Documentazione ONTAP tools for VMware vSphere

ONTAP tools for VMware vSphere 10

NetApp
September 29, 2025

This PDF was generated from https://docs.netapp.com/it-it/ontap-tools-vmware-vsphere-104/index.html on September 29, 2025. Always check docs.netapp.com for the latest.

Sommario

Documentazione ONTAP tools for VMware vSphere . . . 1
Note di rilascio . . . 2
- Note di rilascio . . . 2
- Novità negli ONTAP tools for VMware vSphere 10.4 . . . 2
- Confronto delle funzionalità ONTAP tools for VMware vSphere 9 e ONTAP tools for VMware vSphere 10 . . . 2

Concetti . . . 5
- Panoramica ONTAP tools for VMware vSphere . . . 5
- Concetti e termini chiave . . . 5
- Controllo degli accessi basato sui ruoli . . . 8
  - Scopri di più sugli ONTAP tools for VMware vSphere 10 RBAC . . . 8
  - RBAC con VMware vSphere . . . 9
  - RBAC con ONTAP . . . 13
- Alta disponibilità per gli ONTAP tools for VMware vSphere . . . 16
- Interfaccia utente del gestore degli strumenti ONTAP . . . 16

Distribuisci gli ONTAP tools for VMware vSphere . . . 19
- Avvio rapido per gli ONTAP tools for VMware vSphere . . . 19
- Flusso di lavoro di distribuzione ad alta disponibilità (HA) . . . 20
- ONTAP tools for VMware vSphere . . . 21
  - Requisiti di sistema . . . 21
  - Requisiti minimi di archiviazione e applicazione . . . 22
  - Requisiti portuali . . . 22
  - Limiti di configurazione per distribuire gli ONTAP tools for VMware vSphere . . . 24
  - ONTAP tools for VMware vSphere - Storage Replication Adapter (SRA) . . . 25
- Prima di iniziare… . . . 25
  - Foglio di lavoro per la distribuzione . . . 26
  - Configurazione del firewall di rete . . . 27
  - Impostazioni di archiviazione ONTAP . . . 27
- Distribuisci gli ONTAP tools for VMware vSphere . . . 28
- Codici di errore di distribuzione . . . 33

Configurare gli ONTAP tools for VMware vSphere . . . 36
- Aggiungi istanze di vCenter Server . . . 36
- Registrare il provider VASA con un’istanza di vCenter Server . . . 36
- Installa il plug-in NFS VAAI . . . 37
- Configurare le impostazioni dell’host ESXi . . . 38
  - Configurare le impostazioni multipath e timeout del server ESXi . . . 38
  - Imposta i valori dell’host ESXi . . . 39
- Configurare i ruoli e i privilegi degli utenti ONTAP . . . 40
  - Requisiti di mappatura aggregata SVM . . . 41
  - Creare manualmente l’utente e il ruolo ONTAP . . . 41
  - Aggiorna gli ONTAP tools for VMware vSphere 10.1 a 10.3 . . . 49
  - Aggiorna gli ONTAP tools for VMware vSphere 10.3 a 10.4 . . . 51
- Aggiungi un backend di archiviazione . . . 51
- Associare un backend di archiviazione a un’istanza di vCenter Server . . . 52

Configurare l'accesso alla rete . . . 53
Creare un archivio dati . . . 53
Proteggere datastore e macchine virtuali . . . 58
Proteggere utilizzando la protezione del cluster host . . . 58
Proteggi utilizzando la protezione SRA . . . 59
Configurare SRA per proteggere gli archivi dati . . . 59
Configurare SRA per ambienti SAN e NAS . . . 59
Configurare SRA per ambienti altamente scalabili . . . 61
Configurare SRA sull'appliance VMware Live Site Recovery . . . 61
Aggiorna le credenziali SRA . . . 62
Configurare siti protetti e di ripristino . . . 63
Configurare le risorse del sito protetto e di ripristino . . . 64
Verificare i sistemi di archiviazione replicati . . . 68
Protezione a ventaglio . . . 68
Gestisci gli ONTAP tools for VMware vSphere . . . 72
Panoramica della dashboard ONTAP tools for VMware vSphere . . . 72
Interfaccia utente del gestore degli strumenti ONTAP . . . 73
Comprendere igroup e le policy di esportazione negli ONTAP tools for VMware vSphere . . . 75
Politiche di esportazione . . . 79
Comprendere gli igroup gestiti dagli strumenti ONTAP . . . 79
Abilita gli ONTAP tools for VMware vSphere . . . 83
Modifica gli ONTAP tools for VMware vSphere . . . 84
Gestisci gli archivi dati . . . 85
Montare i datastore NFS e VMFS . . . 85
Smonta i datastore NFS e VMFS . . . 86
Montare un datastore vVols . . . 86
Ridimensiona il datastore NFS e VMFS . . . 87
Espandi i datastore vVols . . . 87
Riduci il datastore vVols . . . 88
Elimina i datastore . . . 88
Viste di archiviazione ONTAP per datastore . . . 89
Visualizzazione dell'archiviazione della macchina virtuale . . . 90
Gestire le soglie di archiviazione . . . 90
Gestire i backend di archiviazione . . . 90
Scopri lo spazio di archiviazione . . . 90
Modificare i backend di archiviazione . . . 91
Rimuovere i backend di archiviazione . . . 91
Visualizzazione dettagliata del backend di archiviazione . . . 92
Gestire le istanze di vCenter Server . . . 92
Dissociare i backend di archiviazione dall'istanza di vCenter Server . . . 92
Modificare un'istanza di vCenter Server . . . 93
Rimuovere un'istanza di vCenter Server . . . 93
Gestisci i certificati . . . 93
Accedi ONTAP tools for VMware vSphere . . . 96
Panoramica degli ONTAP tools for VMware vSphere . . . 96

Configurare l'accesso diagnostico remoto . . . 97
Avvia SSH su altri nodi . . . 98
Aggiornare le credenziali di vCenter Server e ONTAP . . . 98
Report degli strumenti ONTAP . . . 98
Raccogliere i file di registro . . . 99
Gestire macchine virtuali . . . 99
Considerazioni sulla migrazione o la clonazione di macchine virtuali . . . 100
Migrare macchine virtuali con datastore NFS e VMFS su datastore vVols . . . 101
Bonifica VASA . . . 101
Collegare o scollegare un disco dati da una macchina virtuale . . . 101
Scopri i sistemi di archiviazione e gli host . . . 102
Modificare le impostazioni dell'host ESXi utilizzando gli strumenti ONTAP . . . 103
Gestisci le password . . . 104
Cambia la password del gestore degli strumenti ONTAP . . . 104
Reimposta la password del gestore degli strumenti ONTAP . . . 104
Reimposta la password utente dell'applicazione . . . 104
Reimposta la password utente della console di manutenzione . . . 105
Gestire la protezione del cluster host . . . 106
Modifica il cluster host protetto . . . 106
Rimuovere la protezione del cluster host . . . 109
Disabilita AutoSupport . . . 109
Aggiorna l'URL del proxy AutoSupport . . . 110
Aggiungi server NTP . . . 110
Crea un backup e ripristina la configurazione degli strumenti ONTAP . . . 110
Crea un backup e scarica il file di backup . . . 111
Recuperare . . . 111
Disinstallare gli ONTAP tools for VMware vSphere . . . 112
Rimuovere i volumi FlexVol . . . 113
Aggiorna gli ONTAP tools for VMware vSphere . . . 114
Aggiornamento dagli ONTAP tools for VMware vSphere 10.x alla versione 10.4 . . . 114
Codici di errore di aggiornamento . . . 117
Migrare gli ONTAP tools for VMware vSphere 9.xx a 10.4 . . . 122
Migrazione dagli ONTAP tools for VMware vSphere 9.xx a 10.4 . . . 122
Migrare il provider VASA e aggiornare l'SRA . . . 122
Passaggi per migrare il provider VASA . . . 122
Passaggi per aggiornare l'adattatore di replicazione dello storage (SRA) . . . 125
Automatizzare utilizzando l'API REST . . . 127
Scopri di più sugli ONTAP tools for VMware vSphere 10 REST API . . . 127
Fondazione dei servizi web REST . . . 127
Ambiente di gestione degli strumenti ONTAP . . . 127
Dettagli di implementazione per gli ONTAP tools for VMware vSphere 10 REST API . . . 128
Come accedere alla REST API . . . 128
Dettagli HTTP . . . 129
Autenticazione . . . 130
Richieste sincrone e asincrone . . . 130

La tua prima chiamata API REST ONTAP tools for VMware vSphere 10 . . . 131
Prima di iniziare . . . 131
Passaggio 1: acquisire un token di accesso . . . 131
Passaggio 2: emettere la chiamata API REST . . . 132
Riferimento API per gli ONTAP tools for VMware vSphere 10 REST API . . . 132
Note legali . . . 133
Copyright . . . 133
Marchi . . . 133
Brevetti . . . 133
Politica sulla riservatezza . . . 133
Open source . . . 133

Documentazione ONTAP tools for VMware vSphere

Note di rilascio

Note di rilascio

Scopri le nuove e migliorate funzionalità disponibili negli ONTAP tools for VMware vSphere 10.4.

Per un elenco completo delle nuove funzionalità e dei miglioramenti, fare riferimentoNovità negli ONTAP tools for VMware vSphere 10.4 .

Per saperne di più sulla scelta giusta per la tua distribuzione di migrare dagli ONTAP tools for VMware vSphere 9 agli strumenti ONTAP 10.4, fai riferimento aConfronto delle funzionalità ONTAP tools for VMware vSphere 9 e ONTAP tools for VMware vSphere 10 . È supportata la migrazione dagli ONTAP tools for VMware vSphere 9.12-D e 9.13-D agli ONTAP tools for VMware vSphere 10.4.

Per maggiori informazioni, fare riferimento al "Note sulla versione ONTAP tools for VMware vSphere 10.4" . Per accedere alle Note sulla versione è necessario effettuare l'accesso con il proprio account NetApp o creare un account.

Novità negli ONTAP tools for VMware vSphere 10.4

Scopri le nuove funzionalità disponibili negli ONTAP tools for VMware vSphere 10.4.

Aggiornamento	Descrizione
"Supporto per il sistema ASA r2 con 12 nodi per cluster"	Gli ONTAP tools for VMware vSphere 10.4 supportano flussi di lavoro per sistemi di storage ASA r2 con un massimo di 12 nodi per cluster, migliorando l'efficienza e la scalabilità della gestione dei dati. Supporta datastore vVols con protocollo iSCSI e FC e datastore VMFS con protocollo iSCSI, FC e NVMe, offrendo opzioni di archiviazione flessibili e avanzate.
"Miglioramenti dell'interfaccia utente di ONTAP Tools Manager"	Ora è possibile abilitare il server NTP per una sincronizzazione oraria precisa nell'ambiente e configurare le impostazioni di telemetria per monitorare e analizzare le prestazioni del sistema dall'interfaccia di Gestione strumenti ONTAP . Queste impostazioni non sono più disponibili nella console di manutenzione.
Funzionalità di sicurezza avanzate	Le funzionalità di sicurezza offrono ora una protezione avanzata e la conformità agli standard del settore, garantendo un'esperienza solida e intuitiva che aiuta gli amministratori a gestire gli ambienti VMware in modo più efficace.
"Funzionalità avanzate di disaster recovery SRA"	Gli ONTAP tools for VMware vSphere 10.4 ora supportano le operazioni di disaster recovery utilizzando Site Recovery Appliance (SRA) con snapshot con nomi personalizzati, oltre alle copie di snapshot pianificate SnapMirror .

Confronto delle funzionalità ONTAP tools for VMware vSphere 9 e ONTAP tools for VMware vSphere 10

Scopri se la migrazione dagli ONTAP tools for VMware vSphere 9 agli ONTAP tools for VMware vSphere 10.1 o versioni successive è adatta alle tue esigenze.

Per le informazioni più aggiornate sulla compatibilità, fare riferimento "Strumento matrice di interoperabilità NetApp" .

Caratteristica	Strumenti ONTAP 9.13	Strumenti ONTAP 10.1	Strumenti ONTAP 10.2 e successivi
Proposta di valore chiave	Semplifica e ottimizza le operazioni dal giorno 0 al giorno 2 con funzionalità avanzate di sicurezza, conformità e automazione	Evoluzione degli strumenti ONTAP 10.x verso la parità 9.xx, estendendo al contempo i limiti di elevata disponibilità, prestazioni e scalabilità	Supporto esteso per includere FC per VMFS e vVols e NVMe-oF/FC, NVMe-oF/TCP solo per VMFS. Facilità d'uso per NetApp SnapMirror, configurazione semplice per cluster di storage metro vSphere e supporto VMware Live Site Recovery a tre siti
Qualifica di rilascio ONTAP	ONTAP 9.9.1 a ONTAP 9.16.1	ONTAP 9.12.1 a ONTAP 9.14.1	ONTAP 9.12.1 a ONTAP 9.15.1 per gli strumenti ONTAP 10.2. ONTAP 9.14.1, 9.15.1, 9.16.0 e 9.16.1 per gli strumenti ONTAP 10.3. ONTAP 9.14.1, 9.15.1, 9.16.0 e 9.16.1 per gli strumenti ONTAP 10.4. Per gli strumenti ONTAP 10.4 è necessario ONTAP 9.16.1P3 e versioni successive quando si utilizzano sistemi ASA r2.
Supporto per le versioni VMware	vSphere 7.x-8.x VMware Site Recovery Manager (SRM) 8.5 a VMware Live Site Recovery 9.0	vSphere 7.x-8.x VMware Site Recovery Manager (SRM) 8.7 a VMware Live Site Recovery 9.0	vSphere 7.x-8.x VMware Site Recovery Manager (SRM) 8.7 a VMware Live Site Recovery 9.0
Supporto del protocollo	Datastore NFS e VMFS: NFS (v3 e v4.1), VMFS (iSCSI e FCP) Datastore vVols : iSCSI, FCP, NVMe/FC, NFS v3	Datastore NFS e VMFS: NFS (v3 e v4.1), VMFS (iSCSI) Datastore vVols : iSCSI, NFS v3	Datastore NFS e VMFS: NFS (v3 e v4.1), VMFS (iSCSI/FCP/NVMe-oF) Datastore vVols : iSCSI, FCP, NFS v3
Scalabilità	Host e VM: 300 host, fino a 10.000 VM Datastore: 600 NFS, fino a 50 VMFS, fino a 250 vVols vVols: fino a 14.000	Host e VM: 600 host vVols: fino a 140.000	Host e VM: 600 host vVols: fino a 140.000
Osservabilità	Dashboard di prestazioni, capacità e conformità dell'host Report dinamici su VM e datastore	Dashboard aggiornate su prestazioni, capacità e conformità degli host. Report dinamici su VM e datastore.	Dashboard aggiornate su prestazioni, capacità e conformità degli host. Report dinamici su VM e datastore.

Caratteristica	Strumenti ONTAP 9.13	Strumenti ONTAP 10.1	Strumenti ONTAP 10.2 e successivi
Protezione dei dati	Replica SRA per VMFS e NFS Replica basata su FlexVols per vVols Integrazione SCV e interoperabilità per il backup	Replica SRA per datastore iSCSI VMFS e NFS v3	Replica SRA per datastore iSCSI VMFS e NFS v3, protezione a tre siti che combina SMAS e VMware Live Site Recovery.
Supporto del fornitore VASA	VASA 4.0	VASA 3.0	VASA 3.0

Concetti

Panoramica ONTAP tools for VMware vSphere

ONTAP tools for VMware vSphere è un set di strumenti per la gestione del ciclo di vita delle macchine virtuali. Si integra con l'ecosistema VMware per facilitare il provisioning del datastore e fornire una protezione di base per le macchine virtuali. Gli ONTAP tools for VMware vSphere sono una raccolta di microservizi scalabili orizzontalmente e basati su eventi, distribuiti come Open Virtual Appliance (OVA). Questa versione integra l'API REST con ONTAP.

Gli ONTAP tools for VMware vSphere sono costituiti da quanto segue:

- Funzionalità della macchina virtuale come protezione di base e ripristino di emergenza
- Fornitore VASA per la gestione granulare delle VM
- Gestione basata su policy di archiviazione
- Adattatore di replicazione dello storage (SRA)

Concetti e termini chiave

Nella sezione seguente vengono descritti i concetti e i termini chiave utilizzati nel documento.

Sistemi ASA r2

I nuovi sistemi NetApp ASA r2 offrono una soluzione hardware e software unificata che crea un'esperienza semplificata specifica per le esigenze dei clienti SAN-only. "Scopri di più sui sistemi di archiviazione ASA r2" .

Autorità di certificazione (CA)

La CA è un'entità attendibile che rilascia certificati Secure Sockets Layer (SSL).

Gruppo di coerenza (CG)

Un gruppo di coerenza è una raccolta di volumi gestiti come un'unica unità. I CG vengono sincronizzati per garantire la coerenza dei dati tra unità di archiviazione e volumi. In ONTAP, forniscono una gestione semplice e una garanzia di protezione per un carico di lavoro applicativo che si estende su più volumi. Scopri di più su "gruppi di coerenza" .

Doppio stack

Una rete dual-stack è un ambiente di rete che supporta l'uso simultaneo di indirizzi IPv4 e IPv6.

Alta disponibilità (HA)

I nodi del cluster sono configurati in coppie HA per operazioni non disruptive.

Numero di unità logica (LUN)

Un LUN è un numero utilizzato per identificare un'unità logica all'interno di una Storage Area Network (SAN). Questi dispositivi indirizzabili sono in genere dischi logici a cui si accede tramite il protocollo Small Computer System Interface (SCSI) o uno dei suoi derivati incapsulati.

Spazio dei nomi e sottosistema NVMe

Uno spazio dei nomi NVMe è una quantità di memoria non volatile che può essere formattata in blocchi logici. Gli spazi dei nomi sono l'equivalente dei LUN per i protocolli FC e iSCSI, mentre un sottosistema NVMe è analogo a un igroup. Un sottosistema NVMe può essere associato a degli iniziatori in modo che gli iniziatori associati possano accedere agli spazi dei nomi all'interno del sottosistema.

Gestore degli strumenti ONTAP

ONTAP Tools Manager offre agli amministratori ONTAP tools for VMware vSphere sulle istanze di vCenter Server gestite e sui backend di storage integrati. Aiuta a gestire le istanze di vCenter Server, i backend di archiviazione, i certificati, le password e i download dei bundle di log.

Dispositivo virtuale aperto (OVA)

OVA è uno standard aperto per il confezionamento e la distribuzione di appliance virtuali o software che devono essere eseguiti su macchine virtuali.

Obiettivo del punto di ripristino (RPO)

L'RPO misura la frequenza con cui si esegue il backup o la replica dei dati. Specifica il momento esatto in cui è necessario ripristinare i dati dopo un'interruzione per riprendere le operazioni aziendali. Ad esempio, se un'organizzazione ha un RPO di 4 ore, può tollerare la perdita di fino a 4 ore di dati in caso di disastro.

Sincronizzazione attiva SnapMirror

La sincronizzazione attiva SnapMirror consente ai servizi aziendali di continuare a funzionare anche in caso di guasto completo del sito, supportando il failover delle applicazioni in modo trasparente utilizzando una copia secondaria. Per attivare un failover con SnapMirror ActiveSync non è necessario alcun intervento manuale o scripting personalizzato. Scopri di più su "Sincronizzazione attiva SnapMirror" .

Backend di archiviazione

I backend di archiviazione sono l'infrastruttura di archiviazione sottostante utilizzata dall'host ESXi per archiviare file, dati e altre risorse della macchina virtuale. Consentono all'host ESXi di accedere e gestire dati persistenti, fornendo la capacità di archiviazione e le prestazioni richieste per un ambiente virtualizzato.

Cluster globale (backend di archiviazione)

I backend di archiviazione globali, disponibili solo con credenziali del cluster ONTAP , vengono integrati tramite l'interfaccia di gestione degli strumenti ONTAP . Possono essere aggiunti con privilegi minimi per consentire l'individuazione delle risorse cluster essenziali necessarie per la gestione vVols . I cluster globali sono ideali per scenari multi-tenancy in cui un utente SVM viene aggiunto localmente per la gestione vVols .

Backend di archiviazione locale

I backend di archiviazione locale con credenziali cluster o SVM vengono aggiunti tramite l'interfaccia utente degli strumenti ONTAP e sono limitati a un vCenter. Quando si utilizzano le credenziali del cluster in locale, le SVM associate vengono automaticamente mappate con vCenter per gestire vVols o VMFS. Per la gestione VMFS, incluso SRA, gli strumenti ONTAP supportano le credenziali SVM senza bisogno di un cluster globale.

Adattatore di replicazione dello storage (SRA)

SRA è il software specifico del fornitore di storage installato all'interno dell'appliance VMware Live Site Recovery. L'adattatore consente la comunicazione tra Site Recovery Manager e un controller di archiviazione a livello di Storage Virtual Machine (SVM) e la configurazione a livello di cluster.

Macchina virtuale di archiviazione (SVM)

SVM è l'unità di multitenancy in ONTAP. Come una macchina virtuale in esecuzione su un hypervisor, SVM è un'entità logica che astrae le risorse fisiche. SVM contiene volumi di dati e uno o più LIF attraverso i quali vengono forniti dati ai client.

Configurazione uniforme e non uniforme

- **Accesso host uniforme** significa che gli host di due siti sono connessi a tutti i percorsi verso i cluster di storage su entrambi i siti. I percorsi trasversali si estendono su lunghe distanze.
- **Accesso host non uniforme** significa che gli host in ogni sito sono connessi solo al cluster nello stesso sito. I percorsi tra siti e i percorsi estesi non sono collegati.

> L'accesso host uniforme è supportato per qualsiasi distribuzione di sincronizzazione attiva SnapMirror ; l'accesso host non uniforme è supportato solo per le distribuzioni attive/attive simmetriche. Scopri di più su "Panoramica della sincronizzazione attiva SnapMirror in ONTAP" .

Sistema di file di macchina virtuale (VMFS)

VMFS è un file system in cluster progettato per archiviare i file delle macchine virtuali negli ambienti VMware vSphere.

Volumi virtuali (vVols)

I vVols forniscono un'astrazione a livello di volume per l'archiviazione utilizzata da una macchina virtuale. Offre numerosi vantaggi e rappresenta un'alternativa all'utilizzo di una LUN tradizionale. Un datastore vVol è in genere associato a un singolo LUN che funge da contenitore per i vVols.

Criterio di archiviazione della VM

I criteri di archiviazione delle VM vengono creati nel vCenter Server in Criteri e profili. Per vVols , creare un set di regole utilizzando le regole del provider di tipo storage vVols NetApp .

Ripristino del sito live VMware

VMware Live Site Recovery, precedentemente noto come Site Recovery Manager (SRM), offre continuità aziendale, ripristino di emergenza, migrazione del sito e funzionalità di test senza interruzioni per gli ambienti virtuali VMware.

API VMware vSphere per la consapevolezza dello storage (VASA)

VASA è un set di API che integra gli array di storage con vCenter Server per la gestione e l'amministrazione. L'architettura si basa su diversi componenti, tra cui il provider VASA, che gestisce la comunicazione tra VMware vSphere e i sistemi di storage.

API di storage VMware vSphere - Integrazione array (VAAI)

VAAI è un set di API che consente la comunicazione tra gli host VMware vSphere ESXi e i dispositivi di storage. Le API includono un set di operazioni primitive utilizzate dagli host per scaricare le operazioni di archiviazione sull'array. VAAI può apportare significativi miglioramenti delle prestazioni per le attività che richiedono un uso intensivo di spazio di archiviazione.

Cluster di archiviazione metropolitana vSphere

vSphere Metro Storage Cluster (vMSC) è un'architettura che abilita e supporta vSphere in una distribuzione di cluster estesi. Le soluzioni vMSC sono supportate da NetApp MetroCluster e SnapMirror ActiveSync (in precedenza SMBC). Queste soluzioni garantiscono una maggiore continuità aziendale in caso di guasto del dominio. Il modello di resilienza si basa sulle tue specifiche scelte di configurazione. Scopri di più su "Cluster di archiviazione VMware vSphere Metro" .

archivio dati vVols

Il datastore vVols è una rappresentazione logica del datastore di un contenitore vVols creato e gestito da un provider VASA.

RPO zero

RPO è l'acronimo di Recovery Point Objective, ovvero la quantità di dati persi ritenuta accettabile in un dato periodo di tempo. Zero RPO significa che non è accettabile alcuna perdita di dati.

Controllo degli accessi basato sui ruoli

Scopri di più sugli ONTAP tools for VMware vSphere 10 RBAC

Il controllo degli accessi basato sui ruoli (RBAC) è un framework di sicurezza per il controllo dell'accesso alle risorse all'interno di un'organizzazione. RBAC semplifica l'amministrazione definendo ruoli con livelli specifici di autorità per eseguire azioni, anziché assegnare autorizzazioni a singoli utenti. I ruoli definiti vengono assegnati agli utenti, il che contribuisce a ridurre il rischio di errore e semplifica la gestione del controllo degli accessi nell'intera organizzazione.

Il modello standard RBAC è costituito da diverse tecnologie o fasi di implementazione di complessità crescente. Il risultato è che le implementazioni RBAC effettive, basate sulle esigenze dei fornitori di software e dei loro clienti, possono variare e spaziare da relativamente semplici a molto complesse.

Componenti RBAC

Ad alto livello, ci sono diversi componenti che sono generalmente inclusi in ogni implementazione RBAC. Questi componenti sono collegati tra loro in modi diversi nell'ambito della definizione dei processi di autorizzazione.

Privileges

Un *privilegio* è un'azione o una capacità che può essere consentita o negata. Potrebbe trattarsi di qualcosa di semplice, come la possibilità di leggere un file, o di un'operazione più astratta, specifica di un determinato sistema software. I Privileges possono anche essere definiti per limitare l'accesso agli endpoint dell'API REST e ai comandi della CLI. Ogni implementazione RBAC include privilegi predefiniti e potrebbe anche consentire agli amministratori di creare privilegi personalizzati.

Ruoli

Un *ruolo* è un contenitore che include uno o più privilegi. I ruoli sono generalmente definiti in base a compiti o funzioni lavorative particolari. Quando a un utente viene assegnato un ruolo, all'utente vengono concessi tutti i privilegi contenuti nel ruolo. Come per i privilegi, le implementazioni includono ruoli predefiniti e generalmente consentono la creazione di ruoli personalizzati.

Oggetti

Un *oggetto* rappresenta una risorsa reale o astratta identificata all'interno dell'ambiente RBAC. Le azioni definite tramite i privilegi vengono eseguite sugli oggetti associati o con essi. A seconda dell'implementazione, i privilegi possono essere concessi a un tipo di oggetto o a un'istanza specifica di oggetto.

Utenti e gruppi

Agli *utenti* viene assegnato o associato un ruolo applicato dopo l'autenticazione. Alcune implementazioni RBAC consentono di assegnare un solo ruolo a un utente, mentre altre consentono più ruoli per utente, magari con un solo ruolo attivo alla volta. L'assegnazione di ruoli ai *gruppi* può semplificare ulteriormente l'amministrazione della sicurezza.

Permessi

Un *permesso* è una definizione che vincola un utente o un gruppo insieme a un ruolo a un oggetto. Le autorizzazioni possono essere utili con un modello di oggetti gerarchico in cui possono essere facoltativamente ereditate dagli elementi figlio nella gerarchia.

Due ambienti RBAC

Quando si lavora con gli ONTAP tools for VMware vSphere 10, è necessario prendere in considerazione due distinti ambienti RBAC.

Server VMware vCenter

L'implementazione RBAC in VMware vCenter Server viene utilizzata per limitare l'accesso agli oggetti esposti tramite l'interfaccia utente di vSphere Client. Nell'ambito dell'installazione ONTAP tools for VMware vSphere 10, l'ambiente RBAC viene esteso per includere oggetti aggiuntivi che rappresentano le funzionalità degli strumenti ONTAP . L'accesso a questi oggetti è fornito tramite il plug-in remoto. Vedi"Ambiente vCenter Server RBAC" per maggiori informazioni.

Cluster ONTAP

Gli ONTAP tools for VMware vSphere 10 si connettono a un cluster ONTAP tramite l'API REST ONTAP per eseguire operazioni relative all'archiviazione. L'accesso alle risorse di archiviazione è controllato tramite un ruolo ONTAP associato all'utente ONTAP fornito durante l'autenticazione. Vedere "Ambiente ONTAP RBAC" per maggiori informazioni.

RBAC con VMware vSphere

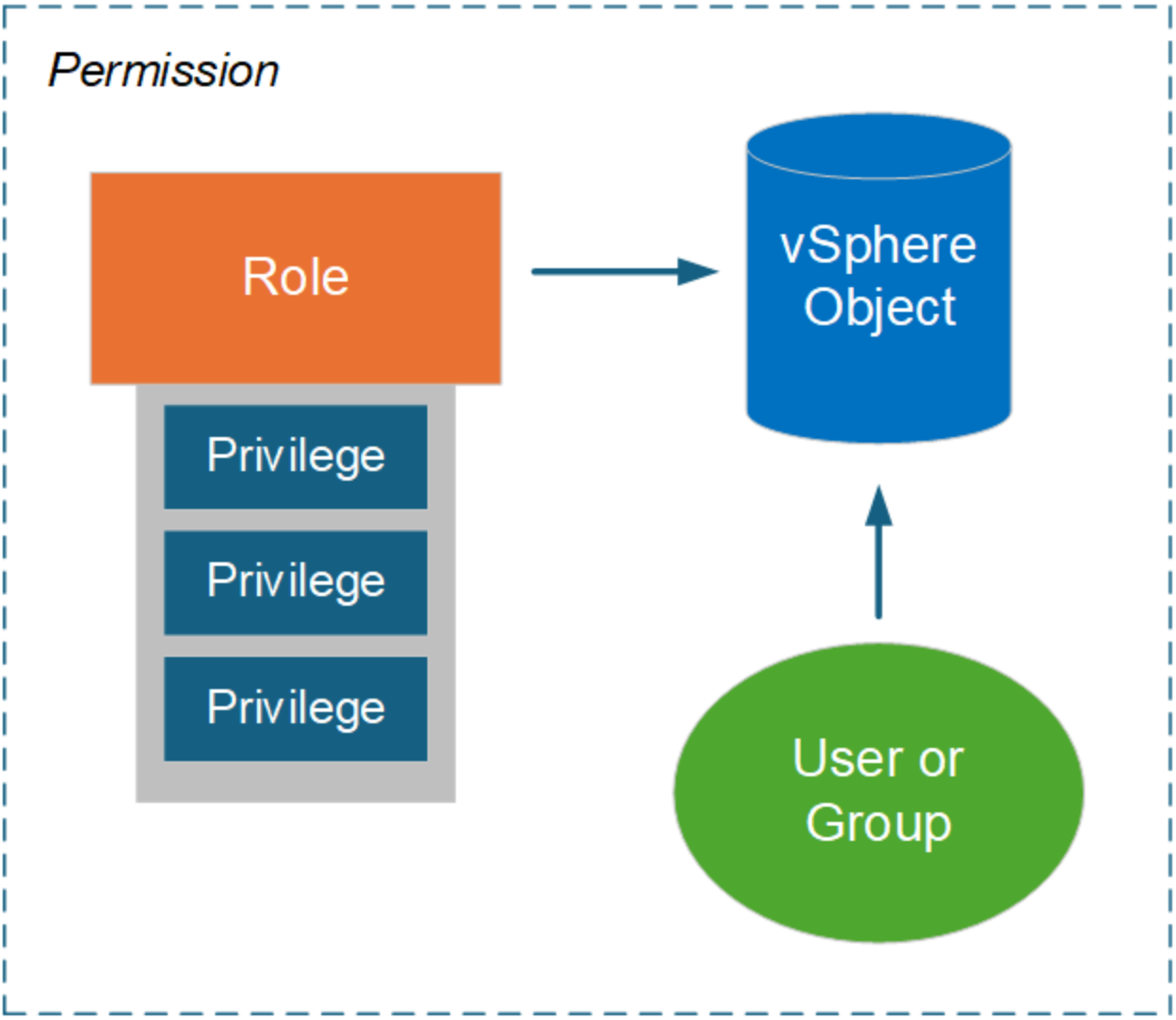
Ambiente vCenter Server RBAC con ONTAP tools for VMware vSphere 10

VMware vCenter Server offre una funzionalità RBAC che consente di controllare l'accesso agli oggetti vSphere. È una parte importante dei servizi di sicurezza di autenticazione e autorizzazione centralizzati di vCenter.

