prove personalizzate

Un **amministratore IaaS** può configurare il servizio di integrità per eseguire una suite di prove personalizzate nell'ambiente vRealize Automation. Quando si configura la suite di prove personalizzate, la suite di prove viene visualizzata nella scheda Prova della pagina Integrità.

Per configurare il servizio di integrità in modo che esegua una suite di prove personalizzate per vRealize Automation, completare la seguente procedura.

Prerequisiti

- [Aggiunta di una suite di prove personalizzate.](#)
- Accedere a vRealize Automation come **amministratore IaaS**.

Procedura

- 1 Selezionare **Amministrazione > Integrità**.
- 2 Fare clic su **Nuova configurazione**.
- 3 Nella pagina dei dettagli della configurazione, fornire le informazioni richieste.

Opzione	Descrizione
Nome	Il titolo per questa configurazione. Questo titolo viene visualizzato nella scheda Prova.
Descrizione	Descrizione della suite di prove.
Prodotto	Selezionare il prodotto che si desidera provare dal menu a discesa Prodotto .
Pianificazione	Selezionare la frequenza con cui si desidera eseguire la suite di prove.

- 4 Fare clic su **Avanti**.
- 5 Nella pagina per la selezione delle suite di prove, selezionare la suite di prove personalizzata e fare clic su **Avanti**.
- 6 Nella pagina per la configurazione dei parametri, inserire le informazioni richieste e fare clic su **Avanti**.
- 7 Nella pagina Riepilogo, esaminare le informazioni e fare clic su **Fine**.

La suite di prove personalizzate viene eseguita in base alla pianificazione selezionata.

Operazioni successive

[Visualizzazione dei risultati della suite di test del servizio di integrità di vRealize Automation](#)

Visualizzazione dei risultati della suite di test del servizio di integrità di vRealize Automation

È possibile visualizzare i risultati delle prove del servizio di integrità dopo l'esecuzione di tali prove.

Nella pagina Integrità ogni suite di test configurata viene visualizzata come una scheda di test. Quando si esegue una suite di test, il risultato viene visualizzato al centro della scheda.

Le schede di test visualizzate nella pagina Integrità vengono filtrate in base al privilegio dell'utente.

- Gli amministratori IaaS possono visualizzare tutte le schede dei test.
- Gli amministratori tenant con il ruolo di consumatore del servizio di integrità possono visualizzare solo la scheda dei test relativi alla propria tenancy.

Prerequisiti

- La suite di prove configurata è stata eseguita in base alla pianificazione.

- Accedere alla console di vRealize Automation come **amministratore laaS** o come **amministratore tenant**.

Procedura

- 1 Selezionare **Amministrazione > Integrità**.
- 2 Se una prova non è pianificata per l'esecuzione, fare clic su **Esegui** nella scheda Prova.
- 3 Fare clic al centro di una scheda Prova dopo l'esecuzione delle prove.

Verrà visualizzata una pagina che mostra lo stato di ogni test. Per visualizzare il motivo per cui un test non è riuscito, fare clic su **Causa**. Per aprire un argomento che spieghi come risolvere il problema, fare clic sul collegamento **Correzione**, se ne è disponibile uno.

Risoluzione dei problemi del servizio di integrità

Gli argomenti relativi alla risoluzione dei problemi del servizio di integrità offrono soluzioni alle problematiche che potrebbero verificarsi durante l'uso di questo servizio.

Test dello stato di un servizio con esito negativo

È possibile correggere il test di un servizio con esito negativo modificando l'impostazione della pianificazione del test.

Problema

Se il test dello stato di un servizio ha esito negativo e si fa clic su **Causa**, viene visualizzato il messaggio: **Impossibile stabilire connessione SSH; Messaggio eccezione: [Aut. non riuscita]**.

Causa

Quando la suite di test è pianificata per l'esecuzione ogni 15 minuti, l'accesso al sistema blocca l'account dell'utente root.

Soluzione

- ◆ Modificare la pianificazione del test impostandola su **Nessuna**, attendere 15 minuti ed eseguire di nuovo il test.

Dopo l'aggiornamento la pagina Integrità nella console dell'appliance risulta vuota

Dopo l'aggiornamento di vRealize Automation, la pagina Integrità nella console dell'appliance risulta vuota.

Problema

Il servizio integrità non viene avviato dopo l'aggiornamento.

Soluzione

- ◆ Su ogni appliance virtuale vRealize Automation, aprire un prompt dei comandi come **root** ed eseguire questi comandi.
 - a Per configurare l'avvio automatico del servizio integrità, eseguire questo comando.

```
chkconfig vrhb-service on
```
 - b Per avviare il servizio integrità in questa appliance virtuale, eseguire questo comando.

```
service vrhb-service start
```

Monitoraggio delle risorse dell'ambiente vRealize Automation tramite SNMP

In qualità di amministratore di sistema che ha familiarità con SNMP, si desidera utilizzare la REST API di vRealize Automation per vSNMP per semplificare il monitoraggio dei nodi di vRealize Automation. Se si utilizza vSNMP, è possibile usare SNMP affinché funga da sistema di preavviso crittografato quando vRealize Automation sta per esaurire la CPU, la RAM o lo spazio su disco, per evitare rallentamenti.

È possibile monitorare manualmente gli OID SNMP oppure monitorare attivamente le risorse impostando trap SNMP.

Ad esempio, se vSNMP invia un evento, come "Rilevato utilizzo elevato della CPU", è possibile iniziare a raccogliere informazioni sui processi che utilizzano la CPU e determinare quale sta utilizzando risorse eccessive. È quindi possibile correlare le informazioni sulla CPU, sulla memoria e sugli altri utilizzi per la risoluzione di ulteriori problemi.

Se si usa vRealize Automation vSNMP, è possibile esporre l'intera struttura di Linux per il monitoraggio e il recupero dei dati utilizzando la REST API oppure il daemon vSNMPD in esecuzione nelle istanze di vRealize Automation.

vRealize Automation SNMP non dispone di un'interfaccia di uso generico. È necessario utilizzare i comandi della REST API o del daemon.

Per ulteriori informazioni, vedere "Utilizzo di SNMP per monitorare vRealize Automation" nella Guida alla programmazione di vRealize Automation. Per individuare la Guida alla programmazione, consultare la [documentazione relativa all'API di vRealize Automation](#) e selezionare il collegamento della versione.

Monitoraggio e gestione delle risorse

I diversi ruoli di vRealize Automation monitorano l'utilizzo delle risorse e gestiscono l'infrastruttura in modi diversi.

Scelta di uno scenario di monitoraggio delle risorse

Amministratori di struttura, amministratori tenant e manager dei gruppi di business hanno preoccupazioni differenti quando si tratta di monitorare le risorse. Per questo motivo, vRealize Automation consente di monitorare aspetti differenti dell'uso delle risorse.

Un amministratore di struttura, ad esempio, si preoccupa di monitorare il consumo di risorse delle prenotazioni e le risorse di elaborazione, mentre un amministratore tenant è interessato all'uso delle risorse dei gruppi di provisioning all'interno di un tenant. In base al ruolo e all'uso specifico di risorse da monitorare, vRealize Automation mette a disposizione diversi modi per tenere traccia del consumo di risorse.

