

Amministrazione di vRealize Automation

Ottobre 2022

vRealize Automation 8.4

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 © 2022 VMware, Inc. Tutti i diritti sono riservati. [Informazioni sul copyright e sui marchi](#)

Sommario

1	Amministrazione di vRealize Automation	4
2	Amministrazione di utenti	5
	Come abilitare i gruppi di Active Directory per i progetti	6
	Come rimuovere utenti in vRealize Automation	7
	Come modificare i ruoli utente in vRealize Automation	8
	Come modificare le assegnazioni dei ruoli dei gruppi in vRealize Automation	8
	Che cosa sono i ruoli utente di vRealize Automation	9
	Abilitazione del banner dell'informativa e del consenso del Dipartimento della Difesa	25
3	Manutenzione dell'appliance	27
	Avvio e arresto di vRealize Automation	27
	Scalabilità orizzontale di vRealize Automation da uno a tre nodi	29
	Sostituzione di un nodo dell'appliance	30
	Aumento delle dimensioni del disco dell'appliance vRealize Automation	32
	Aggiornamento dell'assegnazione DNS per vRealize Automation	32
	Come abilitare la sincronizzazione dell'ora	33
	Come reimpostare la password root	35
4	Utilizzo di configurazioni tenant multi-organizzazione in vRealize Automation	37
	Configurazione della tenancy multi-organizzazione per vRealize Automation	40
	Gestione della configurazione dei certificati e di DNS in distribuzioni di più organizzazioni con un solo nodo	42
	Gestione della configurazione del certificato e di DNS nelle distribuzioni di vRealize Automation in cluster	44
	Accesso ai tenant e aggiunta di utenti in vRealize Automation	46
	Utilizzo di vRealize Orchestrator con le distribuzioni multi-organizzazione di vRealize Automation	47
5	Utilizzo dei registri	48
	Come utilizzare i registri e i bundle di registri	48
	In che modo è possibile configurare l'inoltro dei registri in vRealize Log Insight	51
	Come creare o aggiornare un'integrazione syslog	56
	Come eliminare un'integrazione syslog per la registrazione	57
	Come si utilizzano i pacchetti di contenuti	58
6	Partecipazione al programma Analisi utilizzo software	61
	Come partecipare o abbandonare il programma	61
	Come configurare la data e l'ora di raccolta dati per il programma	62

Amministrazione di vRealize Automation

1

Questa guida descrive come monitorare e gestire gli aspetti critici dell'infrastruttura e della gestione degli utenti di una distribuzione di vRealize Automation.

Le attività qui descritte sono essenziali per garantire il corretto funzionamento di una distribuzione di vRealize Automation. Queste attività includono la gestione di utenti e gruppi e il monitoraggio dei registri di sistema.

Inoltre, descrive come configurare e gestire le distribuzioni con più organizzazioni.

Mentre alcune attività di amministrazione di vRealize Automation vengono completate in vRealize Automation, altre richiedono l'utilizzo di prodotti correlati, ad esempio vRealize Suite Lifecycle Manager e Workspace ONE Access. Gli utenti devono acquisire familiarità con questi prodotti e con le loro funzionalità prima di completare le attività applicabili.

Ad esempio, per informazioni su backup, ripristino e ripristino di emergenza, vedere la sezione **Backup, ripristino e ripristino di emergenza > 2019** nella [documentazione del prodotto vRealize Suite](#).

Nota Il ripristino di emergenza è supportato in vRealize Automation 8.0.1 e versioni successive.

Per informazioni sull'installazione, l'aggiornamento e la gestione di vRealize Suite Lifecycle Manager, vedere la [documentazione del prodotto di Lifecycle Manager](#).

Amministrazione di utenti e gruppi in vRealize Automation

2

vRealize Automation utilizza VMware Workspace ONE Access, l'applicazione di gestione delle identità fornita da VMware per importare e gestire utenti e gruppi. Dopo l'importazione o la creazione di utenti e gruppi, è possibile gestire le assegnazioni dei ruoli per le distribuzioni di singoli tenant utilizzando la pagina Gestione identità e accessi.

vRealize Automation viene installato utilizzando VMware Lifecycle Manager (vRSLCM o LCM). Quando si installa vRealize Automation è necessario importare un'istanza di Workspace ONE Access esistente o distribuirne una nuova per supportare la gestione delle identità. Questi due scenari definiscono le opzioni di gestione.

- Se si distribuisce una nuova istanza di Workspace ONE Access, è possibile gestire utenti e gruppi tramite LCM. Durante l'installazione, è possibile configurare una connessione ad Active Directory utilizzando Workspace ONE Access. In alternativa, è possibile visualizzare e modificare alcuni aspetti di utenti e gruppi all'interno di vRealize Automation utilizzando la pagina Gestione identità e accessi come descritto qui.
- Se si utilizza un'istanza di Workspace ONE Access esistente, è possibile importarla per l'utilizzo con vRealize Automation tramite LCM durante l'installazione. In questo caso, è possibile continuare a utilizzare Workspace ONE Access per gestire utenti e gruppi, oppure è possibile utilizzare le funzioni di gestione in LCM.

Per ulteriori informazioni sulla gestione degli utenti in una distribuzione di più organizzazioni, vedere [Accesso ai tenant e aggiunta di utenti in vRealize Automation](#).

Agli utenti di vRealize Automation devono essere assegnati ruoli. I ruoli definiscono l'accesso alle funzionalità all'interno dell'applicazione. Quando vRealize Automation viene installato con un'istanza di Workspace ONE Access, viene creata un'organizzazione predefinita e all'utente che esegue l'installazione viene assegnato il ruolo di proprietario dell'organizzazione. Tutti gli altri ruoli di vRealize Automation vengono assegnati dal proprietario dell'organizzazione.

In vRealize Automation sono disponibili tre tipi di ruoli, ovvero ruoli dell'organizzazione, ruoli di servizio e ruoli di progetto. Per vRealize Automation Cloud Assembly, Service Broker e Code Stream, i ruoli a livello di utente possono in genere utilizzare le risorse, mentre i ruoli a livello di amministratore sono necessari per creare e configurare le risorse. I ruoli organizzativi definiscono le autorizzazioni all'interno del tenant. I proprietari dell'organizzazione dispongono delle autorizzazioni a livello di amministratore, mentre i membri dell'organizzazione dispongono delle autorizzazioni a livello di utente. I proprietari dell'organizzazione possono aggiungere e gestire altri utenti.

Ruoli dell'organizzazione	Ruoli di servizio
■ Proprietario dell'organizzazione	■ Amministratore di Cloud Assembly
■ Membro dell'organizzazione	■ Utente di Cloud Assembly
	■ Visualizzatore di Cloud Assembly
	■ Amministratore di Service Broker
	■ Utente di Service Broker
	■ Visualizzatore di Service Broker
	■ Amministratore di Code Stream
	■ Utente di Code Stream
	■ Visualizzatore di Code Stream

Sono inoltre disponibili due ruoli principali a livello di progetto che non sono inclusi nella tabella, ovvero amministratore del progetto e utente del progetto. Questi ruoli vengono assegnati ad hoc in base al progetto con Cloud Assembly. Questi ruoli sono piuttosto variabili. Lo stesso utente può essere un amministratore in un progetto e un utente in un altro progetto. Per ulteriori informazioni, vedere [Che cosa sono i ruoli utente di vRealize Automation](#).

Per ulteriori informazioni sull'utilizzo di vRealize Suite Lifecycle Manager e Workspace ONE Access, vedere quanto segue.

Questo capitolo include i seguenti argomenti:

- [Come abilitare i gruppi di Active Directory in vRealize Automation per i progetti](#)
- [Come rimuovere utenti in vRealize Automation](#)
- [Come modificare i ruoli utente in vRealize Automation](#)
- [Come modificare le assegnazioni dei ruoli dei gruppi in vRealize Automation](#)
- [Che cosa sono i ruoli utente di vRealize Automation](#)
- [Abilitazione del banner dell'informativa e del consenso del Dipartimento della Difesa](#)

Come abilitare i gruppi di Active Directory in vRealize Automation per i progetti

Se un gruppo non è disponibile nella pagina Aggiungi gruppi quando si aggiungono utenti ai progetti, controllare la pagina Gestione identità e accessi e aggiungere il gruppo, se disponibile. Se il gruppo non è elencato nella pagina Gestione identità e accessi in vRealize Automation, il gruppo potrebbe non essere sincronizzato nell'istanza di Workspace ONE Access. È possibile verificare che sia stato sincronizzato e quindi utilizzare questa procedura per aggiungere il gruppo come mostrato nel presente documento.

Per aggiungere membri di un gruppo di Active Directory a un progetto, è necessario assicurarsi che il gruppo sia sincronizzato con l'istanza di Workspace ONE Access e che il gruppo venga aggiunto all'organizzazione.

Prerequisiti

Se i gruppi non sono sincronizzati, non sono disponibili quando si tenta di aggiungerli a un progetto. Verificare che i gruppi di Active Directory siano sincronizzati con l'istanza di Lifecycle Manager.

Procedura

- 1 Accedere a vRealize Automation come utente dello stesso dominio di Active Directory che si sta aggiungendo. Ad esempio, @mycompany.com
- 2 In Cloud Assembly, fare clic su Gestione identità e accessi nella barra di navigazione destra dell'interfaccia.
- 3 Fare clic su **Gruppi aziendali**, quindi fare clic su **Assegna ruoli**.
- 4 Utilizzare la funzione di ricerca per trovare il gruppo che si sta aggiungendo e selezionarlo.
- 5 Assegnare un ruolo dell'organizzazione.
Il gruppo deve includere almeno un ruolo Membro dell'organizzazione. Per ulteriori informazioni, vedere [Quali sono i ruoli utente di vRealize Automation Cloud Assembly](#).
- 6 Fare clic su **Aggiungi accesso al servizio**, aggiungere uno o più servizi e selezionare un ruolo per ciascuno di essi.
- 7 Fare clic su **Assegna**.

Risultati

A questo punto, è possibile aggiungere il gruppo di Active Directory a un progetto.

Come rimuovere utenti in vRealize Automation

È possibile rimuovere utenti in vRealize Automation in base alle necessità.

Tutti gli utenti sono elencati per impostazione predefinita e non è possibile aggiungere utenti con la pagina Gestione identità e accessi. È però possibile eliminare gli utenti.

Procedura

- 1 Selezionare la scheda Utenti attivi nella pagina Gestione identità e accessi.
- 2 Individuare e selezionare gli utenti da eliminare.
- 3 Fare clic su **Rimuovi utenti**.

Risultati

Gli utenti selezionati vengono rimossi.

Come modificare i ruoli utente in vRealize Automation

È possibile modificare i ruoli assegnati agli utenti di Workspace One Access che sono stati importati in vRealize Automation.

Prerequisiti

Procedura

- 1 In Cloud Assembly, fare clic su Gestione identità e accessi nella barra di navigazione destra dell'interfaccia.
- 2 Selezionare l'utente desiderato nella scheda Utenti attivi e fare clic su **Modifica ruoli**.
- 3 È possibile modificare i ruoli di organizzazione e servizio per l'utente.
 - Selezionare il menu a discesa accanto all'interfaccia Assegna ruoli organizzazione per modificare la relazione dell'utente con l'organizzazione.
 - Fare clic su Aggiungi accesso al servizio per aggiungere nuovi ruoli di servizio per l'utente.
 - Per rimuovere i ruoli utente, fare clic sulla X accanto al servizio applicabile.
- 4 Fare clic su **Salva**.

Risultati

L'assegnazione del ruolo utente viene aggiornata come specificato.

Come modificare le assegnazioni dei ruoli dei gruppi in vRealize Automation

È possibile modificare le assegnazioni dei ruoli per i gruppi in vRealize Automation

Prerequisiti

Gli utenti e i gruppi sono stati importati da un'istanza di vIDM valida associata alla distribuzione di vRealize Automation.

Procedura

- 1 In Cloud Assembly, fare clic su Gestione identità e accessi nella barra di navigazione destra dell'interfaccia.
- 2 Selezionare la scheda Gruppi aziendali.
- 3 Digitare il nome del gruppo per il quale si desidera modificare le assegnazioni dei ruoli nel campo di ricerca.
- 4 Modificare le assegnazioni dei ruoli per il gruppo selezionato. Sono disponibili due opzioni.
 - Assegna ruoli organizzazione

- Assegna ruoli servizio

5 Fare clic su **Assegna**.

Risultati

Le assegnazioni dei ruoli vengono aggiornate come specificato.

Che cosa sono i ruoli utente di vRealize Automation

In qualità di proprietario dell'organizzazione, è possibile assegnare i ruoli dell'organizzazione e i ruoli di servizio degli utenti. I ruoli determinano ciò che gli utenti possono fare o vedere. Quindi, nei servizi, l'amministratore del servizio può assegnare i ruoli di progetto. Per determinare il ruolo che si desidera assegnare, valutare le attività nelle tabelle seguenti.

Ruoli di servizio di Cloud Assembly

I ruoli di servizio di vRealize Automation Cloud Assembly determinano ciò che è possibile visualizzare ed eseguire in vRealize Automation Cloud Assembly. Questi ruoli di servizio sono definiti nella console da un proprietario dell'organizzazione.

Tabella 2-1. Descrizioni dei ruoli di servizio di vRealize Automation Cloud Assembly

Ruolo	Descrizione
Amministratore di Cloud Assembly	Utente che dispone di accesso in lettura e scrittura all'intera interfaccia utente e alle risorse API. Questo è l'unico ruolo utente che può visualizzare ed eseguire tutto, ad esempio aggiungere account cloud, creare nuovi progetti e assegnare un amministratore del progetto.
Utente di Cloud Assembly	Un utente che non dispone del ruolo di amministratore di Cloud Assembly. In un progetto di vRealize Automation Cloud Assembly, l'amministratore aggiunge gli utenti ai progetti come membri del progetto, amministratori o visualizzatori. L'amministratore può anche aggiungere un amministratore del progetto.
Visualizzatore di Cloud Assembly	Utente che ha accesso in lettura per visualizzare le informazioni ma che non può creare, aggiornare o eliminare valori. Si tratta di un ruolo di sola lettura in tutti i progetti. Gli utenti con il ruolo di visualizzatore possono visualizzare tutte le informazioni disponibili all'amministratore. Non può eseguire alcuna azione a meno che un amministratore non lo renda amministratore del progetto o membro del progetto. Se l'utente è associato a un progetto, dispone delle autorizzazioni correlate al ruolo. Il visualizzatore del progetto non estenderebbe le proprie autorizzazioni nel modo in cui avviene per il ruolo di amministratore o membro.