Illustrazione di un'autorizzazione di vCenter Server

Un'autorizzazione è la base per l'applicazione del controllo degli accessi nell'ambiente vCenter Server. Viene applicato a un oggetto vSphere con un utente o un gruppo incluso nella definizione dell'autorizzazione. Nella

figura seguente è fornita un'illustrazione di alto livello di un'autorizzazione vCenter.



Componenti di un'autorizzazione vCenter Server

Un'autorizzazione vCenter Server è un pacchetto di diversi componenti che vengono associati tra loro quando viene creata l'autorizzazione.

oggetti vSphere

Le autorizzazioni sono associate agli oggetti vSphere, quali vCenter Server, host ESXi, macchine virtuali, datastore, data center e cartelle. In base alle autorizzazioni assegnate all'oggetto, vCenter Server determina quali azioni o attività possono essere eseguite sull'oggetto da ciascun utente o gruppo. Per le attività specifiche degli ONTAP tools for VMware vSphere, tutte le autorizzazioni vengono assegnate e convalidate a livello di radice o di cartella radice di vCenter Server. Vedere "Utilizzare RBAC con il server vCenter" per maggiori informazioni.

Privileges e ruoli

Esistono due tipi di privilegi vSphere utilizzati con gli ONTAP tools for VMware vSphere 10. Per semplificare il lavoro con RBAC in questo ambiente, gli strumenti ONTAP forniscono ruoli contenenti i privilegi nativi e personalizzati richiesti. I privilegi includono:

- Privilegi nativi di vCenter Server

  Questi sono i privilegi forniti da vCenter Server.

- Privilegi specifici degli strumenti ONTAP

  Si tratta di privilegi personalizzati esclusivi ONTAP tools for VMware vSphere.

Utenti e gruppi

È possibile definire utenti e gruppi utilizzando Active Directory o l'istanza locale di vCenter Server. In combinazione con un ruolo, è possibile creare un'autorizzazione su un oggetto nella gerarchia degli oggetti vSphere. L'autorizzazione concede l'accesso in base ai privilegi del ruolo associato. Si noti che i ruoli non vengono assegnati direttamente agli utenti in modo isolato. Invece, utenti e gruppi ottengono l'accesso a un oggetto tramite i privilegi del ruolo, come parte dell'autorizzazione più ampia di vCenter Server.

Utilizzare vCenter Server RBAC con gli ONTAP tools for VMware vSphere 10

Ci sono diversi aspetti degli ONTAP tools for VMware vSphere 10 RBAC con vCenter Server che dovresti considerare prima di utilizzarli in un ambiente di produzione.

Ruoli vCenter e account amministratore

È necessario definire e utilizzare i ruoli vCenter Server personalizzati solo se si desidera limitare l'accesso agli oggetti vSphere e alle attività amministrative associate. Se non è necessario limitare l'accesso, è possibile utilizzare un account amministratore. Ogni account amministratore è definito con il ruolo di Amministratore al livello più alto della gerarchia degli oggetti. Ciò fornisce l'accesso completo agli oggetti vSphere, compresi quelli aggiunti dagli ONTAP tools for VMware vSphere 10.

Gerarchia degli oggetti vSphere

L'inventario degli oggetti vSphere è organizzato in una gerarchia. Ad esempio, è possibile spostarsi verso il basso nella gerarchia come segue:

```
vCenter Server→ Datacenter → Cluster → ESXi host → Virtual Machine
```

Tutte le autorizzazioni vengono convalidate nella gerarchia degli oggetti vSphere, ad eccezione delle operazioni del plug-in VAAI, che vengono convalidate rispetto all'host ESXi di destinazione.

Ruoli inclusi con gli ONTAP tools for VMware vSphere 10

Per semplificare l'utilizzo di vCenter Server RBAC, gli ONTAP tools for VMware vSphere forniscono ruoli predefiniti su misura per diverse attività di amministrazione.

> Se necessario, puoi creare nuovi ruoli personalizzati. In questo caso, dovresti clonare uno dei ruoli degli strumenti ONTAP esistenti e modificarlo secondo necessità. Dopo aver apportato le modifiche alla configurazione, gli utenti del client vSphere interessati devono disconnettersi e riconnettersi per rendere effettive le modifiche.

Per visualizzare gli ONTAP tools for VMware vSphere , selezionare **Menu** nella parte superiore di vSphere Client e fare clic su **Amministrazione** e quindi su **Ruoli** a sinistra. Sono disponibili tre ruoli predefiniti, come descritto di seguito.

ONTAP tools for VMware vSphere NetApp ONTAP per VMware vSphere Administrator

Fornisce tutti i privilegi nativi di vCenter Server e i privilegi specifici degli strumenti ONTAP necessari per eseguire gli ONTAP tools for VMware vSphere .

ONTAP tools for VMware vSphere NetApp ONTAP per VMware vSphere di sola lettura

Fornisce accesso in sola lettura agli strumenti ONTAP . Questi utenti non possono eseguire alcuno ONTAP tools for VMware vSphere con controllo degli accessi.

ONTAP tools for VMware vSphere NetApp ONTAP per VMware vSphere Provision

Fornisce alcuni dei privilegi nativi di vCenter Server e privilegi specifici degli strumenti ONTAP necessari per il provisioning dello storage. È possibile eseguire le seguenti attività:

- Crea nuovi datastore
- Gestisci gli archivi dati

Oggetti vSphere e backend di archiviazione ONTAP

I due ambienti RBAC funzionano insieme. Quando si esegue un'attività nell'interfaccia del client vSphere, vengono prima controllati i ruoli degli strumenti ONTAP definiti per vCenter Server. Se l'operazione è consentita da vSphere, vengono esaminati i privilegi del ruolo ONTAP . Questo secondo passaggio viene eseguito in base al ruolo ONTAP assegnato all'utente al momento della creazione e della configurazione del backend di archiviazione.

Utilizzo di vCenter Server RBAC

Quando si lavora con i privilegi e le autorizzazioni di vCenter Server, ci sono alcuni aspetti da considerare.

Privilegi richiesti

Per accedere all'interfaccia utente degli ONTAP tools for VMware vSphere 10, è necessario disporre del privilegio *View* specifico degli strumenti ONTAP . Se si accede a vSphere senza questo privilegio e si fa clic sull'icona NetApp , gli ONTAP tools for VMware vSphere visualizzano un messaggio di errore e impediscono l'accesso all'interfaccia utente.

Il livello di assegnazione nella gerarchia degli oggetti vSphere determina a quali parti dell'interfaccia utente è possibile accedere. Assegnando il privilegio di visualizzazione all'oggetto root è possibile accedere ONTAP tools for VMware vSphere facendo clic sull'icona NetApp .

In alternativa, è possibile assegnare il privilegio di visualizzazione a un altro livello di oggetto vSphere inferiore. Tuttavia, ciò limiterà gli ONTAP tools for VMware vSphere a cui è possibile accedere e utilizzare.

Assegnazione dei permessi

Se si desidera limitare l'accesso agli oggetti e alle attività di vSphere, è necessario utilizzare le autorizzazioni di vCenter Server. Il punto in cui si assegnano le autorizzazioni nella gerarchia degli oggetti vSphere determina le attività che gli utenti possono eseguire ONTAP tools for VMware vSphere 10.

> A meno che non sia necessario definire un accesso più restrittivo, in genere è buona norma assegnare le autorizzazioni a livello di oggetto radice o di cartella radice.

Le autorizzazioni disponibili con gli ONTAP tools for VMware vSphere 10 si applicano agli oggetti personalizzati non vSphere, come i sistemi di storage. Se possibile, dovresti assegnare queste autorizzazioni agli ONTAP tools for VMware vSphere perché non esiste alcun oggetto vSphere a cui puoi assegnarle. Ad esempio, qualsiasi autorizzazione che includa il privilegio "Aggiungi/Modifica/Rimuovi sistemi di storage" degli ONTAP tools for VMware vSphere deve essere assegnata a livello di oggetto radice.

Quando si definisce un'autorizzazione a un livello superiore nella gerarchia degli oggetti, è possibile configurarla in modo che venga trasmessa ed ereditata dagli oggetti figlio. Se necessario, è possibile assegnare autorizzazioni aggiuntive agli oggetti figlio che sovrascrivono le autorizzazioni ereditate dall'oggetto padre.

È possibile modificare un'autorizzazione in qualsiasi momento. Se si modifica uno qualsiasi dei privilegi all'interno di un'autorizzazione, gli utenti associati all'autorizzazione dovranno disconnettersi da vSphere e riaccedere per abilitare la modifica.

RBAC con ONTAP

Ambiente ONTAP RBAC con ONTAP tools for VMware vSphere 10

ONTAP fornisce un ambiente RBAC robusto ed estensibile. È possibile utilizzare la funzionalità RBAC per controllare l'accesso alle operazioni di archiviazione e di sistema esposte tramite REST API e CLI. È utile avere familiarità con l'ambiente prima di utilizzarlo con uno ONTAP tools for VMware vSphere 10.

Panoramica delle opzioni amministrative

Sono disponibili diverse opzioni quando si utilizza ONTAP RBAC, a seconda dell'ambiente e degli obiettivi. Di seguito viene presentata una panoramica delle principali decisioni amministrative. Vedi anche "Automazione ONTAP : panoramica della sicurezza RBAC" per maggiori informazioni.

> ONTAP RBAC è progettato su misura per un ambiente di archiviazione ed è più semplice dell'implementazione RBAC fornita con vCenter Server. Con ONTAP, assegni un ruolo direttamente all'utente. Con ONTAP RBAC non è necessario configurare autorizzazioni esplicite, come quelle utilizzate con vCenter Server.

Tipi di ruoli e privilegi

Quando si definisce un utente ONTAP è necessario un ruolo ONTAP . Esistono due tipi di ruoli ONTAP :

- RIPOSO

  I ruoli REST sono stati introdotti con ONTAP 9.6 e vengono generalmente applicati agli utenti che accedono a ONTAP tramite l'API REST. I privilegi inclusi in questi ruoli sono definiti in termini di accesso agli endpoint dell'API REST ONTAP e alle azioni associate.

- Tradizionale

  Questi sono i ruoli legacy inclusi prima di ONTAP 9.6. Continuano a essere un aspetto fondamentale dell'RBAC. I privilegi sono definiti in termini di accesso ai comandi CLI ONTAP .

Sebbene i ruoli REST siano stati introdotti più di recente, i ruoli tradizionali presentano alcuni vantaggi. Ad esempio, è possibile includere facoltativamente parametri di query aggiuntivi in modo che i privilegi definiscano con maggiore precisione gli oggetti a cui vengono applicati.

Ambito

I ruoli ONTAP possono essere definiti con uno dei due ambiti diversi. Possono essere applicati a uno specifico SVM di dati (livello SVM) o all'intero cluster ONTAP (livello cluster).

Definizioni dei ruoli

ONTAP fornisce un set di ruoli predefiniti sia a livello di cluster che di SVM. È anche possibile definire ruoli personalizzati.

Lavorare con i ruoli ONTAP REST

Esistono diverse considerazioni da tenere in considerazione quando si utilizzano i ruoli REST ONTAP inclusi negli ONTAP tools for VMware vSphere 10.

Mappatura dei ruoli

Indipendentemente dal fatto che si utilizzi un ruolo tradizionale o REST, tutte le decisioni di accesso ONTAP vengono prese in base al comando CLI sottostante. Tuttavia, poiché i privilegi in un ruolo REST sono definiti in termini di endpoint API REST, ONTAP deve creare un ruolo tradizionale *mappato* per ciascuno dei ruoli REST. Pertanto ogni ruolo REST corrisponde a un ruolo tradizionale sottostante. Ciò consente a ONTAP di prendere decisioni sul controllo degli accessi in modo coerente, indipendentemente dal tipo di ruolo. Non è possibile modificare i ruoli mappati in parallelo.

Definizione di un ruolo REST utilizzando i privilegi CLI

Poiché ONTAP utilizza sempre i comandi CLI per determinare l'accesso a livello base, è possibile esprimere un ruolo REST utilizzando i privilegi dei comandi CLI anziché gli endpoint REST. Uno dei vantaggi di questo approccio è la maggiore granularità disponibile con i ruoli tradizionali.

Interfaccia amministrativa durante la definizione dei ruoli ONTAP

È possibile creare utenti e ruoli con ONTAP CLI e REST API. Tuttavia, è più comodo utilizzare l'interfaccia System Manager insieme al file JSON disponibile tramite ONTAP Tools Manager. Vedere "Utilizzare ONTAP RBAC con gli ONTAP tools for VMware vSphere 10" per maggiori informazioni.

Utilizzare ONTAP RBAC con gli ONTAP tools for VMware vSphere 10

Ci sono diversi aspetti degli ONTAP tools for VMware vSphere 10 RBAC con ONTAP che dovresti considerare prima di utilizzarli in un ambiente di produzione.

Panoramica del processo di configurazione

Gli ONTAP tools for VMware vSphere 10 includono il supporto per la creazione di un utente ONTAP con un ruolo personalizzato. Le definizioni sono impacchettate in un file JSON che è possibile caricare nel cluster ONTAP . Puoi creare l'utente e personalizzare il ruolo in base al tuo ambiente e alle tue esigenze di sicurezza.

Di seguito vengono descritti in dettaglio i principali passaggi della configurazione. Fare riferimento a"Configurare i ruoli e i privilegi degli utenti ONTAP" per maggiori dettagli.

1. Preparare

È necessario disporre delle credenziali amministrative sia per ONTAP Tools Manager che per il cluster ONTAP .

2. Scarica il file di definizione JSON

Dopo aver effettuato l'accesso all'interfaccia utente di ONTAP Tools Manager, è possibile scaricare il file JSON contenente le definizioni RBAC.

3. Creare un utente ONTAP con un ruolo

Dopo aver effettuato l'accesso a System Manager, puoi creare l'utente e il ruolo:

1. Selezionare **Cluster** sulla sinistra e poi **Impostazioni**.
2. Scorri verso il basso fino a **Utenti e ruoli** e fai clic −→ .
3. Selezionare **Aggiungi** in **Utenti** e selezionare **Prodotti di virtualizzazione**.
4. Seleziona il file JSON sulla tua workstation locale e caricalo.

4. Configura il ruolo

Per definire il ruolo, è necessario prendere diverse decisioni amministrative. VedereConfigurare il ruolo utilizzando System Manager per maggiori dettagli.

Configurare il ruolo utilizzando System Manager

Dopo aver iniziato a creare un nuovo utente e ruolo con System Manager e aver caricato il file JSON, puoi personalizzare il ruolo in base al tuo ambiente e alle tue esigenze.

Configurazione principale dell'utente e del ruolo

Le definizioni RBAC sono confezionate come diverse funzionalità di prodotto, tra cui combinazioni di VSC, VASA Provider e SRA. Dovresti selezionare l'ambiente o gli ambienti in cui hai bisogno del supporto RBAC. Ad esempio, se si desidera che i ruoli supportino la funzionalità plug-in remoto, selezionare VSC. È inoltre necessario scegliere il nome utente e la password associata.

Privileges

I privilegi dei ruoli sono organizzati in quattro set in base al livello di accesso necessario all'archiviazione ONTAP . I privilegi su cui si basano i ruoli includono:

- Scoperta

  Questo ruolo consente di aggiungere sistemi di archiviazione.

- Crea spazio di archiviazione

  Questo ruolo consente di creare spazio di archiviazione. Include anche tutti i privilegi associati al ruolo di scoperta.

- Modificare l'archiviazione

  Questo ruolo consente di modificare l'archiviazione. Include inoltre tutti i privilegi associati ai ruoli di individuazione e creazione di archiviazione.

- Distruggere lo stoccaggio

  Questo ruolo consente di distruggere lo spazio di archiviazione. Include inoltre tutti i privilegi associati ai ruoli di individuazione, creazione di storage e modifica di storage.

Genera l'utente con un ruolo

Dopo aver selezionato le opzioni di configurazione per il tuo ambiente, fai clic su **Aggiungi** e ONTAP creerà l'utente e il ruolo. Il nome del ruolo generato è una concatenazione dei seguenti valori:

- Valore del prefisso costante definito nel file JSON (ad esempio "OTV_10")
- Capacità del prodotto selezionata
- Elenco dei set di privilegi.

Esempio

```
OTV_10_VSC_Discovery_Create
```

Il nuovo utente verrà aggiunto all'elenco nella pagina "Utenti e ruoli". Si noti che sono supportati sia i metodi di accesso utente HTTP che ONTAPI.

Alta disponibilità per gli ONTAP tools for VMware vSphere

Gli ONTAP tools for VMware vSphere supportano una configurazione ad alta disponibilità (HA) per garantire la funzionalità ininterrotta degli ONTAP tools for VMware vSphere in caso di errore.

La soluzione ad alta disponibilità (HA) garantisce un rapido ripristino in caso di interruzioni causate da:

- Errore dell'host

  Sono supportati solo i guasti a nodo singolo.

- guasto di rete
- Errore della macchina virtuale (errore del sistema operativo guest)
- Arresto anomalo dell'applicazione (strumenti ONTAP)

Non è richiesta alcuna configurazione aggiuntiva per gli ONTAP tools for VMware vSphere per garantire elevata disponibilità (HA).

Gli ONTAP tools for VMware vSphere non supportano vCenter HA.

Per abilitare la funzionalità HA, è necessario abilitare l'aggiunta a caldo della CPU e il collegamento a caldo della memoria durante la distribuzione o in un secondo momento nelle impostazioni degli ONTAP tools for VMware vSphere VM.

Interfaccia utente del gestore degli strumenti ONTAP

Gli ONTAP tools for VMware vSphere sono un sistema multi-tenant in grado di gestire più istanze di vCenter Server. ONTAP Tools Manager fornisce un maggiore controllo agli ONTAP tools for VMware vSphere sulle istanze di vCenter Server gestite e sui backend di storage integrati.

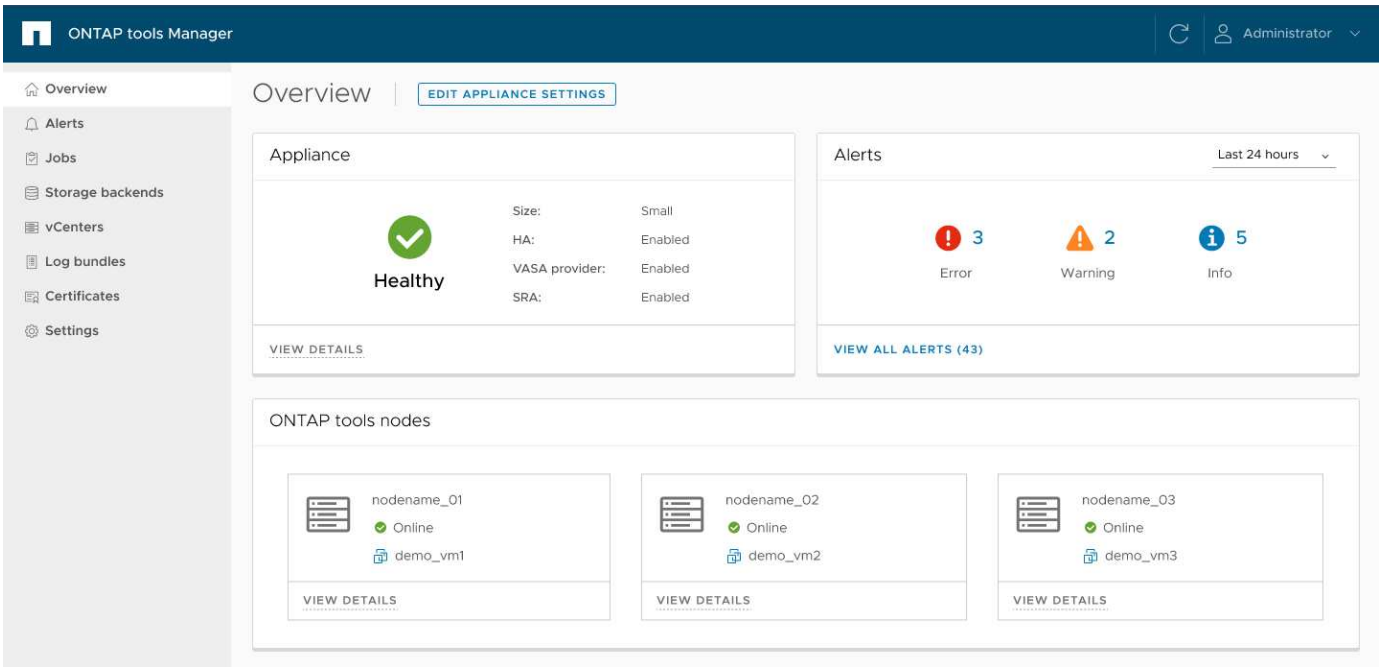
ONTAP Tools Manager aiuta a:

- Gestione delle istanze di vCenter Server: aggiungi e gestisci le istanze di vCenter Server negli strumenti ONTAP .
- Gestione del backend di archiviazione: aggiungi e gestisci i cluster di archiviazione ONTAP negli ONTAP tools for VMware vSphere e mappali alle istanze di vCenter Server integrate a livello globale.

- Download del bundle di log: raccogli i file di log per gli ONTAP tools for VMware vSphere.
- Gestione certificati: modifica il certificato autofirmato in un certificato CA personalizzato e rinnova o aggiorna tutti i certificati degli strumenti VASA Provider e ONTAP .
- Gestione password: reimposta la password dell'applicazione OVA dell'utente.

Per accedere a ONTAP Tools Manager, avviare `https://<ONTAPtoolsIP>:8443/virtualization/ui/` dal browser ed effettuare l'accesso con le credenziali di amministratore ONTAP tools for VMware vSphere fornite durante la distribuzione.

La sezione Panoramica di ONTAP Tools Manager aiuta a gestire la configurazione dell'appliance, ad esempio la gestione dei servizi, l'aumento delle dimensioni dei nodi e l'abilitazione dell'alta disponibilità (HA). È inoltre possibile monitorare le informazioni generali degli strumenti ONTAP relativi ai nodi, come stato di integrità, dettagli di rete e avvisi.



Carta	Descrizione
Scheda elettrodomestico	La scheda dell'apparecchio fornisce lo stato generale dell'apparecchio degli strumenti ONTAP . Mostra i dettagli di configurazione dell'appliance e lo stato dei servizi abilitati. Per ulteriori informazioni sull'appliance degli strumenti ONTAP , selezionare il collegamento **Visualizza dettagli**. Quando è in corso un processo di modifica delle impostazioni dell'appliance, il portlet dell'appliance mostra lo stato e i dettagli del processo.
Scheda avvisi	La scheda Avvisi elenca gli avvisi degli strumenti ONTAP per tipo, inclusi gli avvisi a livello di nodo HA. È possibile visualizzare l'elenco degli avvisi selezionando il testo del conteggio (collegamento ipertestuale). Il collegamento indirizza alla pagina di visualizzazione degli avvisi filtrati in base al tipo selezionato.

Carta	Descrizione
vCenter	La scheda vCenter mostra lo stato di integrità dei vCenter nel sistema.
Backend di archiviazione	La scheda Backend di archiviazione mostra lo stato di integrità dei backend di archiviazione nel sistema.
Scheda nodi strumenti ONTAP	La scheda dei nodi degli strumenti ONTAP mostra l'elenco dei nodi con il nome del nodo, il nome della VM del nodo, lo stato e tutti i dati relativi alla rete. È possibile selezionare **Visualizza dettagli** per visualizzare i dettagli aggiuntivi relativi al nodo selezionato. [NOTA] In una configurazione non HA, viene mostrato solo un nodo. Nella configurazione HA vengono mostrati tre nodi.

Distribuisci gli ONTAP tools for VMware vSphere

Avvio rapido per gli ONTAP tools for VMware vSphere

Con questa sezione di avvio rapido puoi configurare gli ONTAP tools for VMware vSphere .

Inizialmente, distribuirai gli ONTAP tools for VMware vSphere come una configurazione a nodo singolo di piccole dimensioni che fornisce servizi principali per supportare i datastore NFS e VMFS. Se è necessario espandere la configurazione per utilizzare i datastore vVols e l'alta disponibilità (HA), è possibile farlo al termine di questo flusso di lavoro. Per ulteriori informazioni, fare riferimento al "Flusso di lavoro di distribuzione HA" .

1 **Pianifica la tua distribuzione**

Verifica che le versioni degli host vSphere, ONTAP ed ESXi siano compatibili con la versione degli strumenti ONTAP . Alloca CPU, memoria e spazio su disco sufficienti. In base alle tue regole di sicurezza, potrebbe essere necessario configurare firewall o altri strumenti di sicurezza per consentire il traffico di rete.

Assicurarsi che vCenter Server sia installato e accessibile.

- "Strumento di matrice di interoperabilità"
- "ONTAP tools for VMware vSphere"
- "Prima di iniziare"

2 **Distribuisci gli ONTAP tools for VMware vSphere**

Inizialmente, implementerai gli ONTAP tools for VMware vSphere come una configurazione a singolo nodo di piccole dimensioni che fornisce servizi core per supportare datastore NFS e VMFS. Se prevedi di espandere la configurazione per utilizzare datastore vVols e alta disponibilità (HA), lo farai al termine di questo flusso di lavoro. Per espandere la configurazione ad alta disponibilità (HA), assicurati che le opzioni CPU hot-add e memory hot-plug siano abilitate.

- "Distribuisci gli ONTAP tools for VMware vSphere"

3 **Aggiungi istanze di vCenter Server**

Aggiungere istanze di vCenter Server agli ONTAP tools for VMware vSphere per configurare, gestire e proteggere i datastore virtuali nell'ambiente vCenter Server.

- "Aggiungi istanze di vCenter Server"

4 **Configurare i ruoli e i privilegi degli utenti ONTAP**

Configurare nuovi ruoli utente e privilegi per la gestione dei backend di archiviazione utilizzando il file JSON fornito con gli ONTAP tools for VMware vSphere.

- "Configurare i ruoli e i privilegi degli utenti ONTAP"

5 **Configurare i backend di archiviazione**

Aggiungere un backend di archiviazione a un cluster ONTAP . Per le configurazioni multi-tenancy in cui vCenter funge da tenant con una SVM associata, utilizzare ONTAP Tools Manager per aggiungere il cluster. Associare il backend di archiviazione al vCenter Server per mapparlo globalmente all'istanza di vCenter Server integrata.

Aggiungere i backend di archiviazione locale con credenziali cluster o SVM utilizzando l'interfaccia utente degli strumenti ONTAP . Questi backend di archiviazione sono limitati a un singolo vCenter. Quando si utilizzano le credenziali del cluster in locale, le SVM associate vengono automaticamente mappate al vCenter per gestire vVols o VMFS. Per la gestione VMFS, incluso SRA, gli strumenti ONTAP supportano le credenziali SVM senza bisogno di un cluster globale.

- "Aggiungi un backend di archiviazione"
- "Associare il backend di archiviazione a un'istanza di vCenter Server"

6 **Aggiorna i certificati se stai lavorando con più istanze di vCenter Server**

Quando si lavora con più istanze di vCenter Server, aggiornare il certificato autofirmato a un certificato firmato da un'autorità di certificazione (CA).

- "Gestisci i certificati"

7 **(Facoltativo) Configurare la protezione SRA**

Abilita la funzionalità SRA per configurare il disaster recovery e proteggere i datastore NFS o VMFS.

- "Abilita gli ONTAP tools for VMware vSphere"
- "Configurare SRA sull'appliance VMware Live Site Recovery"

8 **(Facoltativo) Abilita la protezione ActiveSync SnapMirror**

Configurare gli ONTAP tools for VMware vSphere per gestire la protezione del cluster host per SnapMirror ActiveSync. Eseguire il cluster ONTAP e il peering SVM nei sistemi ONTAP per utilizzare la sincronizzazione attiva SnapMirror . Questo vale solo per i datastore VMFS.

- "Proteggere utilizzando la protezione del cluster host"

9 **Configura il backup e il ripristino per i tuoi ONTAP tools for VMware vSphere**

Pianifica i backup degli ONTAP tools for VMware vSphere , che puoi utilizzare per ripristinare la configurazione in caso di errore.

- "Crea un backup e ripristina la configurazione degli strumenti ONTAP"

Flusso di lavoro di distribuzione ad alta disponibilità (HA)

Se si utilizzano datastore vVols , è necessario espandere la distribuzione iniziale degli

strumenti ONTAP a una configurazione ad alta disponibilità (HA) e abilitare i servizi VASA Provider.

1 **Ampliare la distribuzione**

È possibile ampliare la configurazione ONTAP tools for VMware vSphere per aumentare il numero di nodi nella distribuzione e modificare la configurazione in un'impostazione HA.

- "Modifica gli ONTAP tools for VMware vSphere"

2 **Abilita i servizi**

Per configurare i datastore vVols è necessario abilitare il servizio VASA Provider. Registra il provider VASA con vCenter e assicurati che i tuoi criteri di archiviazione soddisfino i requisiti HA, incluse le configurazioni di rete e di archiviazione appropriate.

Abilitare i servizi SRA per utilizzare gli strumenti ONTAP Storage Replication Adapter (SRA) per VMware Site Recovery Manager (SRM) o VMware Live Site Recovery (VLSR).