Tabella 1-27. Scelta di uno scenario di monitoraggio delle risorse

Scenario di monitoraggio risorse	Privilegi richiesti	Posizione
Monitorare la quantità di storage fisico e memoria sulle risorse di elaborazione attualmente consumata e determinare la quantità libera rimanente. È possibile anche monitorare il numero di macchine riservate e allocate di cui è stato eseguito il provisioning su ogni risorsa di elaborazione.	Amministratore struttura (monitoraggio dell'uso su risorse di elaborazione nel proprio gruppo di strutture)	Infrastruttura > Risorse di elaborazione > Risorse di elaborazione
Monitorare macchine attualmente fornite in provisioning e sotto la gestione di vRealize Automation.	Amministratore struttura	Infrastruttura > Macchine > Macchine gestite
Monitorare la quantità di storage, memoria e quota macchina della prenotazione attualmente allocata e determinare la capacità rimanente disponibile per la prenotazione.	Amministratore struttura (monitoraggio dell'uso di risorse per prenotazioni su risorse di elaborazione e macchine fisiche)	Infrastruttura > Prenotazioni > Prenotazioni
Monitorare la quantità di storage, memoria e quota macchina che i gruppi di business stanno attualmente consumando e determinare la capacità rimanente in riserva per essi.	<ul style="list-style-type: none"> ■ Amministratore tenant (monitoraggio dell'uso delle risorse per tutti i gruppi del proprio tenant) ■ Manager gruppo di business (monitoraggio dell'uso delle risorse per i gruppi che gestisce) 	Amministrazione > Utenti e gruppi > Gruppi di business

Terminologia sull'utilizzo delle risorse

vRealize Automation adotta una terminologia esplicita per distinguere tra risorse disponibili, risorse che sono state riservate per usi specifici e risorse correntemente e attivamente utilizzate dalle macchine con provisioning eseguito.

Nella tabella Terminologia sull'utilizzo delle risorse sono spiegati i termini utilizzati da vRealize Automation per mostrare l'uso delle risorse.

Tabella 1-28. Terminologia sull'utilizzo delle risorse

Termine	Descrizione
Fisica	Indica la capacità effettiva di memoria o di storage di una risorsa di elaborazione.
Riservata	Indica la capacità di quota macchina, memoria e storage riservata per una prenotazione. Se ad esempio una risorsa di elaborazione ha una capacità fisica di 600 GB e per essa sono presenti tre prenotazioni di 100 GB ognuna, lo storage riservato della risorsa di elaborazione è pari a 300 GB e lo storage riservato è pari al 50 per cento.
Gestito	Indica che una macchina con provisioning eseguito e attualmente sotto la gestione di vRealize Automation.
Allocata	Indica le risorse di quota macchina, memoria e storage correntemente e attivamente utilizzate dalle macchine con provisioning eseguito. Si consideri ad esempio una prenotazione con quota macchina pari a 10. Se per la prenotazione ci sono 15 macchine con provisioning eseguito, ma solo 6 di esse sono attualmente accese, la quota macchina è allocata per il 60 per cento.
In uso	Il valore della colonna In uso è sempre uguale al valore della colonna Allocata .
Libero	Indica la capacità fisica inutilizzata in un percorso di storage.

Connessione a una macchina cloud

Alla prima connessione a una macchina cloud è necessario effettuare l'accesso come amministratore.

Si possono quindi aggiungere le credenziali con cui si intende accedere alla console di vRealize Automation come utente della macchina, dopodiché sarà possibile accedere con le proprie credenziali vRealize Automation.

Importante se si utilizzano i Amazon Web Services, i protocolli RDP o SSH devono essere attivati sull'istanza della macchina Amazon e le macchine devono trovarsi in un gruppo di sicurezza nel quale siano aperte le porte corrette.

Raccolta delle credenziali degli utenti per una macchina Amazon

Per accedere a una macchina Amazon in qualità di amministratore, è necessario ottenere la password di amministratore della macchina.

La password di amministratore è disponibile nella pagina dei dettagli Informazioni macchina. Se l'immagine della macchina Amazon dalla quale è stato eseguito il provisioning della macchina non è configurata per generare la password di amministratore a ogni avvio, sarà necessario trovare la password utilizzando una tecnica alternativa. Per informazioni su come ottenere in modo alternativo la password di amministratore, cercare gli argomenti correlati alla *connessione alle istanze Amazon EC2* nella documentazione di Amazon.

Se necessario, è possibile creare le credenziali utente di vRealize Automation richieste. Queste diventano quindi valide per ogni successivo accesso a tale macchina.

Prerequisiti

- Il provisioning della macchina Amazon è già stato eseguito.
- Accedere a vRealize Automation come proprietario macchina, **manager del gruppo di business** o **utente di supporto**.
- Sulla macchina Amazon è attivo uno dei protocolli RDP o SSH, che sarà utilizzato per il provisioning.
- Le macchine si trovano in un gruppo di sicurezza in cui le porte appropriate sono aperte.

Procedura

- 1 Passare alla pagina **Elementi** e filtrare per ottenere solo i gruppi sotto la propria gestione o un gruppo specifico.

- 2 Selezionare la macchina Amazon nell'elenco delle macchine.

È possibile scegliere **Visualizza dettagli** nel menu a discesa **Azioni** per visualizzare i dettagli quali ad esempio il tipo di macchina.

- 3 Selezionare **Modifica** dal menu a discesa **Azioni**.

- 4 Fare clic su **Mostra password amministratore** per ottenere la password di amministratore della macchina.

In alternativa, è possibile ottenere la password utilizzando una procedura di Amazon esterna.

- 5 Scegliere **Connessione con RDP** dal menu a discesa **Azioni**.

- 6 Quando vengono richieste le credenziali di accesso, fare clic su **Usa un altro account**.

- 7 Quando viene richiesto il nome utente, digitare **LOCAL\Administrator**.

- 8 Quando viene richiesta, digitare la password di amministratore.

- 9 Fare clic su **OK**.

In questo modo si accederà alla macchina come amministratore.

- 10 Aggiungere le proprie credenziali di vRealize Automation. Ad esempio, su una macchina server Windows, aprire Server Manager, selezionare **Configurazione > Utenti e gruppi locali** e aggiungere le proprie credenziali nel formato **DOMINIO\nomeutente**, al gruppo **Utenti desktop remoto**.

A questo punto, il nome utente e la password di vRealize Automation rappresentano credenziali valide per gli accessi successivi alla macchina.

- 11 Disconnettersi dalla macchina Amazon.

- 12 Scegliere **Connessione con RDP** dal menu a discesa **Azioni**.

- 13 Quando viene richiesto di accedere, digitare il nome utente e la password di vRealize Automation per accedere alla macchina.

Risultati

I proprietari della macchina possono ora accedere utilizzando le proprie credenziali vRealize Automation.

Raccolta delle credenziali degli utenti per una macchina vCloud

Per accedere come amministratore a una macchina vCloud Air o vCloud Director, è necessario conoscere la password di amministratore di tale macchina.

La password di amministratore è disponibile nella pagina dei dettagli Informazioni macchina. Se l'immagine della macchina da cui è stato eseguito il provisioning non è configurata per generare la password di amministratore a ogni avvio, è possibile recuperare la password tramite una tecnica alternativa. Per informazioni su come ottenere la password di amministratore mediante altri metodi, vedere la documentazione di vCloud Air o vCloud Director.

Se necessario, è possibile creare le credenziali utente di vRealize Automation richieste. Queste diventano quindi valide per ogni successivo accesso a tale macchina.