Oltre ai ruoli di servizio, vRealize Automation Cloud Assembly dispone di ruoli di progetto. Qualsiasi progetto è disponibile in tutti i servizi.

I ruoli di progetto sono definiti in vRealize Automation Cloud Assembly e possono variare tra i progetti.

Nelle tabelle seguenti, che indicano all'utente cosa possono visualizzare ed eseguire i diversi ruoli di servizio e progetto, tenere presente che gli amministratori del servizio dispongono di autorizzazioni complete in tutte le aree dell'interfaccia utente.

Le descrizioni dei ruoli di progetto consentiranno di decidere quali autorizzazioni concedere agli utenti.

- Gli amministratori del progetto sfruttano l'infrastruttura creata dall'amministratore del servizio per garantire che i loro membri del progetto dispongano delle risorse di cui hanno bisogno per le operazioni di sviluppo.
- I membri del progetto lavorano all'interno dei loro progetti per progettare e distribuire modelli cloud.
- I visualizzatori del progetto sono limitati all'accesso di sola lettura, ad eccezione di alcuni casi in cui possono eseguire operazioni non distruttive come il download di modelli cloud.

Tabella 2-2. Ruoli di servizio e ruoli di progetto di vRealize Automation Cloud Assembly

Contesto dell'interfaccia utente	Attività	Amministratore di Cloud Assembly	Visualizzatore di Cloud Assembly	Utente di Cloud Assembly		
				L'utente deve essere un membro o un amministratore del progetto per visualizzare ed eseguire attività correlate al progetto.		
				Amministratore del progetto	Membro del progetto	Visualizzatore del progetto
Accesso a Cloud Assembly						
Console	Nella console di vRA, è possibile visualizzare e aprire Cloud Assembly	Sì	Sì	Sì	Sì	Sì
Infrastruttura						
	Visualizzare e aprire la scheda Infrastruttura	Sì	Sì	Sì	Sì	Sì
Configurazione - Progetti	Creare progetti	Sì				

Tabella 2-2. Ruoli di servizio e ruoli di progetto di vRealize Automation Cloud Assembly (continua)

Contesto dell'interfaccia utente	Attività	Amministratore di Cloud Assembly	Visualizzatore di Cloud Assembly	Utente di Cloud Assembly L'utente deve essere un membro o un amministratore del progetto per visualizzare ed eseguire attività correlate al progetto.		
				Amministratore del progetto	Membro del progetto	Visualizzatore del progetto
	Aggiornare o eliminare i valori da riepilogo del progetto, provisioning, Kubernetes e integrazioni, nonché testare le configurazioni dei progetti.	Sì				
	Aggiungere utenti e gruppi, nonché assegnare ruoli nei progetti.	Sì		Sì. Progetti personali.		
	Visualizzare i progetti	Sì	Sì	Sì. Progetti personali	Sì. Progetti personali	Sì. Progetti personali
Configurazione - Zone cloud	Creare, aggiornare o eliminare le zone cloud	Sì				
	Visualizzare le zone cloud	Sì	Sì			
	Visualizzare la dashboard Dettagli della zona cloud	Sì	Sì			
	Visualizzare gli avvisi delle zone cloud	Sì	Sì			
Configurazione - Zone Kubernetes	Creare, aggiornare o eliminare le zone Kubernetes	Sì				

Tabella 2-2. Ruoli di servizio e ruoli di progetto di vRealize Automation Cloud Assembly (continua)

Contesto dell'interfaccia utente	Attività	Amministratore di Cloud Assembly	Visualizzatore di Cloud Assembly	Utente di Cloud Assembly L'utente deve essere un membro o un amministratore del progetto per visualizzare ed eseguire attività correlate al progetto.		
				Amministratore del progetto	Membro del progetto	Visualizzatore del progetto
	Visualizzare le zone Kubernetes	Sì	Sì			
Configurazione - Caratteristiche	Creare, aggiornare o eliminare le caratteristiche	Sì				
	Visualizzare le caratteristiche	Sì	Sì			
Configurazione - Mappature dell'immagine	Creare, aggiornare o eliminare le mappature delle immagini	Sì				
	Visualizzare le mappature delle immagini	Sì	Sì			
Configurazione - Profili di rete	Creare, aggiornare o eliminare i profili di rete	Sì				
	Visualizzare i profili di rete delle immagini	Sì	Sì			
Configurazione - Profili di storage	Creare, aggiornare o eliminare i profili di storage	Sì				
	Visualizzare i profili di storage delle immagini	Sì	Sì			
Configurazione - Schede dei prezzi	Creare, aggiornare o eliminare le schede dei prezzi	Sì				

Tabella 2-2. Ruoli di servizio e ruoli di progetto di vRealize Automation Cloud Assembly (continua)

Contesto dell'interfaccia utente	Attività	Amministratore di Cloud Assembly	Visualizzatore di Cloud Assembly	Utente di Cloud Assembly L'utente deve essere un membro o un amministratore del progetto per visualizzare ed eseguire attività correlate al progetto.		
				Amministratore del progetto	Membro del progetto	Visualizzatore del progetto
	Visualizzare le schede dei prezzi	Sì	Sì			
Configurazione - Tag	Creare, aggiornare o eliminare i tag	Sì				
	Visualizzare i tag	Sì	Sì			
Risorse - Risorse di elaborazione	Aggiungere tag alle risorse di elaborazione rilevate	Sì				
	Visualizzare le risorse di elaborazione rilevate	Sì	Sì			
Risorse - Reti	Modificare i tag di rete, gli intervalli IP e gli indirizzi IP	Sì				
	Visualizzare le risorse di rete rilevate	Sì	Sì			
Risorse - Sicurezza	Aggiungere tag ai gruppi di sicurezza rilevati	Sì				
	Visualizzare i gruppi di sicurezza rilevati	Sì	Sì			
Risorse - Storage	Aggiungere tag allo storage rilevato	Sì				
	Visualizzare lo storage	Sì	Sì			

Tabella 2-2. Ruoli di servizio e ruoli di progetto di vRealize Automation Cloud Assembly (continua)

Contesto dell'interfaccia utente	Attività	Amministratore di Cloud Assembly	Visualizzatore di Cloud Assembly	Utente di Cloud Assembly L'utente deve essere un membro o un amministratore del progetto per visualizzare ed eseguire attività correlate al progetto.		
				Amministratore del progetto	Membro del progetto	Visualizzatore del progetto
Risorse - Macchine	Aggiungere ed eliminare macchine	Sì				
	Visualizzare le macchine	Sì	Sì	Sì. Progetti personali	Sì. Progetti personali	Sì. Progetti personali
Risorse - Volumi	Eliminare i volumi di storage rilevati	Sì				
	Visualizzare i volumi di storage rilevati	Sì	Sì	Sì. Progetti personali	Sì. Progetti personali	Sì. Progetti personali.
Risorse - Kubernetes	Distribuire o aggiungere cluster Kubernetes e creare o aggiungere spazi dei nomi	Sì				
	Visualizzare gli spazi dei nomi e i cluster Kubernetes	Sì	Sì	Sì. Progetti personali	Sì. Progetti personali	Sì. Progetti personali
Attività - Richieste	Eliminare i record delle richieste di distribuzione	Sì				
	Visualizzare i record delle richieste di distribuzione	Sì	Sì	Sì. Progetti personali	Sì. Progetti personali	Sì. Progetti personali
Attività - Registri eventi	Visualizzare i registri eventi	Sì	Sì	Sì. Progetti personali	Sì. Progetti personali	Sì. Progetti personali
Connessioni - Account cloud	Creare, aggiornare o eliminare gli account cloud	Sì				

Tabella 2-2. Ruoli di servizio e ruoli di progetto di vRealize Automation Cloud Assembly (continua)

Contesto dell'interfaccia utente	Attività	Amministratore di Cloud Assembly	Visualizzatore di Cloud Assembly	Utente di Cloud Assembly L'utente deve essere un membro o un amministratore del progetto per visualizzare ed eseguire attività correlate al progetto.		
				Amministratore del progetto	Membro del progetto	Visualizzatore del progetto
	Visualizzare gli account cloud	Sì	Sì			
Connessioni - Integrazioni	Creare, aggiornare o eliminare le integrazioni	Sì				
	Visualizzare le integrazioni	Sì	Sì			
Onboarding	Creare, aggiornare o eliminare i piani di onboarding	Sì				
	Visualizzare i piani di onboarding	Sì	Sì			Sì. Progetti personali
Marketplace						
	Visualizzare e aprire la scheda Marketplace	Sì	Sì			
	Utilizzare i modelli cloud scaricati nella scheda Progettazione	Sì		Sì. Se associato ai progetti.	Sì. Se associato ai progetti.	
Marketplace: modelli cloud	Scaricare un modello cloud	Sì				
	Visualizzare i modelli di cloud	Sì	Sì			
Marketplace - Immagini	Scaricare le immagini	Sì				
	Visualizzare le immagini	Sì	Sì			
Marketplace - Download	Visualizzare il registro di tutti gli elementi scaricati	Sì	Sì			
Estendibilità						

Tabella 2-2. Ruoli di servizio e ruoli di progetto di vRealize Automation Cloud Assembly (continua)

Contesto dell'interfaccia utente	Attività	Amministratore di Cloud Assembly	Visualizzatore di Cloud Assembly	Utente di Cloud Assembly L'utente deve essere un membro o un amministratore del progetto per visualizzare ed eseguire attività correlate al progetto.		
				Amministratore del progetto	Membro del progetto	Visualizzatore del progetto
	Visualizzare e aprire la scheda Estendibilità	Sì	Sì			Sì
Eventi	Visualizzare gli eventi di estendibilità	Sì	Sì			
Sottoscrizioni	Creare, aggiornare o eliminare le sottoscrizioni di estendibilità	Sì				
	Disattivare le sottoscrizioni	Sì				
	Visualizzare le sottoscrizioni	Sì	Sì			
Libreria - Argomenti dell'evento	Visualizzare gli argomenti dell'evento	Sì	Sì			
Libreria - Azioni	Creare, aggiornare o eliminare le azioni di estendibilità	Sì				
	Visualizzare le azioni di estendibilità	Sì	Sì			
Libreria - Workflow	Visualizzare i workflow di estendibilità	Sì	Sì			
Attività - Esecuzioni di azione	Annullare o eliminare esecuzioni di azione di estendibilità	Sì				
	Visualizzare le esecuzioni di azione di estendibilità	Sì	Sì			Sì. Progetti personali

Tabella 2-2. Ruoli di servizio e ruoli di progetto di vRealize Automation Cloud Assembly (continua)

Contesto dell'interfaccia utente	Attività	Amministratore di Cloud Assembly	Visualizzatore di Cloud Assembly	Utente di Cloud Assembly L'utente deve essere un membro o un amministratore del progetto per visualizzare ed eseguire attività correlate al progetto.		
				Amministratore del progetto	Membro del progetto	Visualizzatore del progetto
Attività - Esecuzioni di workflow	Visualizzare le esecuzioni di workflow di estendibilità	Sì	Sì			
Progettazione						
Progettazione	Aprire la scheda Progettazione e visualizzare un elenco di modelli cloud	Sì	Sì	Sì. Progetti personali	Sì. Progetti personali	Sì. Progetti personali
Modelli cloud	Creare, aggiornare ed eliminare modelli cloud	Sì		Sì. Progetti personali	Sì. Progetti personali	
	Visualizzare modelli cloud	Sì	Sì	Sì. Progetti personali	Sì. Progetti personali	Sì. Progetti personali
	Scaricare modelli cloud	Sì	Sì	Sì. Progetti personali	Sì. Progetti personali	Sì. Progetti personali
	Caricare modelli cloud	Sì		Sì. Progetti personali	Sì. Progetti personali	
	Distribuire modelli cloud	Sì		Sì. Progetti personali	Sì. Progetti personali	
	Assegnare una versione e ripristinare i modelli cloud	Sì		Sì. Progetti personali	Sì. Progetti personali	
	Rilasciare modelli cloud nel catalogo	Sì		Sì. Progetti personali	Sì. Progetti personali	

Tabella 2-2. Ruoli di servizio e ruoli di progetto di vRealize Automation Cloud Assembly (continua)

Contesto dell'interfaccia utente	Attività	Amministratore di Cloud Assembly	Visualizzatore di Cloud Assembly	Utente di Cloud Assembly L'utente deve essere un membro o un amministratore del progetto per visualizzare ed eseguire attività correlate al progetto.		
				Amministratore del progetto	Membro del progetto	Visualizzatore del progetto
Risorse personalizzate	Creare, aggiornare o eliminare le risorse personalizzate	Sì				
	Visualizzare le risorse personalizzate	Sì	Sì	Sì. Progetti personali	Sì. Progetti personali	Sì. Progetti personali
Azioni personalizzate	Creare, aggiornare o eliminare le azioni personalizzate	Sì				
	Visualizzare le azioni personalizzate	Sì	Sì	Sì. Progetti personali	Sì. Progetti personali	Sì. Progetti personali
Distribuzioni						
	Visualizzare e aprire la scheda Distribuzioni	Sì	Sì	Sì	Sì	Sì
	Visualizzare le distribuzioni, inclusi dettagli della distribuzione, cronologia delle distribuzioni, prezzo, monitoraggio, avvisi, ottimizzazione e informazioni sulla risoluzione dei problemi	Sì	Sì	Sì. Progetti personali	Sì. Progetti personali	Sì. Progetti personali
	Gestire gli avvisi	Sì		Sì. Progetto personale	Sì. progetto personale	

Tabella 2-2. Ruoli di servizio e ruoli di progetto di vRealize Automation Cloud Assembly (continua)

Contesto dell'interfaccia utente	Attività	Amministratore di Cloud Assembly	Visualizzatore di Cloud Assembly	Utente di Cloud Assembly L'utente deve essere un membro o un amministratore del progetto per visualizzare ed eseguire attività correlate al progetto.		
				Amministratore del progetto	Membro del progetto	Visualizzatore del progetto
	Eseguire azioni giorno 2 nelle distribuzioni in base ai criteri	Sì		Sì. Progetti personali	Sì. Progetti personali	
Avvisi						
	Visualizzare e aprire la scheda Avvisi	Sì	Sì	Sì	Sì	Sì
	Gestire gli avvisi	Sì		Sì. Progetti personali	Sì. Progetti personali	
	Visualizzare gli avvisi	Sì	Sì	Sì. Progetti personali	Sì. Progetti personali	Sì. Progetti personali

Ruoli di servizio di Service Broker

I ruoli di servizio di vRealize Automation Service Broker determinano ciò che è possibile visualizzare ed eseguire in vRealize Automation Service Broker. Questi ruoli di servizio sono definiti nella console da un proprietario dell'organizzazione.