- "Abilita i servizi VASA Provider e SRA"

3 **Aggiorna i certificati**

Se si utilizzano datastore vVol con più istanze di vCenter Server, aggiornare il certificato autofirmato a un certificato firmato da un'autorità di certificazione (CA).

- "Gestisci i certificati"

ONTAP tools for VMware vSphere

Prima di distribuire gli ONTAP tools for VMware vSphere, è necessario conoscere i requisiti di spazio per il pacchetto di distribuzione e alcuni requisiti di base del sistema host.

È possibile utilizzare gli ONTAP tools for VMware vSphere con VMware vCenter Server Virtual Appliance (vCSA). È necessario distribuire gli ONTAP tools for VMware vSphere su un client vSphere supportato che includa il sistema ESXi.

Requisiti di sistema

- **Requisiti di spazio del pacchetto di installazione per nodo**
  - 15 GB per installazioni thin provisioning
  - 348 GB per installazioni con provisioning spesso
- **Requisiti di dimensionamento del sistema host** La memoria consigliata in base alle dimensioni della distribuzione è quella indicata nella tabella seguente. Per implementare l'alta disponibilità (HA), sarà necessaria una dimensione dell'appliance pari a tre volte quella specificata nella tabella.

Tipo di distribuzione	CPU per nodo	Memoria (GB) per nodo	Spazio su disco (GB) fornito per nodo
Piccolo	9	18	350
Medio	13	26	350
NOTA: la distribuzione di grandi dimensioni è solo per la configurazione HA.	17	34	350

Quando il backup è abilitato, ogni cluster di strumenti ONTAP necessita di altri 50 GB di spazio sul datastore in cui sono distribuite le VM. Pertanto, la modalità non HA richiede 400 GB, mentre la modalità HA richiede 1100 GB di spazio in totale.

Requisiti minimi di archiviazione e applicazione

Archiviazione, host e applicazioni	Requisiti di versione
ONTAP	9.14.1, 9.15.1, 9.16.0, 9.16.1 e 9.16.1P3 FAS, ASA serie A, ASA serie C, AFF serie A, AFF serie C e ASA r2.
Gli strumenti ONTAP supportano gli host ESXi	7.0.3 in poi
Strumenti ONTAP supportati da vCenter Server	7.0U3 in poi
Fornitore VASA	3,0
Applicazione OVA	10,4
Host ESXi per distribuire la macchina virtuale degli strumenti ONTAP	7.0U3 e 8.0U3
vCenter Server per distribuire la macchina virtuale degli strumenti ONTAP	7.0 e 8.0

A partire dagli ONTAP tools for VMware vSphere 10.4, l'hardware della macchina virtuale è stato modificato dalla versione 10 alla 17.

Lo strumento Interoperability Matrix Tool (IMT) contiene le informazioni più recenti sulle versioni supportate di ONTAP, vCenter Server, host ESXi e applicazioni plug-in.

"Strumento di matrice di interoperabilità"

Requisiti portuali

La tabella seguente illustra le porte di rete utilizzate da NetApp e le relative funzioni. Assicurarsi che queste porte siano aperte e accessibili per facilitare il corretto funzionamento e la comunicazione all'interno del sistema. Assicurarsi che siano presenti le configurazioni di rete necessarie per consentire il traffico su queste porte e il corretto funzionamento dei servizi associati. A seconda delle policy di sicurezza, potrebbe essere necessario configurare firewall o altri dispositivi di sicurezza per consentire questo traffico all'interno della rete.

Porta	Protocollo	Descrizione

8143	TCP	Connessioni HTTP/HTTPS per strumenti ONTAP .
8043	TCP	Connessioni HTTP/HTTPS per strumenti ONTAP .
9060	TCP	Connessioni HTTP/HTTPS per strumenti ONTAP .
22	TCP	Ansible utilizza questa porta SSH per la comunicazione durante il provisioning del cluster. Questa porta è necessaria per funzionalità quali la modifica della password dell'utente addetto alla manutenzione, i messaggi di stato e l'aggiornamento dei valori su tutti e tre i nodi in caso di configurazione HA.
443	TCP	Questa è la porta di passaggio per le comunicazioni in entrata per il servizio VASA Provider. Il certificato autofirmato del provider VASA e il certificato CA personalizzato sono ospitati su questa porta.
8443	TCP	Questa porta ospita la documentazione API tramite Swagger e l'applicazione dell'interfaccia utente Manager.
2379	TCP	Questa è la porta predefinita per le richieste client quali get, put, delete o watch per le chiavi nell'archivio dei valori chiave etcd.
2380	TCP	Questa è la porta predefinita per la comunicazione tra server per il cluster etcd utilizzata per l'algoritmo di consenso raft su cui etcd si basa per la replicazione e la coerenza dei dati.
7472	TCP/UDP	Questa è la porta del servizio Prometheus Metriche.
7946	TCP/UDP	Questa porta viene utilizzata per la scoperta della rete di container di Docker.
9083	TCP	Questa porta è una porta di servizio utilizzata internamente per il servizio VASA Provider.
1162	UDP	Questa è la porta dei pacchetti trap SNMP.

6443	TCP	Origine: nodi degli agenti RKE2. Destinazione: nodi del server REK2. Descrizione: API Kubernetes
9345	TCP	Origine: nodi degli agenti RKE2. Destinazione: nodi del server REK2. Descrizione: API del supervisore REK2
8472	TCP+UDP	Quando si utilizza flannel VXLAN, tutti i nodi devono essere in grado di raggiungere altri nodi tramite la porta UDP 8472. Origine: tutti i nodi RKE2. Destinazione: tutti i nodi REK2. Descrizione: Canale CNI con VXLAN
10250	TCP	Origine: tutti i nodi RKE2. Destinazione: tutti i nodi REK2. Descrizione: Metriche Kubelet
30000-32767	TCP	Origine: tutti i nodi RKE2. Destinazione: tutti i nodi REK2. Descrizione: intervallo di porte NodePort
123	TCP	Ntpd utilizza questa porta per eseguire la convalida del server NTP.
137-139	TCP/UDP	Pacchetti di condivisione SMB/Windows.
6789	TCP	Ceph Monitor (MON)
3300	TCP	Ceph Monitor (MON)
6800-7300	TCP	Ceph Manager, OSD e Filesystem (MDS).
80	TCP	Gateway Ceph RADOS (RGW)
9080	TCP	Connessioni HTTP/HTTPS VP (solo da 127.0.0.0/8 per IPv4 o ::1/128 per IPv6).

Limiti di configurazione per distribuire gli ONTAP tools for VMware vSphere

È possibile utilizzare la seguente tabella come guida per configurare gli ONTAP tools for VMware vSphere.

Dispiegamento	Tipo	Numero di vVols	Numero di host
Non-HA	Piccola (S)	~12K	32
Non-HA	Medio (M)	~24K	64
Alta disponibilità	Piccola (S)	~24K	64

Alta disponibilità	Medio (M)	~50k	128
Alta disponibilità	Grande (L)	~100k	256 [NOTA] Il numero di host nella tabella mostra il numero totale di host da più vCenter.

ONTAP tools for VMware vSphere - Storage Replication Adapter (SRA)

La tabella seguente mostra i numeri supportati per istanza di VMware Live Site Recovery utilizzando gli ONTAP tools for VMware vSphere.

Dimensioni di distribuzione vCenter	**Piccolo**	**Medio**
Numero totale di macchine virtuali configurate per la protezione mediante replica basata su array	2000	5000
Numero totale di gruppi di protezione della replica basati su array	250	250
Numero totale di gruppi di protezione per piano di ripristino	50	50
Numero di datastore replicati	255	255
Numero di VM	4000	7000

Nella tabella seguente viene mostrato il numero di VMware Live Site Recovery e i corrispondenti ONTAP tools for VMware vSphere .

Numero di istanze di VMware Live Site Recovery	* Dimensioni di distribuzione degli strumenti ONTAP *
Fino a 4	Piccolo
da 4 a 8	Medio
Più di 8	Grande

Per ulteriori informazioni, consulta "Limiti operativi di VMware Live Site Recovery" .

Prima di iniziare…

Prima di procedere con la distribuzione, assicurarsi che siano soddisfatti i seguenti requisiti:

Requisiti	**Il tuo stato**
La versione vSphere, la versione ONTAP e la versione host ESXi sono compatibili con la versione degli strumenti ONTP.	☐ Sì ☐ No
L'ambiente vCenter Server è impostato e configurato	☐ Sì ☐ No

Requisiti	Il tuo stato
La cache del browser è stata eliminata	☐ Sì ☐ No
Hai le credenziali del server vCenter padre	☐ Sì ☐ No
Si dispone delle credenziali di accesso per l'istanza di vCenter Server, a cui gli ONTAP tools for VMware vSphere si collegheranno dopo la distribuzione per la registrazione	☐ Sì ☐ No
Il nome di dominio su cui viene emesso il certificato viene mappato all'indirizzo IP virtuale in una distribuzione multi-vCenter in cui i certificati CA personalizzati sono obbligatori.	☐ Sì ☐ No
Hai eseguito il controllo nslookup sul nome di dominio per verificare se il dominio viene risolto nell'indirizzo IP previsto.	☐ Sì ☐ No
Il certificato viene creato con il nome di dominio e l'indirizzo IP degli strumenti ONTAP .	☐ Sì ☐ No
L'applicazione degli strumenti ONTAP e i servizi interni sono raggiungibili dal vCenter Server.	☐ Sì ☐ No
Quando si utilizzano SVM multi-tenant, si dispone di un LIF di gestione SVM su ogni SVM.	☐ Sì ☐ No

Foglio di lavoro per la distribuzione

Per la distribuzione a nodo singolo

Utilizzare il seguente foglio di lavoro per raccogliere le informazioni necessarie per gli ONTAP tools for VMware vSphere :

Requisito	Il tuo valore
Indirizzo IP per l'applicazione degli strumenti ONTAP . Questo è l'indirizzo IP per accedere all'interfaccia web degli strumenti ONTAP	
Gli strumenti ONTAP forniscono un indirizzo IP virtuale per la comunicazione interna. Questo indirizzo IP viene utilizzato per la comunicazione interna in una configurazione con più istanze di strumenti ONTAP . Questo indirizzo IP non deve essere uguale all'indirizzo IP dell'applicazione degli strumenti ONTAP .	
Nome host DNS per il primo nodo	
Server DNS primario	
Server DNS secondario	
Dominio di ricerca DNS	

Requisito	Il tuo valore
Indirizzo IPv4 per il primo nodo. Si tratta di un indirizzo IPv4 univoco per l'interfaccia di gestione del nodo sulla rete di gestione.	
Maschera di sottorete per l'indirizzo IPv4	
Gateway predefinito per l'indirizzo IPv4	
Indirizzo IPv6 (facoltativo)	
Lunghezza del prefisso IPv6 (facoltativa)	
Gateway per l'indirizzo IPv6 (facoltativo)	

Crea record DNS per tutti gli indirizzi IP sopra indicati. Prima di assegnare i nomi host, mapparli agli indirizzi IP liberi sul DNS. Tutti gli indirizzi IP devono trovarsi sulla stessa VLAN selezionata per la distribuzione.

Per la distribuzione ad alta disponibilità (HA)

Oltre ai requisiti di distribuzione del singolo nodo, per la distribuzione HA saranno necessarie le seguenti informazioni:

Requisito	Il tuo valore
Server DNS primario	
Server DNS secondario	
Dominio di ricerca DNS	
Nome host DNS per il secondo nodo	
Indirizzo IP per il secondo nodo	
Nome host DNS per il terzo nodo	
Indirizzo IP per il terzo nodo	

Configurazione del firewall di rete

Aprire le porte richieste per gli indirizzi IP nel firewall di rete. Gli strumenti ONTAP devono essere in grado di raggiungere questo LIF tramite la porta 443. Fare riferimento a"Requisiti portuali" per gli ultimi aggiornamenti.

Impostazioni di archiviazione ONTAP

Per garantire un'integrazione perfetta dello storage ONTAP con gli ONTAP tools for VMware vSphere, prendere in considerazione le seguenti impostazioni:

- Se si utilizza Fibre Channel (FC) per la connettività di archiviazione, configurare la suddivisione in zone sugli switch FC per connettere gli host ESXi con i LIF FC dell'SVM. "Scopri di più sulla zonizzazione FC e FCoE con i sistemi ONTAP"
- Per utilizzare la replica SnapMirror gestita dagli strumenti ONTAP , l'amministratore dell'archiviazione ONTAP deve creare "Relazioni tra pari del cluster ONTAP" E "Relazioni peer SVM intercluster ONTAP" in ONTAP prima di utilizzare SnapMirror.

Distribuisci gli ONTAP tools for VMware vSphere

Gli ONTAP tools for VMware vSphere vengono distribuiti come un singolo nodo di piccole dimensioni con servizi core per supportare datastore NFS e VMFS. Il processo di distribuzione degli strumenti ONTAP potrebbe richiedere fino a 45 minuti.

Prima di iniziare

Una libreria di contenuti in VMware è un oggetto contenitore che archivia modelli di VM, modelli di vApp e altri tipi di file. La distribuzione con la libreria di contenuti offre un'esperienza fluida perché non dipende dalla connettività di rete.

> È consigliabile archiviare la libreria dei contenuti in un datastore condiviso in modo che tutti gli host all'interno di un cluster possano accedervi. Creare una libreria di contenuti per archiviare l'OVA prima di configurare l'appliance in modalità HA. Non eliminare il modello della libreria dei contenuti dopo la distribuzione.

> Per abilitare la distribuzione HA in un secondo momento, non distribuire la macchina virtuale che ospita gli strumenti ONTAP direttamente su un host ESXi. Distribuiscilo invece su un cluster o su un pool di risorse.

Se non disponi di una libreria di contenuti, segui questi passaggi per crearne una:

Creare una libreria di contenuti Se si prevede di utilizzare solo una piccola distribuzione a nodo singolo, non è necessario creare una libreria di contenuti.

1. Scarica il file contenente i file binari (*.ova*) e i certificati firmati per gli ONTAP tools for VMware vSphere da "Sito di supporto NetApp" .
2. Accedi al client vSphere
3. Selezionare il menu vSphere Client e selezionare **Librerie di contenuti**.
4. Seleziona **Crea** sulla destra della pagina.
5. Assegna un nome alla libreria e crea la libreria dei contenuti.
6. Accedi alla libreria dei contenuti che hai creato.
7. Selezionare **Azioni** nella parte destra della pagina, quindi selezionare **Importa elemento** e importare il file OVA.

> Per maggiori informazioni, fare riferimento a "Creazione e utilizzo della libreria di contenuti" blog.

> Prima di procedere con la distribuzione, impostare il Distributed Resource Scheduler (DRS) del cluster nell'inventario su "Conservativo". In questo modo si garantisce che le VM non vengano migrate durante l'installazione.

Inizialmente, gli ONTAP tools for VMware vSphere vengono distribuiti come configurazione non HA. Per passare alla distribuzione HA, sarà necessario abilitare il plug-in a caldo della CPU e il plug-in a caldo della memoria. È possibile eseguire questo passaggio come parte del processo di distribuzione oppure modificare le impostazioni della VM dopo la distribuzione.

Passi

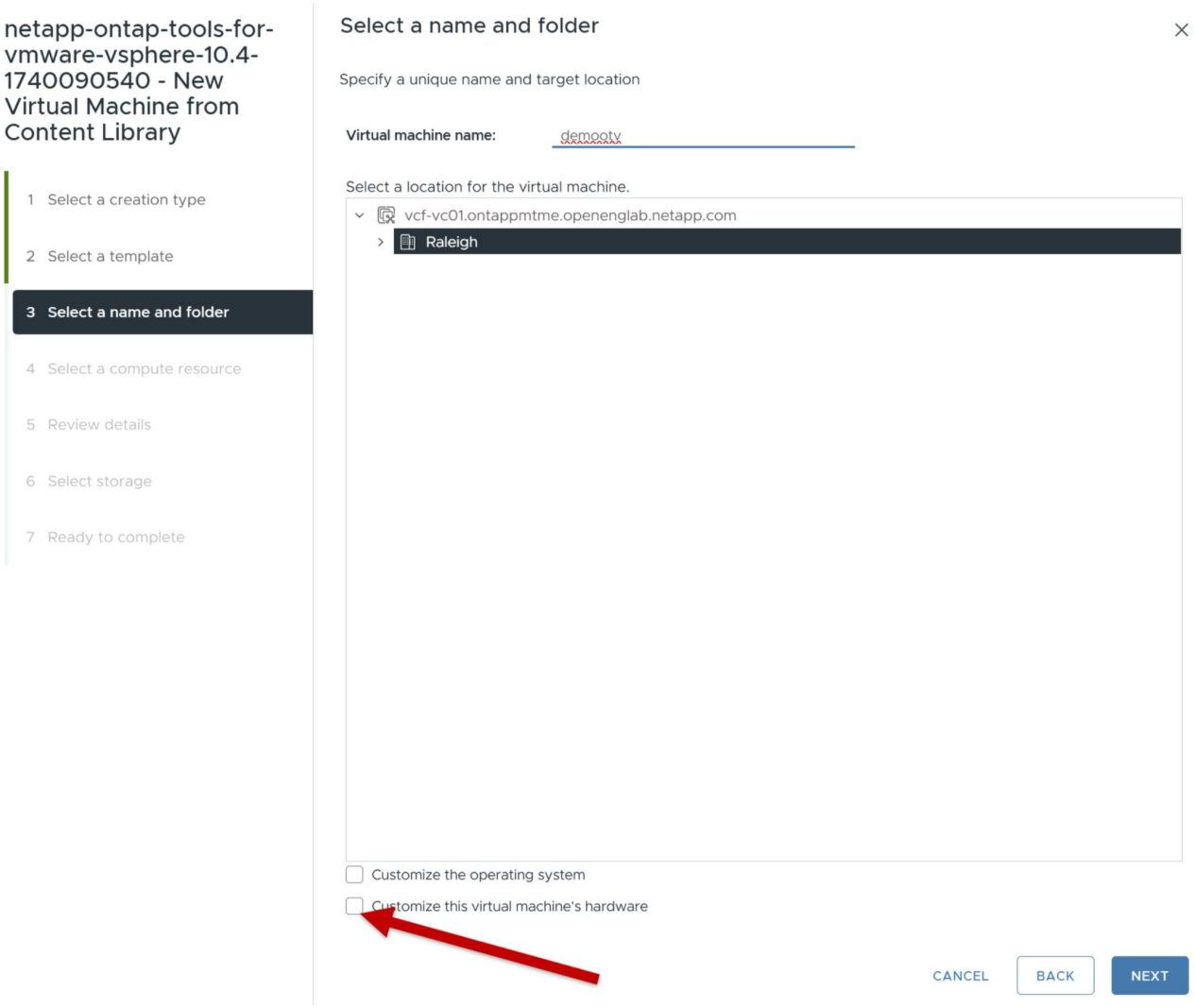
1. Scaricare il file che contiene i file binari (*.ova*) e i certificati firmati per il ONTAP tools for VMware vSphere dal "Sito di supporto NetApp". Se hai importato l'OVA nella libreria dei contenuti, puoi saltare questo passaggio e procedere con quello successivo
2. Accedi al server vSphere.
3. Passare al pool di risorse, al cluster o all'host in cui si intende distribuire l'OVA.

   Non archiviare mai gli ONTAP tools for VMware vSphere sui datastore vVols da essa gestiti.

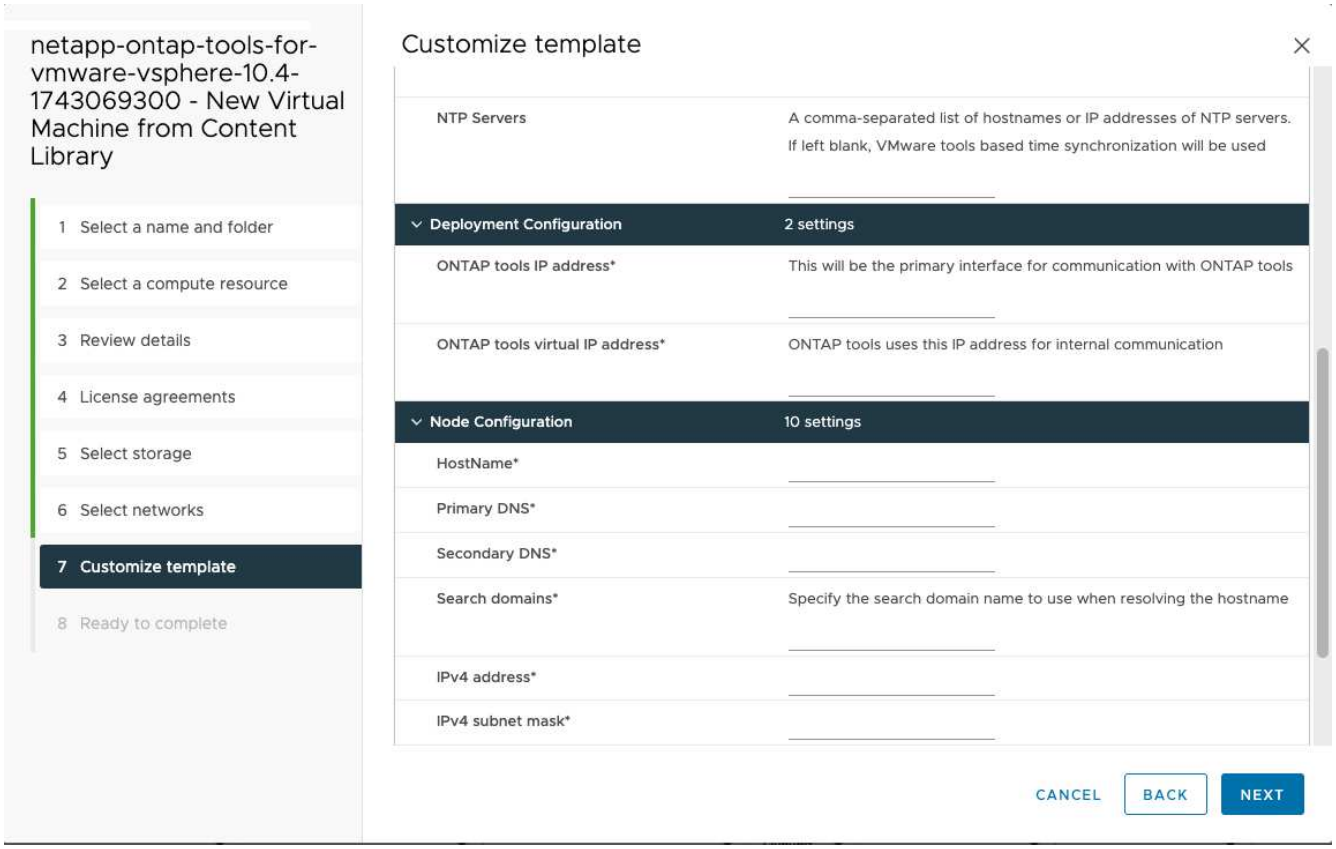
4. È possibile distribuire l'OVA dalla libreria dei contenuti o dal sistema locale.

Dal sistema locale	Dalla libreria dei contenuti
a. Fare clic con il pulsante destro del mouse e selezionare **Distribuisci modello OVF…**. b. Scegliere il file OVA dall'URL o andare alla sua posizione, quindi selezionare **Avanti**.	a. Vai alla tua libreria di contenuti e seleziona l'elemento della libreria che desideri distribuire. b. Seleziona **Azioni** > **Nuova VM da questo modello**

5. Nel campo **Seleziona un nome e una cartella**, inserisci il nome della macchina virtuale e scegline la posizione.
   - Se si utilizza la versione vCenter Server 8.0.3, selezionare l'opzione **Personalizza l'hardware di questa macchina virtuale**, che attiverà un passaggio aggiuntivo denominato **Personalizza hardware** prima di procedere alla finestra **Pronto per il completamento**.
   - Se si utilizza la versione vCenter Server 7.0.3, seguire i passaggi nella sezione **cosa succede dopo?** alla fine della distribuzione.



6. Selezionare una risorsa del computer e fare clic su **Avanti**. Facoltativamente, seleziona la casella per **Accendere automaticamente la VM distribuita**.
7. Rivedi i dettagli del modello e seleziona **Avanti**.
8. Leggere e accettare il contratto di licenza e selezionare **Avanti**.
9. Selezionare l'archiviazione per la configurazione e il formato del disco, quindi selezionare **Avanti**.
10. Selezionare la rete di destinazione per ciascuna rete di origine e selezionare **Avanti**.
11. Nella finestra **Personalizza modello**, compila i campi richiesti e seleziona **Avanti**
    .

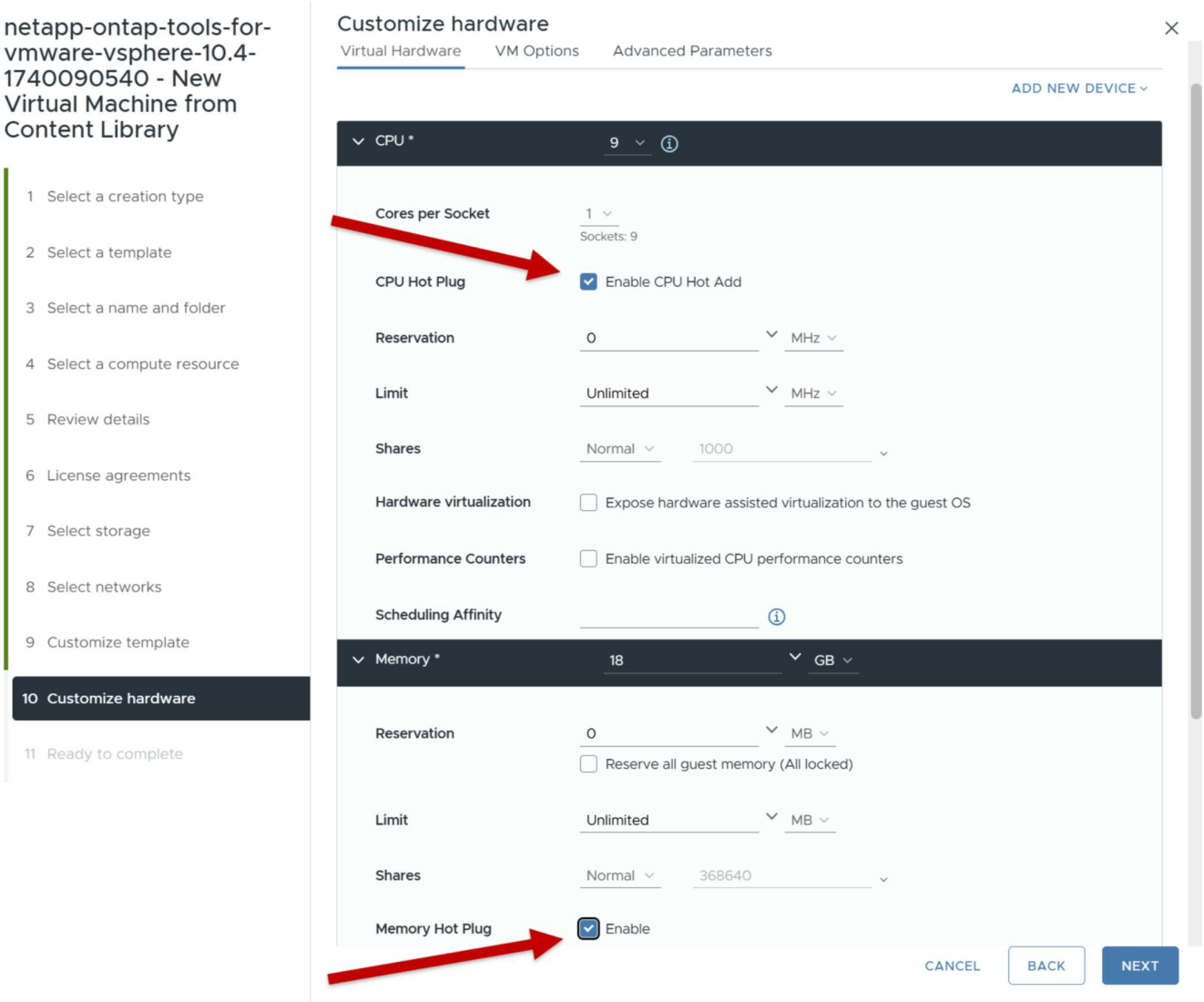


- Le informazioni vengono convalidate durante l'installazione. In caso di discrepanza, sulla console Web viene visualizzato un messaggio di errore e viene richiesto di correggerlo.
- I nomi host devono includere lettere (AZ, az), cifre (0-9) e trattini (-). Per configurare il dual stack, specificare il nome host mappato all'indirizzo IPv6.

> Il protocollo IPv6 puro non è supportato. La modalità mista è supportata con VLAN contenente sia indirizzi IPv6 che IPv4.

- L'indirizzo IP degli strumenti ONTAP è l'interfaccia principale per comunicare con gli strumenti ONTAP .
- IPv4 è il componente dell'indirizzo IP della configurazione del nodo, che può essere utilizzato per abilitare la shell diagnostica e l'accesso SSH sul nodo a fini di debug e manutenzione.

12. Quando si utilizza la versione vCenter Server 8.0.3, nella finestra **Personalizza hardware**, abilitare le opzioni **Aggiunta a caldo CPU** e **Collegamento a caldo della memoria** per consentire la funzionalità HA.



13. Rivedi i dettagli nella finestra **Pronto per il completamento**, seleziona **Fine**.

    Man mano che l'attività di distribuzione viene creata, l'avanzamento viene visualizzato nella barra delle applicazioni di vSphere.

14. Accendere la macchina virtuale dopo aver completato l'attività se non è stata selezionata l'opzione per accendere automaticamente la macchina virtuale.

È possibile monitorare l'avanzamento dell'installazione nella console web della VM.

In caso di discrepanze nel modulo OVF, una finestra di dialogo richiederà un'azione correttiva. Utilizzare il pulsante Tab per navigare, apportare le modifiche necessarie e selezionare **OK**. Hai tre tentativi per risolvere eventuali problemi. Se i problemi persistono dopo tre tentativi, il processo di installazione si interromperà e si consiglia di riprovare l'installazione su una nuova macchina virtuale.

Cosa succederà adesso?

Se si dispone ONTAP tools for VMware vSphere con vCenter Server 7.0.3, seguire questi passaggi dopo la distribuzione.

1. Accedi al client vCenter
2. Spegnere il nodo degli strumenti ONTAP .

3. Passare agli ONTAP tools for VMware vSphere in **Inventari** e selezionare l'opzione **Modifica impostazioni**.
4. Nelle opzioni **CPU**, seleziona la casella di controllo **Abilita aggiunta a caldo CPU**
5. Nelle opzioni **Memoria**, seleziona la casella di controllo **Abilita** accanto a **Hot plug memoria**.