Prerequisiti

- È già stato eseguito il provisioning della macchina vCloud Air o vCloud Director.
- Accedere a vRealize Automation come proprietario macchina, **manager del gruppo di business** o **utente di supporto**.
- RDP o SSH è attivo sull'immagine della macchina vCloud Air o vCloud Director che verrà utilizzata per il provisioning.
- Le macchine si trovano in un gruppo di sicurezza in cui le porte appropriate sono aperte.

Procedura

1 Passare alla pagina **Elementi** e filtrare per ottenere solo i gruppi sotto la propria gestione o un gruppo specifico.

2 Selezionare la macchina vCloud Air o vCloud Director nell'elenco delle macchine.

È possibile scegliere **Visualizza dettagli** nel menu a discesa **Azioni** per visualizzare i dettagli quali ad esempio il tipo di macchina.

3 Selezionare **Modifica** dal menu a discesa **Azioni**.

4 Fare clic su **Mostra password amministratore** per ottenere la password di amministratore della macchina.

In alternativa, è possibile ottenere la password mediante una procedura esterna di vCloud Air o vCloud Director.

5 Scegliere **Connessione con RDP** dal menu a discesa **Azioni**.

6 Quando vengono richieste le credenziali di accesso, fare clic su **Usa un altro account**.

7 Quando viene richiesto il nome utente, digitare **LOCAL\Administrator**.

8 Quando viene richiesta, digitare la password di amministratore.

9 Fare clic su OK.

In questo modo si accederà alla macchina come amministratore.

10 Aggiungere le proprie credenziali di vRealize Automation. Ad esempio, su una macchina server Windows, aprire Server Manager, selezionare **Configurazione > Utenti e gruppi locali e aggiungere le proprie credenziali nel formato **DOMINIO\nomeutente**, al gruppo **Utenti desktop remoto**.**

A questo punto, il nome utente e la password di vRealize Automation rappresentano credenziali valide per gli accessi successivi alla macchina.

11 Disconnettersi dalla macchina vCloud Air o vCloud Director.**12 Scegliere **Connessione con RDP** dal menu a discesa **Azioni**.****13 Quando viene richiesto di accedere, digitare il nome utente e la password di vRealize Automation per accedere alla macchina.****Risultati**

I proprietari della macchina possono ora accedere utilizzando le proprie credenziali vRealize Automation.

Riduzione dell'utilizzo delle prenotazioni per termine naturale

Gli amministratori di struttura possono ridurre sul lungo termine il numero di macchine su una particolare prenotazione, mantenendo al tempo stesso attive la prenotazione e le macchine esistenti che da essa sono state fornite in provisioning.

È possibile ridurre la quota macchina riservata, la memoria e lo storage di una prenotazione virtuale al di sotto della quantità correntemente allocata. Questo consente di continuare la gestione delle macchine esistenti senza cambiamenti, evitando al tempo stesso il provisioning di nuove macchine finché l'allocazione resta al di sotto della nuova quantità riservata.

Nota poiché le macchine virtuali spente non sono incluse nella memoria allocata e nei totali delle quote di macchine, la riduzione della memoria o dell'allocazione di macchine di una prenotazione potrebbe impedire alle macchine correntemente spente di riaccendersi.

Si consideri ad esempio un gruppo di business con una prenotazione che contiene 20 macchine fornite in provisioning, impostate per scadere nei successivi 90 giorni. Se si desidera ridurre per termine naturale questa prenotazione a non più di 15 macchine, è possibile modificare la prenotazione per ridurre la quota da 20 macchine a 15. Non sarà possibile eseguire il provisioning di altre macchine sulla prenotazione finché il numero di macchine sulla prenotazione non si ridurrà naturalmente con il sopraggiungere delle scadenze.

Rimozione delle autorizzazione da un percorso di storage

Se si stanno rimuovendo le autorizzazioni da un percorso di storage e spostando macchine in un nuovo percorso, è necessario che un amministratore di struttura disattivi il percorso di storage in vRealize Automation.

L'elenco che segue è una panoramica ad alto livello della sequenza di passaggi necessari per rimuovere le autorizzazioni da un percorso di storage:

- 1 Un amministratore di struttura disattiva il percorso di storage su tutte le prenotazioni che lo utilizzano. Vedere [Disattivazione di un percorso di storage](#).
- 2 Spostare la macchina in un percorso di storage nuovo esterno a vRealize Automation.
- 3 Attendere che vRealize Automation esegua automaticamente la raccolta dati dell'inventario o avviare manualmente la raccolta dati dell'inventario. Vedere [Configurazione della raccolta dati delle risorse di elaborazione](#).

Disattivazione di un percorso di storage



Gli amministratori di struttura possono disattivare i percorsi di storage nelle prenotazioni quando si rimuovono le autorizzazioni dai percorsi di storage.

Nota Per ogni prenotazione in cui si disattiva un percorso di storage, verificare che vi sia spazio rimanente sufficiente negli altri percorsi di storage abilitati.

Prerequisiti

Accedere a vRealize Automation come **amministratore di struttura**.

Procedura

- 1 Selezionare **Infrastrutture > Prenotazioni > Prenotazioni**.
- 2 Selezionare la prenotazione in cui è utilizzato il percorso di storage da cui si stanno rimuovendo le autorizzazioni e fare clic su **Modifica**.
- 3 Fare clic sulla scheda **Risorse**.
- 4 Individuare il percorso di storage da cui si stanno rimuovendo le autorizzazioni.
- 5 Fare clic sull'icona **Modifica** (.
- 6 Selezionare la casella di controllo nella colonna Disattivato per disattivare il percorso di storage.
- 7 Fare clic sull'icona **Salva** (.
- 8 Fare clic su **OK**.
- 9 Ripetere questa procedura per tutte le prenotazioni che utilizzano il percorso di storage da cui si stanno rimuovendo le autorizzazioni.

Raccolta dati

vRealize Automation raccoglie i dati dagli endpoint di origine delle infrastrutture e dalle relative risorse di elaborazione.

La raccolta dei dati viene effettuata a intervalli regolari. Ogni tipo di raccolta dati ha un intervallo predefinito che è possibile sostituire o modificare. Ogni tipo di raccolta dati presenta anche un intervallo di timeout predefinito che è possibile sostituire o modificare.

Gli amministratori di IaaS possono inizializzare manualmente la raccolta dei dati per gli endpoint dell'origine delle infrastrutture e gli amministratori di struttura fanno altrettanto per le risorse di elaborazione.