Tabella 2-3. Descrizioni dei ruoli di servizio di Service Broker

Ruolo	Descrizione
Amministratore di Service Broker	Deve disporre dell'accesso in lettura e scrittura all'intera interfaccia utente e alle risorse API. Questo è l'unico ruolo utente che può eseguire tutte le attività, ad esempio la creazione di un nuovo progetto e l'assegnazione di un amministratore del progetto.
Utente di Service Broker	Qualsiasi utente che non disponga del ruolo di amministratore di vRealize Automation Service Broker. In un progetto di vRealize Automation Service Broker, l'amministratore aggiunge gli utenti ai progetti come membri del progetto, amministratori o visualizzatori. L'amministratore può anche aggiungere un amministratore del progetto.
Visualizzatore di Service Broker	Utente che ha accesso in lettura per visualizzare le informazioni ma che non può creare, aggiornare o eliminare valori. Gli utenti con il ruolo di visualizzatore possono visualizzare tutte le informazioni disponibili all'amministratore. Non può eseguire alcuna azione a meno che un amministratore non lo renda amministratore del progetto o membro del progetto. Se l'utente è associato a un progetto, dispone delle autorizzazioni correlate al ruolo. Il visualizzatore del progetto non estenderebbe le proprie autorizzazioni nel modo in cui avviene per il ruolo di amministratore o membro.

Oltre ai ruoli di servizio, vRealize Automation Service Broker dispone di ruoli di progetto. Qualsiasi progetto è disponibile in tutti i servizi.

I ruoli di progetto sono definiti in vRealize Automation Service Broker e possono variare tra i progetti.

Nelle tabelle seguenti, che indicano all'utente cosa possono visualizzare ed eseguire i diversi ruoli di servizio e progetto, tenere presente che gli amministratori del servizio dispongono di autorizzazioni complete in tutte le aree dell'interfaccia utente.

L'utilizzo delle seguenti descrizioni dei ruoli di progetto consentirà di decidere quali autorizzazioni concedere agli utenti.

- Gli amministratori del progetto sfruttano l'infrastruttura creata dall'amministratore del servizio per garantire che i loro membri del progetto dispongano delle risorse di cui hanno bisogno per le operazioni di sviluppo.
- I membri del progetto lavorano all'interno dei loro progetti per progettare e distribuire modelli cloud.
- I visualizzatori del progetto sono limitati all'accesso di sola lettura.

Tabella 2-4. Ruoli di servizio e ruoli di progetto di Service Broker

Contesto dell'interfaccia utente	Attività	Amministratore di Service Broker	Visualizzatore di Service Broker	Utente di Service Broker		
				L'utente deve essere un amministratore del progetto per visualizzare ed eseguire attività correlate al progetto.		
				Amministratore del progetto	Membro del progetto	Visualizzatore del progetto
Accesso a Service Broker						
Console	Nella console, è possibile visualizzare e aprire Service Broker	Sì	Sì	Sì	Sì	Sì
Infrastruttura						
	Visualizzare e aprire la scheda Infrastruttura	Sì	Sì			
Configurazione - Progetti	Creare progetti	Sì				
	Aggiornare o eliminare i valori da riepilogo del progetto, provisioning, Kubernetes e integrazioni, nonché testare le configurazioni dei progetti.	Sì				
	Aggiungere utenti e gruppi, nonché assegnare ruoli nei progetti.	Sì		Sì. Progetti personali.		
	Visualizzare i progetti	Sì	Sì	Sì. Progetti personali	Sì. Progetti personali	Sì. Progetti personali
Configurazione - Zone cloud	Creare, aggiornare o eliminare le zone cloud	Sì				
	Visualizzare le zone cloud	Sì	Sì			

Tabella 2-4. Ruoli di servizio e ruoli di progetto di Service Broker (continua)

Contesto dell'interfaccia utente	Attività	Amministratore di Service Broker	Visualizzatore di Service Broker	Utente di Service Broker L'utente deve essere un amministratore del progetto per visualizzare ed eseguire attività correlate al progetto.		
				Amministratore del progetto	Membro del progetto	Visualizzatore del progetto
Configurazione - Zone Kubernetes	Creare, aggiornare o eliminare le zone Kubernetes	Sì				
	Visualizzare le zone Kubernetes	Sì	Sì			
Connessioni - Account cloud	Creare, aggiornare o eliminare gli account cloud	Sì				
	Visualizzare gli account cloud	Sì	Sì			
Connessioni - Integrazioni	Creare, aggiornare o eliminare le integrazioni	Sì				
	Visualizzare le integrazioni	Sì	Sì			
Attività - Richieste	Eliminare i record delle richieste di distribuzione	Sì				
	Visualizzare i record delle richieste di distribuzione	Sì				
Attività - Registri eventi	Visualizzare i registri eventi	Sì				
Contenuto e criteri						
	Visualizzare e aprire la scheda Contenuto e criteri	Sì	Sì			

Tabella 2-4. Ruoli di servizio e ruoli di progetto di Service Broker (continua)

Contesto dell'interfaccia utente	Attività	Amministratore di Service Broker	Visualizzatore di Service Broker	Utente di Service Broker L'utente deve essere un amministratore del progetto per visualizzare ed eseguire attività correlate al progetto.		
				Amministratore del progetto	Membro del progetto	Visualizzatore del progetto
Origini contenuto	Creare, aggiornare o eliminare le origini del contenuto	Sì				
	Visualizzare le origini del contenuto	Sì	Sì			
Condivisione contenuto	Aggiungere o rimuovere il contenuto condiviso	Sì				
	Visualizzare il contenuto condiviso	Sì	Sì			
Contenuto	Personalizzare modulo e configurare l'elemento	Sì				
	Visualizzare il contenuto	Sì	Sì			
Criteri - Definizioni	Creare, aggiornare o eliminare le definizioni dei criteri	Sì				
	Visualizzare le definizioni dei criteri	Sì	Sì			
Criteri - Imposizione	Visualizzare il registro di imposizioni	Sì	Sì			
Notifiche - Server email	Configurare un server email	Sì				
Catalogo						
	Visualizzare e aprire la scheda Catalogo	Sì	Sì	Sì	Sì	Sì

Tabella 2-4. Ruoli di servizio e ruoli di progetto di Service Broker (continua)

Contesto dell'interfaccia utente	Attività	Amministratore di Service Broker	Visualizzatore di Service Broker	Utente di Service Broker L'utente deve essere un amministratore del progetto per visualizzare ed eseguire attività correlate al progetto.		
				Amministratore del progetto	Membro del progetto	Visualizzatore del progetto
	Visualizzare gli elementi del catalogo disponibili	Sì	Sì	Sì. Progetti personali	Sì. Progetti personali	Sì. Progetti personali
	Richiedere un elemento del catalogo	Sì		Sì. Progetti personali	Sì. Progetti personali	
Distribuzioni						
	Visualizzare e aprire la scheda Distribuzioni	Sì	Sì	Sì.	Sì	Sì
	Visualizzare le distribuzioni, inclusi dettagli della distribuzione, cronologia delle distribuzioni, prezzo, monitoraggio, avvisi, ottimizzazione e informazioni sulla risoluzione dei problemi	Sì	Sì	Sì. Progetti personali	Sì. Progetti personali	Sì. Progetti personali
	Gestire gli avvisi	Sì		Sì. Progetti personali	Sì. Progetti personali	
	Eseguire azioni giorno 2 nelle distribuzioni in base ai criteri	Sì		Sì. Progetti personali	Sì. Progetti personali	
Approvazioni						

Tabella 2-4. Ruoli di servizio e ruoli di progetto di Service Broker (continua)

Contesto dell'interfaccia utente	Attività	Amministratore di Service Broker	Visualizzatore di Service Broker	Utente di Service Broker L'utente deve essere un amministratore del progetto per visualizzare ed eseguire attività correlate al progetto.		
				Amministratore del progetto	Membro del progetto	Visualizzatore del progetto
	Visualizzare e aprire la scheda Approvazioni	Sì	Sì	Sì	Sì	Sì
	Rispondere alle richieste di approvazione	Sì		Solo ruolo utente di Service Broker	Solo ruolo utente di Service Broker	Solo ruolo utente di Service Broker

Abilitazione del banner dell'informativa e del consenso del Dipartimento della Difesa

Per alcuni clienti governativi, per consentire agli utenti di accedere a vRealize Automation, un amministratore deve configurare il banner standard dell'informativa e del consenso del Dipartimento della Difesa (DoD) in Workspace ONE Access.

Il testo del banner obbligatorio standard dell'informativa e del consenso del Dipartimento della Difesa è il seguente:

Stai per accedere al Sistema informativo (IS) del Governo degli Stati Uniti (USG), utilizzabile solo previa autorizzazione dell'USG. Utilizzando questo IS, inclusi tutti i dispositivi allegati a questo IS, accetti implicitamente le seguenti condizioni:

- L'USG intercetta e monitora regolarmente le comunicazioni su questo IS per diverse finalità, inclusi a titolo esemplificativo test di penetrazione, monitoraggio COMSEC, operazioni e difesa di rete, cattiva condotta del personale (PM), imposizione della legge (LE) e investigazioni del controspionaggio (CI).
- In qualsiasi momento, l'USG può ispezionare e analizzare i dati archiviati nell'IS.
- Le comunicazioni che utilizzano questo IS o i dati ivi memorizzati non sono privati e sono regolarmente soggetti a monitoraggio, intercettazioni e ricerche e possono essere divulgati o utilizzati per qualsiasi scopo autorizzato dall'USG.

La procedura seguente descrive come configurare questo banner in Workspace ONE Access. Per ulteriori informazioni, vedere la documentazione della console di amministrazione di Workspace ONE Access.

Procedura

- 1 Accedere alla console di amministrazione di Workspace ONE Access come amministratore.

- 2 Nella console di VMware Identity Manager, fare clic sulla scheda Gestione identità e accessi.
- 3 Fare clic su Configurazione e quindi sulla scheda Connettori.
- 4 Fare clic sul collegamento Worker per ogni connettore che si desidera configurare.
- 5 Fare clic sulla scheda Adattatori autenticazione e quindi su `CertificateAuthAdapter`.
- 6 Fare clic sulla casella di controllo Abilita modulo di consenso prima dell'autenticazione.
- 7 Incollare il testo del banner standard dell'informativa e del consenso del Dipartimento della Difesa nella casella Contenuto modulo di consenso.
- 8 Salvare le modifiche.

Risultati

Manutenzione dell'appliance vRealize Automation

3

In qualità di amministratore di sistema, potrebbe essere necessario eseguire varie attività per garantire il corretto funzionamento dell'applicazione vRealize Automation installata.

Se si sta iniziando a utilizzare vRealize Automation, queste attività non sono necessarie. Sapere come eseguire queste attività è utile per risolvere i problemi relativi alle prestazioni o al comportamento del prodotto.

Questo capitolo include i seguenti argomenti:

- [Avvio e arresto di vRealize Automation](#)
- [Scalabilità orizzontale di vRealize Automation da uno a tre nodi](#)
- [Sostituzione di un nodo dell'appliance vRealize Automation](#)
- [Aumento delle dimensioni del disco dell'appliance vRealize Automation](#)
- [Aggiornamento dell'assegnazione DNS per vRealize Automation](#)
- [Come abilitare la sincronizzazione dell'ora di vRealize Automation](#)
- [Come reimpostare la password root per vRealize Automation](#)

Avvio e arresto di vRealize Automation

Osservare le procedure appropriate all'avvio o all'arresto di vRealize Automation.

La modalità consigliata per arrestare e avviare i componenti di vRealize Automation consiste nell'utilizzare la funzionalità di spegnimento e accensione fornita nella sezione **Lifecycle Operations > Ambienti** di vRealize Suite Lifecycle Manager. Le procedure seguenti illustrano i metodi manuali per arrestare e avviare componenti di vRealize Automation nel caso in cui vRealize Suite Lifecycle Manager non sia disponibile per qualche motivo.

Arresto di vRealize Automation

Per preservare l'integrità dei dati, arrestare i servizi di vRealize Automation prima di spegnere le appliance virtuali. Quando si utilizza SSH o VMRC, è possibile arrestare o avviare tutti i nodi da qualsiasi appliance singola.

Nota Evitare di utilizzare i comandi `vracli reset vidm`, se possibile. Questo comando reimposta tutte le configurazioni di Workspace ONE Access e interrompe l'associazione tra gli utenti e le risorse sottoposte a provisioning.

- 1 Accedere alla console di qualsiasi appliance vRealize Automation utilizzando SSH o VMRC.
- 2 Per arrestare i servizi di vRealize Automation in tutti i nodi del cluster, eseguire la seguente serie di comandi.

Nota Se si copia uno di questi comandi da eseguire e questi non riescono, incollarli prima in Blocco note, quindi copiarli di nuovo prima di eseguirli. Questa procedura rimuove tutti i caratteri nascosti e gli altri artefatti che potrebbero esistere nell'origine della documentazione.

```
/opt/scripts/svc-stop.sh  
sleep 120  
/opt/scripts/deploy.sh --onlyClean
```

- 3 Arrestare le appliance vRealize Automation.

La distribuzione di vRealize Automation è ora arrestata.

Avvio di vRealize Automation

Dopo un arresto non pianificato, un arresto controllato o una procedura di ripristino, è necessario riavviare i componenti di vRealize Automation in un ordine specifico. vRLCM è un componente non critico, quindi è possibile avviarlo in qualsiasi momento. I componenti di VMware Workspace ONE Access, in precedenza denominato VMware Identity Management, devono essere avviati prima di avviare vRealize Automation.

Nota Verificare che i bilanciamenti del carico applicabili siano in esecuzione prima di avviare i componenti di vRealize Automation.

- 1 Accendere tutte le appliance vRealize Automation e attendere che vengano avviate.
- 2 Accedere alla console di qualsiasi appliance utilizzando SSH o VMRC ed eseguire il comando seguente per ripristinare i servizi in tutti i nodi.

```
/opt/scripts/deploy.sh
```

- 3 Verificare che tutti i servizi siano attivi e in esecuzione con il seguente comando.

```
kubectl get pods --all-namespaces
```

Nota Dovrebbero essere visualizzate tre istanze di ogni servizio, con lo stato In esecuzione o Completato.

Quando tutti i servizi sono elencati come In Esecuzione o Completato, vRealize Automation è già pronto per l'uso.

Riavvio di vRealize Automation

È possibile riavviare tutti i servizi di vRealize Automation centralmente da qualsiasi appliance nel cluster. Seguire le istruzioni precedenti per arrestare vRealize Automation, quindi attenersi alle istruzioni per avviare vRealize Automation. Prima di riavviare vRealize Automation, verificare che tutti i componenti di bilanciamento del carico e VMware Workspace ONE Access applicabili siano in esecuzione.