Codici di errore di distribuzione

Potrebbero verificarsi codici di errore durante le operazioni di distribuzione, riavvio e ripristino ONTAP tools for VMware vSphere . I codici di errore sono lunghi cinque cifre: le prime due rappresentano lo script che ha riscontrato il problema, mentre le ultime tre rappresentano il flusso di lavoro specifico all'interno di quello script.

Tutti i log degli errori vengono registrati nel file ansible-perl-errors.log per facilitare il monitoraggio e la risoluzione dei problemi. Questo file di registro contiene il codice di errore e l'attività Ansible non riuscita.

> I codici di errore forniti in questa pagina sono solo a scopo di riferimento. Se l'errore persiste o se non viene indicata alcuna soluzione, contattare il team di supporto.

Nella tabella seguente sono elencati i codici di errore e i nomi dei file corrispondenti.

Codice di errore	Nome dello script
00	firstboot-network-config.pl, modalità di distribuzione
01	firstboot-network-config.pl, aggiornamento della modalità
02	firstboot-inputs-validation.pl
03	firstboot-deploy-otv-ng.pl, distribuzione, HA
04	firstboot-deploy-otv-ng.pl, distribuzione, non HA
05	firstboot-deploy-otv-ng.pl, riavvio
06	firstboot-deploy-otv-ng.pl, aggiornamento, HA
07	firstboot-deploy-otv-ng.pl, aggiornamento, non-HA
08	firstboot-otv-recovery.pl
09	post-deploy-upgrade.pl

Le ultime tre cifre del codice di errore indicano l'errore specifico del flusso di lavoro all'interno dello script:

Codice di errore di distribuzione	Flusso di lavoro	Risoluzione
049	Per la rete e la convalida lo script perl li assegnerà a breve	-
050	Generazione della chiave Ssh non riuscita	Riavviare la macchina virtuale (VM) primaria.

053	Installazione di RKE2 non riuscita	Eseguire quanto segue e riavviare la VM primaria oppure ridistribuire: sudo rke2-killall.sh (tutte le VM) sudo rke2-uninstall.sh (tutte le VM).
054	Impostazione kubeconfig non riuscita	Ridistribuire
055	Distribuzione del registro non riuscita	Se il pod del registro è presente, attendere che sia pronto, quindi riavviare la VM primaria oppure ridistribuirla.
059	La distribuzione di KubeVip non è riuscita	Assicurarsi che l'indirizzo IP virtuale per il piano di controllo Kubernetes e l'indirizzo IP degli strumenti ONTAP forniti durante la distribuzione appartengano alla stessa VLAN e siano indirizzi IP liberi. Riavviare se tutti i punti precedenti sono corretti. Altrimenti, ridistribuisci.
060	L'implementazione dell'operatore non è riuscita	Ricomincia
061	La distribuzione dei servizi non è riuscita	Eseguire il debug di base di Kubernetes come ottenere pod, ottenere rs, ottenere svc e così via nello spazio dei nomi ntv-system per maggiori dettagli e registri degli errori in /var/log/ansible-perl-errors.log e /var/log/ansible-run.log e ridistribuire.
062	La distribuzione dei servizi degli strumenti ONTAP non è riuscita	Per maggiori dettagli e per ripetere l'operazione, fare riferimento ai log degli errori in /var/log/ansible-perl-errors.log.
065	L'URL della pagina Swagger non è raggiungibile	Ridistribuire
066	I passaggi successivi alla distribuzione per il certificato gateway non sono riusciti	Per ripristinare/completare l'aggiornamento, procedere come segue: * Abilitare la shell diagnostica. * Eseguire il comando 'sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postDeploy'. * Controllare i log in /var/log/post-deploy-upgrade.log.
088	La configurazione della rotazione dei log per journald non è riuscita	Verificare che le impostazioni di rete della VM siano compatibili con l'host su cui è ospitata la VM. Puoi provare a migrare verso un altro host e riavviare la VM.

089	La modifica della proprietà del file di configurazione di rotazione del registro di riepilogo non è riuscita	Riavviare la macchina virtuale primaria.
096	Installa il provisioner di archiviazione dinamica	-
108	Script di seeding non riuscito	-

Codice di errore di riavvio	Flusso di lavoro	Risoluzione
067	L'attesa per rke2-server è scaduta.	-
101	Impossibile reimpostare la password utente Maint/Console.	-
102	Impossibile eliminare il file della password durante il ripristino della password utente di manutenzione/console.	-
103	Impossibile aggiornare la nuova password utente di manutenzione/console nel vault.	-
088	La configurazione della rotazione dei log per journald non è riuscita.	Verificare che le impostazioni di rete della VM siano compatibili con l'host su cui è ospitata la VM. Puoi provare a migrare verso un altro host e riavviare la VM.
089	La modifica della proprietà del file di configurazione di rotazione del registro di riepilogo non è riuscita.	Riavviare la macchina virtuale.

Configurare gli ONTAP tools for VMware vSphere

Aggiungi istanze di vCenter Server

Aggiungi istanze di vCenter Server agli ONTAP tools for VMware vSphere per configurare, gestire e proteggere i tuoi datastore virtuali nel tuo ambiente vCenter Server. Quando si aggiungono più istanze di vCenter Server, sono necessari certificati CA personalizzati per la comunicazione sicura tra gli strumenti ONTAP e ciascun vCenter Server.

Informazioni su questo compito

Grazie all'integrazione con vCenter, gli strumenti ONTAP consentono di eseguire attività di storage come provisioning, snapshot e protezione dei dati direttamente dal client vSphere, eliminando la necessità di passare a console di gestione dello storage separate.

Passi

1. Apri un browser web e vai all'URL: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con le credenziali di amministratore ONTAP tools for VMware vSphere fornite durante la distribuzione.
3. Selezionare **vCenter** > **Aggiungi** per integrare le istanze di vCenter Server. Fornisci l'indirizzo IP o il nome host del tuo vCenter, il nome utente, la password e i dettagli della porta.

> Non è necessario un account amministratore per aggiungere istanze vCenter agli strumenti ONTAP . È possibile creare un ruolo personalizzato senza l'account amministratore con autorizzazioni limitate. Fare riferimento a"Utilizzare vCenter Server RBAC con gli ONTAP tools for VMware vSphere 10" per i dettagli.

L'aggiunta di un'istanza di vCenter Server agli strumenti ONTAP attiva automaticamente le seguenti azioni:

- Il plug-in del client vCenter è registrato come plug-in remoto.
- I privilegi personalizzati per i plug-in e le API vengono applicati all'istanza di vCenter Server.
- Per gestire gli utenti vengono creati ruoli personalizzati.
- Il plug-in viene visualizzato come collegamento nell'interfaccia utente di vSphere.

Registrare il provider VASA con un'istanza di vCenter Server

È possibile registrare il provider VASA con un'istanza di vCenter Server utilizzando gli ONTAP tools for VMware vSphere. La sezione Impostazioni provider VASA visualizza lo stato di registrazione del provider VASA per il vCenter Server selezionato. In una distribuzione multi-vCenter, assicurati di disporre di certificati CA personalizzati per ogni istanza di vCenter Server.

Passi

1. Accedi al client vSphere.

2. Selezionare **Scelte rapide** > *Strumenti NetApp ONTAP * nella sezione plug-in.
3. Selezionare **Impostazioni** > **Impostazioni provider VASA**. Lo stato di registrazione del fornitore VASA verrà visualizzato come non registrato.
4. Selezionare il pulsante **Registra** per registrare il fornitore VASA.
5. Inserisci un nome e le credenziali per il fornitore VASA. Il nome utente può contenere solo lettere, numeri e caratteri di sottolineatura. La lunghezza della password deve essere compresa tra 8 e 256 caratteri.
6. Seleziona **Registrati**.
7. Dopo una registrazione riuscita e l'aggiornamento della pagina, vengono visualizzati lo stato, il nome e la versione del provider VASA registrato. Dopo la registrazione viene attivata l'azione di annullamento della registrazione.

Cosa c'è dopo?

Verificare che il provider VASA integrato sia elencato in Provider VASA dal client vCenter:

Passi

1. Passare all'istanza di vCenter Server.
2. Accedi con le credenziali di amministratore.
3. Selezionare **Provider di archiviazione** > **Configura**. Verificare che il fornitore VASA integrato sia elencato correttamente.

Installa il plug-in NFS VAAI

Il plug-in NFS vStorage API for Array Integration (NFS VAAI) è un componente software che integra VMware vSphere e gli array di archiviazione NFS. Installare il plug-in NFS VAAI utilizzando gli ONTAP tools for VMware vSphere per sfruttare le funzionalità avanzate dell'array di archiviazione NFS per trasferire determinate operazioni relative all'archiviazione dagli host ESXi all'array di archiviazione stesso.

Prima di iniziare

- Scarica il "Plug-in NetApp NFS per VMware VAAI" pacchetto di installazione.
- Assicurati di disporre dell'host ESXi e della patch più recente di vSphere 7.0U3 o versioni successive e ONTAP 9.14.1 o versioni successive.
- Montare un datastore NFS.

Passi

1. Accedi al client vSphere.
2. Selezionare **Scelte rapide** > *Strumenti NetApp ONTAP * nella sezione plug-in.
3. Selezionare **Impostazioni** > **Strumenti NFS VAAI**.
4. Una volta caricato il plug-in VAAI su vCenter Server, selezionare **Modifica** nella sezione **Versione esistente**. Se un plug-in VAAI non è caricato sul vCenter Server, selezionare il pulsante **Carica**.
5. Sfoglia e seleziona il `.vib` file e seleziona **Carica** per caricare il file sugli strumenti ONTAP .
6. Selezionare **Installa su host ESXI**, selezionare l'host ESXi su cui si desidera installare il plug-in NFS VAAI, quindi selezionare **Installa**.

   Vengono visualizzati solo gli host ESXi idonei per l'installazione del plug-in. È possibile monitorare

l'avanzamento dell'installazione nella sezione delle attività recenti di vSphere Web Client.

7. Dopo l'installazione, riavviare manualmente l'host ESXi.

   Quando l'amministratore VMware riavvia l'host ESXi, gli ONTAP tools for VMware vSphere rilevano e abilitano automaticamente il plug-in NFS VAAI.

Cosa succederà ora?

Dopo aver installato il plug-in NFS VAAI e riavviato l'host ESXi, è necessario configurare i criteri di esportazione NFS corretti per l'offload della copia VAAI. Quando si configura VAAI in un ambiente NFS, configurare le regole dei criteri di esportazione tenendo presenti i seguenti requisiti:

- Il volume ONTAP pertinente deve consentire le chiamate NFSv4.
- L'utente root dovrebbe rimanere root e NFSv4 dovrebbe essere consentito in tutti i volumi padre di giunzione.
- L'opzione per il supporto VAAI deve essere impostata sul server NFS pertinente.

Per maggiori informazioni sulla procedura, fare riferimento a "Configurare i criteri di esportazione NFS corretti per l'offload della copia VAAI" Articolo della Knowledge Base.

Informazioni correlate

"Supporto per VMware vStorage su NFS"

"Abilita o disabilita NFSv4.0"

"Supporto ONTAP per NFSv4.2"

Configurare le impostazioni dell'host ESXi

La configurazione delle impostazioni multipath e timeout del server ESXi garantisce elevata disponibilità e integrità dei dati, consentendo di passare senza problemi a un percorso di archiviazione di backup in caso di errore del percorso primario.

Configurare le impostazioni multipath e timeout del server ESXi

Gli ONTAP tools for VMware vSphere controllano e impostano le impostazioni multipath dell'host ESXi e le impostazioni di timeout HBA che funzionano meglio con i sistemi di storage NetApp .

Informazioni su questo compito

A seconda della configurazione e del carico del sistema, questo processo potrebbe richiedere molto tempo. L'avanzamento dell'attività viene visualizzato nel pannello Attività recenti.

Passi

1. Dalla home page del client Web VMware vSphere, selezionare **Host e cluster**.
2. Fare clic con il pulsante destro del mouse su un host e selezionare **Strumenti NetApp ONTAP * > *Aggiorna dati host**.
3. Nella pagina dei collegamenti del client Web VMware vSphere, selezionare *Strumenti NetApp ONTAP * nella sezione plug-in.
4. Accedere alla scheda **Conformità host ESXi** nella panoramica (dashboard) del plug-in ONTAP tools for

VMware vSphere .

5. Selezionare il collegamento **Applica impostazioni consigliate**.
6. Nella finestra **Applica impostazioni host consigliate**, seleziona gli host che desideri aggiornare per renderli conformi alle impostazioni consigliate da NetApp e seleziona **Avanti**.

   È possibile espandere l'host ESXi per visualizzare i valori correnti.

7. Nella pagina delle impostazioni, seleziona i valori consigliati in base alle tue esigenze.
8. Nel riquadro di riepilogo, controlla i valori e seleziona **Fine**. È possibile monitorare l'avanzamento nel pannello delle attività recenti.

Imposta i valori dell'host ESXi

Utilizzando gli ONTAP tools for VMware vSphere, è possibile impostare timeout e altri valori sugli host ESXi per garantire le migliori prestazioni e un failover riuscito. I valori impostati ONTAP tools for VMware vSphere si basano su test interni NetApp .

È possibile impostare i seguenti valori su un host ESXi:

Impostazioni dell'adattatore HBA/CNA

Imposta i seguenti parametri sui valori predefiniti:

- Disk.QFullSampleSize
- Disco.QFullThreshold
- Timeout HBA Emulex FC
- Timeout HBA QLogic FC

Impostazioni MPIO

Le impostazioni MPIO definiscono i percorsi preferiti per i sistemi di archiviazione NetApp . Determinano quali percorsi disponibili sono ottimizzati (a differenza dei percorsi non ottimizzati che attraversano il cavo di interconnessione) e impostano il percorso preferito su uno di questi percorsi.

In ambienti ad alte prestazioni o quando si testano le prestazioni con un singolo datastore LUN, valutare la possibilità di modificare l'impostazione del bilanciamento del carico del criterio di selezione del percorso (PSP) round-robin (VMW_PSP_RR) dall'impostazione IOPS predefinita di 1000 a un valore di 1.

Le impostazioni MPIO non si applicano ai protocolli NVMe, NVMe/FC e NVMe/TCP.

Impostazioni NFS

Parametro	Imposta questo valore su…
Net.TcpipHeapSize	32
Net.TcpipHeapMax	1024 MB
NFS.MaxVolumes	256
NFS41.MaxVolumes	256

NFS.MaxQueueDepth	128 o superiore
NFS.HeartbeatMaxFailures	10
NFS.Frequenza del battito cardiaco	12
NFS.HeartbeatTimeout	5

Configurare i ruoli e i privilegi degli utenti ONTAP

È possibile configurare nuovi ruoli utente e privilegi per la gestione dei backend di archiviazione utilizzando il file JSON fornito con gli ONTAP tools for VMware vSphere e ONTAP System Manager.

Prima di iniziare

- Dovresti aver scaricato il file dei privilegi ONTAP dagli ONTAP tools for VMware vSphere utilizzando *https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip*.
- Dovresti aver scaricato il file ONTAP Privileges dagli strumenti ONTAP utilizzando `https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip`.

> È possibile creare utenti a livello di cluster o direttamente a livello di macchine virtuali di archiviazione (SVM). È anche possibile creare utenti senza utilizzare il file user_roles.json e, in tal caso, è necessario disporre di un set minimo di privilegi a livello SVM.

- Dovresti aver effettuato l'accesso con privilegi di amministratore per il backend di archiviazione.

Passi

1. Estrarre il file scaricato *https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip*.
2. Accedere a ONTAP System Manager utilizzando l'indirizzo IP di gestione del cluster.
3. Accedi al cluster con privilegi di amministratore. Per configurare un utente, procedere come segue:
   a. Per configurare l'utente degli strumenti ONTAP del cluster, selezionare il riquadro **Cluster** > **Impostazioni** > **Utenti e ruoli**.
   b. Per configurare l'utente degli strumenti SVM ONTAP , selezionare il riquadro **Storage SVM** > **Impostazioni** > **Utenti e ruoli**.
   c. Selezionare **Aggiungi** in Utenti.
   d. Nella finestra di dialogo **Aggiungi utente**, seleziona **Prodotti di virtualizzazione**.
   e. **Sfoglia** per selezionare e caricare il file JSON Privileges ONTAP .

      Il campo Prodotto viene compilato automaticamente.

   f. Selezionare la funzionalità del prodotto come **VSC, VASA Provider e SRA** dal menu a discesa.

      Il campo **Ruolo** viene compilato automaticamente in base alla funzionalità del prodotto selezionata.

   g. Inserisci il nome utente e la password richiesti.
   h. Selezionare i privilegi (Discovery, Create Storage, Edit Storage, Destroy Storage, NAS/SAN Role) richiesti per l'utente, quindi selezionare **Aggiungi**.

Il nuovo ruolo e utente vengono aggiunti e puoi visualizzare i privilegi dettagliati del ruolo che hai configurato.

Requisiti di mappatura aggregata SVM

Per utilizzare le credenziali utente SVM per il provisioning degli archivi dati, gli ONTAP tools for VMware vSphere creano volumi sull'aggregato specificato nell'API POST degli archivi dati. ONTAP non consente la creazione di volumi su aggregati non mappati su una SVM utilizzando le credenziali utente SVM. Per risolvere questo problema, è necessario mappare gli SVM con gli aggregati utilizzando l'API REST o la CLI ONTAP come descritto qui.

API REST:

```
PATCH "/api/svm/svms/f16f0935-5281-11e8-b94d-005056b46485"
'{"aggregates":{"name":["aggr1","aggr2","aggr3"]}}'
```

ONTAP CLI:

```
sti115_vsim_ucs630f_aggr1 vserver show-aggregates
AvailableVserver        Aggregate      State         Size Type    SnapLock
Type-------------- -------------- ------- ---------- -------
--------------svm_test       sti115_vsim_ucs630f_aggr1
online     10.11GB vmdisk  non-snaplock
```

Creare manualmente l'utente e il ruolo ONTAP

Seguire le istruzioni in questa sezione per creare manualmente l'utente e i ruoli senza utilizzare il file JSON.

1. Accedere a ONTAP System Manager utilizzando l'indirizzo IP di gestione del cluster.
2. Accedi al cluster con privilegi di amministratore.
   a. Per configurare i ruoli degli strumenti ONTAP del cluster, selezionare il riquadro **Cluster** > **Impostazioni** > **Utenti e ruoli**.
   b. Per configurare i ruoli degli strumenti SVM ONTAP del cluster, selezionare il riquadro **Storage SVM** > **Impostazioni** > **Utenti e ruoli**
3. Crea ruoli:
   a. Selezionare **Aggiungi** nella tabella **Ruoli**.
   b. Inserisci i dettagli **Nome del ruolo** e **Attributi del ruolo**.

      Aggiungere il **Percorso API REST** e il rispettivo accesso dal menu a discesa.

   c. Aggiungi tutte le API necessarie e salva le modifiche.
4. Crea utenti:
   a. Selezionare **Aggiungi** nella tabella **Utenti**.
   b. Nella finestra di dialogo **Aggiungi utente**, selezionare **Gestore di sistema**.
   c. Inserisci **Nome utente**.
   d. Selezionare **Ruolo** tra le opzioni create nel passaggio **Crea ruoli** sopra.
   e. Inserisci le applicazioni a cui consentire l'accesso e il metodo di autenticazione. ONTAPI e HTTP sono

le applicazioni richieste e il tipo di autenticazione è **Password**.

f. Imposta la **Password per l'utente** e **Salva** l'utente.

Elenco dei privilegi minimi richiesti per l'utente del cluster con ambito globale non amministratore

In questa sezione sono elencati i privilegi minimi richiesti per gli utenti di cluster con ambito globale non amministratore creati senza utilizzare il file JSON degli utenti. Se un cluster viene aggiunto in ambito locale, si consiglia di utilizzare il file JSON per creare gli utenti, poiché gli ONTAP tools for VMware vSphere richiedono privilegi di lettura superiori a quelli di semplice accesso per il provisioning su ONTAP.

Utilizzo delle API:

API	Livello di accesso	Utilizzato per
/api/cluster	Sola lettura	Rilevamento della configurazione del cluster
/api/cluster/licenze/licenze	Sola lettura	Controllo della licenza per licenze specifiche del protocollo
/api/cluster/nodi	Sola lettura	Scoperta del tipo di piattaforma
/api/sicurezza/account	Sola lettura	Scoperta dei privilegi
/api/sicurezza/ruoli	Sola lettura	Scoperta dei privilegi
/api/storage/aggregati	Sola lettura	Controllo dello spazio aggregato durante il provisioning di Datastore/Volume
/api/archiviazione/cluster	Sola lettura	Per ottenere i dati sullo spazio e l'efficienza a livello di cluster
/api/storage/dischi	Sola lettura	Per ottenere i dischi associati in un aggregato
/api/storage/qos/policies	Leggi/Crea/Modifica	Gestione QoS e policy VM
/api/svm/svms	Sola lettura	Per ottenere la configurazione SVM nel caso in cui il cluster venga aggiunto localmente.
/api/network/ip/interfacce	Sola lettura	Aggiungi backend di archiviazione: per identificare l'ambito di gestione LIF è Cluster/SVM
/api/storage/zone-di-disponibilità	Sola lettura	Scoperta SAZ. Applicabile alla versione ONTAP 9.16.1 e successive e ai sistemi ASA r2.

Crea ONTAP tools for VMware vSphere ONTAP basata su cluster con ambito utente

> Sono necessari Privileges individuazione, creazione, modifica e distruzione per eseguire operazioni PATCH e rollback automatico in caso di errore sui datastore. La mancanza di tutti questi privilegi porta a interruzioni del flusso di lavoro e problemi di pulizia.

La creazione ONTAP tools for VMware vSphere ONTAP API basata sull'utente con privilegi di individuazione, creazione di storage, modifica di storage, eliminazione di storage consente di avviare rilevazioni e gestire i

flussi di lavoro degli strumenti ONTAP .

Per creare un utente con ambito cluster dotato di tutti i privilegi sopra menzionati, eseguire i seguenti comandi:

```
security login rest-role create -role <role-name> -api
/api/application/consistency-groups -access all

security login rest-role create -role <role-name> -api
/api/private/cli/snapmirror -access all

security login rest-role create -role <role-name> -api
/api/protocols/nfs/export-policies -access all

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystem-maps -access all

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystems -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/igroups -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/lun-maps -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/vvol-bindings -access all

security login rest-role create -role <role-name> -api
/api/snapmirror/relationships -access all

security login rest-role create -role <role-name> -api
/api/storage/volumes -access all

security login rest-role create -role <role-name> -api
"/api/storage/volumes/*/snapshots" -access all

security login rest-role create -role <role-name> -api /api/storage/luns
-access all

security login rest-role create -role <role-name> -api
/api/storage/namespaces -access all

security login rest-role create -role <role-name> -api
/api/storage/qos/policies -access all

security login rest-role create -role <role-name> -api
```

```
/api/cluster/schedules -access read_create

security login rest-role create -role <role-name> -api
/api/snapmirror/policies -access read_create

security login rest-role create -role <role-name> -api
/api/storage/file/clone -access read_create

security login rest-role create -role <role-name> -api
/api/storage/file/copy -access read_create

security login rest-role create -role <role-name> -api
/api/support/ems/application-logs -access read_create

security login rest-role create -role <role-name> -api
/api/protocols/nfs/services -access read_modify

security login rest-role create -role <role-name> -api /api/cluster
-access readonly

security login rest-role create -role <role-name> -api /api/cluster/jobs
-access readonly

security login rest-role create -role <role-name> -api
/api/cluster/licensing/licenses -access readonly

security login rest-role create -role <role-name> -api /api/cluster/nodes
-access readonly

security login rest-role create -role <role-name> -api /api/cluster/peers
-access readonly

security login rest-role create -role <role-name> -api /api/name-
services/name-mappings -access readonly

security login rest-role create -role <role-name> -api
/api/network/ethernet/ports -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/logins -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/ports -access readonly
```

```
security login rest-role create -role <role-name> -api
/api/network/ip/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/nfs/kerberos/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/nvme/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/san/fcp/services -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/san/iscsi/services -access readonly

security login rest-role create -role <role-name> -api
/api/security/accounts -access readonly

security login rest-role create -role <role-name> -api /api/security/roles
-access readonly

security login rest-role create -role <role-name> -api
/api/storage/aggregates -access readonly

security login rest-role create -role <role-name> -api
/api/storage/cluster -access readonly

security login rest-role create -role <role-name> -api /api/storage/disks
-access readonly

security login rest-role create -role <role-name> -api /api/storage/qtrees
-access readonly

security login rest-role create -role <role-name> -api
/api/storage/quota/reports -access readonly

security login rest-role create -role <role-name> -api
/api/storage/snapshot-policies -access readonly

security login rest-role create -role <role-name> -api /api/svm/peers
-access readonly

security login rest-role create -role <role-name> -api /api/svm/svms
-access readonly
```

Inoltre, per le versioni ONTAP 9.16.0 e successive, eseguire il seguente comando:

```
security login rest-role create -role <role-name> -api
/api/storage/storage-units -access all
```

Per i sistemi ASA r2 su ONTAP versione 9.16.1 e successive, eseguire il seguente comando:

```
security login rest-role create -role <role-name> -api
/api/storage/availability-zones -access readonly
```

Crea ONTAP tools for VMware vSphere ONTAP

Per creare un utente con ambito SVM dotato di tutti i privilegi, eseguire i seguenti comandi:

```
security login rest-role create -role <role-name> -api
/api/application/consistency-groups -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/private/cli/snapmirror -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nfs/export-policies -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystem-maps -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystems -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/igroups -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/lun-maps -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/vvol-bindings -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/snapmirror/relationships -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/volumes -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
"/api/storage/volumes/*/snapshots" -access all -vserver <vserver-name>
```

```
security login rest-role create -role <role-name> -api /api/storage/luns
-access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/namespaces -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/cluster/schedules -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/snapmirror/policies -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/file/clone -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/file/copy -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/support/ems/application-logs -access read_create -vserver <vserver-
name>

security login rest-role create -role <role-name> -api
/api/protocols/nfs/services -access read_modify -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/cluster
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/cluster/jobs
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/cluster/peers
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/name-
services/name-mappings -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/ethernet/ports -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/fc/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/fc/logins -access readonly -vserver <vserver-name>
```

```
security login rest-role create -role <role-name> -api
/api/network/ip/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nfs/kerberos/interfaces -access readonly -vserver <vserver-
name>

security login rest-role create -role <role-name> -api
/api/protocols/nvme/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/fcp/services -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/iscsi/services -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/security/accounts -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/security/roles
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/storage/qtrees
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/quota/reports -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/snapshot-policies -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/svm/peers
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/svm/svms
-access readonly -vserver <vserver-name>
```

Inoltre, per le versioni ONTAP 9.16.0 e successive, eseguire il seguente comando:

```
security login rest-role create -role <role-name> -api
/api/storage/storage-units -access all -vserver <vserver-name>
```

Per creare un nuovo utente basato su API utilizzando i ruoli basati su API creati sopra, eseguire il seguente comando:

```
security login create -user-or-group-name <user-name> -application http
-authentication-method password -role <role-name> -vserver <cluster-or-
vserver-name>
```

Esempio:

```
security login create -user-or-group-name testvpsraall -application http
-authentication-method password -role
OTV_10_VP_SRA_Discovery_Create_Modify_Destroy -vserver C1_sti160-cluster_
```

Per sbloccare l'account e abilitare l'accesso all'interfaccia di gestione, eseguire il seguente comando:

```
security login unlock -user <user-name> -vserver <cluster-or-vserver-name>
```

Esempio:

```
security login unlock -username testvpsraall -vserver C1_sti160-cluster
```

Aggiorna gli ONTAP tools for VMware vSphere 10.1 a 10.3

Per gli ONTAP tools for VMware vSphere 10.1 con un utente con ambito cluster creato tramite il file JSON, utilizzare i seguenti comandi ONTAP CLI con privilegi di amministratore utente per eseguire l'aggiornamento alla versione 10.3.

Per le capacità del prodotto:

- VSC
- Fornitore VSC e VASA
- VSC e SRA
- VSC, fornitore VASA e SRA.

Privilegi del cluster:

creazione ruolo di accesso di sicurezza -role <nome-ruolo-esistente> -cmddirname "mostra spazio dei nomi nvme vserver" -access all

creazione ruolo di accesso di sicurezza -role <nome-ruolo-esistente> -cmddirname "mostra sottosistema vserver nvme" -access all

creazione ruolo di accesso di sicurezza -role <nome-ruolo-esistente> -cmddirname "host sottosistema nvme vserver mostra" -access all

creazione ruolo di accesso di sicurezza -role <nome-ruolo-esistente> -cmddirname "mostra mappa sottosistema nvme vserver" -access all

creazione ruolo di accesso di sicurezza -role <nome-ruolo-esistente> -cmddirname "vserver nvme show-

interface" -access read

creazione ruolo di accesso di sicurezza -role <nome-ruolo-esistente> -cmddirname "aggiunta host sottosistema nvme vserver" -access all

creazione ruolo di accesso di sicurezza -role <nome-ruolo-esistente> -cmddirname "aggiunta mappa sottosistema nvme vserver" -access all

creazione ruolo di accesso di sicurezza -role <nome-ruolo-esistente> -cmddirname "eliminazione spazio dei nomi nvme vserver" -access all

creazione ruolo di accesso di sicurezza -role <nome-ruolo-esistente> -cmddirname "eliminazione sottosistema nvme vserver" -access all

creazione ruolo di accesso di sicurezza -role <nome-ruolo-esistente> -cmddirname "rimozione host sottosistema nvme vserver" -access all

creazione ruolo di accesso di sicurezza -role <nome-ruolo-esistente> -cmddirname "rimozione mappa sottosistema nvme vserver" -access all

Per gli ONTAP tools for VMware vSphere 10.1 con un utente con ambito SVM creato tramite il file json, utilizzare i comandi ONTAP CLI con privilegi di utente amministratore per eseguire l'aggiornamento alla versione 10.3.