Tabella 1-29. Tipi di raccolta dati

Tipo di raccolta dati	Descrizione
Raccolta dati per gli endpoint dell'origine delle infrastrutture	<p>Aggiorna le informazioni sugli host di virtualizzazione, i modelli e le immagini ISO per gli ambienti di virtualizzazione. Aggiorna i modelli e i virtual data center per vCloud Director. Aggiorna le regioni e le macchine Amazon con provisioning nelle regioni Amazon.</p> <p>La raccolta dati degli endpoint viene eseguita ogni 4 ore.</p>
Raccolta dati dell'inventario	<p>Aggiorna il record delle macchine virtuali il cui uso della risorsa è legato a una risorsa di elaborazione specifica, incluse informazioni dettagliate su reti, storage e macchine virtuali. Questo record include inoltre informazioni sulle macchine virtuali non gestite, che sono macchine sottoposte a provisioning fuori da vRealize Automation.</p> <p>La raccolta dati degli inventari viene eseguita ogni 24 ore. L'intervallo di timeout predefinito per la raccolta dati degli inventari è di 2 ore.</p>
Raccolta dati dello stato	<p>Aggiorna il record dello stato di alimentazione di ciascuna macchina individuato tramite la raccolta dati dell'inventario. La raccolta dati dello stato registra inoltre le macchine mancanti che vRealize Automation gestisce ma che non possono essere rilevate nell'endpoint cloud o nella risorsa di elaborazione della virtualizzazione.</p> <p>La raccolta dati degli stati viene eseguita ogni 15 minuti. L'intervallo di timeout predefinito per la raccolta dati degli stati è di 1 ora.</p>
Raccolta dati delle prestazioni (solo risorse di elaborazione vSphere)	<p>Aggiorna il record dell'uso medio di CPU, storage, memoria e rete per ogni macchina virtuale individuata tramite la raccolta di dati dell'inventario.</p> <p>La raccolta dati delle prestazioni viene eseguita ogni 24 ore.</p> <p>L'intervallo di timeout predefinito per la raccolta dati delle prestazioni è di 2 ore.</p>

Tabella 1-29. Tipi di raccolta dati (continua)

Tipo di raccolta dati	Descrizione
Raccolta dati degli inventari rete e sicurezza (solo risorse di elaborazione di vSphere)	Aggiorna il record dei dati di protezione e di rete relativi a vCloud Networking and Security e NSX, in particolare le informazioni sui gruppi di protezione e il bilanciamento del carico, per ogni macchina che segue la raccolta dati dell'inventario.
Raccolta dati WMI (solo per risorse di elaborazione Windows)	Aggiorna il record dei dati di gestione per ogni macchina Windows. È necessario installare un agente WMI, in genere sull'host del servizio di gestione, e attivarlo per la raccolta di dati dalle macchine Windows.

Avvio manuale della raccolta dati degli endpoint

La raccolta dati degli endpoint viene eseguita automaticamente ogni 4 ore, ma in qualsiasi momento gli amministratori di IaaS possono avviare manualmente la raccolta dati degli endpoint che non richiedono agenti proxy.

Nella pagina **Raccolta dati** sono elencate le informazioni sullo stato e sull'età delle raccolte dati ed è possibile avviare manualmente una nuova raccolta dati di endpoint.

Prerequisiti

Accedere a vRealize Automation come **amministratore IaaS**.

Procedura

- 1 Selezionare **Infrastruttura > Endpoint > Endpoint**.
- 2 Fare clic sulla riga dell'endpoint di cui si desidera raccogliere dati.
- 3 Selezionare un'azione di raccolta dati disponibile.

Configurazione della raccolta dati delle risorse di elaborazione

È possibile attivare o disattivare la raccolta dati, configurare la frequenza di raccolta dati o richiedere manualmente la raccolta dati.

Nella pagina **Raccolta dati** sono elencate le informazioni sullo stato e sull'età delle raccolte dati. Dalla pagina è inoltre possibile configurare la raccolta dati per le proprie risorse di elaborazione.

Prerequisiti

Accedere a vRealize Automation come **amministratore di struttura**.

Procedura

- 1 Selezionare **Infrastruttura > Risorse di elaborazione > Risorse di elaborazione**.
- 2 Puntare sulla risorsa di elaborazione per cui configurare la raccolta dati e fare clic su **Raccolta dati**.

3 Configurare le specifiche di raccolta dati della **Risorsa di elaborazione**.

- Selezionare **Attivato** per attivare la raccolta dati.
- Selezionare **Disattivato** per disattivare la raccolta dati.

4 Configurare la raccolta dati dell'**Inventario**.

- Selezionare **Attivato** per attivare la raccolta dati.
- Selezionare **Disattivato** per disattivare la raccolta dati.
- Immettere un numero nella casella di testo **Frequenza** per configurare l'intervallo di tempo, espresso in ore, tra una raccolta dati di inventario e la successiva.
- Fare clic su **Richiedi ora** per avviare manualmente la raccolta dati.

5 Configurare la raccolta dati di **Stato**.

- Selezionare **Attivato** per attivare la raccolta dati.
- Selezionare **Disattivato** per disattivare la raccolta dati.
- Immettere un numero nella casella di testo **Frequenza** per configurare l'intervallo di tempo, espresso in minuti, tra una raccolta dati di stato e la successiva.
- Fare clic su **Richiedi ora** per avviare manualmente la raccolta dati.

6 Configurare la raccolta dati di **Prestazioni**.

Questa è disponibile solo per le integrazioni di vSphere.

- Selezionare **Attivato** per attivare la raccolta dati.
- Selezionare **Disattivato** per disattivare la raccolta dati.
- Immettere un numero nella casella di testo **Frequenza** per configurare l'intervallo di tempo, espresso in ore, tra una raccolta dati di prestazioni e la successiva.
- Fare clic su **Richiedi ora** per avviare manualmente la raccolta dati.

7 Configurare la raccolta dati dell'**Inventario snapshot**.

Questa opzione è disponibile per le risorse di elaborazione gestite da vRealize Business for Cloud.

- Selezionare **Attivato** per attivare la raccolta dati.
- Selezionare **Disattivato** per disattivare la raccolta dati.
- Immettere un numero nella casella di testo **Frequenza** per configurare l'intervallo di tempo, espresso in ore, tra una raccolta dati di snapshot e la successiva.
- Fare clic su **Richiedi ora** per avviare manualmente la raccolta dati.

8 Fare clic su **OK**.

Aggiornamento dei dati di costo per tutte le risorse di elaborazione

Gli amministratori di struttura possono aggiornare manualmente le informazioni sui costi per tutte le risorse di elaborazione gestite da vRealize Business for Cloud.

Prerequisiti

Accedere a vRealize Automation come **amministratore di struttura**.

Procedura

- 1 Selezionare **Infrastruttura > Risorse di elaborazione > Risorse di elaborazione**.
- 2 Fare clic su **Aggiorna costi**.
- 3 Fare clic su **Richiedi ora**.

Risultati

Lo stato cambia e mostra l'avvenuto aggiornamento dei costi.

Il controllo allocazione eseguito da vSwap per gli endpoint vCenter Server

È possibile utilizzare vSwap per sapere se c'è spazio di scambio sufficiente ad accogliere il file di scambio di dimensione massima su una macchina target. Il controllo di vSwap viene eseguito quando si crea o si riconfigura una macchina virtuale da vRealize Automation. Il controllo allocazione di vSwap è disponibile solo per gli endpoint vCenter Server.

L'allocazione di storage di vRealize Automation controlla se sul datastore è disponibile spazio sufficiente ad accogliere i dischi della macchina virtuale durante una richiesta di creazione o riconfigurazione. Se quando la macchina verrà accesa sull'endpoint vCenter Server non sarà disponibile uno spazio sufficiente a creare i file di scambio, la macchina non si accenderà. Quando un'operazione di accensione ha esito negativo, anche tutte le personalizzazioni che dipendono dalla macchina hanno esito negativo. La macchina potrebbe anche essere eliminata. In base alla dimensione della richiesta, potrebbe non essere immediatamente chiaro un esito negativo dell'accensione o del provisioning di quella macchina.