Quando tutti i servizi sono elencati come In Esecuzione o Completato, vRealize Automation è già pronto per l'uso.

Eseguire il comando seguente per verificare che tutti i servizi siano in esecuzione:

```
kubectl -n prelude get pods
```

Scalabilità orizzontale di vRealize Automation da uno a tre nodi

Quando è necessario espandere, è possibile scalare orizzontalmente una distribuzione di vRealize Automation da un nodo a tre nodi.

Per completare molti passaggi di questa procedura, è necessario utilizzare le funzionalità di vRealize Suite Lifecycle Manager. Per informazioni sull'installazione, l'aggiornamento e la gestione di vRealize Suite Lifecycle Manager, vedere la [documentazione del prodotto di Lifecycle Manager](#).

Se si utilizza una distribuzione in cluster a tre nodi, vRealize Automation in genere può resistere all'errore di un nodo e continuare a funzionare. L'errore di due nodi in un cluster a tre nodi renderà vRealize Automation non funzionante.

Prerequisiti

Questa procedura presuppone che si disponga già di una distribuzione di un singolo nodo di vRealize Automation funzionante.

Procedura

1 Arrestare tutte le appliance vRealize Automation.

Per arrestare i servizi di vRealize Automation in tutti i nodi del cluster, eseguire il seguente set di comandi.

```
/opt/scripts/svc-stop.sh
sleep 120
/opt/scripts/deploy.sh --onlyClean
```

A questo punto è possibile arrestare le appliance vRealize Automation.

2 Acquisire uno snapshot della distribuzione.

Utilizzare l'opzione Crea snapshot in vRealize Suite Lifecycle Manager **Lifecycle Operations > Ambienti > vRA > Visualizza dettagli**.

Nota Gli snapshot online, acquisiti senza arrestare i nodi di vRealize Automation, sono supportati dalla versione 8.0.1. Per gli ambienti vRealize Automation 8.0, è necessario arrestare prima i nodi di vRealize Automation.

3 Accendere l'appliance vRealize Automation e richiamare tutti i contenitori.

4 Utilizzando la funzionalità di Locker situata in **LCM > Locker > Certificati** in vRealize Suite Lifecycle Manager, generare o importare i certificati di vRealize Automation per tutti i componenti, inclusi nomi di dominio completi del nodo di vRealize Suite Lifecycle Manager e il nome di dominio completo del bilanciamento del carico di vRealize Automation.

Aggiungere i nomi di tutte e tre le appliance nei SAN (Subject Alternative Name).

5 Importare il nuovo certificato in vRealize Suite Lifecycle Manager.

6 Sostituire il certificato di vRealize Suite Lifecycle Manager esistente con quello generato nel passaggio precedente utilizzando l'opzione LCM **Lifecycle Operations > Ambienti > vRA > Visualizza dettagli** Sostituisci certificato.

7 Scalare in orizzontale vRealize Automation a tre nodi utilizzando la selezione Aggiungi componenti in **LCM > Lifecycle Operations > Ambienti > vRA > Visualizza dettagli**.

Risultati

vRealize Automation è stato scalato a una distribuzione a tre nodi.

Sostituzione di un nodo dell'appliance vRealize Automation

Quando un'appliance vRealize Automation in una configurazione a più nodi con alta disponibilità (HA) non riesce, potrebbe essere necessario sostituire il nodo in cui si è verificato il problema.

Attenzione Prima di procedere, VMware consiglia di contattare il supporto tecnico per risolvere il problema relativo all'alta disponibilità e verificare che il problema sia isolato in un solo nodo.

Se il supporto tecnico stabilisce che è necessario sostituire il nodo, eseguire i passaggi seguenti.

- 1 In vCenter, creare snapshot di backup di ogni appliance nella configurazione HA.

Negli snapshot di backup, non includere la memoria della macchina virtuale.

- 2 Arrestare il nodo in cui si è verificato il problema.
- 3 Prendere nota delle impostazioni di rete e del numero di build del software vRealize Automation del nodo in cui si è verificato il problema.

Prendere nota del nome di dominio completo, dell'indirizzo IP, del gateway, dei server DNS e in particolare dell'indirizzo MAC. Più tardi sarà necessario assegnare gli stessi valori al nodo sostitutivo.

- 4 Il nodo primario del database deve essere uno dei nodi integri. Eseguire i passaggi seguenti:

- a Accedere come root alla riga di comando di un nodo integro.
- b Individuare il nome del nodo primario del database eseguendo il comando seguente.

```
vracli status | grep primary -B 1
```

Il risultato deve essere simile a questo esempio, dove postgres-1 è il nodo primario del database.

```
"Conninfo":
"host=postgres-1.postgres.prelude.svc.cluster.local
dbname=repmgr-db user=repmgr-db passfile=/scratch/repmgr-db.cred
connect_timeout=10",
"Role": "primary",
```

- c Verificare che il nodo primario del database sia integro eseguendo il comando seguente.

```
kubectl -n prelude get pods -o wide | grep postgres
```

Il risultato deve essere simile a questo esempio, dove postgres-1 risulta in esecuzione e integro nell'elenco.

```
postgres-1 1/1 Running 0 39h 12.123.2.14 vc-vm-224-84.company.com <none> <none>
postgres-2 1/1 Running 0 39h 12.123.1.14 vc-vm-224-85.company.com <none> <none>
```

Importante Se è presente un problema nel nodo primario del database, contattare il supporto tecnico anziché procedere.

- 5 Dalla riga di comando root del nodo integro, rimuovere il nodo in cui si è verificato il problema.

```
vracli cluster remove faulty-node-FQDN
```

- 6 Utilizzare vCenter per distribuire un nuovo nodo di vRealize Automation sostitutivo.

Distribuire lo stesso numero di build del software vRealize Automation e applicare le impostazioni di rete del nodo in cui si è verificato il problema. Includere il nome di dominio completo, l'indirizzo IP, il gateway, i server DNS e in particolare l'indirizzo MAC di cui si è preso nota in precedenza.

- 7 Accendere il nodo sostitutivo.
- 8 Accedere come root alla riga di comando del nodo sostitutivo.
- 9 Verificare che la sequenza di avvio iniziale sia terminata eseguendo il comando seguente.

```
vracli status first-boot
```

Cercare un messaggio `First boot complete`.

- 10 Dal nodo sostitutivo, aggiungere il cluster di vRealize Automation.

```
vracli cluster join primary-DB-node-FQDN
```

- 11 Accedere come root alla riga di comando del nodo primario del database.
- 12 Distribuire il cluster riparato eseguendo lo script seguente.

```
/opt/scripts/deploy.sh
```

Aumento delle dimensioni del disco dell'appliance vRealize Automation

Potrebbe essere necessario aumentare lo spazio del disco dell'appliance vRealize Automation, ad esempio per lo storage del file di registro.

Procedura

- 1 Utilizzare vSphere per espandere il VMDK nell'appliance vRealize Automation.
- 2 Accedere alla riga di comando dell'appliance vRealize Automation come utente root.
- 3 Dal prompt dei comandi, eseguire il comando di vRealize Automation seguente:

```
vracli disk-mgr resize
```

Se il ridimensionamento di vRealize Automation non riesce, consultare l'[articolo 79925 della Knowledge Base](#).

Aggiornamento dell'assegnazione DNS per vRealize Automation

Un amministratore può aggiornare le assegnazioni DNS per vRealize Automation.

Procedura

- 1 Accedere alla console di un'appliance qualsiasi di vRealize Automation utilizzando SSH o VMRC.
- 2 Eseguire il comando seguente.

```
vracli network dns set --servers DNS1,DNS2
```


- 3 Verificare che i nuovi server DNS siano stati applicati correttamente a tutti i nodi di vRealize Automation con il comando `vracli network dns status`.
- 4 Eseguire il seguente set di comandi per arrestare i servizi di vRealize Automation in tutti i nodi del cluster.

```
/opt/scripts/svc-stop.sh  
sleep 120  
/opt/scripts/deploy.sh --onlyClean
```

- 5 Riavviare i nodi di vRealize Automation e attendere che vengano avviati completamente.
- 6 Accedere a ciascun nodo di vRealize Automation con SSH e verificare che i nuovi server DNS siano elencati in `/etc/resolve.conf`.
- 7 In uno dei nodi di vRealize Automation, eseguire il comando seguente per avviare i servizi di vRealize Automation: `/opt/scripts/deploy.sh`

Risultati

Le impostazioni DNS di vRealize Automation vengono modificate come specificato.

Come abilitare la sincronizzazione dell'ora di vRealize Automation

È possibile abilitare la sincronizzazione dell'ora nella distribuzione di vRealize Automation utilizzando la riga di comando dell'appliance vRealize Automation.

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

Configurazione NTP	Descrizione
ESXi	<p>È possibile utilizzare questa configurazione quando il server ESXi che ospita vRealize Automation è sincronizzato con un server NTP. Se si utilizza una distribuzione in cluster, tutti gli host di ESXi devono essere sincronizzati con un server NTP. Per ulteriori informazioni sulla configurazione di NTP per ESXi, vedere l'articolo KB 57147 Configurazione del protocollo NTP (Network Time Protocol) in un host di ESXi tramite vSphere Web Client.</p> <p>Nota È possibile che si verifichi una deviazione dell'orologio se la distribuzione di vRealize Automation viene migrata in un host ESXi non sincronizzato con un server NTP.</p>
systemd	<p>Questa configurazione utilizza il daemon systemd-timesyncd per sincronizzare gli orologi della distribuzione di vRealize Automation.</p> <p>Nota Per impostazione predefinita, il daemon systemd-timesyncd è abilitato, ma è configurato senza server NTP. Se l'appliance vRealize Automation utilizza una configurazione IP dinamica, l'appliance può utilizzare tutti i server NTP ricevuti dal protocollo DHCP.</p>

Procedura

- 1 Accedere alla riga di comando dell'appliance vRealize Automation come **root**.
- 2 Abilitare NTP con ESXi.
 - a Eseguire il comando `vracli ntp esxi`.
 - b (Facoltativo) Per verificare lo stato della configurazione NTP, eseguire il comando `vracli ntp status`.

È inoltre possibile reimpostare la configurazione NTP allo stato predefinito eseguendo il comando `vracli ntp reset`.

- 3 Abilitare NTP con systemd.
 - a Eseguire il comando `vracli ntp systemd --set FQDN_or_IP_of_systemd_server`.

Nota È possibile aggiungere più server NTP di systemd separando gli indirizzi di rete con una virgola. Ogni indirizzo di rete deve essere racchiuso tra apici. Ad esempio `vracli ntp systemd --set 'ntp_address_1','ntp_address_2'`

- b (Facoltativo) Per verificare lo stato della configurazione NTP, eseguire il comando `vracli ntp status`.

Risultati

È stata abilitata la sincronizzazione dell'ora per la distribuzione dell'appliance vRealize Automation.

Operazioni successive

La configurazione NTP può non riuscire se è presente una differenza temporale superiore a 10 minuti tra il server NTP e la distribuzione di vRealize Automation. Per risolvere questo problema, riavviare l'appliance vRealize Automation.

Come reimpostare la password root per vRealize Automation

È possibile reimpostare una password root di vRealize Automation se è stata persa o dimenticata.

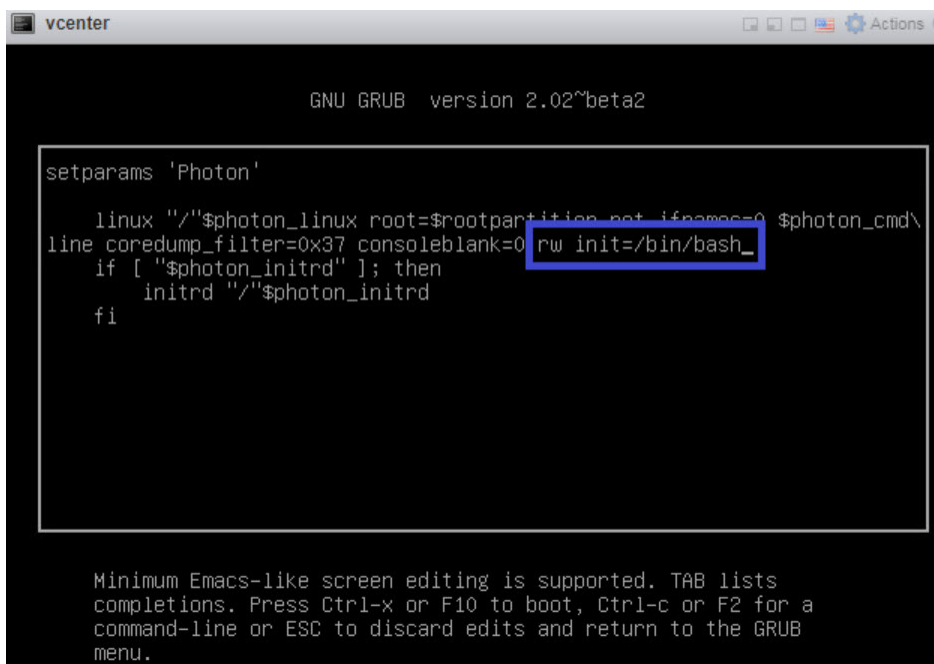
In questa procedura, si utilizza una finestra della riga di comando nell'appliance vCenter host per reimpostare la password root di vRealize Automation dell'organizzazione.

Prerequisiti

Questo processo può essere eseguito dagli amministratori di vRealize Automation e richiede le credenziali necessarie per accedere all'appliance vCenter host.

Procedura

- 1 Arrestare e avviare vRealize Automation utilizzando la procedura descritta in [Avvio e arresto di vRealize Automation](#).
- 2 Quando viene visualizzata la finestra della riga di comando del sistema operativo Photon, immettere `e` e premere il tasto **Invio** per aprire l'editor del menu di avvio di GNU GRUB.
- 3 Nell'editor di GNU GRUB, immettere `rw init=/bin/bash` alla fine della riga che inizia con `linux` `"/" $photon_linux root=rootpartition` come illustrato di seguito:



```

vcenter
GNU GRUB version 2.02~beta2

setparams 'Photon'

linux "/"$photon_linux root=$rootpartition not_ifnops=0 $photon_cmd\
line coredump_filter=0x37 consoleblank=0 rw init=/bin/bash_
if [ "$photon_initrd" ]; then
    initrd "/"$photon_initrd
fi

Minimum Emacs-like screen editing is supported. TAB lists
completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a
command-line or ESC to discard edits and return to the GRUB
menu.
  
```

- 4 Premere il tasto **F10** per eseguire il push della modifica e riavviare vRealize Automation.