Privilegi SVM:

creazione ruolo di accesso di sicurezza -role <nome-ruolo-esistente> -cmddirname "mostra spazio dei nomi nvme vserver" -access all -vserver <nome-vserver>

creazione ruolo di accesso di sicurezza -role <nome-ruolo-esistente> -cmddirname "mostra sottosistema nvme vserver" -access all -vserver <nome-vserver>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host show" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map show" -access all -vserver <vserver-name>

security login ruolo create -role <nome-ruolo-esistente> -cmddirname "vserver nvme show-interface" -access read -vserver <nome-vserver>

creazione ruolo di accesso di sicurezza -role <nome-ruolo-esistente> -cmddirname "aggiunta host sottosistema nvme vserver" -access all -vserver <nome-vserver>

creazione ruolo di accesso di sicurezza -role <nome-ruolo-esistente> -cmddirname "aggiunta mappa sottosistema nvme vserver" -access all -vserver <nome-vserver>

creazione ruolo di accesso di sicurezza -role <nome-ruolo-esistente> -cmddirname "eliminazione spazio nomi nvme vserver" -access all -vserver <nome-vserver>

creazione ruolo di accesso di sicurezza -role <nome-ruolo-esistente> -cmddirname "eliminazione sottosistema nvme vserver" -access all -vserver <nome-vserver>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host remove" -access all -vserver <vserver-name>

creazione ruolo di accesso di sicurezza -role <nome-ruolo-esistente> -cmddirname "rimozione mappa sottosistema nvme vserver" -access all -vserver <nome-vserver>

Aggiungendo il comando *vserver nvme namespace show* e *vserver nvme subsystem show* al ruolo esistente vengono aggiunti i seguenti comandi.

```
vserver nvme namespace create

vserver nvme namespace modify

vserver nvme subsystem create

vserver nvme subsystem modify
```

Aggiorna gli ONTAP tools for VMware vSphere 10.3 a 10.4

A partire da ONTAP 9.16.1, aggiornare gli ONTAP tools for VMware vSphere 10.3 alla versione 10.4.

Per gli ONTAP tools for VMware vSphere 10.3 con un utente con ambito cluster creato utilizzando il file JSON e ONTAP versione 9.16.1 o successiva, utilizzare il comando ONTAP CLI con privilegi di utente amministratore per eseguire l'aggiornamento alla versione 10.4.

Per le capacità del prodotto:

- VSC
- Fornitore VSC e VASA
- VSC e SRA
- VSC, fornitore VASA e SRA.

Privilegi del cluster:

```
security login role create -role <existing-role-name> -cmddirname "storage
availability-zone show" -access all
```

Aggiungi un backend di archiviazione

L'aggiunta di un backend di archiviazione consente di integrare un cluster ONTAP .

Informazioni su questo compito

In caso di configurazioni multi-tenancy in cui vCenter funge da tenant con una SVM associata, utilizzare ONTAP Tools Manager per aggiungere il cluster. Associare il backend di archiviazione al vCenter Server per mapparlo globalmente all'istanza di vCenter Server integrata. Il tenant vCenter deve integrare le Storage Virtual Machine (SVM) desiderate. Ciò consente a un utente SVM di effettuare il provisioning di datastore vVols . È possibile aggiungere storage in vCenter utilizzando SVM.

Aggiungere i backend di archiviazione locale con credenziali cluster o SVM utilizzando l'interfaccia utente degli strumenti ONTAP . Questi backend di archiviazione sono limitati a un singolo vCenter. Quando si utilizzano le

credenziali del cluster in locale, le SVM associate vengono automaticamente mappate al vCenter per gestire vVols o VMFS. Per la gestione VMFS, incluso SRA, gli strumenti ONTAP supportano le credenziali SVM senza bisogno di un cluster globale.

Utilizzo di ONTAP Tools Manager

> In una configurazione multi-tenant, è possibile aggiungere un cluster backend di archiviazione a livello globale e SVM a livello locale per utilizzare le credenziali utente SVM.

Passi

1. Avviare ONTAP Tools Manager da un browser web: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con le credenziali di amministratore ONTAP tools for VMware vSphere fornite durante la distribuzione.
3. Seleziona **Backend di archiviazione** dalla barra laterale.
4. Aggiungere il backend di archiviazione e fornire l'indirizzo IP del server o il nome di dominio completo (FQDN), il nome utente e la password.

   > Sono supportati i LIF di gestione degli indirizzi IPv4 e IPv6.

Utilizzo dell'interfaccia utente del client vSphere

> Quando si configura un backend di storage tramite l'interfaccia utente del client vSphere, è importante notare che i datastore vVols non supportano l'aggiunta diretta di un utente SVM.

1. Accedi al client vSphere.
2. Nella pagina dei collegamenti, seleziona *Strumenti NetApp ONTAP * nella sezione plug-in.
3. Seleziona **Backend di archiviazione** dalla barra laterale.
4. Aggiungere il backend di archiviazione e fornire l'indirizzo IP del server, il nome utente, la password e i dettagli della porta.

   > Per aggiungere direttamente un utente SVM, è possibile aggiungere credenziali basate su cluster e LIF di gestione degli indirizzi IPv4 e IPv6 oppure fornire credenziali basate su SVM con un LIF di gestione SVM.

Cosa succederà adesso?

L'elenco verrà aggiornato e potrai vedere il backend di archiviazione appena aggiunto.

Associare un backend di archiviazione a un'istanza di vCenter Server

Associare un backend di archiviazione al vCenter Server per creare una mappatura tra il backend di archiviazione e l'istanza di vCenter Server integrata a livello globale.

Passi

1. Avviare ONTAP Tools Manager da un browser web: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con le credenziali di amministratore ONTAP tools for VMware vSphere fornite durante la distribuzione.
3. Selezionare vCenter dalla barra laterale.
4. Selezionare le ellissi verticali in corrispondenza dell'istanza di vCenter Server che si desidera associare ai backend di archiviazione.
5. Selezionare il backend di archiviazione dal menu a discesa per associare l'istanza di vCenter Server al backend di archiviazione richiesto.

Configurare l'accesso alla rete

Se non hai configurato l'accesso alla rete, tutti gli indirizzi IP rilevati dall'host ESXi vengono aggiunti per impostazione predefinita al criterio di esportazione. È possibile configurarlo in modo da aggiungere alcuni indirizzi IP specifici alla policy di esportazione ed escludere il resto. Tuttavia, quando si esegue un'operazione di montaggio sugli host ESXi esclusi, l'operazione fallisce.

Passi

1. Accedi al client vSphere.
2. Selezionare *Strumenti NetApp ONTAP * nella pagina dei collegamenti nella sezione plug-in.
3. Nel riquadro sinistro degli strumenti ONTAP , vai su **Impostazioni** > **Gestisci accesso alla rete** > **Modifica**.

   Per aggiungere più indirizzi IP, separare l'elenco con virgole, intervallo, Classless Inter-Domain Routing (CIDR) o una combinazione di tutti e tre.

4. Seleziona **Salva**.

Creare un archivio dati

Quando si crea un datastore a livello di cluster host, il datastore viene creato e montato su tutti gli host della destinazione e l'azione è abilitata solo se l'utente corrente ha il privilegio di esecuzione.

*Interoperabilità tra datastore nativi con vCenter Server e datastore gestiti dagli strumenti ONTAP *

Gli ONTAP tools for VMware vSphere 10 creano igroup annidati per i datastore, con igroup padre specifici per i datastore e igroup figlio mappati agli host. È possibile creare igroup piatti dal gestore di sistema ONTAP e utilizzarli per creare datastore VMFS senza ricorrere agli strumenti ONTAP . Fare riferimento a "Gestire gli iniziatori SAN e gli igroup" per maggiori informazioni.

Quando l'archiviazione viene integrata negli strumenti ONTAP e viene eseguita la scoperta del datastore, gli igroup piatti e i datastore VMFS diventano gestiti dagli strumenti ONTAP e vengono convertiti in igroup annidati. Non è possibile utilizzare i precedenti igroup piatti per creare nuovi datastore; è necessario utilizzare l'interfaccia utente degli strumenti ONTAP o l'API REST per riutilizzare gli igroup annidati.

Creare un datastore vVols

A partire dagli ONTAP tools for VMware vSphere 10.3, è possibile creare un datastore vVols su sistemi ASA r2 con efficienza di spazio come thin.vVol. Il provider VASA crea un contenitore e gli endpoint del protocollo desiderati durante la creazione del datastore vVol. Questo contenitore non avrà alcun volume di supporto.

Prima di iniziare

- Assicurarsi che gli aggregati radice non siano mappati su SVM.
- Assicurarsi che il provider VASA sia registrato con il vCenter selezionato.
- Nel sistema di archiviazione ASA r2, SVM deve essere mappato per aggregare l'utente SVM.

Passi

1. Accedi al client vSphere.
2. Fare clic con il pulsante destro del mouse su un sistema host, un cluster host o un data center e selezionare **Strumenti NetApp ONTAP * > *Crea datastore**.
3. Selezionare vVols **Tipo di datastore**.
4. Immettere le informazioni **Nome del datastore** e **Protocollo**.

   Il sistema ASA r2 supporta i protocolli iSCSI e FC per vVols.

5. Selezionare la VM di archiviazione in cui si desidera creare il datastore.
6. Nelle opzioni avanzate:
   - Se selezioni **Criterio di esportazione personalizzato**, assicurati di eseguire l'individuazione in vCenter per tutti gli oggetti. Si consiglia di non utilizzare questa opzione.
   - È possibile selezionare il nome **Gruppo iniziatori personalizzato** per i protocolli iSCSI e FC.

   Nel sistema di archiviazione ASA r2 di tipo SVM, le unità di archiviazione (LUN/namespace) non vengono create perché l'archivio dati è solo un contenitore logico.

7. Nel riquadro **Attributi di archiviazione** è possibile creare nuovi volumi o utilizzare quelli esistenti. Tuttavia, non è possibile combinare questi due tipi di volumi per creare un datastore vVols .

   Quando si crea un nuovo volume, è possibile abilitare QoS sul datastore. Per impostazione predefinita, viene creato un volume per ogni richiesta di creazione LUN. Questo passaggio non è applicabile ai datastore vVols che utilizzano i sistemi di archiviazione ASA r2.

8. Rivedi la tua selezione nel riquadro **Riepilogo** e seleziona **Fine**.

Creare un datastore NFS

Un datastore VMware Network File System (NFS) utilizza il protocollo NFS per connettere gli host ESXi a un dispositivo di archiviazione condiviso tramite una rete. Gli archivi dati NFS sono comunemente utilizzati negli ambienti VMware vSphere e offrono numerosi vantaggi, tra cui semplicità e flessibilità.

Passi

1. Accedi al client vSphere.
2. Fare clic con il pulsante destro del mouse su un sistema host, un cluster host o un data center e

selezionare **Strumenti NetApp ONTAP * > *Crea datastore**.

3. Selezionare NFS nel campo **Tipo di datastore**.
4. Immettere il nome del datastore, le dimensioni e le informazioni sul protocollo nel riquadro **Nome e protocollo**. Selezionare **Cluster Datastore** e **Autenticazione Kerberos** nelle opzioni avanzate.

> L'autenticazione Kerberos è disponibile solo quando è selezionato il protocollo NFS 4.1.

5. Selezionare **Piattaforma** e **VM di archiviazione** nel riquadro **Archiviazione**.
6. Se si seleziona **Criterio di esportazione personalizzato** nelle opzioni avanzate, eseguire l'individuazione in vCenter per tutti gli oggetti. Si consiglia di non utilizzare questa opzione.

> Non è possibile creare un datastore NFS utilizzando il criterio del volume predefinito/root dell'SVM.

   - Nelle opzioni avanzate, il pulsante di attivazione/disattivazione **Asimmetrico** è visibile solo se nel menu a discesa della piattaforma è selezionata l'opzione prestazioni o capacità.
   - Quando si seleziona l'opzione **Qualsiasi** nel menu a discesa della piattaforma, è possibile visualizzare le SVM che fanno parte di vCenter indipendentemente dalla piattaforma o dal flag asimmetrico.
7. Selezionare l'aggregato per la creazione del volume nel riquadro **Attributi di archiviazione**. Nelle opzioni avanzate, seleziona **Spazio riservato** e **Abilita QoS** come richiesto.
8. Rivedere le selezioni nel riquadro **Riepilogo** e selezionare **Fine**.

Il datastore NFS viene creato e montato su tutti gli host.

Creare un datastore VMFS

Virtual Machine File System (VMFS) è un file system in cluster che archivia i file delle macchine virtuali negli ambienti VMware vSphere. VMFS consente a più host ESXi di accedere contemporaneamente agli stessi file della macchina virtuale, abilitando funzionalità come vMotion e High Availability.

Su un cluster protetto:

- È possibile creare solo datastore VMFS. Quando si aggiunge un datastore VMFS a un cluster protetto, il datastore diventa automaticamente protetto.
- Non è possibile creare un datastore su un data center con uno o più cluster host protetti.
- Non è possibile creare un datastore sull'host ESXi se il cluster host padre è protetto con una relazione di tipo "Policy duplex di failover automatico" (configurazione uniforme/non uniforme).
- È possibile creare un datastore VMFS solo su un host ESXi protetto da una relazione asincrona. Non è possibile creare e montare un datastore su un host ESXi che fa parte di un cluster host protetto dalla policy "Automated Failover Duplex".

Prima di iniziare

- Abilitare servizi e LIF per ciascun protocollo sul lato di archiviazione ONTAP .
- Mappare SVM per aggregare l'utente SVM nel sistema di archiviazione ASA r2.
- Configurare l'host ESXi se si utilizza il protocollo NVMe/TCP:
  a. Rivedere il "Guida alla compatibilità VMware"

> VMware vSphere 7.0 U3 e le versioni successive supportano il protocollo NVMe/TCP. Tuttavia, si consiglia VMware vSphere 8.0 e versioni successive.

b. Verificare se il fornitore della scheda di interfaccia di rete (NIC) supporta la NIC ESXi con il protocollo NVMe/TCP.

c. Configurare la scheda di rete ESXi per NVMe/TCP in base alle specifiche del fornitore della scheda di rete.

d. Quando si utilizza la versione VMware vSphere 7, seguire le istruzioni sul sito VMware "Configurare il binding VMkernel per l'adattatore NVMe su TCP" per configurare il binding della porta NVMe/TCP. Quando si utilizza la versione VMware vSphere 8, seguire "Configurazione di NVMe su TCP su ESXi" , per configurare il binding della porta NVMe/TCP.

e. Per la versione VMware vSphere 7, seguire le istruzioni a pagina "Abilita gli adattatori software NVMe su RDMA o NVMe su TCP" per configurare gli adattatori software NVMe/TCP. Per la versione VMware vSphere 8, seguire "Aggiungi adattatori software NVMe su RDMA o NVMe su TCP" per configurare gli adattatori software NVMe/TCP.

f. Correre"Scopri i sistemi di archiviazione e gli host" azione sull'host ESXi. Per ulteriori informazioni, consulta "Come configurare NVMe/TCP con vSphere 8.0 Update 1 e ONTAP 9.13.1 per i datastore VMFS" .

- Se si utilizza il protocollo NVME/FC, procedere come segue per configurare l'host ESXi:

  a. Se non è già abilitato, abilita NVMe over Fabrics (NVMe-oF) sui tuoi host ESXi.

  b. Completa suddivisione in zone SCSI.

  c. Assicurarsi che gli host ESXi e il sistema ONTAP siano connessi a livello fisico e logico.

Per configurare un ONTAP SVM per il protocollo FC, fare riferimento a "Configurare un SVM per FC" .

Per ulteriori informazioni sull'utilizzo del protocollo NVMe/FC con VMware vSphere 8.0, fare riferimento a "Configurazione host NVMe-oF per ESXi 8.x con ONTAP" .

Per ulteriori informazioni sull'utilizzo di NVMe/FC con VMware vSphere 7.0, fare riferimento a "Guida alla configurazione dell'host ONTAP NVMe/FC" E "TR-4684" .

Passi

1. Accedi al client vSphere.
2. Fare clic con il pulsante destro del mouse su un sistema host, un cluster host o un data center e selezionare **Strumenti NetApp ONTAP * > *Crea datastore**.
3. Selezionare il tipo di datastore VMFS.
4. Immettere il nome del datastore, le dimensioni e le informazioni sul protocollo nel riquadro **Nome e protocollo**. Se si sceglie di aggiungere il nuovo datastore a un cluster di datastore VMFS esistente, selezionare il selettore del cluster di datastore in Opzioni avanzate.
5. Selezionare la VM di archiviazione nel riquadro **Archiviazione**. Specificare il **Nome del gruppo di iniziatori personalizzato** nella sezione **Opzioni avanzate** come richiesto. È possibile scegliere un igroup esistente per il datastore oppure crearne uno nuovo con un nome personalizzato.

   Quando si seleziona il protocollo NVMe/FC o NVMe/TCP, viene creato un nuovo sottosistema di namespace che viene utilizzato per la mappatura degli spazi dei nomi. Il sottosistema dello spazio dei nomi viene creato utilizzando il nome generato automaticamente che include il nome del datastore. È possibile rinominare il sottosistema dello spazio dei nomi nel campo **nome del sottosistema dello spazio dei nomi personalizzato** nelle opzioni avanzate del riquadro **Archiviazione**.

6. Dal riquadro **attributi di archiviazione**:

   a. Selezionare **Aggregato** dalle opzioni a discesa.

   > Per i sistemi di storage ASA r2, l'opzione **Aggregate** non viene visualizzata perché lo storage ASA r2 è disaggregato. Quando si sceglie un sistema di storage ASA r2 di tipo SVM, la pagina degli attributi di storage mostra le opzioni per abilitare la QoS.

   b. In base al protocollo selezionato, viene creata un'unità di archiviazione (LUN/Namespace) con una riserva di spazio di tipo thin.

   > A partire da ONTAP 9.16.1, i sistemi di storage ASA r2 supportano fino a 12 nodi per cluster.

   c. Selezionare il **livello di servizio Performance** per i sistemi di storage ASA r2 con 12 nodi SVM che costituiscono un cluster eterogeneo. Questa opzione non è disponibile se l'SVM selezionato è un cluster omogeneo o utilizza un utente SVM.

      'Qualsiasi' è il valore predefinito del livello di servizio delle prestazioni (PSL). Questa impostazione crea l'unità di archiviazione utilizzando l'algoritmo di posizionamento bilanciato ONTAP . Tuttavia, è possibile selezionare l'opzione Performance o Extreme, a seconda delle esigenze.

   d. Selezionare le opzioni **Usa volume esistente**, **Abilita QoS** come richiesto e fornire i dettagli.

   > Nel tipo di archiviazione ASA r2, la creazione o la selezione del volume non si applica alla creazione dell'unità di archiviazione (LUN/Namespace). Pertanto, queste opzioni non vengono mostrate.

   > Non è possibile utilizzare il volume esistente per creare un datastore VMFS con protocollo NVMe/FC o NVMe/TCP; è necessario creare un nuovo volume.

7. Esaminare i dettagli del datastore nel riquadro **Riepilogo** e selezionare **Fine**.

   > Se si crea il datastore su un cluster protetto, verrà visualizzato un messaggio di sola lettura: "Il datastore è in fase di montaggio su un cluster protetto".

Risultato

Il datastore VMFS viene creato e montato su tutti gli host.

Proteggere datastore e macchine virtuali

Proteggere utilizzando la protezione del cluster host

Gli ONTAP tools for VMware vSphere gestiscono la protezione dei cluster host. Tutti i datastore appartenenti all'SVM selezionato e montati su uno o più host del cluster sono protetti da un cluster host.

Prima di iniziare

Assicurarsi che siano soddisfatti i seguenti prerequisiti:

- Il cluster host dispone di datastore provenienti da una sola SVM.
- Il datastore montato sul cluster host non deve essere montato su alcun host esterno al cluster.
- Tutti i datastore montati sul cluster host devono essere datastore VMFS con protocollo iSCSI/FC. I datastore vVols, NFS o VMFS con protocolli NVMe/FC e NVMe/TCP non sono supportati.
- I datastore di formazione FlexVol/LUN montati sul cluster host non devono far parte di alcun gruppo di coerenza (CG) esistente.
- I datastore di formazione FlexVol/LUN montati sul cluster host non devono far parte di alcuna relazione SnapMirror esistente.
- Il cluster host dovrebbe avere almeno un datastore.

Passi

1. Accedi al client vSphere.
2. Fare clic con il pulsante destro del mouse su un cluster host e selezionare **Strumenti NetApp ONTAP * > *Proteggi cluster**.
3. Nella finestra di protezione del cluster, i dettagli relativi al tipo di datastore e alla macchina virtuale (VM) di archiviazione di origine vengono compilati automaticamente. Selezionare il collegamento datastore per visualizzare i datastore protetti.
4. Inserisci il **nome del gruppo di coerenza**.
5. Seleziona **Aggiungi relazione**.
6. Nella finestra **Aggiungi relazione SnapMirror *, seleziona la *VM di archiviazione di destinazione** e il tipo di **Criterio**.

   Il tipo di policy può essere asincrono o automatizzato FailOverDuplex.

   Quando si aggiunge la relazione SnapMirror come policy di tipo AutomatedFailOverDuplex, è necessario aggiungere la VM di storage di destinazione come backend di storage allo stesso vCenter in cui sono distribuiti gli ONTAP tools for VMware vSphere .

   Nel tipo di policy AutomatedFailOverDuplex sono presenti configurazioni host uniformi e non uniformi. Quando si seleziona il pulsante di attivazione/disattivazione **configurazione host uniforme**, la configurazione del gruppo di iniziatori host viene replicata implicitamente sul sito di destinazione. Per i dettagli, fare riferimento a"Concetti e termini chiave" .

7. Se si sceglie di avere una configurazione host non uniforme, selezionare l'accesso host (origine/destinazione) per ciascun host all'interno del cluster.
8. Selezionare **Aggiungi**.

9. Nella finestra **Proteggi cluster** non è possibile modificare il cluster protetto durante l'operazione di creazione. È possibile eliminare e aggiungere nuovamente la protezione. Durante l'operazione di modifica della protezione del cluster host, è disponibile l'opzione di modifica. È possibile modificare o eliminare le relazioni utilizzando le opzioni del menu con i puntini di sospensione.
10. Selezionare il pulsante **Proteggi**.

    Viene creata un'attività vCenter con i dettagli dell'ID del processo e il suo avanzamento viene visualizzato nel pannello delle attività recenti. Si tratta di un'attività asincrona: l'interfaccia utente mostra solo lo stato di invio della richiesta e non attende il completamento dell'attività.

11. Per visualizzare i cluster host protetti, accedere a **Strumenti NetApp ONTAP * > *Protezione** > **Relazioni tra cluster host**.

Proteggi utilizzando la protezione SRA

Configurare SRA per proteggere gli archivi dati

Gli ONTAP tools for VMware vSphere offrono la possibilità di abilitare la funzionalità SRA per configurare il disaster recovery.

Prima di iniziare

- Dovresti aver configurato l'istanza di vCenter Server e l'host ESXi.
- Dovresti aver distribuito gli ONTAP tools for VMware vSphere.
- Dovresti aver scaricato l'adattatore SRA `.tar.gz` file dal "Sito di supporto NetApp" .
- I cluster ONTAP di origine e di destinazione devono avere le stesse pianificazioni SnapMirror personalizzate create prima di eseguire i flussi di lavoro SRA.
- "Abilita gli ONTAP tools for VMware vSphere" per abilitare la funzionalità SRA.

Passi

1. Accedi all'interfaccia di gestione dell'appliance VMware Live Site Recovery utilizzando l'URL: `https://:<srm_ip>:5480` e quindi vai a Storage Replication Adapters nell'interfaccia di gestione dell'appliance VMware Live Site Recovery.
2. Selezionare **Nuovo adattatore**.
3. Caricare il programma di installazione *.tar.gz* per il plug-in SRA su VMware Live Site Recovery.
4. Eseguire nuovamente la scansione degli adattatori per verificare che i dettagli siano aggiornati nella pagina Adattatori VMware Live Site Recovery Storage Replication.

Configurare SRA per ambienti SAN e NAS

È necessario configurare i sistemi di archiviazione prima di eseguire Storage Replication Adapter (SRA) per VMware Live Site Recovery.

Configurare SRA per ambienti SAN

Prima di iniziare

Dovresti avere i seguenti programmi installati sul sito protetto e sul sito di ripristino:

- Ripristino del sito live VMware

La documentazione sull'installazione di VMware Live Site Recovery è disponibile sul sito VMware.

"Informazioni su VMware Live Site Recovery"

- SRA

  L'adattatore è installato su VMware Live Site Recovery.

Passi

1. Verificare che gli host ESXi primari siano connessi alle LUN nel sistema di storage primario sul sito protetto.
2. Verificare che i LUN siano in igroup che hanno il `ostype` opzione impostata su *VMware* sul sistema di archiviazione primario.
3. Verificare che gli host ESXi nel sito di ripristino dispongano di una connettività iSCSI appropriata alla macchina virtuale di archiviazione (SVM). Gli host ESXi del sito secondario devono avere accesso allo storage del sito secondario, mentre gli host ESXi del sito primario devono avere accesso allo storage del sito primario.

   È possibile farlo verificando che gli host ESXi abbiano LUN locali connessi all'SVM o `iscsi show initiators` comando sugli SVM. Controllare l'accesso LUN per i LUN mappati nell'host ESXi per verificare la connettività iSCSI.

Configurare SRA per ambienti NAS

Prima di iniziare

Dovresti avere i seguenti programmi installati sul sito protetto e sul sito di ripristino:

- Ripristino del sito live VMware

  La documentazione sull'installazione di VMware Live Site Recovery è disponibile sul sito VMware.

  "Informazioni su VMware Live Site Recovery"

- SRA

  L'adattatore è installato su VMware Live Site Recovery e sul server SRA.

Passi

1. Verificare che gli archivi dati nel sito protetto contengano macchine virtuali registrate con vCenter Server.
2. Verificare che gli host ESXi nel sito protetto abbiano montato i volumi di esportazione NFS dalla macchina virtuale di archiviazione (SVM).
3. Verificare che nel campo **Indirizzi NFS** siano specificati indirizzi validi, come l'indirizzo IP o il nome di dominio completo (FQDN) su cui sono presenti le esportazioni NFS, quando si utilizza la procedura guidata di Array Manager per aggiungere array a VMware Live Site Recovery. Non utilizzare il nome host NFS nel campo **Indirizzi NFS**.
4. Utilizzare il `ping` comando su ciascun host ESXi nel sito di ripristino per verificare che l'host disponga di una porta VMkernel in grado di accedere agli indirizzi IP utilizzati per gestire le esportazioni NFS dall'SVM.

Configurare SRA per ambienti altamente scalabili

Per ottenere prestazioni ottimali in ambienti con scalabilità elevata, è necessario configurare gli intervalli di timeout di archiviazione in base alle impostazioni consigliate per Storage Replication Adapter (SRA).

Impostazioni del provider di archiviazione

È necessario impostare i seguenti valori di timeout su VMware Live Site Recovery per ambienti scalati:

Impostazioni avanzate	Valori di timeout
`StorageProvider.resignatureTimeout`	Aumentare il valore dell'impostazione da 900 secondi a 12000 secondi.
`storageProvider.hostRescanDelaySec`	60
`storageProvider.hostRescanRepeatCnt`	20
`storageProvider.hostRescanTimeoutSec`	Imposta un valore alto (ad esempio: 99999)

Dovresti anche abilitare l' `StorageProvider.autoResignatureMode` opzione.

Fare riferimento a "Modifica le impostazioni del provider di archiviazione" per ulteriori informazioni sulla modifica delle impostazioni del provider di archiviazione.

Impostazioni di archiviazione

Quando si raggiunge un timeout, aumentare i valori di `storage.commandTimeout` E `storage.maxConcurrentCommandCnt` a un valore più alto.

> L'intervallo di timeout specificato è il valore massimo. Non è necessario attendere che venga raggiunto il timeout massimo. La maggior parte dei comandi termina entro l'intervallo di timeout massimo impostato.

Fare riferimento a "Modifica le impostazioni di archiviazione" per modificare le impostazioni del provider SAN.

Configurare SRA sull'appliance VMware Live Site Recovery

Dopo aver distribuito l'appliance VMware Live Site Recovery, configurare Storage Replication Adapter (SRA) per abilitare la gestione del disaster recovery.

La configurazione di SRA sull'appliance VMware Live Site Recovery salva le credenziali ONTAP tools for VMware vSphere all'interno dell'appliance, consentendo la comunicazione tra VMware Live Site Recovery e SRA.

Prima di iniziare

- Scarica il file *.tar.gz* dal "Sito di supporto NetApp" .
- Abilitare i servizi SRA in ONTAP Tools Manager. Per ulteriori informazioni, consulta "Abilita i servizi"

sezione.

- Aggiungere vCenter Server agli strumenti ONTATP per l'appliance VMware vSphere. Per ulteriori informazioni, consulta "Aggiungi server vCenter" sezione.
- Aggiungere backend di storage agli ONTAP tools for VMware vSphere. Per ulteriori informazioni, consulta "Aggiungere backend di archiviazione" sezione.

Passi

1. Nella schermata dell'appliance VMware Live Site Recovery, seleziona **Storage Replication Adapter** > **Nuovo adattatore**.
2. Carica il file *.tar.gz* su VMware Live Site Recovery.
3. Accedere al dispositivo VMware Live Site Recovery utilizzando un account amministratore tramite un client SSH come PuTTY.
4. Passare all'utente root utilizzando il comando: `su root`
5. Esegui il comando `cd /var/log/vmware/srm` per passare alla directory del registro.
6. Nella posizione del registro, immettere il comando per ottenere l'ID docker utilizzato da SRA: `docker ps -l`
7. Per accedere all'ID contenitore, immettere il comando: `docker exec -it -u srm <container id> sh`
8. Configurare VMware Live Site Recovery con gli ONTAP tools for VMware vSphere utilizzando il comando: `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <Application username> --otv-password <Application password> --vcenter-guid <VCENTER_GUID>`
   - Fornire la password tra virgolette singole in modo che lo script Perl tratti i caratteri speciali come parte della password e non come delimitatori.
   - È possibile impostare il nome utente e la password dell'applicazione (VASA Provider/SRA) in ONTAP Tools Manager quando si abilitano questi servizi per la prima volta. Utilizzare queste credenziali per registrare SRA con VMware Live Site Recovery.
   - Per individuare il GUID di vCenter, accedere alla pagina vCenter Server in ONTAP Tools Manager dopo aver aggiunto l'istanza di vCenter. Fare riferimento a"Aggiungi server vCenter" sezione.
9. Eseguire nuovamente la scansione degli adattatori per confermare che i dettagli aggiornati siano visualizzati nella pagina Adattatori VMware Live Site Recovery Storage Replication.

Risultati

Viene visualizzato un messaggio di conferma che indica che le credenziali di archiviazione sono state salvate. SRA può ora comunicare con il server SRA utilizzando l'indirizzo IP, la porta e le credenziali specificati.

Aggiorna le credenziali SRA

Per consentire a VMware Live Site Recovery di comunicare con SRA, è necessario aggiornare le credenziali SRA sul server VMware Live Site Recovery se sono state modificate.

Prima di iniziare

Avresti dovuto eseguire i passaggi menzionati nell'argomento"Configurazione di SRA sull'appliance VMware Live Site Recovery" .

Passi

1. Eseguire i seguenti comandi per eliminare la cartella della macchina VMware Live Site Recovery memorizzata nella cache degli strumenti ONTAP , nome utente e password:
   a. `sudo su <enter root password>`
   b. `docker ps`
   c. `docker exec -it <container_id> sh`
   d. `cd conf/`
   e. `rm -rf *`
2. Eseguire il comando Perl per configurare SRA con le nuove credenziali:
   a. `cd ..`
   b. `perl command.pl -l --otv-ip <OTV_IP>:8443 --otv-username <OTV_ADMIN_USERNAME> --otv -password <OTV_ADMIN_PASSWORD> --vcenter-guid <VCENTER_GUID>`È necessario racchiudere il valore della password tra virgolette singole.