È possibile utilizzare il controllo allocazione di vSwap come strumento utile a superare queste limitazioni, integrando nel processo di creazione e riconfigurazione di vRealize Automation per gli endpoint vCenter Server l'operazione di controllo della disponibilità dello spazio necessario ad accogliere il file di scambio di dimensione massima. Per abilitare il controllo allocazione di vSwap, impostare su True la proprietà personalizzata `VirtualMachine.Storage.ReserveMemory` nel componente o nel blueprint della macchina.

Per utilizzare al meglio i controlli allocazione di vSwap, tenere in considerazione gli aspetti seguenti:

- Il file di scambio viene posizionato nel datastore che contiene la macchina virtuale. Non è possibile realizzare configurazioni alternative di vCenter Server per posizionare i file di scambio su datastore dedicati o differenti.

- La dimensione dello scambio viene presa in considerazione quando si crea o si riconfigura una macchina virtuale. La dimensione di scambio massima è pari alla dimensione della memoria della macchina virtuale.
- I valori riservati per le prenotazioni storage di vRealize Automation in un host non devono superare la capacità fisica della risorsa di elaborazione.
- Quando si crea una prenotazione, la somma dei valori riservati non deve superare lo spazio di storage disponibile.
- Le prenotazioni di memoria a livello host o di macchina virtuale e dei pool di risorse su vSphere non vengono raccolte dall'endpoint vSphere e non vengono considerate nei calcoli su vRealize Automation.
- vSwap non convalida lo spazio di scambio disponibile durante le operazioni di accensione per le macchine esistenti.
- È necessario eseguire nuovamente la raccolta dati per catturare eventuali modifiche apportate all'endpoint vSphere relativo a vSwap.

Rimozione di posizioni di data center

Per rimuovere la posizione di un datacenter da un menu dell'utente, l'amministratore di sistema deve rimuovere le informazioni sulla posizione dal file delle posizioni e un amministratore di struttura deve rimuovere le informazioni sulla posizione dalla risorsa di elaborazione.

Ad esempio, se si aggiunge Roma al file delle posizioni, si associano dieci risorse di elaborazione a quella posizione e poi si rimuove Roma dal file, le risorse di elaborazione saranno ancora associate alla posizione Roma e Roma verrà ancora inclusa nell'elenco a discesa delle posizioni nella pagina Conferma richiesta macchina. Per rimuovere la posizione dall'elenco a discesa, un amministratore di struttura dovrà modificare tutte le risorse di elaborazione associate a quella posizione, cancellando il campo della posizione e lasciandolo vuoto.

L'elenco che segue è una panoramica ad alto livello della sequenza di passaggi necessari per rimuovere una posizione di data center:

- 1 Un amministratore di sistema rimuove le informazioni sulla posizione del data center dal file delle posizioni.
- 2 Un amministratore di struttura rimuove tutte le associazioni alla posizione delle risorse di elaborazione, modificando le posizioni di ciascuna risorsa di elaborazione associata.

Monitoraggio dei contenitori

È possibile monitorare lo stato di un contenitore creato in Contenitori per vRealize Automation

Dopo aver creato i contenitori in base a un modello, è possibile monitorarne lo stato. Facendo clic su **Dettagli** su un contenitore, è possibile monitorare la larghezza di banda di rete, l'uso di CPU e memoria, i registri e le proprietà di tale contenitore.

Importazione di massa, aggiornamento e migrazione di macchine virtuali

È possibile utilizzare la funzione Importazioni di massa per importare, aggiornare o migrare le macchine virtuali in vRealize Automation. Importazioni di massa semplifica la gestione di macchine multiple in ambienti multipli.

Importazioni di massa crea un file CSV che contiene dati di macchina virtuale di definizione quali prenotazione, percorso di archiviazione, blueprint, proprietario ed eventuali proprietà personalizzate. Il file CSV viene utilizzato per importare le macchine virtuali nell'ambiente vRealize Automation. Importazioni di massa supporta le seguenti attività amministrative:

- Importazione di una o più macchine virtuali non gestite, affinché queste possano essere gestite in un ambiente vRealize Automation.
- Esecuzione di una modifica globale su una proprietà di una macchina virtuale, ad esempio un percorso di storage.
- Migrazione di una macchina virtuale da un ambiente vRealize Automation a un altro.

Nota L'importazione di massa è supportata solo per vCloud Director e vSphere. L'impostazione del filtro su un altro tipo di endpoint non genera dati nel file CSV.

È possibile eseguire i comandi della funzionalità Importazioni di massa utilizzando la console di vRealize Automation o l'interfaccia della riga di comando CloudUtil. Per ulteriori informazioni sull'uso dell'interfaccia a riga di comando CloudUtil, consultare la documentazione di *Estensibilità del ciclo di vita*.

Nota L'importazione in blocco delle macchine non esclude i normali passaggi del provisioning. Tutti i workflow esterni esistenti che vengono attivati dal gestore eventi durante il provisioning vengono eseguiti per le macchine importate. È possibile disattivare temporaneamente i workflow per le macchine importate eseguendo una delle seguenti operazioni:

- Disattivare tutte le sottoscrizioni del gestore eventi. Se si disattivano le sottoscrizioni, è necessario pianificare un'interruzione del servizio per il cluster di vRealize Automation perché l'estensibilità non verrà applicata ad alcuna macchina normale il cui provisioning viene eseguito durante questo periodo di tempo.
 - Aggiungere una condizione in modo che le sottoscrizioni evento non vengano attivate quando una macchina viene importata. Per aggiungere questa condizione, passare alla sezione delle sottoscrizioni evento, selezionare la sottoscrizione da disattivare e aggiungere una proprietà personalizzata `VirtualMachine.Imported.ConvergedBlueprint` diversa da `<ID del blueprint da importare>`. Questa condizione non influisce sulle macchine normalmente sottoposte a provisioning, ma viene applicata solo alle macchine importate.
-

Prerequisiti

- Accedere a vRealize Automation come **amministratore di struttura** e **manager del gruppo di business**.

- Se si importano macchine virtuali che utilizzano indirizzi IP statici, preparare un pool di indirizzi correttamente configurato.

Importazione di una macchina virtuale in un ambiente vRealize Automation

È possibile importare una macchina virtuale non gestita in un ambiente vRealize Automation.

Una macchina virtuale non gestita esiste in un hypervisor, ma non è gestita in un ambiente vRealize Automation e non è visualizzabile nella console. Dopo aver importato una macchina virtuale non gestita, questa viene gestita utilizzando l'interfaccia di gestione di vRealize Automation. A seconda dei privilegi di cui si dispone, è possibile visualizzare la macchina virtuale nella scheda **Macchine gestite** o nella scheda **Distribuzioni**.

L'opzione di importazione di massa non supporta le distribuzioni il cui provisioning viene eseguito da un blueprint che contiene una rete NSX e un componente di sicurezza o un componente software.

Prerequisiti

- Accedere a vRealize Automation come **amministratore di struttura** e **manager del gruppo di business**.
- Se si importano macchine virtuali che utilizzano indirizzi IP statici, preparare un pool di indirizzi correttamente configurato. Per ulteriori informazioni sull'utilizzo di un profilo di rete per controllare gli intervalli di indirizzi IP, vedere *Configurazione di vRealize Automation*.
- Se si utilizza l'importazione di massa per importare una macchina virtuale con un indirizzo IP statico che è allocato in un'altra macchina virtuale, l'importazione non riesce.