- 5 Attendere il riavvio di vRealize Automation.
- 6 Al prompt `root [/]#`, immettere `passwd` e premere il tasto **Invio**.
- 7 Al prompt `New password:`, immettere la nuova password e premere il tasto **Invio**.
- 8 Al prompt `Retype new password:`, immettere di nuovo la nuova password e premere il tasto **Invio**.
- 9 Al prompt `root [/]#`, immettere `reboot -f` e premere il tasto **Invio** per completare il processo di reimpostazione della password root.

```
root [ / ]# passwd
New password:
Retype new password:
passwd: password updated successfully
root [ / ]# reboot -f_
```

Operazioni successive

In qualità di amministratore di vRealize Automation, è ora possibile accedere a vRealize Automation con la nuova password root.

Utilizzo di configurazioni tenant multi-organizzazione in vRealize Automation

4

vRealize Automation consente ai provider IT di configurare più tenant oppure organizzazioni all'interno di ciascuna distribuzione. I provider possono configurare più organizzazioni tenant e allocare l'infrastruttura all'interno di ogni distribuzione. I provider possono anche gestire gli utenti per i tenant. Ogni tenant gestisce i propri progetti, risorse e distribuzioni.

In una configurazione multi-organizzazione di vRealize Automation, i provider possono creare più organizzazioni e ogni organizzazione tenant utilizza i propri progetti, risorse e distribuzioni. Sebbene i provider non possano gestire l'infrastruttura tenant da remoto, possono accedere ai tenant e gestire l'infrastruttura all'interno dei relativi tenant.

La multi-tenancy si basa sulla coordinazione e sulla configurazione di tre diversi prodotti VMware, come indicato di seguito:

- **Workspace ONE Access:** questo prodotto fornisce il supporto dell'infrastruttura per la multi-tenancy e le connessioni al dominio di Active Directory che forniscono la gestione di utenti e gruppi all'interno delle organizzazioni tenant.
- **vRealize Suite Lifecycle Manager:** questo prodotto supporta la creazione e la configurazione dei tenant per i prodotti supportati, ad esempio vRealize Automation. Inoltre, fornisce alcune funzionalità di gestione dei certificati.
- **vRealize Automation:** i provider e gli utenti accedono a vRealize Automation per accedere ai tenant in cui creano e gestiscono le distribuzioni.

Quando si configura la multi-tenancy, gli utenti devono avere familiarità con tutti i tre prodotti e la documentazione associata.

Per ulteriori informazioni sull'utilizzo di vRealize Suite Lifecycle Manager e Workspace ONE Access, vedere quanto segue.

- **vRealize Suite Lifecycle Manager:** vedere la [documentazione del prodotto Lifecycle Manager](#)
- **Workspace ONE Access:** vedere [Gestione utenti con VMware Identity Manager e Amministrazione di VMware Workspace ONE Access](#)

Gli amministratori con privilegi di vRealize Suite Lifecycle Manager creano e gestiscono i tenant utilizzando la pagina Tenant di Lifecycle Manager situata sotto il servizio Gestione di identità e tenant. I tenant vengono creati utilizzando una connessione IWA o LDAP di Active Directory e sono supportati dall'istanza di VMware Workspace ONE Access associata necessaria per le distribuzioni di vRealize Automation. Per informazioni sull'utilizzo di Lifecycle Manager, vedere la documentazione associata.

Quando si configura la multi-tenancy, si inizia con un tenant di base o master. Questo tenant è il tenant predefinito creato quando viene distribuita l'applicazione Workspace ONE Access sottostante. Gli altri tenant, noti come tenant secondari, possono essere basati sul tenant master. vRealize Automation attualmente supporta fino a 20 organizzazioni tenant con la distribuzione standard di tre nodi.

Prima di abilitare vRealize Automation per la multi-tenancy, è innanzitutto necessario installare l'applicazione in una singola configurazione dell'organizzazione e quindi utilizzare Lifecycle Manager per configurare una configurazione multi-organizzazione. Una distribuzione di Workspace ONE Access supporta la gestione dei tenant e le connessioni al dominio di Active Directory associate.

Durante la configurazione iniziale della multi-tenancy, viene designato un amministratore del provider in Lifecycle Manager. Se necessario, è possibile modificare questa designazione o aggiungere gli amministratori in un secondo momento. Nelle configurazioni con più organizzazioni, gli utenti e i gruppi di vRealize Automation vengono gestiti principalmente tramite Workspace ONE Access.

Dopo avere creato le organizzazioni, gli utenti autorizzati possono accedere alle proprie applicazioni per creare o lavorare con progetti e risorse e creare distribuzioni. Gli amministratori possono gestire i ruoli degli utenti in vRealize Automation.

Impostazione di una configurazione multi-organizzazione

È possibile abilitare una distribuzione multi-organizzazione dopo aver completato un'installazione di vRealize Automation. Quando si configura una configurazione multi-organizzazione, è necessario configurare il Workspace ONE Access esterno per l'utilizzo della multi-tenancy e quindi utilizzare Lifecycle Manager per creare e configurare i tenant. Questo vale per le distribuzioni nuove ed esistenti. Come passaggio iniziale per l'impostazione dei tenant, è necessario utilizzare Lifecycle Manager per impostare un alias per il tenant master creato per impostazione predefinita in Workspace ONE Access. I tenant secondari creati in base a questo tenant master ereditano le configurazioni del dominio di Active Directory da questo tenant master.

In Lifecycle Manager, assegnare i tenant a un prodotto, ad esempio vRealize Automation, e a un ambiente specifico. Quando si configura un tenant, è necessario designare anche un amministratore tenant. Per impostazione predefinita, la multi-tenancy è abilitata in base al nome host del tenant. Gli utenti possono scegliere di configurare manualmente il nome del tenant in base al nome DNS. Durante questa procedura, è necessario impostare diversi contrassegni per supportare la multi-tenancy ed è necessario configurare anche il bilanciamento del carico.

Se si utilizza un'istanza in cluster, i nomi host basati sui tenant di Workspace ONE Access e vRealize Automation faranno riferimento al bilanciamento del carico.

Se i bilanciamenti del carico di vRealize Automation e Workspace ONE Access in cluster non utilizzano certificati con caratteri jolly, gli utenti devono aggiungere i nomi host dei tenant come voci SAN nei certificati per ogni nuovo tenant creato.

Non è possibile eliminare i tenant in vRealize Automation o in Lifecycle Manager. Se è necessario aggiungere tenant a una distribuzione multi-tenancy esistente, è possibile eseguire questa operazione utilizzando Lifecycle Manager, ma richiederà un tempo di inattività di tre o quattro ore.

Per ulteriori informazioni sull'utilizzo di vRealize Suite Lifecycle Manager Workspace ONE Access, fare riferimento ai collegamenti della documentazione all'inizio di questo argomento.

Nomi host e multi-tenancy

Nelle versioni precedenti di vRealize Automation, gli utenti effettuavano l'accesso ai tenant con URL basati sul percorso della directory. Nell'implementazione multi-tenancy corrente, gli utenti accedono ai tenant in base al nome host.

Inoltre, il formato del nome host che gli utenti di vRealize Automation utilizzeranno per accedere ai tenant differisce dal formato utilizzato per accedere ai tenant all'interno di Workspace ONE Access. Ad esempio, un nome host valido sarà simile al seguente:

`tenant1.example.eng.vmware.com` in contrapposizione a `vidm-node1.eng.vmware.com`.

Multi-tenancy e certificati

È necessario creare certificati per tutti i componenti coinvolti in una configurazione multi-organizzazione. È necessario disporre di uno o più certificati per Workspace ONE Access, Lifecycle Manager e vRealize Automation, a seconda che si stia utilizzando una configurazione di un singolo nodo o una configurazione in cluster.

Quando si configurano i certificati, è possibile utilizzare i caratteri jolly con i nomi di SAN o i nomi dedicati. L'utilizzo dei caratteri jolly semplifica in qualche modo la gestione dei certificati, poiché i certificati devono essere aggiornati ogni volta che si aggiungono nuovi tenant. Se i bilanciamenti del carico di vRealize Automation e Workspace ONE Access non utilizzano certificati con caratteri jolly, è necessario aggiungere nomi host tenant come voci SAN nei certificati per ogni nuovo tenant creato. Inoltre, se si utilizza SAN, i certificati devono essere aggiornati manualmente se si aggiungono o eliminano host oppure si modifica un nome host. È inoltre necessario aggiornare le voci DNS per i tenant.

Si tenga presente che Lifecycle Manager non crea certificati separati per ogni tenant. Crea invece un certificato singolo con il nome host di ogni tenant elencato. Per le configurazioni di base, il CNAME del tenant utilizza il formato seguente: `tenantname.vrahostname.domain`. Per le configurazioni ad alta disponibilità, il nome utilizza il formato seguente: `tenantname.vraLBhostname.domain`.

Se si utilizza una configurazione di Workspace ONE Access in cluster, tenere presente che Lifecycle Manager non è in grado di aggiornare il certificato di bilanciamento del carico, quindi è necessario aggiornarlo manualmente. Inoltre, se è necessario registrare nuovamente i prodotti o i servizi esterni a Lifecycle Manager, si tratta di un processo manuale.

Questo capitolo include i seguenti argomenti:

- [Configurazione della tenancy multi-organizzazione per vRealize Automation](#)
- [Accesso ai tenant e aggiunta di utenti in vRealize Automation](#)
- [Utilizzo di vRealize Orchestrator con le distribuzioni multi-organizzazione di vRealize Automation](#)

Configurazione della tenancy multi-organizzazione per vRealize Automation

È possibile configurare la tenancy multi-organizzazione per vRealize Automation utilizzando vRealize Suite Lifecycle Manager.

Di seguito è riportata una descrizione di alto livello della procedura per configurare la multi-tenancy per vRealize Automation, inclusa la configurazione di DNS e certificati. Si concentra su una distribuzione di un singolo nodo, ma include note per una configurazione in cluster.

Vedere <https://vmwarelab.org/2020/04/14/vrealize-automation-8-1-multi-tenancy-setup-with-vrealize-suite-lifecycle-manager-8-1/> per ulteriori informazioni e una dimostrazione video sulla configurazione di una configurazione multi-organizzazione di vRealize Automation.

Prerequisiti

- Installare e configurare Workspace ONE Access versione 3.3.4.
- Installare e configurare vRealize Suite Lifecycle Manager versione 8.3.

Procedura

1 Creare i record DNS di tipo A e CNAME richiesti.

- Per il tenant master e ciascun sub-tenant, è necessario creare e applicare un certificato SAN.
- Per le distribuzioni con un singolo nodo, il nome di dominio completo di vRealize Automation fa riferimento all'appliance vRealize Automation e il nome di dominio completo di Workspace ONE Access fa riferimento all'appliance Workspace ONE Access.
- Per le distribuzioni in cluster, i nomi di dominio completi basati su tenant di Workspace ONE Access e vRealize Automation devono puntare ai rispettivi bilanciamenti del carico. Workspace ONE Access è configurato con la terminazione SSL, quindi il certificato viene applicato sia nel cluster che nel bilanciamento del carico di Workspace ONE Access. Il bilanciamento del carico di vRealize Automation utilizza il passthrough SSL, quindi il certificato viene applicato solo nel cluster di vRealize Automation.

Per ulteriori dettagli, vedere [Gestione della configurazione dei certificati e di DNS in distribuzioni di più organizzazioni con un solo nodo](#) e [Gestione della configurazione del certificato e di DNS nelle distribuzioni di vRealize Automation in cluster](#).

- 2 Creare o importare i certificati SAN multi-dominio richiesti sia per Workspace ONE Access che per vRealize Automation.

È possibile creare certificati in Lifecycle Manager utilizzando il servizio Locker che consente di creare licenze di certificati e password. In alternativa, è possibile utilizzare un server CA o un altro meccanismo per generare certificati.

Se è necessario aggiungere o creare tenant aggiuntivi, è necessario ricreare e applicare i tenant di vRealize Automation e Workspace ONE Access.

Dopo aver creato i certificati, è possibile applicarli in Lifecycle Manager utilizzando la funzionalità Lifecycle Operations. È necessario selezionare l'ambiente e il prodotto e quindi l'opzione Sostituisci certificato nel menu a destra. È quindi possibile selezionare il prodotto. Quando si sostituisce un certificato, è necessario considerare di nuovo attendibili tutti i prodotti associati nell'ambiente in uso.

È necessario attendere l'applicazione del certificato e riavviare tutti i servizi prima di procedere con il passaggio successivo.

Per ulteriori dettagli, vedere [Gestione della configurazione dei certificati e di DNS in distribuzioni di più organizzazioni con un solo nodo](#) e [Gestione della configurazione del certificato e di DNS nelle distribuzioni di vRealize Automation in cluster](#).

- 3 Applicare il certificato SAN di Workspace ONE Access nell'istanza o nel cluster di Workspace ONE Access.
- 4 In vRealize Suite Lifecycle Manager, eseguire la procedura guidata Abilita tenancy per abilitare la multi-tenancy e creare un alias per il tenant master predefinito.

L'abilitazione della tenancy richiede la creazione di un alias per il tenant master dell'organizzazione del provider o il tenant predefinito. Dopo aver abilitato la tenancy, è possibile accedere a Workspace ONE Access tramite il nome di dominio completo del tenant master.

Ad esempio, se il nome di dominio completo di Workspace ONE Access esistente è `idm.example.local` e si crea un alias di tenant predefinito, dopo avere abilitato la tenancy, il nome di dominio completo di Workspace ONE Access viene modificato in `default-tenant.example.local` e tutti i client che comunicano con Workspace ONE Access ora comunicano con `default-tenant.example.local`.

- 5 Applicare i certificati SAN di vRealize Automation nell'istanza o nel cluster di vRealize Automation.

È possibile applicare certificati SAN tramite il servizio Lifecycle Manager Lifecycle Operations. È necessario visualizzare i dettagli dell'ambiente, quindi selezionare Sostituisci certificati nel menu a destra. Prima di aggiungere i tenant, è necessario attendere il completamento dell'attività di sostituzione del certificato. Come parte della sostituzione del certificato, i servizi di vRealize Automation verranno riavviati.

- 6 In Lifecycle Manager, eseguire la procedura guidata Aggiungi tenant per configurare i tenant desiderati.

È possibile aggiungere tenant utilizzando la pagina Gestione tenant di Lifecycle Manager, ubicata in Gestione identità e tenant. È possibile aggiungere solo i tenant per cui sono già stati configurati certificati e impostazioni DNS.

Quando si crea un tenant, è necessario designare un amministratore tenant ed è possibile selezionare le connessioni di Active Directory per questo tenant. Le connessioni disponibili sono basate su quelle configurate nel tenant predefinito o master. È inoltre necessario selezionare il prodotto o l'istanza del prodotto a cui verrà associato il tenant.