      Viene visualizzato un messaggio di conferma che le credenziali di archiviazione sono state archiviate. SRA può comunicare con il server SRA utilizzando l'indirizzo IP, la porta e le credenziali forniti.

Configurare siti protetti e di ripristino

È necessario creare gruppi di protezione per proteggere un gruppo di macchine virtuali sul sito protetto.

Quando si aggiunge un nuovo datastore, è possibile includerlo nel gruppo di datastore esistente oppure aggiungere un nuovo datastore e creare un nuovo volume o gruppo di coerenza per la protezione. Dopo aver aggiunto un nuovo datastore a un gruppo di coerenza o volume protetto, aggiornare SnapMirror ed eseguire il discovery dello storage sia sul sito protetto che su quello di ripristino. È possibile eseguire il discovery manualmente o in base a una pianificazione per garantire che il nuovo datastore venga rilevato e protetto.

Siti protetti e di recupero in coppia

È necessario associare i siti protetti e di ripristino creati utilizzando vSphere Client per consentire a Storage Replication Adapter (SRA) di rilevare i sistemi di archiviazione.

> Storage Replication Adapter (SRA) supporta il fan-out con una relazione di sincronizzazione di tipo Automated Failover Duplex e una relazione asincrona SnapMirror sul gruppo di coerenza. Tuttavia, il fan-out con due SnapMirror asincroni su un gruppo di coerenza o con due SnapMirror fan-out su un volume non è supportato.

Prima di iniziare

- Dovresti avere VMware Live Site Recovery installato sui siti protetti e di ripristino.
- Dovresti avere SRA installato sui siti protetti e di ripristino.

Passi

1. Fare doppio clic su **Site Recovery** nella home page di vSphere Client e selezionare **Siti**.
2. Selezionare **Oggetti** > **Azioni** > **Associa siti**.
3. Nella finestra di dialogo **Associa server Site Recovery Manager**, immettere l'indirizzo del Platform Services Controller del sito protetto, quindi selezionare **Avanti**.

4. Nella sezione Seleziona vCenter Server, procedi come segue:
    a. Verificare che il vCenter Server del sito protetto venga visualizzato come candidato corrispondente per l'associazione.
    b. Immettere le credenziali amministrative SSO, quindi selezionare **Fine**.
5. Se richiesto, selezionare **Sì** per accettare i certificati di sicurezza.

Risultato

Nella finestra di dialogo Oggetti verranno visualizzati sia i siti protetti che quelli di ripristino.

Configurare i gruppi di protezione

Prima di iniziare

È necessario assicurarsi che sia il sito di origine che quello di destinazione siano configurati per quanto segue:

- Stessa versione di VMware Live Site Recovery installata
- Macchine virtuali
- Siti protetti e di recupero accoppiati
- I datastore di origine e di destinazione devono essere montati sui rispettivi siti

Passi

1. Accedi a vCenter Server e seleziona **Site Recovery** > **Gruppi di protezione**.
2. Nel riquadro **Gruppi di protezione**, selezionare **Nuovo**.
3. Specificare un nome e una descrizione per il gruppo di protezione, la direzione e selezionare **Avanti**.
4. Nel campo **Tipo**, seleziona l'opzione **Tipo…** come gruppi di datastore (replica basata su array) per datastore NFS e VMFS. Il dominio di errore è costituito esclusivamente da SVM con replica abilitata. Vengono visualizzate le SVM che hanno implementato solo il peering e non presentano problemi.
5. Nella scheda Gruppi di replica, seleziona la coppia di array abilitata o i gruppi di replica che contengono la macchina virtuale configurata, quindi seleziona **Avanti**.

   Tutte le macchine virtuali nel gruppo di replica vengono aggiunte al gruppo di protezione.

6. È possibile selezionare il piano di ripristino esistente oppure crearne uno nuovo selezionando **Aggiungi al nuovo piano di ripristino.**
7. Nella scheda Pronto per il completamento, rivedi i dettagli del gruppo di protezione creato, quindi seleziona **Fine**.

Configurare le risorse del sito protetto e di ripristino

Configurare le mappature di rete

È necessario configurare i mapping delle risorse, come reti VM, host ESXi e cartelle su entrambi i siti, per abilitare il mapping di ciascuna risorsa dal sito protetto alla risorsa appropriata nel sito di ripristino.

Dovresti completare le seguenti configurazioni delle risorse:

- Mappature di rete

- Mappature delle cartelle
- Mappature delle risorse
- Datastore segnaposto

Prima di iniziare

Dovresti aver collegato i siti protetti e di ripristino.

Passi

1. Accedi a vCenter Server e seleziona **Site Recovery** > **Siti**.
2. Seleziona il tuo sito protetto e seleziona **Gestisci**.
3. Selezionare **Mappature di rete** > **Nuovo** nella scheda Gestisci per creare una nuova mappatura di rete.
4. Nella procedura guidata Crea mappatura di rete, procedere come segue:
   a. Selezionare **Prepara automaticamente i mapping per le reti con nomi corrispondenti** e selezionare **Avanti**.
   b. Selezionare gli oggetti del data center richiesti per i siti protetti e di ripristino e selezionare **Aggiungi mapping**.
   c. Selezionare **Avanti** dopo aver creato correttamente le mappature.
   d. Selezionare l'oggetto utilizzato in precedenza per creare la mappatura inversa, quindi selezionare **Fine**.

Risultato

La pagina Mappature di rete visualizza le risorse del sito protetto e le risorse del sito di ripristino. Puoi seguire gli stessi passaggi per altre reti nel tuo ambiente.

Configurare le mappature delle cartelle

Dovresti mappare le tue cartelle sul sito protetto e sul sito di ripristino per consentire la comunicazione tra di loro.

Prima di iniziare

Dovresti aver collegato i siti protetti e di ripristino.

Passi

1. Accedi a vCenter Server e seleziona **Site Recovery** > **Siti**.
2. Seleziona il tuo sito protetto e seleziona **Gestisci**.
3. Selezionare **Mappature cartelle** > icona **Cartella** nella scheda Gestisci per creare una nuova mappatura cartelle.
4. Nella procedura guidata Crea mapping cartella, procedere come segue:
   a. Selezionare **Prepara automaticamente i mapping per le cartelle con nomi corrispondenti** e selezionare **Avanti**.
   b. Selezionare gli oggetti del data center richiesti per i siti protetti e di ripristino e selezionare **Aggiungi mapping**.
   c. Selezionare **Avanti** dopo aver creato correttamente le mappature.
   d. Selezionare l'oggetto utilizzato in precedenza per creare la mappatura inversa, quindi selezionare **Fine**.

Risultato

La pagina Mapping cartelle visualizza le risorse del sito protetto e le risorse del sito di ripristino. Puoi seguire gli stessi passaggi per altre reti nel tuo ambiente.

Configurare le mappature delle risorse

È necessario mappare le risorse sul sito protetto e sul sito di ripristino in modo che le macchine virtuali siano configurate per il failover in un gruppo di host o nell'altro.

Prima di iniziare

Dovresti aver collegato i siti protetti e di ripristino.

> In VMware Live Site Recovery, le risorse possono essere pool di risorse, host ESXi o cluster vSphere.

Passi

1. Accedi a vCenter Server e seleziona **Site Recovery** > **Siti**.
2. Seleziona il tuo sito protetto e seleziona **Gestisci**.
3. Selezionare **Mappature risorse** > **Nuovo** nella scheda Gestisci per creare una nuova mappatura delle risorse.
4. Nella procedura guidata Crea mappatura risorse, procedere come segue:
   a. Selezionare **Prepara automaticamente i mapping per le risorse con nomi corrispondenti** e selezionare **Avanti**.
   b. Selezionare gli oggetti del data center richiesti per i siti protetti e di ripristino e selezionare **Aggiungi mapping**.
   c. Selezionare **Avanti** dopo aver creato correttamente le mappature.
   d. Selezionare l'oggetto utilizzato in precedenza per creare la mappatura inversa, quindi selezionare **Fine**.

Risultato

La pagina Mappature risorse visualizza le risorse del sito protetto e le risorse del sito di ripristino. Puoi seguire gli stessi passaggi per altre reti nel tuo ambiente.

Configurare i datastore segnaposto

È necessario configurare un datastore segnaposto per occupare una posizione nell'inventario vCenter nel sito di ripristino per la macchina virtuale (VM) protetta. Il datastore segnaposto non deve essere di grandi dimensioni, poiché le VM segnaposto sono piccole e utilizzano solo poche centinaia di kilobyte o meno.

Prima di iniziare

- Dovresti aver collegato i siti protetti e di ripristino.
- Dovresti aver configurato le mappature delle risorse.

Passi

1. Accedi a vCenter Server e seleziona **Site Recovery** > **Siti**.
2. Seleziona il tuo sito protetto e seleziona **Gestisci**.

3. Selezionare **Datastore segnaposto** > **Nuovo** nella scheda Gestisci per creare un nuovo datastore segnaposto.
4. Selezionare il datastore appropriato e fare clic su **OK**.

> Gli archivi dati segnaposto possono essere locali o remoti e non devono essere replicati.

5. Ripetere i passaggi da 3 a 5 per configurare un datastore segnaposto per il sito di ripristino.

Configurare SRA utilizzando il gestore array

È possibile configurare Storage Replication Adapter (SRA) utilizzando la procedura guidata Array Manager di VMware Live Site Recovery per abilitare le interazioni tra VMware Live Site Recovery e le macchine virtuali di archiviazione (SVM).

Prima di iniziare

- Dovresti aver associato i siti protetti e i siti di ripristino in VMware Live Site Recovery.
- Prima di configurare il gestore array, è necessario configurare lo storage integrato.
- Dovresti aver configurato e replicato le relazioni SnapMirror tra i siti protetti e i siti di ripristino.
- Avresti dovuto abilitare i LIF di gestione SVM per abilitare il multi-tenancy.

SRA supporta la gestione a livello di cluster e la gestione a livello di SVM. Se si aggiunge storage a livello di cluster, è possibile individuare ed eseguire operazioni su tutte le SVM nel cluster. Se si aggiunge storage a livello di SVM, è possibile gestire solo quello specifico SVM.

Passi

1. In VMware Live Site Recovery, seleziona **Gestione array** > **Aggiungi gestore array**.
2. Immettere le seguenti informazioni per descrivere l'array in VMware Live Site Recovery:

   a. Immettere un nome per identificare il gestore dell'array nel campo **Nome visualizzato**.

   b. Nel campo **Tipo SRA**, selezionare * NetApp Storage Replication Adapter for ONTAP*.

   c. Immettere le informazioni per connettersi al cluster o all'SVM:

      - Se ci si connette a un cluster, è necessario immettere il LIF di gestione del cluster.
      - Se ci si connette direttamente a una SVM, è necessario immettere l'indirizzo IP del LIF di gestione della SVM.

      > Quando si configura il gestore array, è necessario utilizzare la stessa connessione (indirizzo IP) per il sistema di storage utilizzata per integrare il sistema di storage negli ONTAP tools for VMware vSphere. Ad esempio, se la configurazione del gestore array è basata sull'ambito SVM, lo storage negli ONTAP tools for VMware vSphere deve essere aggiunto a livello SVM.

   d. Se ci si connette a un cluster, specificare il nome SVM nel campo **Nome SVM** oppure lasciarlo vuoto per gestire tutte le SVM nel cluster.

   e. Immettere i volumi da rilevare nel campo **Elenco volumi inclusi**.

      È possibile immettere il volume di origine nel sito protetto e il volume di destinazione replicato nel sito di ripristino.

Ad esempio, se si desidera individuare il volume src_vol1 che si trova in una relazione SnapMirror con il volume dst_vol1, è necessario specificare src_vol1 nel campo del sito protetto e dst_vol1 nel campo del sito di ripristino.

f. **(Facoltativo)** Inserire i volumi da escludere dall'individuazione nel campo **Elenco volumi esclusi**.

   È possibile immettere il volume di origine nel sito protetto e il volume di destinazione replicato nel sito di ripristino.

Ad esempio, se si desidera escludere il volume *src_vol1* che si trova in una relazione SnapMirror con il volume *dst_vol1*, è necessario specificare *src_vol1* nel campo del sito protetto e *dst_vol1* nel campo del sito di ripristino.

3. Selezionare **Avanti**.
4. Verificare che l'array sia stato rilevato e visualizzato nella parte inferiore della finestra Aggiungi Array Manager e selezionare **Fine**.

È possibile seguire gli stessi passaggi per il sito di ripristino utilizzando gli indirizzi IP e le credenziali di gestione SVM appropriati. Nella schermata Abilita coppie di array della procedura guidata Aggiungi gestore array, è necessario verificare che sia selezionata la coppia di array corretta e che venga visualizzata come pronta per essere abilitata.

Verificare i sistemi di archiviazione replicati

Dopo aver configurato Storage Replication Adapter (SRA), è necessario verificare che il sito protetto e il sito di ripristino siano stati associati correttamente. Il sistema di archiviazione replicato deve essere rilevabile sia dal sito protetto che dal sito di ripristino.

Prima di iniziare

- Dovresti aver configurato il tuo sistema di archiviazione.
- Dovresti aver associato il sito protetto e il sito di ripristino utilizzando il gestore array VMware Live Site Recovery.
- Prima di eseguire l'operazione di failover di prova e l'operazione di failover per SRA, è necessario abilitare la licenza FlexClone e la licenza SnapMirror .
- Dovresti avere le stesse policy e pianificazioni SnapMirror sui siti di origine e di destinazione.

Passi

1. Accedi al tuo vCenter Server.
2. Passare a **Site Recovery** > **Array Based Replication**.
3. Selezionare la coppia di array richiesta e verificare i dettagli corrispondenti.

   I sistemi di archiviazione devono essere rilevati nel sito protetto e nel sito di ripristino con lo stato "Abilitato".

Protezione a ventaglio

In una protezione fan-out, il gruppo di coerenza è doppiamente protetto con una relazione sincrona sul primo cluster ONTAP di destinazione e con una relazione asincrona sul secondo cluster ONTAP di destinazione. I flussi di lavoro di creazione,

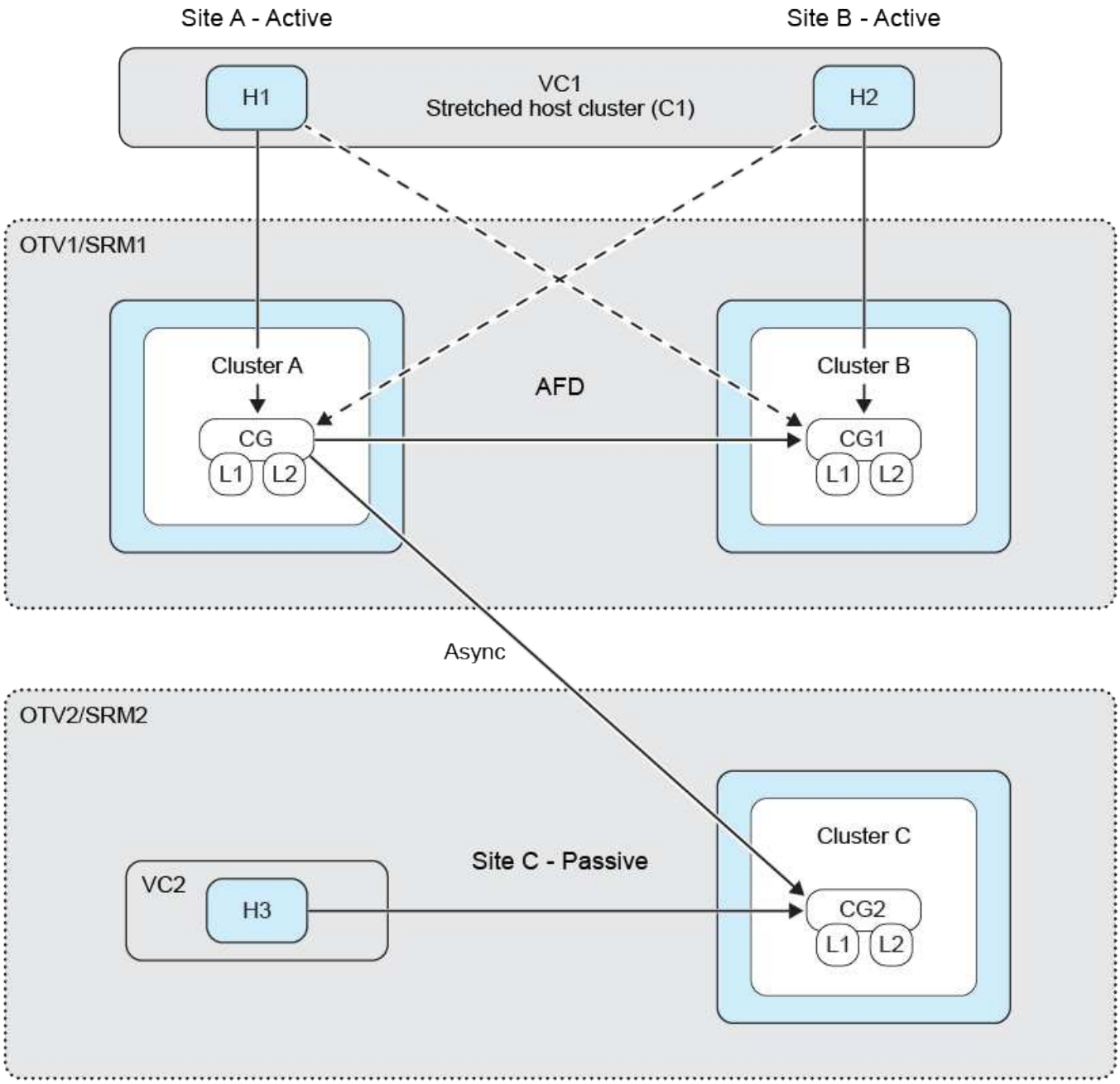
modifica ed eliminazione della protezione ActiveSync SnapMirror mantengono la protezione sincrona. I flussi di lavoro di failover e riprotezione SRM mantengono la protezione asincrona.

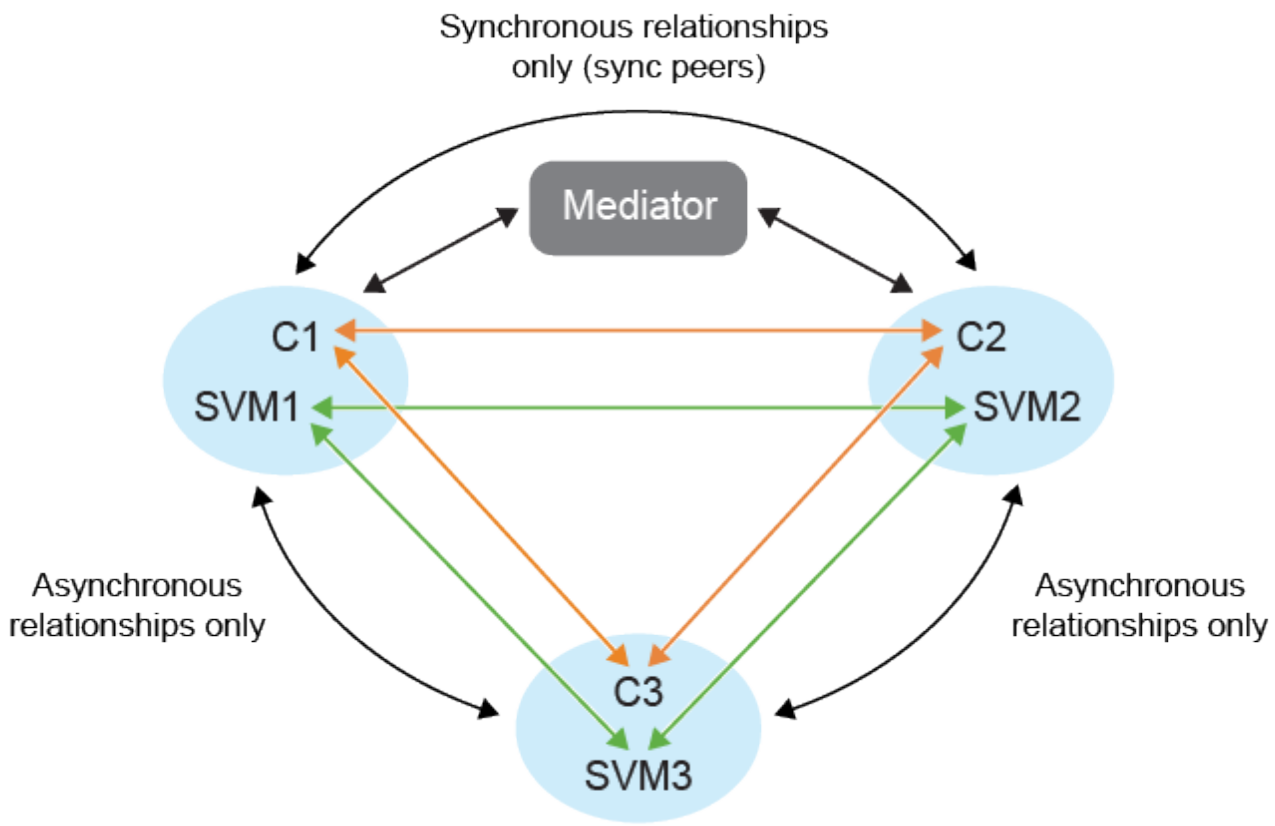
Per stabilire la protezione fan-out è necessario collegare tre cluster di siti e SVM.

Esempio:

Se	Poi
• Il gruppo di coerenza della sorgente si trova sul cluster c1 e SVM svm1 • Il primo gruppo di coerenza di destinazione è sul cluster c2 e SVM svm2 e • Il secondo gruppo di coerenza di destinazione si trova sul cluster c3 e SVM svm3	• Il cluster peering sul cluster ONTAP sorgente sarà (C1, C2) e (C1, C3). • Il cluster peering sul primo cluster ONTAP di destinazione sarà (C2, C1) e (C2, C3) e • Il cluster peering sul secondo cluster ONTAP di destinazione sarà (C3, C1) e (C3, C2). • Il peering SVM sulla SVM sorgente sarà (svm1, svm2) e (svm1, svm3). • Il peering SVM sul primo SVM di destinazione sarà (svm2, svm1) e (svm2, svm3) e • Il peering SVM sulla seconda destinazione svm sarà (svm3, svm1) e (svm3, svm2).

Il diagramma seguente mostra la configurazione della protezione fan out:


Site A - Active
Site B - Active
VC1
Stretched host cluster (C1)
H1
H2
OTV1/SRM1
Cluster A
Cluster B
AFD
CG
CG1
L1
L2
L1
L2
Async
OTV2/SRM2
Cluster C
Site C - Passive
VC2
H3
CG2
L1
L2



Passi

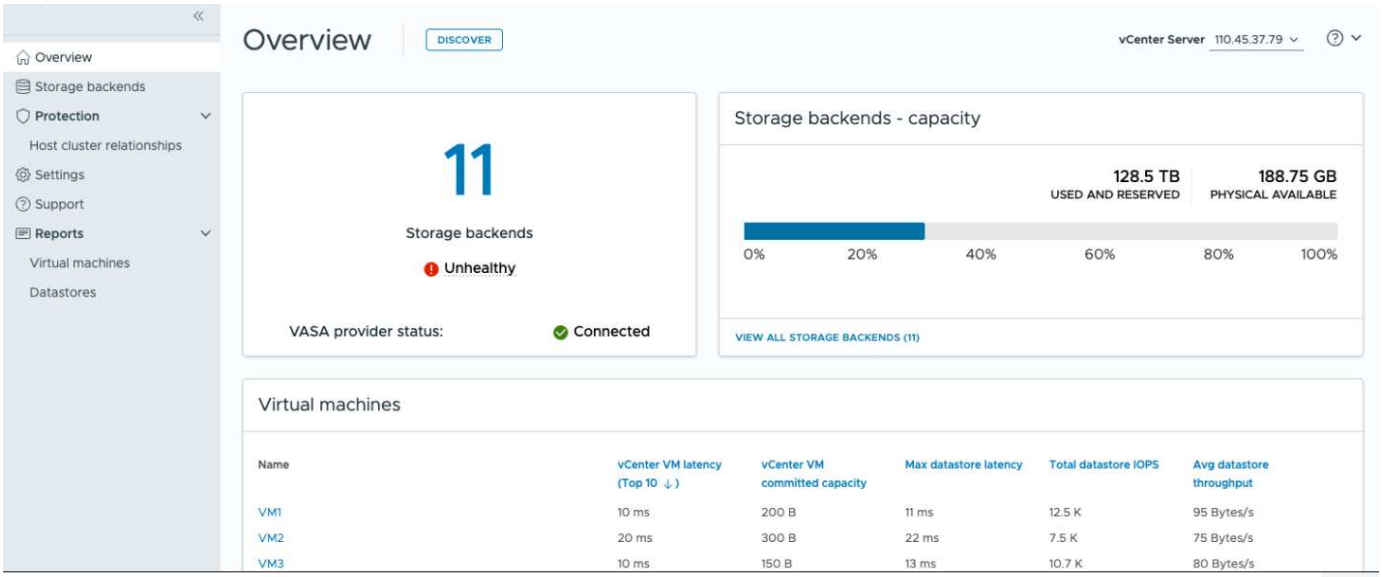
1. Crea un nuovo datastore segnaposto. Fare riferimento "Seleziona un datastore segnaposto"
2. Aggiungi datastore per ospitare la protezione del cluster"Modifica il cluster host protetto" . È necessario aggiungere sia i tipi di policy asincroni che quelli sincroni.

Gestisci gli ONTAP tools for VMware vSphere

Panoramica della dashboard ONTAP tools for VMware vSphere

Quando si seleziona l'icona del plug-in ONTAP tools for VMware vSphere nella sezione dei collegamenti sul client vCenter, l'interfaccia utente passa alla pagina di panoramica. Questa pagina funziona come una dashboard e fornisce un riepilogo degli ONTAP tools for VMware vSphere .

Nel caso di configurazione Enhanced Linked Mode (ELM), viene visualizzato il menu a discesa di selezione del vCenter Server ed è possibile selezionare il vCenter Server desiderato per visualizzare i dati ad esso pertinenti. Questo menu a discesa è disponibile per tutte le altre visualizzazioni di elenco del plugin. La selezione di vCenter Server effettuata in una pagina viene mantenuta in tutte le schede del plugin.



Dalla pagina di panoramica è possibile eseguire l'azione **Discovery**. L'azione di individuazione esegue l'individuazione a livello di vCenter per rilevare eventuali backend di storage, host, datastore e stati/relazioni di protezione aggiunti o aggiornati di recente. È possibile eseguire un'individuazione su richiesta delle entità senza dover attendere l'individuazione pianificata.

> Il pulsante Azione sarà abilitato solo se si dispone del privilegio per eseguire l'azione di individuazione.

Dopo aver inviato la richiesta di individuazione, è possibile monitorare l'avanzamento dell'azione nel pannello delle attività recenti.

Il cruscotto presenta diverse schede che mostrano i diversi elementi del sistema. La tabella seguente mostra le diverse carte e cosa rappresentano.

Carta	Descrizione

Stato	La scheda Stato mostra il numero di backend di archiviazione e lo stato di integrità generale dei backend di archiviazione e del provider VASA. Lo stato dei backend di archiviazione è **Integro** quando lo stato di tutti i backend di archiviazione è normale, mentre è **Non integro** se uno qualsiasi dei backend di archiviazione presenta un problema (stato Sconosciuto/Non raggiungibile/Degradato). Selezionare la descrizione comandi per aprire i dettagli sullo stato dei backend di archiviazione. Per maggiori dettagli puoi selezionare qualsiasi backend di archiviazione. Il collegamento **Altri stati del provider VASA** mostra lo stato corrente del provider VASA registrato nel vCenter Server.
Backend di archiviazione - Capacità	Questa scheda mostra la capacità aggregata utilizzata e disponibile di tutti i backend di storage per l'istanza di vCenter Server selezionata. Nel caso di sistemi di storage ASA r2, i dati sulla capacità non vengono visualizzati perché si tratta di un sistema disaggregato.
Macchine virtuali	Questa scheda mostra le prime 10 VM ordinate in base alla metrica delle prestazioni. È possibile selezionare l'intestazione per ottenere le prime 10 VM per la metrica selezionata, ordinate in ordine crescente o decrescente. Le modifiche di ordinamento e filtraggio apportate alla scheda persistono finché non modifichi o svuoti la cache del browser.
Datastore	Questa scheda mostra i primi 10 datastore ordinati in base a una metrica delle prestazioni. È possibile selezionare l'intestazione per ottenere i primi 10 datastore per la metrica selezionata, ordinati in ordine crescente o decrescente. Le modifiche di ordinamento e filtraggio apportate alla scheda persistono finché non modifichi o svuoti la cache del browser. È presente un menu a discesa Tipo di datastore per selezionare il tipo di datastore: NFS, VMFS o vVols.
Scheda di conformità dell'host ESXi	Questa scheda mostra lo stato di conformità generale di tutte le impostazioni degli host ESXi (per il vCenter selezionato) rispetto alle impostazioni host NetApp consigliate per gruppo/categoria di impostazioni. È possibile selezionare il collegamento **Applica impostazioni consigliate** per applicare le impostazioni consigliate. È possibile selezionare lo stato di conformità degli host per visualizzarne l'elenco.