Procedura

- 1 Disattivare temporaneamente tutte le sottoscrizioni di Event Broker.

Nota Quando si disabilitano le sottoscrizioni, è necessario pianificare un'interruzione del servizio per il cluster di vRealize Automation. Durante questo processo, l'estendibilità non viene applicata a una macchina normalmente sottoposta a provisioning. La mancata disattivazione delle sottoscrizioni può causare la perdita di dati e l'eliminazione definitiva delle macchine dall'infrastruttura di supporto.

- 2 Generazione del file di dati CSV di una macchina virtuale
 - a Selezionare **Infrastruttura > Amministrazione > Importazioni di massa**.
 - b Fare clic su **Genera file CSV**.
 - c Selezionare **Non gestito** dal menu a discesa **Macchine**.
 - d Selezionare il valore **Gruppo di business** dal menu a discesa.
 - e Immettere il valore predefinito **Proprietario**.

- f Selezionare il valore predefinito **Blueprint** dal menu a discesa.

Per poter completare l'importazione è necessario che il blueprint venga pubblicato e aggiunto a un permesso.

- g Selezionare il valore predefinito **Macchina componente** dal menu a discesa.

Se si seleziona un valore per **Gruppo di business** e **Blueprint**, nel file di dati CSV potrebbero essere visualizzati i seguenti risultati:

- Host Reservation (Name or ID) = INVALID_RESERVATION
- Host To Storage (Name or ID) = INVALID_HOST_RESERVATION_TO_STORAGE

Questi messaggi vengono visualizzati quando non si dispone di una prenotazione nel gruppo di business selezionato per la macchina virtuale host che ospita anche la macchina virtuale non gestita. Se si dispone di una prenotazione in quel gruppo di business per l'host della macchina virtuale non gestita, i valori di Host Reservation e Host to Storage vengono compilati correttamente.

- h Selezionare uno dei tipi di risorsa disponibili dal menu a discesa **Risorsa**.

Voce di menu	Descrizione
Endpoint	Informazioni necessarie per accedere a un host di virtualizzazione.
Risorsa di elaborazione	Informazioni necessarie per accedere a un gruppo di macchine virtuali che eseguono una funzione simile.

- i Selezionare il nome della risorsa macchina virtuale dal menu a discesa **Nome**.
- j Fare clic su **OK**.

3 Modificare il file di dati CSV della macchina virtuale.

- a Aprire il file CSV e modificare le categorie di dati per fare in modo che corrispondano alle categorie esistenti nell'ambiente vRealize Automation di destinazione.

Per importare le macchine virtuali contenute in un file di dati CSV, è necessario che ogni macchina virtuale sia associata agli elementi seguenti:

- Prenotazione
- Posizione di storage
- Blueprint
- Componente macchina virtuale
- Proprietario della distribuzione di destinazione

Affinché l'importazione abbia esito positivo, tutti i valori di ciascuna macchina virtuale devono essere presenti nell'ambiente vRealize Automation target. È possibile cambiare i valori relativi a prenotazione, posizione di storage, blueprint e proprietario, oppure aggiungere un indirizzo IP statico alle singole macchine virtuali modificando il file CSV.

Intestazione	Commento
# Import—Yes or No	Cambiare in No per evitare che una particolare macchina virtuale venga importata.
Virtual Machine Name	Non modificare.
Virtual Machine ID	Non modificare.
Host Reservation (Name or ID)	Immettere il nome o l'ID di una prenotazione presente nell'ambiente vRealize Automation di destinazione.
Host To Storage (Name or ID)	Immettere il nome o l'ID di una posizione di storage presente nell'ambiente vRealize Automation di destinazione.
Deployment Name	Immettere un nuovo nome per la distribuzione, ad esempio il nome della macchina virtuale che si sta creando nell'istanza dell'ambiente vRealize Automation di destinazione. Nota È necessario importare ogni macchina virtuale nella relativa distribuzione. Non è possibile importare una singola macchina virtuale in una distribuzione esistente, né importare più macchine virtuali in una singola distribuzione.
ID blueprint	Immettere l'ID del blueprint nell'ambiente vRealize Automation di destinazione utilizzata per importare la macchina virtuale. Nota Immettere solo l'ID blueprint, non il nome del blueprint. È necessario selezionare un blueprint che contenga un singolo componente macchina virtuale. Il blueprint deve essere pubblicato e aggiunto a un permesso. Per le macchine virtuali importate, non associare un blueprint che includa profili dei componenti. Le impostazioni esistenti nelle macchine virtuali importate, come la memoria o le dimensioni dello storage, possono non rientrare nei limiti del profilo. In tal caso, la convalida per qualsiasi futura riconfigurazione basata su blueprint delle macchine virtuali non riesce.

Intestazione	Commento
Component Machine ID	Immettere il nome di un componente macchina virtuale contenuto nel blueprint scelto. Non è possibile importare una macchina virtuale in un blueprint contenente più componenti.
Owner Name	Immettere un utente nell'ambiente vRealize Automation di destinazione che disponga di un permesso per il blueprint.

Se si importa una macchina virtuale con una o più proprietà personalizzate, si identifica ciascuna proprietà personalizzata utilizzando tre valori separati da virgola aggiunti alla riga contenente i valori per tale macchina. Utilizzare questo formato per ogni proprietà personalizzata.

,Custom.Property.Name, Value, FLAGS

FLAGS rappresenta tre caratteri che descrivono in che modo la proprietà viene gestita da vRealize Automation. In base all'ordine di utilizzo, i flag sono:

- 1 H o N = nascosto o non nascosto
- 2 E o O = crittografato o non crittografato
- 3 R o P = runtime o non runtime

Ad esempio, è possibile aggiungere una proprietà personalizzata per configurare un indirizzo IP statico per una macchina. Utilizzando il formato seguente, questa proprietà personalizzata esegue l'allocazione di un indirizzo IP statico disponibile da un profilo di rete.

,VirtualMachine.Network n .Address, w.x.y.z, HOP

Modificare le variabili utilizzando le informazioni appropriate per la macchina virtuale.

- Sostituire # con il numero dell'interfaccia di rete che si sta configurando con l'indirizzo IP statico. Ad esempio `VirtualMachine.Network0.Address`.
- Sostituire w.x.y.z con l'indirizzo IP statico della macchina virtuale. Ad esempio `11.27.42.57`.

La stringa del flag HOP, ovvero nascosto, non crittografato, non runtime, imposta la visibilità della proprietà. Poiché questa particolare proprietà viene utilizzata solo per l'importazione di massa, viene rimossa dalla macchina virtuale dopo il completamento dell'importazione.

Affinché questa proprietà personalizzata funzioni, l'indirizzo IP deve essere disponibile in un pool di indirizzi correttamente configurato. Se l'indirizzo non viene trovato o è già in uso, l'importazione riesce comunque senza la definizione dell'indirizzo IP statico e viene registrato un errore.

- b Salvare il file CSV.

- 4 Utilizzare l'interfaccia di gestione di vRealize Automation per importare la macchina virtuale in un ambiente vRealize Automation.
 - a Selezionare **Infrastruttura > Amministrazione > Importazioni di massa**.
 - b Fare clic su **Nuovo**.
 - c Immettere un nome univoco per questa attività nella casella di testo **Nome**, ad esempio "Importazione non gestita 10".
 - d Selezionare il nome file CSV con il mouse o specificare direttamente il nome nella casella di testo **File CSV**.
 - e Selezionare le opzioni di importazione.