Operazioni successive

Dopo aver creato i tenant, è possibile utilizzare la pagina Gestione tenant di Lifecycle Manager ubicata in Gestione identità e tenant per modificare o aggiungere amministratori tenant, aggiungere directory di Active Directory al tenant e modificare le associazioni di prodotti per il tenant.

È inoltre possibile accedere all'istanza di Workspace ONE Access per visualizzare e convalidare la configurazione del tenant.

Gestione della configurazione dei certificati e di DNS in distribuzioni di più organizzazioni con un solo nodo

Le configurazioni di vRealize Automation di tenancy di più organizzazioni si basano su una configurazione coordinata tra diversi prodotti ed è necessario assicurarsi che i certificati e le impostazioni DNS siano configurati correttamente affinché la configurazione di tenancy di più organizzazioni funzioni correttamente.

Questa configurazione di più organizzazioni presuppone la distribuzione di un singolo nodo per i seguenti componenti:

- Lifecycle Manager
- Workspace ONE Access Identity Manager
- vRealize Automation

Presuppone inoltre che si stia iniziando con un tenant predefinito, ovvero l'organizzazione del provider, e che si stiano creando due tenant secondari, denominati tenant-1 e tenant-2.

È possibile creare e applicare certificati utilizzando il servizio Locker in vRealize Suite Lifecycle Manager oppure usare un altro meccanismo. Lifecycle Manager consente inoltre di sostituire o considerare di nuovo attendibili i certificati in vRealize Automation o Workspace ONE Access.

Requisiti DNS

È necessario creare sia record di tipo A principale sia record di tipo CNAME per i componenti del sistema, come descritto di seguito.

- Creare entrambi i record di tipo A principali per ciascun componente di sistema e per ognuno dei tenant creati quando si abilita il multi-tenancy.
- Creare record di tipo A multi-tenancy per ogni tenant che verrà creato e per il tenant master.
- Creare record di tipo CNAME multi-tenancy per ogni tenant che verrà creato, senza includere il tenant master.

Requisiti del certificato per la distribuzione multi-tenancy con un solo nodo

È necessario creare due certificati SAN (Subject Alternative Name), uno per Workspace ONE Access e uno per vRealize Automation.

- Nel certificato di vRealize Automation sono elencati il nome host del server di vRealize Automation e i nomi dei tenant che verranno creati.
- Nel certificato di Workspace ONE Access vengono elencati il nome host del server di Workspace ONE Access e i nomi dei tenant che si stanno creando.
- Se si utilizzano nomi SAN dedicati, i certificati devono essere aggiornati manualmente quando si aggiungono o si eliminano host o si modifica un nome host. È inoltre necessario aggiornare le voci DNS per i tenant. Come opzione per semplificare la configurazione, è possibile utilizzare i caratteri jolly per i certificati di Workspace ONE Access e vRealize Automation. Ad esempio, `*.example.com` e `*.vra.example.com`.

Nota vRealize Automation 8.x supporta i certificati con caratteri jolly solo per i nomi DNS che soddisfano le specifiche nell'elenco di suffissi pubblici all'indirizzo <https://publicsuffix.org>. Ad esempio `*.myorg.com` è un nome valido, mentre `*.myorg.local` non è valido.

Si tenga presente che Lifecycle Manager non crea certificati separati per ogni tenant. Crea invece un certificato singolo con il nome host di ogni tenant elencato. Per le configurazioni di base, il CNAME del tenant utilizza il formato seguente: `tenantname.vrahostname.domain`. Per le configurazioni ad alta disponibilità, il nome utilizza il formato seguente: `tenantname.vraLBhostname.domain`.

Riepilogo

La tabella seguente riepiloga i requisiti del DNS e del certificato per una distribuzione di Workspace ONE Access con un solo nodo e di vRealize Automation con un solo nodo.

Requisiti DNS	Requisiti del certificato SAN
Main A Type Records lcm.example.local WorkspaceOne.example.local vra.example.local	Workspace One Certificate Nome host: WorkspaceOne.example.local, default-tenant.example.local, tenant-1.vra.example.local, tenant-2.vra.example.local
Multi-tenancy A Type Records default-tenant.example.local tenant-1.example.local tenant-2.example.local	
Multi-Tenancy CNAME Type Records tenant-1.vra.example.local tenant-2.vra.example.local	vRealize Automation Certificate Nome host: vra.example.local, tenant-1.vra.example.local, tenant-2.vra.example.local

Gestione della configurazione del certificato e di DNS nelle distribuzioni di vRealize Automation in cluster

È necessario coordinare la configurazione del certificato e di DNS fra tutti i componenti applicabili per configurare una distribuzione di più organizzazioni di vRealize Automation in cluster.

In una tipica configurazione in cluster, sono presenti tre appliance Workspace ONE Access e tre appliance vRealize Automation, nonché una singola appliance Lifecycle Manager.

Questa configurazione presuppone distribuzioni in cluster per i seguenti componenti:

- Appliance Workspace ONE Access Identity Manager:
 - idm1.example.local
 - idm2.example.local
 - idm3.example.local
 - idm-lb.example.local
- Appliance vRealize Automation:
 - vra-1.example.local
 - vra-2.example.local
 - vra-3.example.local
 - vra-lb.example.local
- Appliance Lifecycle Manager

Requisiti DNS

È necessario creare entrambi i record di tipo A principali per ciascun componente e per ognuno dei tenant che verranno creati quando si abilita il multi-tenancy. Inoltre, è necessario creare record di tipo CNAME multi-tenancy per ogni tenant che verrà creato, senza includere il tenant master. Infine, è inoltre necessario creare record di tipo A principali per i bilanciamenti del carico di Workspace ONE Access e vRealize Automation.

- Creare record di tipo A per le tre appliance Workspace ONE Access e per le appliance vRealize Automation che puntino ai loro nomi di dominio completi.
- Creare inoltre record di tipo A per il bilanciamento del carico di Workspace ONE Access e il bilanciamento del carico di vRealize Automation che puntino ai loro nomi di dominio completi.
- Creare record di tipo A multi-tenancy per il tenant predefinito e per tenant-1 e tenant-2 che puntino all'indirizzo IP del bilanciamento del carico di Workspace ONE Access.
- Creare record CNAME per tenant-1 e tenant-2 che puntino all'indirizzo IP del bilanciamento del carico di vRealize Automation.

Requisiti del certificato SAN (Subject Alternative Name)

È necessario creare due certificati di Workspace ONE Access, uno da applicare alle appliance del cluster e uno da applicare al bilanciamento del carico. Creare inoltre un certificato da applicare alle appliance vRealize Automation, ai tenant che si stanno creando, escludendo il tenant predefinito, e al bilanciamento del carico.

- Creare un certificato per le appliance Workspace ONE Access in cui siano elencati i nomi di dominio completi delle appliance Workspace ONE Access, nonché il tenant predefinito e gli altri tenant creati. Questo certificato deve includere gli indirizzi IP delle appliance Workspace ONE Access.
- È consigliabile creare una terminazione SSL nel bilanciamento del carico. Per supportare questa terminazione, creare un certificato per il bilanciamento del carico di Workspace ONE Access in cui siano elencati il nome di dominio completo del bilanciamento del carico di Workspace ONE Access, nonché il tenant predefinito e tutti gli altri tenant creati. Questo certificato deve includere l'indirizzo IP del bilanciamento del carico.
- È necessario creare un certificato per vRealize Automation in cui siano elencati i nomi host delle tre appliance vRealize Automation, nonché il bilanciamento del carico correlato e i tenant che si stanno creando. Deve inoltre includere gli indirizzi IP delle tre appliance vRealize Automation.
- Per semplificare la configurazione, è possibile utilizzare i caratteri jolly per i certificati di Workspace ONE Access e vRealize Automation. Ad esempio `*.example.com`, `*.vra.example.com` e `*.vra-lb.example.com`.

Nota vRealize Automation 8.x supporta i certificati con caratteri jolly solo per i nomi DNS che soddisfano le specifiche nell'elenco di suffissi pubblici all'indirizzo <https://publicsuffix.org>. Ad esempio `*.myorg.com` è un nome valido, mentre `*.myorg.local` non è valido.

Se si utilizza una configurazione di Workspace ONE Access in cluster, tenere presente che Lifecycle Manager non è in grado di aggiornare i certificati di bilanciamento del carico, quindi è necessario aggiornarli manualmente. Inoltre, se è necessario registrare nuovamente i prodotti o i servizi esterni a Lifecycle Manager, si tratta di un processo manuale.

Riepilogo delle voci DNS e dei certificati per una configurazione di più organizzazioni in cluster

La tabella seguente illustra i requisiti del DNS e del certificato per una distribuzione di più organizzazioni di Workspace ONE Access in cluster e di vRealize Automation in cluster.

Requisiti DNS	Requisiti del certificato SAN
Main A Type Records lcm.example.local WorkspaceOne-1.example.local WorkspaceOne-2.example.local WorkspaceOne-3.example.local vra-1.example.local vra-2.example.local vra-3.example.local	Workspace One Certificate Nome host: WorkspaceOne-1.example.local, WorkspaceOne-2.example.local, WorkspaceOne-3.example.local, default-tenant.example.local, tenant-1.example.local, tenant-2.example.local
Multi-Tenancy A Type Records default-tenant.example.local tenant-1.vra.example.local tenant-2.vra.example.local	Workspace One LB Certificate (LB Terminated) Nome host: WorkSpaceOne-lb.example.local, default-tenant.example.local, vra.example.local, tenant-1.example.local, tenant-2.example.local
Multi-Tenancy CNAME Type Records tenant-1.vra-lb.example.local - vra-lb.example.local tenant-2.vra-lb.example.local - vra-lb.example.local	vRealize Automation Certificate Nome host: vra-1.example.local, vra-2.example.local, vra-3.example.local, vra-lb.example.local, tenant-1.example.local, tenant-2.example.local Non è necessario alcun certificato nel bilanciamento del carico di vRealize Automation poiché utilizza il passthrough SSL.

Accesso ai tenant e aggiunta di utenti in vRealize Automation

Dopo aver creato i tenant per vRealize Automation in Lifecycle Manager, è possibile accedere a Workspace ONE Access per visualizzare i tenant e aggiungere utenti.

È possibile visualizzare i tenant creati per una distribuzione di vRealize Automation accedendo all'istanza di Workspace ONE Access associata. L'URL da utilizzare è `https://default-tenant.name.domainname.local` o, per una distribuzione non in cluster, `https://idm.domainname.local` che reindirizzerà all'URL di Workspace ONE Access del tenant predefinito.

È possibile convalidare tenant specifici in Workspace ONE Access utilizzando il seguente URL: `https://tenant-1.domainname.local`. Questo URL apre una pagina che mostra gli utenti per il tenant specificato. È possibile fare clic su **Aggiungi utente** per creare altri utenti ad hoc.

Gli utenti autorizzati possono accedere all'organizzazione del provider principale in vRealize Automation utilizzando `https://vra.domainname.local`. Questa visualizzazione consente di accedere a tutti i servizi correlati a vRealize Automation.

Gli utenti autorizzati possono accedere ai tenant applicabili in vRealize Automation utilizzando `https://tenantname.vra.domainname.local`.

Per ulteriori informazioni sulla gestione degli utenti in Workspace ONE Access, vedere [Gestione di utenti e gruppi](#).

Aggiunta di utenti locali

È possibile aggiungere utenti locali alla distribuzione utilizzando l'istanza di Workspace ONE Access associata. Gli utenti locali sono utenti che non sono archiviati in alcun provider di identità esterno.

Utilizzo di vRealize Orchestrator con le distribuzioni multi-organizzazione di vRealize Automation

È possibile utilizzare vRealize Orchestrator con distribuzioni di tenancy multi-organizzazione di vRealize Automation.

Il tenant predefinito supporta l'integrazione immediata con l'integrazione di vRealize Orchestrator incorporata. vRealize Orchestrator è disponibile preconfigurato nella pagina Integrazioni. I tenant secondari non dispongono di alcuna integrazione di vRealize Orchestrator preregistrata. Sono disponibili diverse opzioni per aggiungere l'integrazione di vRealize Orchestrator.

- È possibile aggiungere l'integrazione con il vRealize Orchestrator incorporato accedendo alla configurazione del provider di autenticazione in vRealize Orchestrator e connettendosi utilizzando l'indirizzo host del tenant di vRealize Automation applicabile. È quindi possibile selezionare **Infrastruttura > Connessioni > Integrazioni** e aggiungere il vRO incorporato come integrazione.
- È possibile aggiungere un'istanza di vRealize Orchestrator esterna che utilizza il vRealize Automation multi-organizzazione come provider di autenticazione.

Qualsiasi istanza di vRealize Orchestrator che utilizza una distribuzione multi-organizzazione di vRealize Automation come provider di autenticazione può essere registrata in tutti i tenant creando una nuova integrazione e specificando il nome di dominio completo di vRealize Orchestrator senza fornire alcuna credenziale.

Utilizzo dei registri in vRealize Automation

5

È possibile utilizzare l'utilità della riga di comando `vraccli` fornita per creare e utilizzare i registri in vRealize Automation.

È possibile utilizzare i registri direttamente in vRealize Automation oppure è possibile inoltrare tutti i registri a vRealize Log Insight.

Questo capitolo include i seguenti argomenti:

- [Come utilizzare i registri e i bundle di registri in vRealize Automation](#)
- [In che modo è possibile configurare l'inoltro dei registri a vRealize Log Insight in vRealize Automation](#)
- [Come creare o aggiornare un'integrazione syslog in vRealize Automation](#)
- [Come si utilizzano i pacchetti di contenuti](#)

Come utilizzare i registri e i bundle di registri in vRealize Automation

I registri vengono generati automaticamente da vari servizi. È possibile generare bundle di registri in vRealize Automation. È inoltre possibile configurare l'ambiente in modo che invii i registri a vRealize Log Insight.

Le informazioni su come utilizzare l'utilità della riga di comando `vraccli` per generare bundle di registri possono essere visualizzate utilizzando l'argomento `--help` nell'utilità della riga di comando `vraccli` (ad esempio: `vraccli log-bundle --help`).

Per informazioni correlate all'utilizzo di vRealize Log Insight, vedere [In che modo è possibile configurare l'inoltro dei registri a vRealize Log Insight in vRealize Automation](#).

Comandi del bundle di registri

È possibile creare un bundle di registri contenente tutti i registri generati dai servizi eseguiti. Un bundle di registri contiene tutti i registri del servizio ed è necessario per la risoluzione dei problemi.