Interfaccia utente del gestore degli strumenti ONTAP

Gli ONTAP tools for VMware vSphere sono un sistema multi-tenant in grado di gestire più istanze di vCenter Server. ONTAP Tools Manager fornisce un maggiore controllo agli

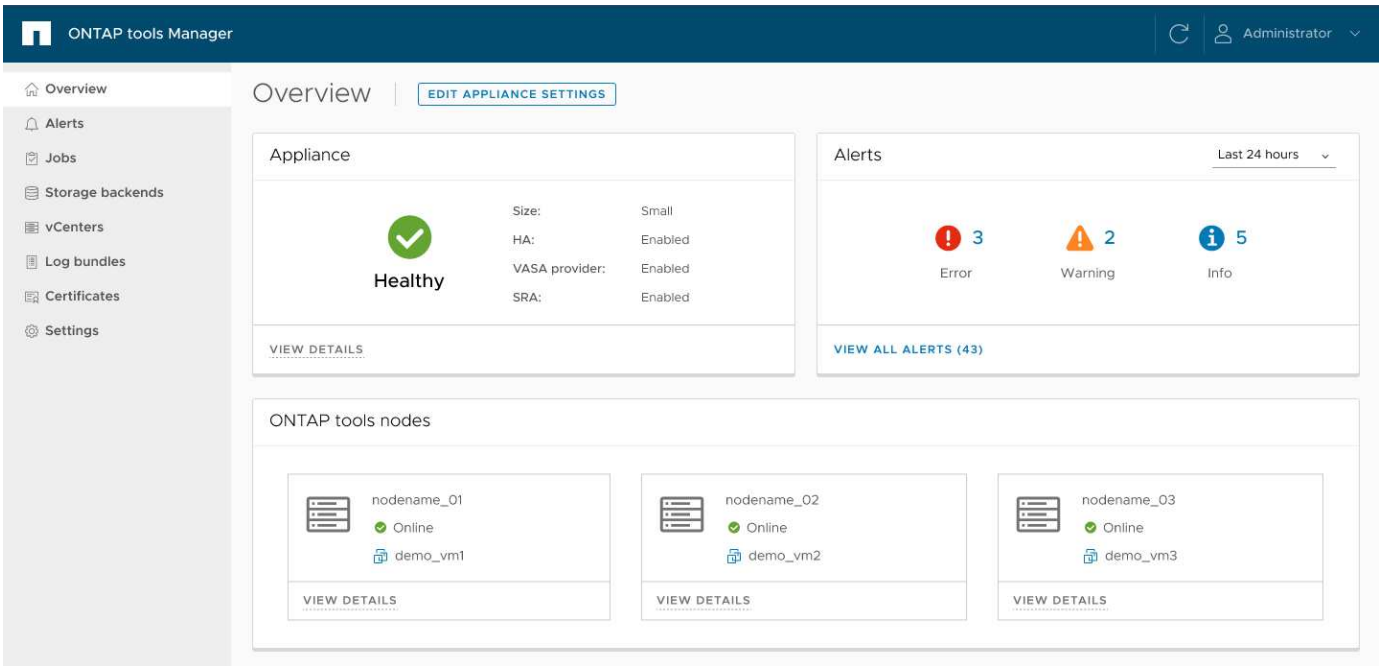
ONTAP tools for VMware vSphere sulle istanze di vCenter Server gestite e sui backend di storage integrati.

ONTAP Tools Manager aiuta a:

- Gestione delle istanze di vCenter Server: aggiungi e gestisci le istanze di vCenter Server negli strumenti ONTAP .
- Gestione del backend di archiviazione: aggiungi e gestisci i cluster di archiviazione ONTAP negli ONTAP tools for VMware vSphere e mappali alle istanze di vCenter Server integrate a livello globale.
- Download del bundle di log: raccogli i file di log per gli ONTAP tools for VMware vSphere.
- Gestione certificati: modifica il certificato autofirmato in un certificato CA personalizzato e rinnova o aggiorna tutti i certificati degli strumenti VASA Provider e ONTAP .
- Gestione password: reimposta la password dell'applicazione OVA dell'utente.

Per accedere a ONTAP Tools Manager, avviare `https://<ONTAPtoolsIP>:8443/virtualization/ui/` dal browser ed effettuare l'accesso con le credenziali di amministratore ONTAP tools for VMware vSphere fornite durante la distribuzione.

La sezione Panoramica di ONTAP Tools Manager aiuta a gestire la configurazione dell'appliance, ad esempio la gestione dei servizi, l'aumento delle dimensioni dei nodi e l'abilitazione dell'alta disponibilità (HA). È inoltre possibile monitorare le informazioni generali degli strumenti ONTAP relativi ai nodi, come stato di integrità, dettagli di rete e avvisi.



Carta	Descrizione
Scheda elettrodomestico	La scheda dell'apparecchio fornisce lo stato generale dell'apparecchio degli strumenti ONTAP . Mostra i dettagli di configurazione dell'appliance e lo stato dei servizi abilitati. Per ulteriori informazioni sull'appliance degli strumenti ONTAP , selezionare il collegamento **Visualizza dettagli**. Quando è in corso un processo di modifica delle impostazioni dell'appliance, il portlet dell'appliance mostra lo stato e i dettagli del processo.
Scheda avvisi	La scheda Avvisi elenca gli avvisi degli strumenti ONTAP per tipo, inclusi gli avvisi a livello di nodo HA. È possibile visualizzare l'elenco degli avvisi selezionando il testo del conteggio (collegamento ipertestuale). Il collegamento indirizza alla pagina di visualizzazione degli avvisi filtrati in base al tipo selezionato.
vCenter	La scheda vCenter mostra lo stato di integrità dei vCenter nel sistema.
Backend di archiviazione	La scheda Backend di archiviazione mostra lo stato di integrità dei backend di archiviazione nel sistema.
Scheda nodi strumenti ONTAP	La scheda dei nodi degli strumenti ONTAP mostra l'elenco dei nodi con il nome del nodo, il nome della VM del nodo, lo stato e tutti i dati relativi alla rete. È possibile selezionare **Visualizza dettagli** per visualizzare i dettagli aggiuntivi relativi al nodo selezionato. [NOTA] In una configurazione non HA, viene mostrato solo un nodo. Nella configurazione HA vengono mostrati tre nodi.

Comprendere igroup e le policy di esportazione negli ONTAP tools for VMware vSphere

I gruppi di iniziatori (igroup) sono tabelle di nomi di porte mondiali (WWPN) dell'host del protocollo FC o nomi di nodi qualificati dell'host iSCSI. È possibile definire igroup e mapparli alle LUN per controllare quali iniziatori hanno accesso alle LUN.

Negli ONTAP tools for VMware vSphere 9.x, gli igroup venivano creati e gestiti in una struttura piatta, in cui ogni datastore in vCenter era associato a un singolo igroup. Questo modello limitava la flessibilità e il riutilizzo degli igroup su più datastore. Gli ONTAP tools for VMware vSphere 10.x introducono igroup annidati, in cui ogni datastore in vCenter è associato a un igroup padre, mentre ogni host è collegato a un igroup figlio sotto tale padre. È possibile definire igroup padre personalizzati con nomi definiti dall'utente per riutilizzarli in più datastore, consentendo una gestione più flessibile e interconnessa degli igroup. La comprensione del flusso di lavoro igroup è essenziale per gestire efficacemente LUN e datastore negli ONTAP tools for VMware vSphere. Flussi di lavoro diversi generano configurazioni igroup diverse, come mostrato negli esempi seguenti:

> I nomi menzionati sono solo a scopo illustrativo e non si riferiscono ai nomi reali dei gruppi i. Gli igroup gestiti dagli strumenti ONTAP utilizzano il prefisso "otv_". È possibile assegnare qualsiasi nome agli igroup personalizzati.

Termine	Descrizione
DS<numero>	Archivio dati
iqn<numero>	Iniziatore IQN
host<numero>	Ospita MoRef
lun<numero>	ID LUN
<DSName>Igroup<numero>	Gruppo padre predefinito (gestito dagli strumenti ONTAP)
<Host-Moref>Igroup<numero>	Gruppo figlio
CustomIgroup<numero>	Gruppo padre personalizzato definito dall'utente
ClassicIgroup<numero>	Igroup utilizzato nelle versioni 9.x degli strumenti ONTAP .

Esempio 1:
Crea un datastore su un singolo host con un iniziatore

Flusso di lavoro: [Crea] DS1 (lun1): host1 (iqn1)

Risultato:

- DS1Igroup:
  - host1Igroup → (iqn1: lun1)

Un igroup padre DS1Igroup viene creato sui sistemi ONTAP per DS1, con un igroup figlio host1Igroup mappato su lun1. I LUN vengono sempre mappati su igroup figlio.

Esempio 2:
Montare il datastore esistente su un host aggiuntivo

Flusso di lavoro: [Montaggio] DS1 (lun1): host2 (iqn2)

Risultato:

- DS1Igroup:
  - host1Igroup → (iqn1: lun1)
  - host2Igroup → (iqn2: lun1)

Viene creato un igroup figlio host2Igroup e aggiunto all'igroup padre esistente DS1Igroup.

Esempio 3:
Smontare un datastore da un host

Flusso di lavoro: [Smonta] DS1 (lun1): host1 (iqn1)

Risultato:

- DS1Igroup:
  - host2Igroup → (iqn2: lun1)

L'host1Igroup viene rimosso dalla gerarchia. Gli igroup figlio non vengono eliminati esplicitamente. L'eliminazione avviene in queste due condizioni:

- Se non viene mappato alcun LUN, il sistema ONTAP elimina l'igroup figlio.
- Un processo di pulizia pianificato rimuove gli igroup figlio sospesi senza mapping LUN. Questi scenari si applicano solo agli igroup gestiti dagli strumenti ONTAP , non a quelli creati personalizzati.

Esempio 4:

Elimina datastore

Flusso di lavoro: [Elimina] DS1 (lun1): host2 (iqn2)

Risultato:

- DS1Igroup:
  - host2Igroup → (iqn2: lun1)

Gli igroup padre e figlio vengono rimossi se un altro datastore non riutilizza l'igroup padre. Gli igroup figlio non vengono mai eliminati esplicitamente

Esempio 5:

Crea più datastore sotto un igroup padre personalizzato

Flusso di lavoro:

- [Crea] DS2 (lun2): host1 (iqn1), host2 (iqn2)
- [Crea] DS3 (lun3): host1 (iqn1), host3 (iqn3)

Risultato:

- CustomIgroup1:
  - host1Igruppo → (iqn1: lun2, lun3)
  - host2Igroup → (iqn2: lun2)
  - host3Igroup → (iqn3: lun3)

CustomIgroup1 viene creato per DS2 e riutilizzato per DS3. Gli igroup figlio vengono creati o aggiornati sotto il genitore condiviso, con ogni igroup figlio mappato ai suoi LUN pertinenti.

Esempio 6:

Eliminare un datastore sotto un igroup padre personalizzato.

Flusso di lavoro: [Elimina] DS2 (lun2): host1 (iqn1), host2 (iqn2)

Risultato:

- CustomIgroup1:
  - host1Igroup → (iqn1: lun3)
  - host3Igroup → (iqn3: lun3)
- Anche se CustomIgroup1 non viene riutilizzato, non viene eliminato.
- Se non viene mappato alcun LUN, il sistema ONTAP elimina host2Igroup.

- host1Igroup non viene eliminato perché è mappato a lun3 di DS3. Gli igroup personalizzati non vengono mai eliminati, indipendentemente dallo stato di riutilizzo.

Esempio 7:
Espandi datastore vVols (Aggiungi volume)

Flusso di lavoro:

Prima dell'espansione:

[Espandi] DS4 (lun4): host4 (iqn4)

- DS4Igroup: host4Igroup → (iqn4: lun4)

Dopo l'espansione:

[Espandi] DS4 (lun4, lun5): host4 (iqn4)

- DS4Igroup: host4Igroup → (iqn4: lun4, lun5)

Viene creato un nuovo LUN e mappato all'igroup figlio esistente host4Igroup.

Esempio 8:
Riduci datastore vVols (rimuovi volume)

Flusso di lavoro:

Prima del restringimento:

[Riduci] DS4 (lun4, lun5): host4 (iqn4)

- DS4Igroup: host4Igroup → (iqn4: lun4, lun5)

Dopo il restringimento:

[Riduci] DS4 (lun4): host4 (iqn4)

- DS4Igroup: host4Igroup → (iqn4: lun4)

Il LUN specificato (lun5) non è mappato dall'igroup figlio. L'igroup rimane attivo finché ha almeno una LUN mappata.

Esempio 9:
Migrazione dagli strumenti ONTAP 9 a 10 (normalizzazione igroup)

Flusso di lavoro

Gli strumenti ONTAP per le versioni VMware vSPhere 9.x non supportano igroup gerarchici. Durante la migrazione alla versione 10.3 o successive, gli igroup devono essere normalizzati nella struttura gerarchica.

Prima della migrazione:

[Migrazione] DS6 (lun6, lun7): host6 (iqn6), host7 (iqn7) → ClassicIgroup1 (iqn6 e iqn7: lun6, lun7)

La logica degli strumenti ONTAP 9.x consente più iniziatori per igroup senza imporre la mappatura host uno a

uno.

Dopo la migrazione:

[Migrazione] DS6 (lun6, lun7): host6 (iqn6), host7 (iqn7) → ClassicIgroup1: otv_ClassicIgroup1 (iqn6 e iqn7: lun6, lun7)

Durante la migrazione:

- Viene creato un nuovo igroup padre (ClassicIgroup1).
- L'igroup originale viene rinominato con il prefisso otv_ e diventa un igroup figlio.

Ciò garantisce la conformità al modello gerarchico.

Argomenti correlati

"Informazioni su igroups"

Politiche di esportazione

Le policy di esportazione controllano l'accesso ai datastore NFS negli ONTAP tools for VMware vSphere. Definiscono quali client possono accedere ai datastore e quali autorizzazioni hanno. Le policy di esportazione vengono create e gestite nei sistemi ONTAP e possono essere associate agli archivi dati NFS per applicare il controllo degli accessi. Ogni policy di esportazione è composta da regole che specificano i client (indirizzi IP o subnet) a cui è consentito l'accesso e le autorizzazioni concesse (sola lettura o lettura-scrittura).

Quando si crea un datastore NFS negli ONTAP tools for VMware vSphere, è possibile selezionare un criterio di esportazione esistente o crearne uno nuovo. La politica di esportazione viene quindi applicata al datastore, garantendo che solo i client autorizzati possano accedervi.

Quando si monta un datastore NFS su un nuovo host ESXi, gli ONTAP tools for VMware vSphere aggiungono l'indirizzo IP dell'host alla policy di esportazione esistente associata al datastore. Ciò consente al nuovo host di accedere al datastore senza creare una nuova policy di esportazione.

Quando si elimina o si smonta un datastore NFS da un host ESXi, gli ONTAP tools for VMware vSphere rimuovono l'indirizzo IP dell'host dalla policy di esportazione. Se nessun altro host utilizza tale criterio di esportazione, verrà eliminato. Quando si elimina un datastore NFS, gli ONTAP tools for VMware vSphere rimuovono la policy di esportazione associata a tale datastore se non viene riutilizzata da altri datastore. Se la policy di esportazione viene riutilizzata, mantiene l'indirizzo IP dell'host e rimane invariata. Quando si eliminano i datastore, la policy di esportazione annulla l'assegnazione dell'indirizzo IP dell'host e assegna una policy di esportazione predefinita, in modo che i sistemi ONTAP possano accedervi se necessario.

L'assegnazione della policy di esportazione varia a seconda che venga riutilizzata su datastore diversi. Quando si riutilizza la policy di esportazione, è possibile aggiungerla con il nuovo indirizzo IP host. Quando si elimina o si smonta un datastore che utilizza una policy di esportazione condivisa, la policy non verrà eliminata. Rimane invariata e l'indirizzo IP host non viene rimosso, poiché è condivisa con gli altri datastore. Il riutilizzo delle policy di esportazione è sconsigliato, poiché può causare problemi di accesso e latenza.

Argomenti correlati

"Creare una politica di esportazione"

Comprendere gli igroup gestiti dagli strumenti ONTAP

Quando si gestiscono sia le VM degli strumenti ONTAP sia i sistemi di archiviazione

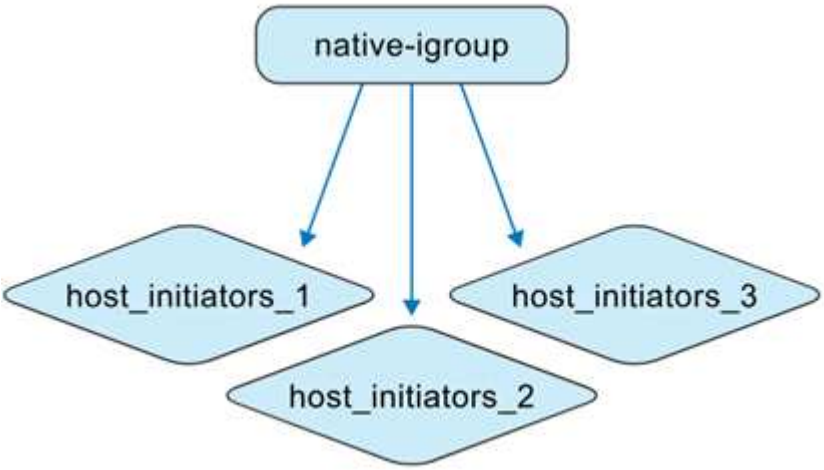
ONTAP , è essenziale comprendere il comportamento di igroup, soprattutto quando si migrano gli archivi dati da ambienti di gestione di strumenti non ONTAP alla gestione di strumenti ONTAP . Questa sezione descrive come gli igroup vengono aggiornati durante questa transizione.

Gli ONTAP tools for VMware vSphere 10.4 semplificano la gestione dei datastore automatizzando la creazione e la manutenzione degli oggetti ONTAP e vCenter negli ambienti data center VMware.

Gli ONTAP tools for VMware vSphere 10.4 interpretano gli igroup in due contesti diversi:

Strumenti non ONTAP gestiti da igroup

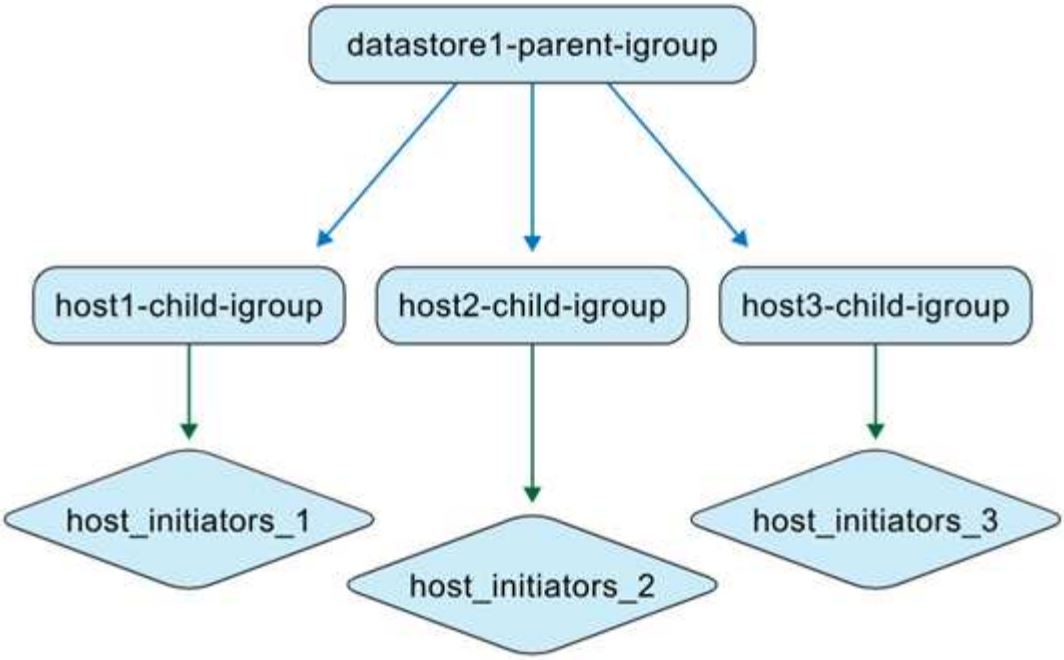
In qualità di amministratore di storage, puoi creare igroup sul sistema ONTAP come strutture semplici o nidificate. L'illustrazione mostra un igroup piatto creato nel sistema ONTAP .

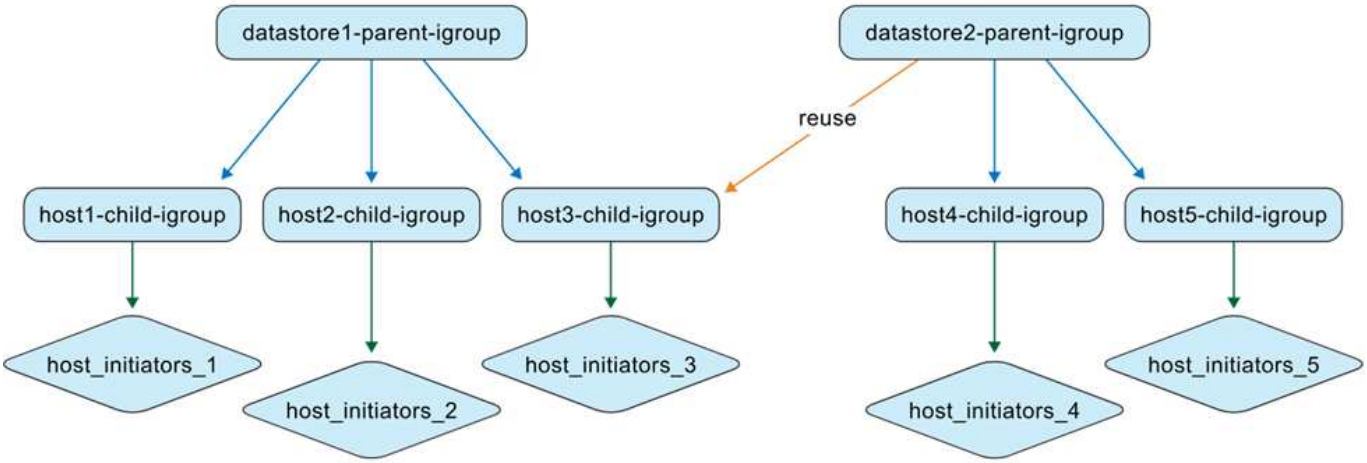


Strumenti ONTAP gestiti igroup

Quando si creano datastore, gli ONTAP tools for VMware vSphere 10.4 creano automaticamente igroup utilizzando una struttura annidata per semplificare la mappatura LUN.

Ad esempio, quando datastore1 viene creato e montato sugli host 1, 2 e 3 e un nuovo datastore (datastore2) viene creato e montato sugli host 3, 4 e 5, gli strumenti ONTAP riutilizzano l'igroup a livello di host per una gestione efficiente.





Ecco alcuni casi di utilizzo ONTAP tools for VMware vSphere .

Quando si crea un datastore con impostazioni igroup predefinite

Quando si crea un datastore e si lascia vuoto il campo igroup (impostazione predefinita), gli strumenti ONTAP generano automaticamente una struttura igroup annidata per quel datastore. L'igroup padre a livello di datastore viene denominato utilizzando il modello: otv_<vcguid>_<host_parent_datacenterMoref>_<datastore_name>. Ogni igroup figlio a livello di host segue il modello: otv_<hostMoref>_<vcguid>. È possibile visualizzare l'associazione tra igroup padre (a livello di datastore) e figlio (a livello di host) nella sezione **Parent Initiator Group** dell'interfaccia di archiviazione ONTAP .

Con l'approccio igroup annidato, le LUN vengono mappate solo agli igroup figlio. L'inventario di vCenter Server visualizza quindi il nuovo datastore.

Quando si crea un datastore con un nome igroup personalizzato

Durante la creazione del datastore negli strumenti ONTAP , è possibile immettere un nome igroup

personalizzato anziché selezionarlo dal menu a discesa. Gli strumenti ONTAP creano quindi un igroup padre a livello di datastore utilizzando il nome specificato. Se lo stesso host viene utilizzato per più datastore, viene riutilizzato l'igroup (figlio) a livello di host esistente. Di conseguenza, il LUN per il nuovo datastore viene mappato su questo igroup figlio esistente, che ora potrebbe essere associato a più igroup padre (uno per ciascun datastore). L'elenco dei datastore dell'interfaccia utente di vCenter Server conferma la creazione corretta del nuovo datastore con il nome igroup personalizzato.

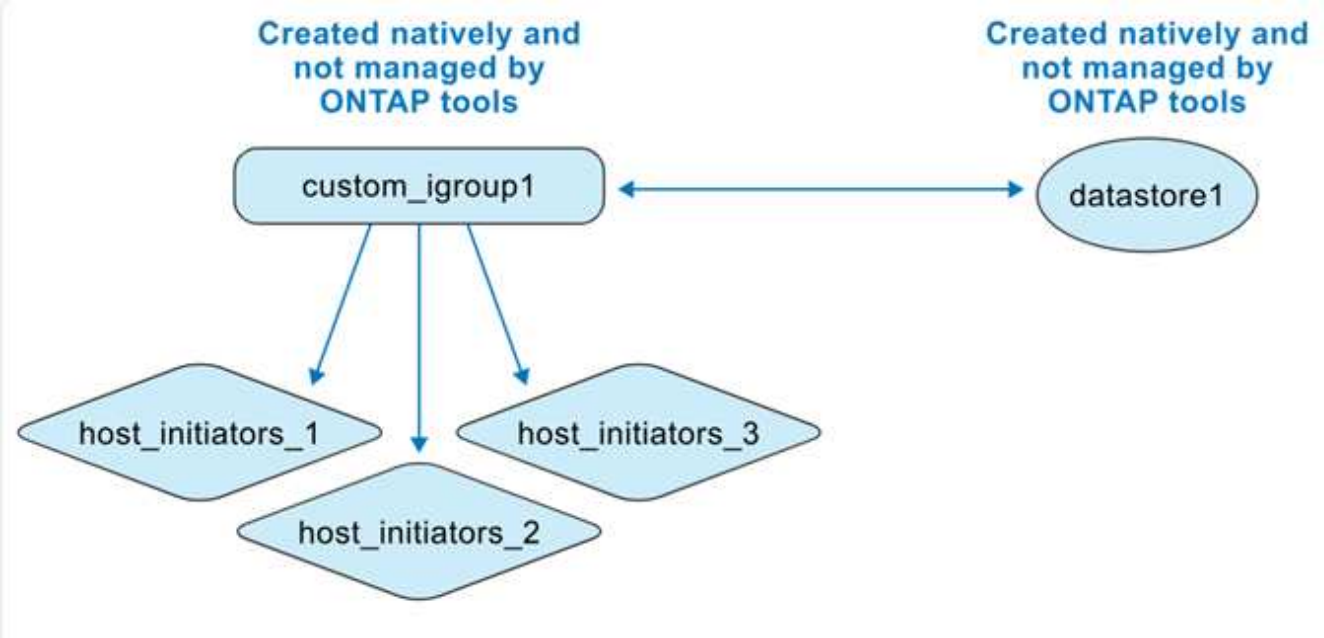
Quando si riutilizza il nome igroup durante la creazione del datastore

Quando si crea un datastore utilizzando l'interfaccia utente degli strumenti ONTAP , è possibile scegliere un igroup padre personalizzato esistente dall'elenco a discesa. Dopo aver riutilizzato l'igroup padre per creare un altro datastore, l'interfaccia utente dei sistemi ONTAP mostra questa associazione. Il nuovo datastore viene visualizzato anche nell'interfaccia utente di vCenter Server.

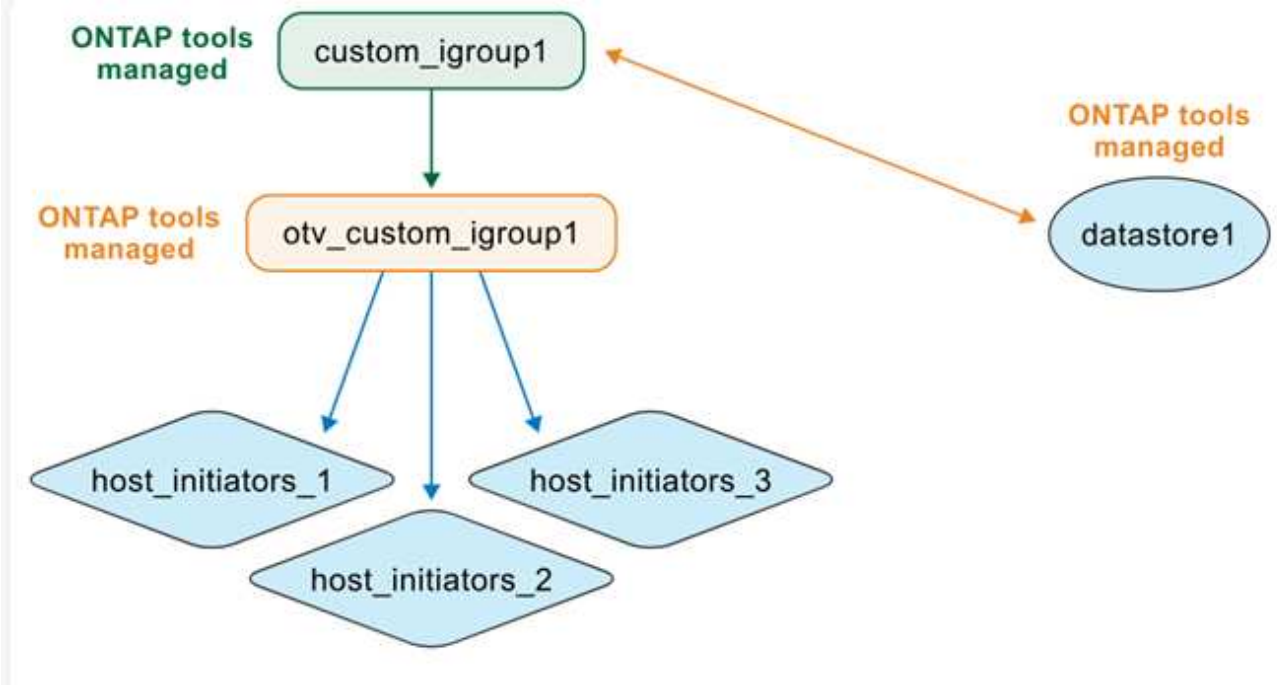
Questa operazione può essere eseguita anche tramite API. Per riutilizzare un igroup esistente durante la creazione del datastore, specificare l'UUID dell'igroup nel payload della richiesta API.

Quando si crea un datastore e un igroup in modo nativo da ONTAP e vCenter

Se si creano igroup e datastore direttamente nei sistemi ONTAP e negli ambienti VMware, gli strumenti ONTAP non gestiscono inizialmente questi oggetti. Ciò crea una struttura igroup piatta.



Per gestire un datastore e un igroup esistenti con gli strumenti ONTAP , è necessario eseguire un'individuazione del datastore. Gli strumenti ONTAP identificano e registrano il datastore e l'igroup e li convertono in una struttura annidata nel proprio database. Viene creato un nuovo igroup padre utilizzando il nome personalizzato, mentre l'igroup esistente viene rinominato con il prefisso "otv_" e diventa l'igroup figlio. Le mappature degli iniziatori rimangono invariate. Durante l'individuazione vengono convertiti solo gli igroup mappati sui datastore. Dopodiché la struttura igroup appare come nell'illustrazione sottostante.



È possibile creare un datastore direttamente in vCenter Server e successivamente inserirlo nella gestione degli strumenti ONTAP . Per prima cosa, creare un igroup piatto nei sistemi ONTAP e mapparvi una LUN. Dopo aver eseguito la scoperta del datastore negli strumenti ONTAP , l'igroup piatto viene convertito in una struttura annidata. Gli strumenti ONTAP gestiscono quindi l'igroup, rinominandolo con il prefisso 'otv_'. Durante tutto il processo, la LUN rimane mappata sullo stesso igroup.