Opzione	Descrizione
Ora di inizio	Consente di pianificare una data di avvio futura. L'ora di inizio scelta corrisponde all'ora locale del server e non all'ora locale della workstation dell'utente.
Ora	Avvia il processo di importazione immediatamente.
Ritardo (secondi)	Se si stanno importando molte macchine virtuali, selezionare il numero di secondi da attendere per ritardare la registrazione di ciascuna macchina virtuale. La selezione di questa voce di menu rallenta il processo di importazione. Lasciare vuoto il campo per selezionare nessun ritardo.
Dimensioni batch	Se si stanno importando molte macchine virtuali, selezionare il numero totale di macchine virtuali da registrare a un dato orario. La selezione di questa voce di menu rallenta il processo di importazione. Lasciare vuoto il campo per selezionare nessun limite.
Ignora macchine gestite	Lasciare deselezionato.
Salta convalida utente	La selezione di questa voce di menu consente di impostare il proprietario della macchina virtuale sul valore riportato nella colonna Proprietario del file di dati CSV senza verificare l'effettiva esistenza dell'utente. La selezione di questa voce di menu può ridurre la durata dell'importazione.
Prova importazione	Esegue un test del processo di importazione senza importare le macchine virtuali, in modo da rilevare eventuali errori nel file CSV.

- f Fare clic su **OK**.

Nella pagina Importazioni di massa viene mostrato l'avanzamento dell'operazione.

Aggiornamento di una macchina virtuale in un ambiente vRealize Automation

È possibile apportare una modifica a una proprietà di una macchina virtuale, ad esempio un percorso di storage, per aggiornare una o più macchine virtuali gestite in un ambiente vRealize Automation.

Una macchina virtuale gestita è una macchina gestita in un ambiente vRealize Automation e visualizzabile nella console.

Prerequisiti

- Accedere a vRealize Automation come **amministratore di struttura** e **manager del gruppo di business**.

Procedura

- 1 Generazione del file di dati CSV di una macchina virtuale
 - a Selezionare **Infrastruttura > Amministrazione > Importazioni di massa**.
 - b Fare clic su **Genera file CSV**.
 - c Selezionare **Gestito** dal menu a discesa **Macchine**.
 - d Selezionare uno dei tipi di risorsa disponibili dal menu a discesa **Risorsa**.

Opzione	Descrizione
Endpoint	Informazioni necessarie per accedere a un host di virtualizzazione.
Risorsa di elaborazione	Informazioni necessarie per accedere a un gruppo di macchine virtuali che eseguono una funzione simile.

- e Selezionare il nome della risorsa macchina virtuale dal menu a discesa **Nome**.
- f (Facoltativo) Selezionare **Includi proprietà personalizzate** se si desidera eseguire la migrazione delle proprietà personalizzate della macchina virtuale.
- g Fare clic su **OK**.

2 Modificare il file di dati CSV della macchina virtuale.

- a Aprire il file CSV con un editor di testo e modificare le categorie di dati che si desidera modificare globalmente.

Per aggiornare le macchine virtuali contenute in un file di dati CSV, è necessario che ogni macchina sia associata agli elementi seguenti:

- Prenotazione
- Posizione di storage
- Blueprint
- Componente macchina
- Proprietario della distribuzione di destinazione

Affinché l'aggiornamento abbia esito positivo, tutti i valori di ciascuna macchina devono essere presenti nell'ambiente vRealize Automation di destinazione. È possibile cambiare i valori relativi a prenotazione, posizione di storage, blueprint e proprietario, oppure aggiungere un indirizzo IP statico alle singole macchine modificando il file CSV.

- b Se si sta modificando l'indirizzo IP statico di una macchina virtuale, aggiungere al file CSV il comando riportato di seguito.

```
,VirtualMachine.Network $n$ .Address,  $w.x.y.z$ , HOP
```

Configurare il comando utilizzando le informazioni appropriate per la macchina virtuale specifica.

- Sostituire n con il numero dell'interfaccia di rete che si sta configurando con l'indirizzo IP statico. Ad esempio VirtualMachineNetwork0.Address.
- Sostituire $w.x.y.z$ con l'indirizzo IP statico della macchina virtuale. Ad esempio 11.27.42.57.
- La stringa *HOP* (Hidden, Not encrypted, Not runtime) imposta la visibilità della proprietà. Questa proprietà personalizzata viene rimossa dalla macchina virtuale dopo un'importazione terminata con successo.

Per garantire l'esito positivo dell'aggiornamento, l'indirizzo IP deve essere disponibile all'interno di un pool di indirizzi correttamente configurato. Se l'indirizzo non viene trovato o è già in uso, l'aggiornamento riesce comunque senza la definizione dell'indirizzo IP statico e viene registrato un errore.

- c Salvare il file CSV e chiudere l'editor di testo.

3 Utilizzare l'interfaccia di gestione di vRealize Automation per aggiornare una o più macchine virtuali in un ambiente vRealize Automation.

- a Selezionare **Infrastruttura > Amministrazione > Importazioni di massa**.
- b Fare clic su **Nuovo**.

- c Immettere un nome univoco per questa attività nella casella di testo **Nome**, ad esempio "Aggiornamento gestito globale 10".
- d Selezionare il file CSV con il mouse o specificare direttamente il nome nella casella di testo **File CSV**.
- e Selezionare le opzioni di importazione.

Opzione	Descrizione
Ora di inizio	Consente di pianificare una data di avvio futura. L'ora di inizio specificata corrisponde all'ora locale del server e non all'ora locale della workstation dell'utente.
Ora	Avvia il processo di importazione immediatamente.
Ritardo (secondi)	Se si sta aggiornando un numero elevato di macchine virtuali, selezionare il numero di secondi da attendere per ritardare l'aggiornamento di ciascuna macchina virtuale. La selezione di questa opzione rallenta il processo di aggiornamento. Lasciare vuoto il campo per specificare nessun ritardo.
Dimensioni batch	Se si sta aggiornando un numero elevato di macchine virtuali, selezionare il numero totale di macchine da aggiornare a un dato orario. La selezione di questa opzione rallenta il processo di aggiornamento. Lasciare vuoto il campo per specificare nessun limite.
Ignora macchine gestite	Lasciare deselezionato.
Salta convalida utente	La selezione di questa opzione consente di impostare il proprietario della macchina sul valore riportato nella colonna Proprietario del file di dati CSV senza verificare l'effettiva esistenza dell'utente. La selezione di questa opzione può ridurre la durata dell'aggiornamento.
Prova importazione	Lasciare deselezionato.

- f Fare clic su **OK**.

Nella pagina Importazione di massa viene mostrato l'avanzamento dell'operazione.

Migrazione di una macchina virtuale in un ambiente vRealize Automation differente

È possibile eseguire la migrazione di una o più macchine virtuali gestite in un ambiente VMware vRealize™ Automation verso un ambiente vRealize Automation differente.

Una macchina virtuale gestita è una macchina virtuale gestita in un ambiente vRealize Automation e visualizzabile nella console.

Prerequisiti

- Accedere a vRealize Automation come **amministratore di struttura** e **manager del gruppo di business**.
- Se si importano macchine virtuali che utilizzano indirizzi IP statici, preparare un pool di indirizzi correttamente configurato. Per ulteriori informazioni sull'utilizzo di un profilo di rete per controllare gli intervalli di indirizzi IP, vedere *Configurazione di vRealize Automation*.