In un ambiente di cluster (modalità ad alta disponibilità), eseguire il comando `vracli log-bundle` in un solo nodo. I registri vengono trascinati da tutti i nodi nell'ambiente. Tuttavia, se si verifica un problema di rete o un altro problema relativo al cluster, i registri vengono estratti da tutti i nodi che è possibile raggiungere. Ad esempio, se un nodo è disconnesso in un cluster di tre nodi, i registri vengono raccolti solo dai due nodi integri. L'output del comando `vracli log-bundle` contiene informazioni sugli eventuali problemi rilevati e i passaggi della soluzione.

- Per creare un bundle di registri, accedere tramite SSH a un nodo qualsiasi ed eseguire il seguente comando `vracli`:

```
vracli log-bundle
```

- Per modificare il valore di timeout per la raccolta dei registri da ciascun nodo, eseguire il seguente comando `vracli`:

```
vracli log-bundle --collector-timeout $CUSTOM_TIMEOUT_IN_SECONDS
```

Ad esempio, se l'ambiente contiene file di registro di grandi dimensioni, una rete lenta o un utilizzo elevato della CPU, è possibile impostare il timeout su un valore superiore ai 1000 secondi predefiniti.

- Per configurare altre opzioni, come il timeout dell'assembly e la posizione del buffer, utilizzare il seguente comando della guida `vracli`:

```
vracli log-bundle --help
```

Struttura del bundle di registri

Il bundle di registri è un file tar con data e ora. Il nome del bundle corrisponde al file `log-bundle-<date>T<time>.tar` modello, ad esempio `log-bundle-20200629T131312.tar`. Il bundle di registri contiene in genere i registri di tutti i nodi nell'ambiente. In caso di errore, contiene quanti più registri possibile. Contiene almeno i registri del nodo locale.

Il bundle di registri è composto dai seguenti contenuti:

- File di ambiente

Il file di ambiente contiene l'output di vari comandi di manutenzione di Kubernetes. Fornisce informazioni sull'utilizzo corrente delle risorse per nodo e per pod. Contiene inoltre le informazioni e la descrizione del cluster per tutte le entità Kubernetes disponibili.

- Registri e configurazione di host

La configurazione di ogni host (ad esempio la relativa directory `/etc`) e i registri specifici dell'host (ad esempio `journald`) vengono raccolti in una directory per ogni nodo o host del cluster. Il nome della directory corrisponde al nome host del nodo. I contenuti interni della directory corrispondono al file system dell'host. Il numero di tali directory corrisponde al numero di nodi del cluster.

- Registri dei servizi

I registri per i servizi Kubernetes si trovano nella seguente struttura di cartelle:

- `<hostname>/services-logs/<namespace>/<app-name>/file-logs/<container-name>.log`
- `<hostname>/services-logs/<namespace>/<app-name>/console-logs/<container-name>.log`

Un nome di file di esempio è `my-host-01/services-logs/prelude/vco-app/file-logs/vco-server-app.log`.

- *hostname* è il nome host del nodo in cui il contenitore dell'applicazione è o era in esecuzione. In genere, è presente una sola istanza per ogni nodo per ogni servizio. Ad esempio, 3 nodi = 3 istanze.
- *namespace* è lo spazio dei nomi di Kubernetes in cui l'applicazione è o era distribuita. Per i servizi rivolti all'utente, questo valore è `prelude`.
- *app-name* è il nome dell'applicazione Kubernetes che ha generato i registri, ad esempio `provisioning-service-app`.
- *container-name* è il nome del contenitore che ha generato i registri. Alcune app sono composte da più contenitori. Ad esempio, `vco-app` contiene i contenitori `vco-server-app` e `vco-controlcenter-app`.
- **Registri pod (legacy)**
Prima delle modifiche apportate all'architettura di registrazione in vRealize Automation 8.2, i registri dei servizi (descritti nel punto precedente) si trovavano nella directory di ciascun pod nel bundle di registri. Anche se è possibile continuare a generare i registri dei pod nel bundle utilizzando la riga di comando `vracli log-bundle --include-legacy-pod-logs`, questa operazione è sconsigliata perché tutte le informazioni dei registri si trovano già nei registri di ciascun servizio. L'inclusione dei registri dei pod può aumentare inutilmente il tempo e lo spazio necessari per generare il bundle di registri.

Riduzione della dimensione del bundle di registri

Per generare un bundle di registri di dimensioni più piccole, utilizzare uno dei seguenti comandi `vracli log-bundle`:

- `vracli log-bundle --since-days n`

Utilizzare questo comando per raccogliere solo i file di registro generati nell'ultimo numero di giorni. In caso contrario, i registri vengono conservati e raccolti per 7 giorni. Ad esempio:

```
vracli log-bundle --since-days 3
```

- `vracli log-bundle --services service_A,service_B,service_C`

Utilizzare questo comando per raccogliere solo i registri per i servizi forniti denominati. Ad esempio:

```
vracli log-bundle --services ebs-app,vco-app
```

- `vracli log-bundle --skip-heap-dumps`

Utilizzare questo comando per escludere tutti i dump dell'heap dal bundle di registri generato.

Comprendere la rotazione del registro

I registri del servizio esistono inizialmente in uno stato non compresso. Dopo che un agente di vRealize Log Insight elabora i dati del registro, un processo di vRealize Automation `cron` comprime i registri del servizio.

Quando si utilizza il 70% della partizione del disco `/var/log`, un processo di vRealize Automation `cron` elimina i registri del servizio meno recenti.

Per esaminare le informazioni di rotazione dei registri, eseguire i comandi `vracli` seguenti.

```
vracli cluster exec -- bash -c 'current_node; vracli disk-mgr; exit 0'
vracli cluster exec -- bash -c 'current_node; service prune-logs status; exit 0'
```

In che modo è possibile configurare l'inoltro dei registri a vRealize Log Insight in vRealize Automation

È possibile inoltrare i registri da vRealize Automation a vRealize Log Insight per sfruttare i vantaggi di un'analisi dei registri e una generazione di report più potenti.

vRealize Automation viene fornito in bundle con un agente di registrazione [basato su fluentd](#).

L'agente raccoglie e archivia i registri in modo che possano essere inclusi in un bundle di registri ed esaminati in un secondo momento. È possibile configurare l'agente in modo che inoltri una copia dei registri a un server vRealize Log Insight utilizzando la REST API di vRealize Log Insight. L'API consente agli altri programmi di comunicare con vRealize Log Insight.

Per ulteriori informazioni su vRealize Log Insight, inclusa la documentazione relativa alla REST API di vRealize Log Insight, consultare la [documentazione di vRealize Log Insight](#).

Configurare l'agente di registrazione affinché inoltri in modo continuativo i registri di vRealize Automation a vRealize Log Insight utilizzando l'utilità della riga di comando `vracli` fornita.

Tutte le righe di registro sono contrassegnate con un nome host e un tag environment e possono essere esaminate in vRealize Log Insight. In un ambiente ad alta disponibilità (HA), i registri vengono contrassegnati con nomi host diversi, in base al nodo in cui vengono originati. Il tag environment è configurabile utilizzando l'opzione `--environment ENV` come descritto di seguito nella sezione *Configurazione o aggiornamento dell'integrazione di vRealize Log Insight*. In un ambiente HA, il tag environment ha lo stesso valore per tutte le righe dei registri, indipendentemente dal nodo in cui vengono originate.

Le informazioni su come utilizzare l'utilità della riga di comando `vracli` possono essere visualizzate utilizzando l'argomento `--help` nell'utilità della riga di comando `vracli`. Ad esempio: `vracli vrli --help`.

Nota È possibile configurare solo una singola integrazione di registrazione remota. A vRealize Log Insight sarà assegnata la priorità nel caso in cui siano disponibili sia un server vRealize Log Insight sia un server syslog.

Controllare la configurazione esistente di vRealize Log Insight

Command

```
vracli vrli
```

Arguments

Non sono presenti argomenti della riga di comando.

Output

La configurazione corrente per l'integrazione di vRealize Log Insight viene restituita in formato JSON.

Exit codes

Sono possibili i seguenti codici di uscita:

- 0: l'integrazione con vRealize Log Insight è configurata.
- 1: si è verificata un'eccezione come parte dell'esecuzione del comando. Per dettagli, esaminare il messaggio di errore.
- 61 (ENODATA): l'integrazione con vRealize Log Insight non è configurata. Per dettagli, esaminare il messaggio di errore.

Example - check integration configuration

```
$ vracli vrli
No vRLI integration configured

$ vracli vrli
{
  "agentId": "0",
  "environment": "prod",
  "host": "my-vrli.local",
  "port": 9543,
  "scheme": "https",
  "sslVerify": false
}
```

Configurazione o aggiornamento dell'integrazione di vRealize Log Insight

Command

```
vracli vrli set [options] IP_OR_URL
```

Nota Dopo aver eseguito il comando, l'agente di registrazione può richiedere fino a 2 minuti per applicare la configurazione specificata.

Arguments

■ IP_OR_URL

Specifica l'indirizzo IP o l'indirizzo URL del server di vRealize Log Insight da utilizzare per la pubblicazione dei registri. Per impostazione predefinita, vengono utilizzate la porta 9543 e HTTPS. Se è necessario modificare una di queste impostazioni, è possibile utilizzare un URL.

Nota È possibile impostare uno schema host (il valore predefinito è HTTPS) e una porta (il valore predefinito per HTTPS è 9543, il valore predefinito per HTTP è 9000) diversi da utilizzare per l'invio dei registri, come illustrato negli esempi seguenti:

```
vracli vrli set https://IP:9543
vracli vrli set --insecure IP
vracli vrli set http://http://IP:9000
```

Le porte 9543 per HTTP e 9000 per HTTP sono utilizzate dalla REST API di inserimento di vRealize Log Insight come descritto nell'argomento *Amministrazione di vRealize Log Insight, Porte e interfacce esterne* nella [documentazione di vRealize Log Insight](#).

■ Opzioni

■ --agent-id SOME_ID

Imposta l'ID dell'agente di registrazione per questa appliance. Il valore predefinito è 0. Utilizzato per identificare l'agente durante la pubblicazione dei registri in vRealize Log Insight tramite la REST API di vRealize Log Insight.

■ --environment ENV

Imposta un identificatore per l'ambiente corrente. Sarà disponibile nei registri di vRealize Log Insight come tag per ogni voce di registro. Il valore predefinito è `prod`.

■ --ca-file /path/to/server-ca.crt

Specifica un file che contiene il certificato dell'autorità di certificazione (CA) utilizzata per firmare il certificato del server di vRealize Log Insight. In questo modo l'agente di registrazione considera attendibile l'autorità di certificazione specificata e la abilita alla verifica del certificato del server di vRealize Log Insight se è stato firmato da un'autorità non attendibile. Il file può contenere un'intera catena di certificati per verificare il certificato. Nel caso di un certificato autofirmato, passare il certificato stesso.

■ --ca-cert CA_CERT

La definizione è identica a quella di `--ca-file` precedente, ma al contrario passa il certificato (catena) inline come stringa.

■ --insecure

Disattiva la verifica SSL del certificato del server. Di conseguenza, forza l'agente di registrazione in modo che accetti qualsiasi certificato SSL durante la pubblicazione dei registri.

- Opzioni avanzate

- --request-max-size BYTES

Più eventi di registro vengono acquisiti con una singola chiamata API. Questo argomento controlla la dimensione massima del payload, in byte, per ogni richiesta. I valori validi sono compresi tra 4000 e 4000000. Il valore predefinito è 256000. Per informazioni correlate ai valori consentiti, vedere Acquisizione degli eventi di vRealize Log Insight nella documentazione della REST API di vRealize Log Insight. Se si imposta questa opzione su un valore troppo basso, è possibile che gli eventi di registrazione che superano le dimensioni consentite vengano rimossi.

- --request-timeout SECONDS

Una chiamata all'API può bloccarsi per una serie di motivi, tra cui problemi di rete, remoti e così via. Questo parametro controlla il numero di secondi di attesa per il completamento di ciascuna operazione, ad esempio l'apertura di una connessione, la scrittura di dati o l'attesa di una risposta, prima che la chiamata venga riconosciuta come non riuscita. Il valore non può essere inferiore a 1 secondo. Il valore predefinito è 30.

- --request-immediate-retries RETRIES

Viene eseguito il buffering dei registri in blocchi aggregati prima che vengano inviati a vRealize Log Insight (vedere --buffer-flush-thread-count di seguito). Se una richiesta API non riesce, il registro viene ripetuto immediatamente. Il numero predefinito di tentativi immediati è 3. Se nessuno dei tentativi ha esito positivo, l'intero blocco di registri viene sottoposto a rollback e viene ripetuto nuovamente in un secondo momento.

- --request-http-compress

Per ridurre i volumi di traffico di rete, è possibile applicare la compressione GZIP alle richieste inviate al server vRealize Log Insight. Se questo parametro non viene specificato, non viene utilizzata alcuna compressione.

- --buffer-flush-thread-count THREADS

Per migliorare le prestazioni e limitare il traffico di rete, viene eseguito il buffering locale dei registri in blocchi prima che vengano scaricati e inviati al server dei registri. Ogni blocco contiene i registri di un singolo servizio. In base all'ambiente in cui si trovano, i blocchi possono aumentare notevolmente e richiedere molto tempo per lo scaricamento. Questo argomento controlla il numero di blocchi che possono essere scaricati simultaneamente. Il valore predefinito è 2.

Nota Quando si configura l'integrazione tramite HTTPS, se il server di vRealize Log Insight è configurato per l'utilizzo di un certificato non attendibile, ad esempio un certificato autofirmato o un certificato firmato da un'autorità non attendibile, è necessario utilizzare una delle opzioni `--ca-file`, `--ca-cert` o `--insecure` oppure l'agente di registrazione non riesce a convalidare l'identità del server e non invia i registri. Quando si utilizza `--ca-file` o `--ca-cert`, il certificato del server di vRealize Log Insight deve essere valido per il nome host del server. In tutti i casi, verificare l'integrazione attendendo alcuni minuti per il completamento dell'elaborazione e controllando che vRealize Log Insight abbia ricevuto i registri.

Output

Non è previsto alcun output.

Exit codes

Sono possibili i seguenti codici di uscita:

- 0: la configurazione è stata aggiornata.
- 1: si è verificata un'eccezione come parte dell'esecuzione. Per dettagli, esaminare il messaggio di errore.

Examples - Configure or update integration configuration

Le seguenti istruzioni di esempio sono mostrate in righe di comando separate, tuttavia gli argomenti possono essere combinati in una singola riga di comando. Ad esempio, è possibile includere più argomenti quando si utilizza `vracli vrli set {somehost}` o `vracli vrli set --ca-file path/to/server-ca.crt` per modificare l'ID dell'agente predefinito o i valori dell'ambiente. Per informazioni correlate, vedere la guida in linea del comando qui: `vracli vrli --help`.

```
$ vracli vrli set my-vrli.local
$ vracli vrli set 10.20.30.40
$ vracli vrli set --ca-file /etc/ssl/certs/ca.crt 10.20.30.40
$ vracli vrli set --ca-cert "$(cat /etc/ssl/certs/ca.crt)" 10.20.30.40
$ vracli vrli set --insecure http://my-vrli.local:8080
$ vracli vrli set --agent-id my-vrli-agent my-vrli.local
$ vracli vrli set --request-http-compress
$ vracli vrli set --environment staging my-vrli.local
$ vracli vrli set --environment staging --request-max-size 10000 --request-timeout 120 --
request-immediate-retries 5 --buffer-flush-thread-count 4 my-vrli.local
```

Integrazione chiara di vRealize Log Insight

Command

```
vracli vrli unset
```

Nota Dopo aver eseguito il comando, l'agente di registrazione può richiedere fino a 2 minuti per applicare la configurazione specificata.

Arguments

Non sono presenti argomenti della riga di comando.

Output

La conferma viene emessa in formato testo normale.

Exit codes

Sono disponibili i seguenti codici di uscita:

- 0: la configurazione è stata cancellata o non esisteva alcuna configurazione.
- 1: si è verificata un'eccezione come parte dell'esecuzione. Per dettagli, esaminare il messaggio di errore.

Examples - Clear integration

```
$ vracli vrli unset
Clearing vRLI integration configuration

$ vracli vrli unset
No vRLI integration configured
```

Come creare o aggiornare un'integrazione syslog in vRealize Automation

È possibile configurare vRealize Automation in modo da inviare le informazioni di registrazione a server syslog remoti.

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

L'integrazione syslog remota di vRealize Automation supporta i seguenti tipi di connessione:

- Tramite UDP.
- Tramite TCP senza TLS.

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

- Tramite TCP con TLS.

Nota È possibile configurare solo una singola integrazione di registrazione remota. A vRealize Log Insight sarà assegnata la priorità nel caso in cui siano disponibili sia un server vRealize Log Insight sia un server syslog.

Per informazioni sulla configurazione dell'integrazione della registrazione con vRealize Log Insight, vedere [In che modo è possibile configurare l'inoltro dei registri a vRealize Log Insight in vRealize Automation](#).

Prerequisiti

Configurare un server syslog remoto.

Procedura

- 1 Accedere alla riga di comando dell'appliance vRealize Automation come **root**.
- 2 Per creare un'integrazione in un server syslog, eseguire il comando `vracli remote-syslog set`.

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

Nota Se non si immette una porta nel comando `vracli remote-syslog set`, il valore della porta viene impostato su 514.

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

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

Nota Per impostazione predefinita, l'appliance vRealize Automation richiede di confermare che si desidera sovrascrivere l'integrazione syslog. Per ignorare la richiesta di conferma, aggiungere il contrassegno `-f` o `--force` al comando `vracli remote-syslog set`.

Operazioni successive

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

Come eliminare un'integrazione syslog per la registrazione in vRealize Automation

È possibile eliminare le integrazioni syslog dall'appliance vRealize Automation eseguendo il comando `vracli remote-syslog unset`.

Prerequisiti

Creare una o più integrazioni syslog nell'appliance vRealize Automation. Vedere [Come creare o aggiornare un'integrazione syslog in vRealize Automation](#).

Procedura

- 1 Accedere alla riga di comando dell'appliance vRealize Automation come **root**.
- 2 Eliminare le integrazioni syslog dall'appliance vRealize Automation utilizzando uno dei seguenti metodi:
 - Per eliminare un'integrazione syslog specifica, eseguire il comando `vracli remote-syslog unset -id Integration_name`.
 - Per eliminare tutte le integrazioni syslog nell'appliance vRealize Automation, eseguire il comando `vracli remote-syslog unset` senza il contrassegno `-id`.

Nota Per impostazione predefinita, l'appliance vRealize Automation richiede di confermare che si desidera eliminare tutte le integrazioni syslog. Per ignorare la richiesta di conferma, aggiungere il contrassegno `-f` o `--force` al comando `vracli remote-syslog unset`.

Come si utilizzano i pacchetti di contenuti

I pacchetti di contenuti sono ospitati in Log Insight e contengono dashboard, campi estratti, query salvate e avvisi correlati a un prodotto o a un set di registri specifici. È possibile installare i pacchetti di contenuti supportati dalla community da VMware Sample Exchange e altri pacchetti di contenuti da Content Pack Marketplace.

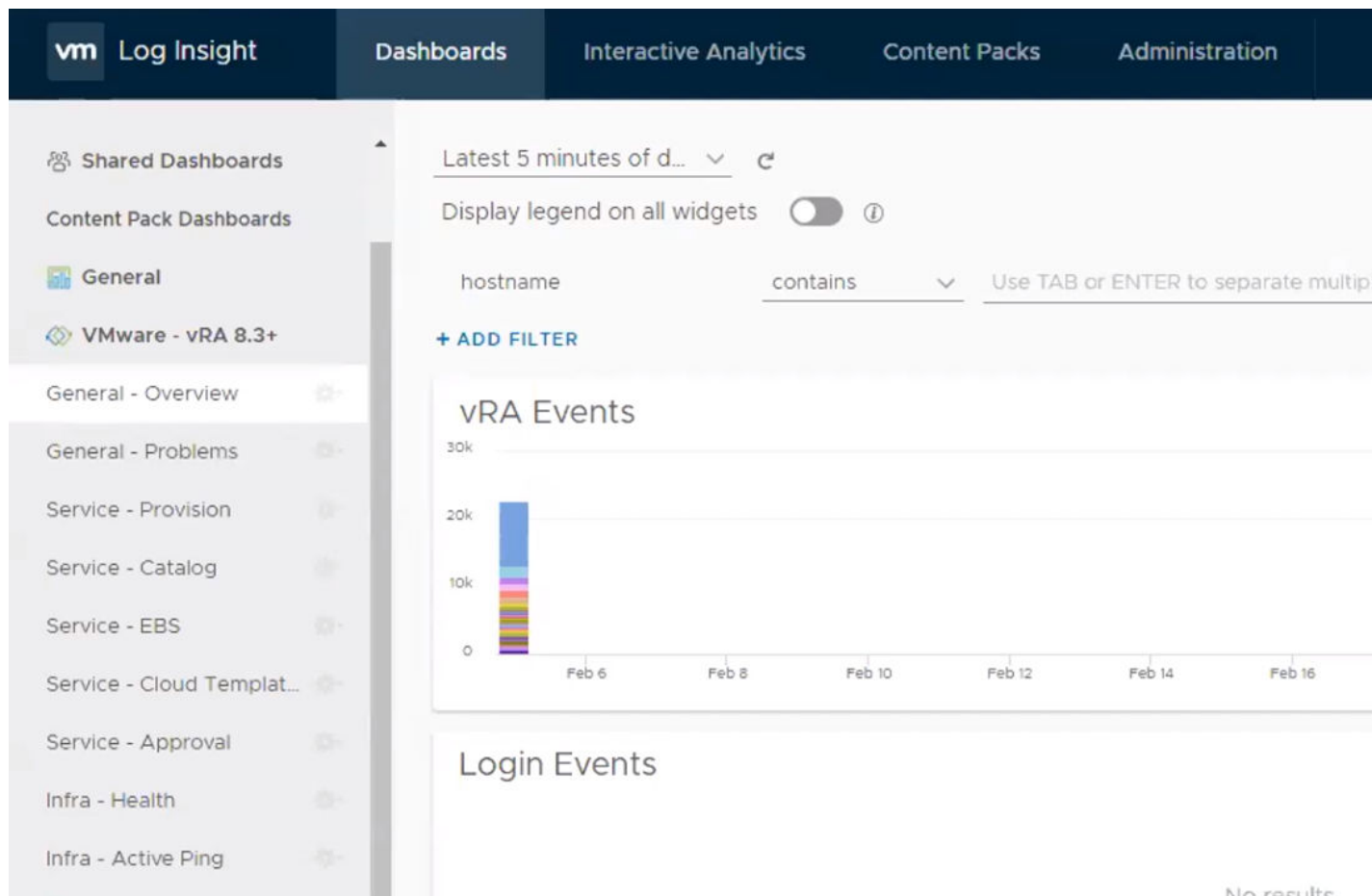
VMware vRealize Log Insight offre la gestione automatica dei registri tramite l'aggregazione, l'analisi e la ricerca abilitando l'intelligence operativa e la visibilità a livello aziendale negli ambienti cloud ibridi dinamici. I pacchetti di contenuti sono plug-in di VMware vRealize Log Insight che forniscono una conoscenza predefinita relativa a tipi di eventi specifici, come i messaggi di registro.

Per scaricare un pacchetto di contenuti, da Log Insight passare a **Pacchetti di contenuti > Marketplace**. È inoltre possibile importare i pacchetti di contenuti facendo clic su **+ Importa pacchetto di contenuti**.

Pacchetto di contenuti di vRA 8.x

Il pacchetto di contenuti di VMware vRealize Automation offre un riepilogo consolidato degli eventi di registro di tutti i componenti dell'ambiente vRA. Include diversi dashboard che forniscono una panoramica generale, dettagli su errori e operazioni, nonché lo stato generale dell'istanza di vRA. Questi dashboard sono elencati nella scheda **Dashboard** insieme a tutti gli altri dashboard di Log Insight. Dopo il caricamento, possono essere necessari fino a 30 secondi per il popolamento dei dashboard con le metriche.

Nota Non è possibile eseguire l'aggiornamento dal pacchetto di contenuti di vRA 7.5 o versione successive al pacchetto di contenuti di vRA 8.3. È necessario installare il pacchetto di contenuti di vRA 8.3. Una volta installati, i pacchetti di contenuti delle versioni 8.3 e 7.5 funzionano separatamente.



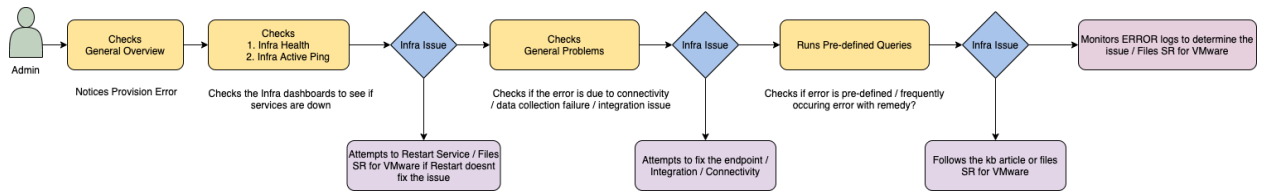
Il pacchetto di contenuti di vRealize Automation include i seguenti dashboard:

- Generale - Panoramica: acquisisce una panoramica delle metriche generali per vRA.
- Generale - Problemi:
- Servizio - Provisioning: acquisisce i problemi relativi al servizio di provisioning.
- Servizio - Catalogo: acquisisce i problemi relativi al servizio del catalogo.
- Servizio - EBS: acquisisce i problemi relativi al servizio del gestore eventi.
- Servizio - Modelli cloud: acquisisce errori e metriche relativi ai modelli cloud, alle risorse personalizzate e alle azioni risorsa di Cloud Assembly.
- Servizio - Approvazione: acquisisce errori e metriche relativi alle approvazioni.
- Infrastruttura - Integrità: acquisisce quando i pod vengono riavviati nel tempo. Questo dashboard è essenziale per rilevare le interruzioni a causa dei limiti delle risorse.
- Infrastruttura - Ping attivo: acquisisce l'URL del controllo dello stato nel tempo.

Ogni dashboard contiene singoli widget che forniscono analisi più incentrate. Per visualizzare

quale tipo di analisi viene eseguita in ciascun widget, fare clic sull'icona  delle informazioni.

In qualità di amministratore di vRealize Automation, è possibile eseguire questo workflow generale dei pacchetti di contenuti per identificare gli errori e risolvere i problemi.



Per ulteriori informazioni sul pacchetto di contenuti di vRealize Automation 8.3, vedere [Pacchetto di contenuti di vRealize Automation 8.3+ Log Insight](#) e [Come configurare l'inoltro dei registri a vRealize Log Insight](#).

Partecipazione al programma Analisi utilizzo software per vRealize Automation

6

Questo prodotto partecipa al programma Analisi utilizzo software (CEIP) di VMware. Il programma CEIP fornisce informazioni che consentono a VMware di migliorare i prodotti e i servizi, di correggere i problemi, nonché di consigliarti su come installare ed utilizzare al meglio i prodotti VMware.

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

Questo capitolo include i seguenti argomenti:

- Come partecipare o abbandonare il programma Analisi utilizzo software per vRealize Automation
- Come configurare la data e l'ora di raccolta dati per il programma Analisi utilizzo software per vRealize Automation

Come partecipare o abbandonare il programma Analisi utilizzo software per vRealize Automation

È possibile partecipare al programma Analisi utilizzo software dalla riga di comando dell'appliance vRealize Automation.

È possibile partecipare al programma Analisi utilizzo software quando si installa vRealize Automation e con vRealize Lifecycle Manager (LCM). È inoltre possibile partecipare o abbandonare il programma utilizzando le opzioni della riga di comando dopo l'installazione.

Per partecipare al programma Analisi utilizzo software utilizzando le opzioni della riga di comando:

- 1 Accedere alla riga di comando dell'appliance vRealize Automation come **root**.
- 2 Eseguire il comando `vracli ceip on`.
- 3 Rivedere le informazioni del programma Analisi utilizzo software ed eseguire il comando `vracli ceip on --acknowledge-ceip`.
- 4 Per riavviare i servizi di vRealize Automation, eseguire il comando `/opt/scripts/deploy.sh`.

Per abbandonare il programma Analisi utilizzo software utilizzando le opzioni della riga di comando:

- 1 Accedere alla riga di comando dell'appliance vRealize Automation come **root**.
- 2 Eseguire il comando `vracli ceip off`.
- 3 Per riavviare i servizi di vRealize Automation, eseguire il comando `/opt/scripts/deploy.sh`.

Come configurare la data e l'ora di raccolta dati per il programma Analisi utilizzo software per vRealize Automation

È possibile impostare la data e l'ora in cui il programma Analisi utilizzo software invia i dati a VMware.

Procedura

- 1 Accedere alla riga di comando dell'appliance vRealize Automation come **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 l'ora del giorno (hod).

Proprietà	Descrizione
<code>frequency.dow=<day-of-week></code>	Giorno in cui viene effettuata la raccolta dei dati.
<code>frequency.hod=<hour-of-day></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.