Procedura**1** Generazione del file di dati CSV di una macchina virtuale

- a Selezionare **Infrastruttura > Amministrazione > Importazioni di massa**.
- b Fare clic su **Genera file CSV**.
- c Selezionare **Gestito** dal menu a discesa **Macchine**.
- d Selezionare uno dei tipi di risorsa disponibili dal menu a discesa **Risorsa**.

Opzione	Descrizione
Endpoint	Informazioni necessarie per accedere a un host di virtualizzazione.
Risorsa di elaborazione	Informazioni necessarie per accedere a un gruppo di macchine virtuali che eseguono una funzione simile.

- e Selezionare il nome della risorsa macchina virtuale dal menu a discesa **Nome**.
- f (Facoltativo) Selezionare **Includi proprietà personalizzate**.
È necessario includere proprietà personalizzate quando si importa una macchina virtuale in una nuova distribuzione con le stesse proprietà.
- g Fare clic su **OK**.

2 Modificare il file di dati CSV della macchina virtuale.

La necessità di modificare il file di dati CSV dipende dalla somiglianza tra gli ambienti di origine e target. Se i valori di configurazione dell'ambiente di origine non corrispondono ai valori dell'ambiente target, è necessario modificare il file di dati CSV in modo da creare una corrispondenza tra tali valori prima di iniziare la migrazione.

- a Aprire il file CSV e modificare le categorie di dati per fare in modo che corrispondano alle categorie esistenti nell'ambiente vRealize Automation di destinazione.

Per eseguire la migrazione delle macchine virtuali contenute in un file di dati CSV, ogni macchina virtuale deve essere associata a una prenotazione, una posizione di storage, un blueprint, un componente macchina e un proprietario esistenti nell'ambiente vRealize Automation target. Affinché la migrazione avvenga correttamente, tutti i valori di ciascuna macchina virtuale devono essere presenti nell'ambiente vRealize Automation target. È possibile cambiare i valori relativi a prenotazione, posizione di storage, blueprint e proprietario, oppure aggiungere un indirizzo IP statico alle singole macchine virtuali modificando il file CSV.

Intestazione	Commento	Esempio
# Import--Yes or No	Cambiare in No per evitare che una particolare macchina virtuale venga importata.	Sì
Virtual Machine Name	Non modificare.	MyMachine
Virtual Machine ID	Non modificare.	a6e05812-0b06-4d4e-a84a-fed242340426a
Host Reservation (Name or ID)	Immettere il nome o l'ID di una prenotazione presente nell'ambiente vRealize Automation di destinazione.	DevReservation
Host To Storage (Name or ID)	Immettere il nome o l'ID di una posizione di storage presente nell'ambiente vRealize Automation di destinazione.	ce-san-1:custom-nfs-2
Deployment Name	Immettere il nuovo nome per la distribuzione che si sta creando nell'ambiente vRealize Automation di destinazione. È necessario migrare ogni macchina virtuale nella relativa distribuzione. Non è possibile importare una singola macchina virtuale in una distribuzione esistente, né importare più macchine virtuali in un singolo ambiente.	ImportedDeployment0001
Converged Blueprint ID	Immettere l'ID del blueprint nell'ambiente vRealize Automation di destinazione utilizzata per importare la macchina virtuale. Assicurarsi di immettere solo l'ID del blueprint. Non immettere il nome del blueprint. È necessario selezionare un blueprint che contenga un singolo componente macchina virtuale. Il blueprint deve essere pubblicato e aggiunto a un permesso.	ImportBlueprint

Intestazione	Commento	Esempio
Component Blueprint ID	Immettere il nome di un componente macchina virtuale contenuto nel blueprint scelto. Non è possibile importare una macchina virtuale in un blueprint contenente più componenti.	ImportedMachine
Owner Name	Immettere un utente nell'ambiente vRealize Automation di destinazione.	user@tenant

Esempio di una riga CSV completa, correttamente formattata: Sì, MyMachine, a6e05812-0b06-4d4e-a84a-fed242340426, DevReservation, ce-san-1:custom-nfs-2, Imported Deployment 0001, ImportBlueprint, ImportedMachine, user@tenant

- b Se si sta eseguendo la migrazione di una macchina virtuale con indirizzo IP statico, aggiungere al file CSV il comando riportato di seguito.

```
,VirtualMachine.Network#.Address, w.x.y.z, HOP
```

Configurare il comando utilizzando le informazioni appropriate per la macchina virtuale specifica.

- Sostituire *n*. con il numero dell'interfaccia di rete che si sta configurando con l'indirizzo IP statico. Ad esempio `VirtualMachineNetwork0.Address`.
- Sostituire *w.x.y.z* con l'indirizzo IP statico della macchina virtuale. Ad esempio `11.27.42.57`.
- La stringa *HOP* (Hidden, Not encrypted, Not runtime) imposta la visibilità della proprietà. Questa proprietà personalizzata viene rimossa dalla macchina virtuale dopo un'importazione terminata con successo.

Per garantire l'esito positivo della migrazione, l'indirizzo IP deve essere disponibile all'interno di un pool di indirizzi correttamente configurato. Se l'indirizzo non viene trovato o è già in uso, la migrazione riesce comunque senza la definizione dell'indirizzo IP statico e viene registrato un errore.

- c Salvare il file CSV.

- 3 Utilizzare l'interfaccia di gestione di vRealize Automation per migrare la macchina virtuale in un ambiente vRealize Automation.

- a Selezionare **Infrastruttura > Amministrazione > Importazioni di massa**.
- b Fare clic su **Nuovo**.
- c Immettere un nome univoco per questa attività nella casella di testo **Nome**, ad esempio "Migrazione gestita 10".
- d Selezionare il nome file CSV con il mouse o specificare direttamente il nome nella casella di testo **File CSV**.

- e Selezionare le opzioni di importazione.

Opzione	Descrizione
Ora di inizio	Consente di pianificare una data di avvio futura. L'ora di inizio scelta corrisponde all'ora locale del server e non all'ora locale della workstation dell'utente.
Ora	Avvia il processo di migrazione immediatamente.
Ritardo (secondi)	Se si stanno migrando molte macchine virtuali, selezionare il numero di secondi da attendere per ritardare la registrazione di ciascuna macchina virtuale. La selezione di questa opzione rallenta il processo di migrazione. Lasciare vuoto il campo per selezionare nessun ritardo.
Dimensioni batch	Se si stanno migrando molte macchine virtuali, selezionare il numero totale di macchine virtuali da registrare a un dato orario. La selezione di questa opzione rallenta il processo di migrazione. Lasciare vuoto il campo per selezionare nessun limite.
Ignora macchine gestite	Lasciare deselezionato.
Salta convalida utente	La selezione di questa opzione consente di impostare il proprietario della macchina virtuale sul valore riportato nella colonna Proprietario del file di dati CSV senza verificare l'effettiva esistenza dell'utente. La selezione di questa opzione può ridurre la durata della migrazione.
Prova importazione	Esegue un test del processo di migrazione senza eseguire la migrazione delle macchine virtuali, in modo da rilevare eventuali errori nel file CSV.

- f Fare clic su **OK**.

Nella pagina Importazione di massa viene mostrato l'avanzamento dell'operazione.