Come gli strumenti ONTAP riutilizzano gli igroup creati in modo nativo

È possibile predisporre un datastore negli strumenti ONTAP utilizzando un igroup creato originariamente nei sistemi ONTAP , dopo averlo gestito tramite gli strumenti ONTAP . Questi igroup vengono visualizzati nell'elenco a discesa del nome del gruppo di iniziatori personalizzato. Il nuovo LUN per il datastore viene quindi mappato al corrispondente igroup figlio normalizzato, ad esempio "otv_NativeIgroup1".

Gli ONTAP tools for VMware vSphere non rilevano né utilizzano gli igroup creati nel sistema ONTAP che non sono gestiti dagli strumenti ONTAP o collegati a un datastore.

Abilita gli ONTAP tools for VMware vSphere

È possibile modificare la password dell'amministratore utilizzando ONTAP Tools Manager per abilitare servizi quali VASA Provider, importazione della configurazione vVols e disaster recovery (SRA) utilizzando ONTAP Tools Manager.

Passi

1. Avviare ONTAP Tools Manager da un browser web: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con le credenziali di amministratore ONTAP tools for VMware vSphere fornite durante la distribuzione.
3. Selezionare **Modifica impostazioni apparecchio** nella sezione panoramica.
4. Nella sezione **Servizi**, puoi abilitare servizi opzionali come VASA Provider, importazione della configurazione vVols e disaster recovery (SRA) in base alle tue esigenze.

Quando si abilitano i servizi per la prima volta, è necessario creare le credenziali VASA Provider e SRA. Vengono utilizzati per registrare o abilitare i servizi VASA Provider e SRA sul vCenter Server. Il nome utente può contenere solo lettere, numeri e caratteri di sottolineatura. La lunghezza della password deve essere compresa tra 8 e 256 caratteri.

> Prima di disabilitare qualsiasi servizio opzionale, assicurarsi che i vCenter Server gestiti dagli strumenti ONTAP non li utilizzino.

L'opzione *Consenti importazione della configurazione vVols * viene visualizzata solo quando è abilitato il servizio VASA Provider. Questa opzione consente la migrazione dei dati vVols dagli strumenti ONTAP 9.xx agli strumenti ONTAP 10.4.

Modifica gli ONTAP tools for VMware vSphere

Utilizzando ONTAP Tools Manager è possibile ampliare la configurazione ONTAP tools for VMware vSphere per aumentare il numero di nodi nella distribuzione o modificare la configurazione in modalità High Availability (HA). Gli ONTAP tools for VMware vSphere vengono inizialmente distribuiti in una configurazione non HA a nodo singolo.

> Per migrare ad HA quando è abilitato il backup non HA, disabilitare prima il backup e riabilitarlo dopo la migrazione.

Prima di iniziare

- Assicurati che il tuo modello OVA abbia la stessa versione OVA del Nodo 1. Il nodo 1 è il nodo predefinito in cui vengono inizialmente distribuiti gli ONTAP tools for VMware vSphere OVA.
- Assicurarsi che l'aggiunta a caldo della CPU e l'inserimento a caldo della memoria siano abilitati.
- Nel vCenter Server, impostare il livello di automazione del Disaster Recovery Service (DRS) su parzialmente automatizzato. Dopo aver implementato HA, ripristinarlo completamente automatizzato.
- I nomi host dei nodi nella configurazione HA devono essere in minuscolo.

Passi

1. Avviare ONTAP Tools Manager da un browser web:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con le credenziali di amministratore ONTAP tools for VMware vSphere fornite durante la distribuzione.
3. Selezionare **Modifica impostazioni apparecchio** nella sezione panoramica.
4. Nella sezione **Configurazione** è possibile aumentare le dimensioni del nodo e abilitare la configurazione HA in base alle proprie esigenze. Per apportare modifiche sono necessarie le credenziali di vCenter Server.

   Quando gli strumenti ONTAP sono in configurazione HA, è possibile modificare i dettagli della libreria dei contenuti. Dovresti fornire nuovamente la password per la nuova modifica inviata.

   > Negli ONTAP tools for VMware vSphere è consentito solo aumentare le dimensioni del nodo; non è possibile ridurle. In una configurazione non HA è supportata solo una configurazione di medie dimensioni. In una configurazione HA sono supportate configurazioni medie e grandi.

5. Utilizzare il pulsante di attivazione/disattivazione HA per abilitare la configurazione HA. Nella pagina **Impostazioni HA**, assicurati che:
   - La libreria di contenuti appartiene allo stesso vCenter Server in cui vengono eseguite le VM del nodo degli strumenti ONTAP . Le credenziali di vCenter Server vengono utilizzate per convalidare e scaricare il modello OVA per le modifiche all'appliance.
   - La macchina virtuale che ospita gli strumenti ONTAP non è distribuita direttamente su un host ESXi. La VM dovrebbe essere distribuita su un cluster o un pool di risorse.

   > Dopo aver abilitato la configurazione HA, non è possibile tornare a una configurazione a nodo singolo non HA.

6. Nella sezione **Impostazioni HA** della finestra **Modifica impostazioni appliance**, è possibile immettere i dettagli dei nodi 2 e 3. Gli ONTAP tools for VMware vSphere supportano tre nodi nella configurazione HA.

   > La maggior parte delle opzioni di input sono precompilate con i dettagli della rete Nodo 1 per semplificare il flusso di lavoro. Tuttavia, è possibile modificare i dati di input prima di passare alla pagina finale della procedura guidata. È possibile immettere i dettagli dell'indirizzo IPv6 per gli altri due nodi solo quando l'indirizzo IPv6 è abilitato sul primo nodo.

   Assicurarsi che un host ESXi contenga una sola VM degli strumenti ONTAP . Gli input vengono convalidati ogni volta che si passa alla finestra successiva.

7. Rivedi i dettagli nella sezione **Riepilogo** e **Salva** le modifiche.

Cosa succederà ora?

La pagina **Panoramica** mostra lo stato della distribuzione. Utilizzando l'ID del processo, è anche possibile monitorare lo stato del processo di modifica delle impostazioni dell'appliance dalla vista processi.

Se la distribuzione HA non riesce e lo stato del nuovo nodo viene visualizzato come "Nuovo", eliminare la nuova VM in vCenter prima di riprovare l'operazione di abilitazione HA.

La scheda **Avvisi** nel pannello di sinistra elenca gli avvisi per gli ONTAP tools for VMware vSphere.

Gestisci gli archivi dati

Montare i datastore NFS e VMFS

Il montaggio di un datastore fornisce accesso allo storage per host aggiuntivi. È possibile montare il datastore sugli host aggiuntivi dopo averli aggiunti all'ambiente VMware.

Informazioni su questo compito

- Alcune azioni del tasto destro del mouse sono disabilitate o non disponibili a seconda della versione del client vSphere e del tipo di datastore selezionato.
  - Se si utilizza vSphere Client 8.0 o versioni successive, alcune delle opzioni del tasto destro del mouse sono nascoste.
  - Dalle versioni vSphere 7.0U3 a vSphere 8.0, anche se le opzioni vengono visualizzate, l'azione sarà disabilitata.
- L'opzione di montaggio del datastore è disabilitata quando il cluster host è protetto con configurazioni uniformi.

Passi

1. Dalla home page di vSphere Client, seleziona **Host e cluster**.
2. Nel riquadro di navigazione a sinistra, seleziona i data center che contengono gli host.
3. Per montare i datastore NFS/VMFS sull'host o sul cluster host, fare clic con il pulsante destro del mouse e selezionare **Strumenti NetApp ONTAP * > *Monta datastore**.
4. Selezionare i datastore che si desidera montare e selezionare **Monta**.

Cosa succederà ora?

È possibile monitorare l'avanzamento nel pannello delle attività recenti.

Smonta i datastore NFS e VMFS

L'azione Smonta datastore smonta un datastore NFS o VMFS dagli host ESXi. L'azione di smontaggio del datastore è abilitata per i datastore NFS e VMFS rilevati o gestiti dagli ONTAP tools for VMware vSphere.

Passi

1. Accedi al client vSphere.
2. Fare clic con il pulsante destro del mouse su un oggetto datastore NFS o VMFS e selezionare **Smonta datastore**.

   Si apre una finestra di dialogo in cui sono elencati gli host ESXi su cui è montato il datastore. Quando l'operazione viene eseguita su un datastore protetto, sullo schermo viene visualizzato un messaggio di avviso.

3. Selezionare uno o più host ESXi per smontare il datastore.

   Non è possibile smontare il datastore da tutti gli host. L'interfaccia utente suggerisce di utilizzare invece l'operazione di eliminazione del datastore.

4. Selezionare il pulsante **Smonta**.

   Se il datastore fa parte di un cluster host protetto, viene visualizzato un messaggio di avviso.

> Se il datastore protetto viene smontato, l'impostazione di protezione esistente potrebbe comportare una protezione parziale. Fare riferimento a "Modifica il cluster host protetto" per consentire una protezione completa.

Cosa succederà ora?

È possibile monitorare i progressi nel pannello delle attività recenti.

Montare un datastore vVols

È possibile montare un datastore VMware Virtual Volumes (vVols) su uno o più host aggiuntivi per fornire accesso allo storage ad altri host. È possibile smontare il datastore vVols solo tramite le API.

Passi

1. Dalla home page di vSphere Client, seleziona **Host e cluster**.

2. Nel riquadro di navigazione, seleziona il data center che contiene il datastore.
3. Fare clic con il pulsante destro del mouse sul datastore e selezionare **Strumenti NetApp ONTAP * > *Monta datastore**.
4. Nella finestra di dialogo **Monta datastore su host**, seleziona gli host su cui desideri montare il datastore, quindi seleziona **Monta**.

È possibile monitorare l'avanzamento nel pannello delle attività recenti.

Ridimensiona il datastore NFS e VMFS

Ridimensionando un datastore puoi aumentare lo spazio di archiviazione per i file della tua macchina virtuale. È possibile modificare le dimensioni di un datastore in base alle esigenze della propria infrastruttura.

Informazioni su questo compito

È possibile aumentare solo le dimensioni dei datastore NFS e VMFS. Un FlexVol volume che fa parte di un datastore NFS e VMFS non può ridursi al di sotto delle dimensioni esistenti, ma può aumentare al massimo del 120%.

Passi

1. Dalla home page di vSphere Client, seleziona **Host e cluster**.
2. Nel riquadro di navigazione, seleziona il data center che contiene il datastore.
3. Fare clic con il pulsante destro del mouse sul datastore NFS o VMFS e selezionare **Strumenti NetApp ONTAP * > *Ridimensiona datastore**.
4. Nella finestra di dialogo Ridimensiona, specificare una nuova dimensione per il datastore e selezionare **OK**.

Espandi i datastore vVols

Facendo clic con il pulsante destro del mouse sull'oggetto datastore nella vista oggetti vCenter, nella sezione plug-in vengono visualizzati gli ONTAP tools for VMware vSphere . A seconda del tipo di datastore e dei privilegi utente correnti, vengono abilitate azioni specifiche.

> L'operazione di espansione del datastore vVols non è applicabile ai datastore vVols basati sul sistema ASA r2.

Passi

1. Dalla home page di vSphere Client, seleziona **Host e cluster**.
2. Nel riquadro di navigazione, seleziona il data center che contiene il datastore.
3. Fare clic con il pulsante destro del mouse sul datastore e selezionare **Strumenti NetApp ONTAP * > *Aggiungi storage al datastore**.
4. Nella finestra **Crea o Seleziona volumi**, è possibile creare nuovi volumi oppure scegliere tra quelli esistenti. L'interfaccia utente è autoesplicativa. Segui le istruzioni in base alla tua scelta.
5. Nella finestra **Riepilogo**, rivedere le selezioni e selezionare **Espandi**. È possibile monitorare i progressi nel pannello delle attività recenti.

Riduci il datastore vVols

L'azione Elimina datastore elimina il datastore quando non sono presenti vVols sul datastore selezionato.

> L'operazione di riduzione del datastore vVols non è supportata per il datastore vVols basato sul sistema ASA r2.

Passi

1. Dalla home page di vSphere Client, seleziona **Host e cluster**.
2. Nel riquadro di navigazione, seleziona il data center che contiene il datastore.
3. Fare clic con il pulsante destro del mouse sul datastore vVol e selezionare **Strumenti NetApp ONTAP * > *Rimuovi storage dal datastore**.
4. Selezionare i volumi che non hanno vVols e selezionare **Rimuovi**.

   > L'opzione per selezionare il volume su cui risiede vVols è disabilitata.

5. Nel pop-up **Rimuovi storage**, seleziona la casella di controllo **Elimina volumi dal cluster ONTAP * per eliminare i volumi dal datastore e dallo storage ONTAP e seleziona *Elimina**.

Elimina i datastore

L'azione di rimozione dello storage dal datastore è supportata su tutti gli ONTAP tools for VMware vSphere i datastore vVols VMware vSphere rilevati o gestiti nel vCenter Server. Questa azione consente la rimozione dei volumi dagli archivi dati vVols .

L'opzione di rimozione è disabilitata quando sono presenti vVols residenti su un volume specifico. Oltre a rimuovere i volumi dal datastore, è possibile eliminare il volume selezionato nell'archiviazione ONTAP .

L'attività di eliminazione del datastore dagli ONTAP tools for VMware vSphere in vCenter Server esegue le seguenti operazioni:

- Smonta il contenitore vVol.
- Pulisce igroup. Se igroup non è in uso, rimuove iqn da igroup.
- Elimina il contenitore Vvol.
- Lascia i volumi Flex nell'array di archiviazione.

Per eliminare il datastore NFS, VMFS o vVOL dagli strumenti ONTAP dal vCenter Server, seguire i passaggi indicati di seguito:

Passi

1. Accedi al client vSphere.
2. Fare clic con il pulsante destro del mouse su un sistema host, un cluster host o un data center e selezionare **Strumenti NetApp ONTAP * > *Elimina datastore**.

> Non è possibile eliminare i datastore se sono presenti macchine virtuali che li utilizzano. Prima di eliminare il datastore, è necessario spostare le macchine virtuali in un datastore diverso. Non è possibile selezionare la casella di controllo Elimina volume se il datastore appartiene a un cluster host protetto.

a. Nel caso di un datastore NFS o VMFS, viene visualizzata una finestra di dialogo con l'elenco delle VM che utilizzano il datastore.
b. Se il datastore VMFS viene creato su sistemi ASA r2 e fa parte della protezione, è necessario rimuovere la protezione dal datastore prima di eliminarlo.
c. Nel caso di datastore vVols , l'azione di eliminazione del datastore elimina il datastore solo quando non vi sono vVols associati. La finestra di dialogo Elimina datastore fornisce un'opzione per eliminare i volumi dal cluster ONTAP .
d. Nel caso di datastore vVols basati su sistemi ASA r2, la casella di controllo per eliminare i volumi di supporto non è applicabile.

3. Per eliminare i volumi di backup sullo storage ONTAP , selezionare *Elimina volumi sul cluster ONTAP *.

> Non è possibile eliminare il volume sul cluster ONTAP per un datastore VMFS che fa parte del cluster host protetto.

Viste di archiviazione ONTAP per datastore

Gli ONTAP tools for VMware vSphere mostrano la vista laterale dell'archiviazione ONTAP dei datastore e dei relativi volumi nella scheda di configurazione.

Passi

1. Dal client vSphere, accedere al datastore.
2. Selezionare la scheda **Configura** nel riquadro di destra.
3. Selezionare *Strumenti NetApp ONTAP * > * Archiviazione ONTAP *. La visualizzazione cambia a seconda del tipo di datastore. Per informazioni, fare riferimento alla tabella sottostante:

Tipo di archivio dati	Informazioni disponibili
Archivio dati NFS	La pagina **Dettagli di archiviazione** contiene informazioni sui backend di archiviazione, aggregati e volumi. La pagina **Dettagli NFS** contiene dati relativi al datastore NFS.
Datastore VMFS	La pagina **Dettagli di archiviazione** contiene dettagli sul backend di archiviazione, sull'aggregato, sul volume e sulla zona di disponibilità di archiviazione (SAZ). La pagina **Dettagli unità di stoccaggio** contiene i dettagli dell'unità di stoccaggio.
Datastore vVols	Elenca tutti i volumi. È possibile espandere o rimuovere lo spazio di archiviazione dal riquadro di archiviazione ONTAP . Questa visualizzazione non è supportata per il datastore vVols basato sul sistema ASA r2.

Visualizzazione dell'archiviazione della macchina virtuale

La vista di archiviazione mostra l'elenco dei vVols creati dalla macchina virtuale.

> Questa vista è applicabile alla VM su cui è montato almeno un disco correlato al datastore vVols gestito ONTAP tools for VMware vSphere .

Passi

1. Da vSphere Client passare alla macchina virtuale.
2. Selezionare la scheda **Monitor** nel riquadro di destra.
3. Selezionare **Strumenti NetApp ONTAP * > *Archiviazione**. I dettagli di **Archiviazione** vengono visualizzati nel riquadro di destra. È possibile visualizzare l'elenco dei vVols presenti sulla VM.

   È possibile utilizzare l'opzione "Gestisci colonne" per nascondere o mostrare colonne diverse.

Gestire le soglie di archiviazione

È possibile impostare la soglia per ricevere notifiche in vCenter Server quando il volume e la capacità aggregata raggiungono determinati livelli.

Passaggi:

1. Accedi al client vSphere.
2. Nella pagina dei collegamenti, seleziona *Strumenti NetApp ONTAP * nella sezione plug-in.
3. Nel riquadro sinistro degli strumenti ONTAP , vai su **Impostazioni** > **Impostazioni soglia** > **Modifica**.
4. Nella finestra **Modifica soglia**, immettere i valori desiderati nei campi **Quasi pieno** e **Pieno** e selezionare **Salva**. È possibile reimpostare i numeri sui valori consigliati, ovvero 80 per Quasi pieno e 90 per Pieno.

Gestire i backend di archiviazione

I backend di archiviazione sono sistemi utilizzati dagli host ESXi per l'archiviazione dei dati.

Scopri lo spazio di archiviazione

È possibile eseguire l'individuazione di un backend di archiviazione su richiesta senza attendere un'individuazione pianificata per aggiornare i dettagli di archiviazione.

Per scoprire i backend di archiviazione, seguire i passaggi indicati di seguito.

Passi

1. Accedi al client vSphere.
2. Nella pagina dei collegamenti, seleziona *Strumenti NetApp ONTAP * nella sezione plug-in.
3. Nel riquadro sinistro degli strumenti ONTAP , vai su **Backend di archiviazione** e seleziona un backend di archiviazione.
4. Seleziona il menu delle ellissi verticali e seleziona **Scopri spazio di archiviazione**

È possibile monitorare i progressi nel pannello delle attività recenti.

Modificare i backend di archiviazione

Per modificare un backend di archiviazione, seguire i passaggi descritti in questa sezione.

1. Accedi al client vSphere.
2. Nella pagina dei collegamenti, seleziona *Strumenti NetApp ONTAP * nella sezione plug-in.
3. Nel riquadro sinistro degli strumenti ONTAP , vai su **Backend di archiviazione** e seleziona un backend di archiviazione.
4. Selezionare il menu con le ellissi verticali e selezionare **Modifica** per modificare le credenziali o il nome della porta. È possibile monitorare i progressi nel pannello delle attività recenti.

È possibile eseguire l'operazione di modifica per i cluster ONTAP globali utilizzando ONTAP Tools Manager seguendo i passaggi seguenti.

1. Avviare ONTAP Tools Manager da un browser web: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con le credenziali di amministratore ONTAP tools for VMware vSphere fornite durante la distribuzione.
3. Seleziona i backend di archiviazione dalla barra laterale.
4. Seleziona il backend di archiviazione che desideri modificare.
5. Selezionare il menu delle ellissi verticali e selezionare **Modifica**.
6. È possibile modificare le credenziali o la porta. Inserisci **Nome utente** e **Password** per modificare il backend di archiviazione.

Rimuovere i backend di archiviazione

Prima di rimuovere il backend di archiviazione, è necessario eliminare tutti i datastore collegati. Per rimuovere un backend di archiviazione, seguire i passaggi indicati di seguito.

1. Accedi al client vSphere.
2. Nella pagina dei collegamenti, seleziona *Strumenti NetApp ONTAP * nella sezione plug-in.
3. Nel riquadro sinistro degli strumenti ONTAP , vai su **Backend di archiviazione** e seleziona un backend di archiviazione.
4. Selezionare il menu delle ellissi verticali e selezionare **Rimuovi**. Assicurarsi che il backend di archiviazione non contenga alcun archivio dati. È possibile monitorare i progressi nel pannello delle attività recenti.

È possibile eseguire l'operazione di rimozione per i cluster ONTAP globali utilizzando ONTAP Tools Manager.

1. Avviare ONTAP Tools Manager da un browser web: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con le credenziali di amministratore ONTAP tools for VMware vSphere fornite durante la distribuzione.
3. Seleziona **Backend di archiviazione** dalla barra laterale.
4. Seleziona il backend di archiviazione che desideri rimuovere
5. Selezionare il menu delle ellissi verticali e selezionare **Rimuovi**.

Visualizzazione dettagliata del backend di archiviazione

Nella pagina del backend di archiviazione sono elencati tutti i backend di archiviazione. È possibile eseguire operazioni di individuazione, modifica e rimozione dell'archiviazione sui backend di archiviazione aggiunti e non sulla singola SVM figlio nel cluster.

Quando selezioni il cluster padre o quello figlio nel backend di archiviazione, puoi visualizzare il riepilogo generale del componente. Quando selezioni il cluster padre, viene visualizzato un menu a discesa con le azioni da cui puoi eseguire le operazioni di individuazione, modifica e rimozione dell'archiviazione.

La pagina di riepilogo fornisce i seguenti dettagli:

- Stato del backend di archiviazione
- Informazioni sulla capacità
- Informazioni di base sulla VM
- Informazioni di rete come l'indirizzo IP e la porta della rete. Per l'SVM figlio, le informazioni saranno le stesse del backend di archiviazione padre.
- Privileges consentiti e limitati per il backend di archiviazione. Per l'SVM figlio, le informazioni saranno le stesse del backend di archiviazione padre. I Privileges vengono visualizzati solo sui backend di archiviazione basati su cluster. Se si aggiunge SVM come backend di archiviazione, le informazioni sui privilegi non verranno visualizzate.
- La visualizzazione dettagliata del cluster di sistema ASA r2 non include la scheda dei livelli locali quando la proprietà disaggregata è impostata su "true" per l'SVM o il cluster.
- Per i sistemi ASA r2 SVM, il portlet di capacità non viene visualizzato. Il portale della capacità è necessario solo quando la proprietà disaggregata è impostata su "true" per l'SVM o il cluster.
- Per i sistemi ASA r2 SVM, la sezione delle informazioni di base mostra il tipo di piattaforma.

La scheda Interfaccia fornisce informazioni dettagliate sull'interfaccia.

La scheda Livelli locali fornisce informazioni dettagliate sull'elenco aggregato.

Gestire le istanze di vCenter Server

Le istanze di vCenter Server sono piattaforme di gestione centralizzate che consentono di controllare host, macchine virtuali e backend di storage.

Dissociare i backend di archiviazione dall'istanza di vCenter Server

Nella pagina di elenco di vCenter Server viene visualizzato il numero associato di backend di archiviazione. Ogni istanza di vCenter Server ha la possibilità di associarsi o disassociarsi a un backend di archiviazione.

Passi

1. Avviare ONTAP Tools Manager da un browser web: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con le credenziali di amministratore ONTAP tools for VMware vSphere fornite durante la distribuzione.
3. Selezionare l'istanza di vCenter Server richiesta dalla barra laterale.
4. Selezionare le ellissi verticali in corrispondenza del vCenter Server che si desidera associare o dissociare

dai backend di archiviazione.

5. Seleziona **Disassocia backend di archiviazione**.

Modificare un'istanza di vCenter Server

Per modificare le istanze di vCenter Server, seguire i passaggi indicati di seguito.

1. Avviare ONTAP Tools Manager da un browser web: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con le credenziali di amministratore ONTAP tools for VMware vSphere fornite durante la distribuzione.
3. Seleziona l'istanza di vCenter Server applicabile dalla barra laterale
4. Selezionare le ellissi verticali sul vCenter Server che si desidera modificare e selezionare **Modifica**.
5. Modificare i dettagli dell'istanza di vCenter Server e selezionare **Modifica**.

Rimuovere un'istanza di vCenter Server

Prima di rimuovere vCenter Server, è necessario rimuovere tutti i backend di archiviazione collegati a quest'ultimo.

1. Avviare ONTAP Tools Manager da un browser web: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con le credenziali di amministratore ONTAP tools for VMware vSphere fornite durante la distribuzione.
3. Seleziona le istanze di vCenter Server applicabili dalla barra laterale
4. Selezionare le ellissi verticali sul vCenter Server che si desidera rimuovere e selezionare **Rimuovi**.

> Dopo aver rimosso le istanze di vCenter Server, queste non saranno più gestite dall'applicazione.

Quando si rimuovono istanze di vCenter Server negli strumenti ONTAP , vengono eseguite automaticamente le seguenti azioni:

- Il plug-in non è registrato.
- I privilegi e i ruoli dei plug-in vengono rimossi.

Gestisci i certificati

Per impostazione predefinita, durante la distribuzione viene generato un certificato autofirmato per gli strumenti ONTAP e VASA Provider. Utilizzando l'interfaccia di ONTAP Tools Manager, è possibile rinnovare il certificato o aggiornarlo a una CA personalizzata. I certificati CA personalizzati sono obbligatori in una distribuzione multi-vCenter.

Prima di iniziare

- Il nome di dominio su cui viene emesso il certificato deve essere mappato all'indirizzo IP virtuale.
- Eseguire il controllo nslookup sul nome di dominio per verificare se il dominio viene risolto nell'indirizzo IP previsto.

- I certificati devono essere creati con il nome di dominio e l'indirizzo IP degli strumenti ONTAP .

> Un indirizzo IP degli strumenti ONTAP deve corrispondere a un nome di dominio completamente qualificato (FQDN). I certificati devono contenere lo stesso FQDN mappato all'indirizzo IP degli strumenti ONTAP nei nomi oggetto o nei nomi alternativi dell'oggetto.

> Non è possibile passare da un certificato firmato da una CA a un certificato autofirmato.

Aggiorna il certificato degli strumenti ONTAP

La scheda Strumenti ONTAP mostra dettagli come il tipo di certificato (autofirmato/firmato da CA) e il nome di dominio. Durante la distribuzione, per impostazione predefinita viene generato un certificato autofirmato. È possibile rinnovare il certificato o aggiornarlo a CA.

Passi

1. Avviare ONTAP Tools Manager da un browser web:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con le credenziali di amministratore ONTAP tools for VMware vSphere fornite durante la distribuzione.
3. Selezionare **Certificati** > **Strumenti ONTAP * > *Rinnova** per rinnovare i certificati.

   È possibile rinnovare il certificato se è scaduto o se sta per scadere. L'opzione di rinnovo è disponibile quando il tipo di certificato è firmato da una CA. Nella finestra pop-up, fornire i dettagli del certificato del server, della chiave privata, della CA radice e del certificato intermedio.

   > Il sistema sarà offline finché il certificato non verrà rinnovato e verrai disconnesso dall'interfaccia di ONTAP Tools Manager.

4. Per aggiornare il certificato autofirmato a un certificato CA personalizzato, selezionare l'opzione **Certificati** > **Strumenti ONTAP * > *Aggiorna a CA**.
   a. Nella finestra pop-up, carica il certificato del server, la chiave privata del certificato del server, il certificato CA radice e i file del certificato intermedio.
   b. Inserisci il nome di dominio per il quale hai generato questo certificato e aggiorna il certificato.

   > Il sistema sarà offline fino al completamento dell'aggiornamento e l'utente verrà disconnesso dall'interfaccia di ONTAP Tools Manager.

Aggiorna il certificato del fornitore VASA

Gli ONTAP tools for VMware vSphere vengono distribuiti con un certificato autofirmato per VASA Provider. In questo modo è possibile gestire una sola istanza di vCenter Server per i datastore vVols . Quando si gestiscono più istanze di vCenter Server e si desidera abilitare la funzionalità vVols su di esse, è necessario modificare il certificato autofirmato in un certificato CA personalizzato.

Passi

1. Avviare ONTAP Tools Manager da un browser web:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con le credenziali di amministratore ONTAP tools for VMware vSphere fornite durante la distribuzione.
3. Selezionare **Certificati** > **Fornitore VASA** o **Strumenti ONTAP * > *Rinnova** per rinnovare i certificati.
4. Selezionare **Certificati** > **Provider VASA** o **Strumenti ONTAP * > *Aggiorna a CA** per aggiornare il certificato autofirmato in un certificato CA personalizzato.
   a. Nella finestra pop-up, carica il certificato del server, la chiave privata del certificato del server, il certificato CA radice e i file del certificato intermedio.
   b. Inserisci il nome di dominio per il quale hai generato questo certificato e aggiorna il certificato.

Il sistema sarà offline fino al completamento dell'aggiornamento e l'utente verrà disconnesso dall'interfaccia di ONTAP Tools Manager.

Accedi ONTAP tools for VMware vSphere

Panoramica degli ONTAP tools for VMware vSphere

È possibile gestire le configurazioni delle applicazioni, del sistema e della rete utilizzando la console di manutenzione degli strumenti ONTAP . È possibile modificare la password dell'amministratore e la password di manutenzione. È inoltre possibile generare pacchetti di supporto, impostare diversi livelli di registro, visualizzare e gestire le configurazioni TLS e avviare la diagnostica remota.

Dopo aver distribuito gli ONTAP tools for VMware vSphere, è necessario installare VMware Tools per accedere alla console di manutenzione. Dovresti usare `maint` come nome utente e password configurati durante la distribuzione per accedere alla console di manutenzione degli strumenti ONTAP . Dovresti usare **nano** per modificare i file nella console di manutenzione o di accesso root.

Dovresti impostare una password per `diag` utente durante l'abilitazione della diagnostica remota.

Per accedere alla console di manutenzione, è necessario utilizzare la scheda **Riepilogo** degli ONTAP tools for VMware vSphere . Quando selezioni , la console di manutenzione si avvia.

Menù della console	Opzioni
Configurazione dell'applicazione	1. Visualizza il riepilogo dello stato del server 2. Modifica il livello LOG per i servizi del fornitore VASA e i servizi SRA
Configurazione del sistema	1. Riavviare la macchina virtuale 2. Arresto della macchina virtuale 3. Cambia la password dell'utente 'maint' 4. Cambia fuso orario 5. Aumentare la dimensione del disco jail (/jail) 6. Aggiornamento 7. Installa VMware Tools

Configurazione di rete	1. Visualizza le impostazioni dell'indirizzo IP 2. Visualizza le impostazioni di ricerca del nome di dominio 3. Modifica le impostazioni di ricerca del nome di dominio 4. Visualizza percorsi statici 5. Modificare i percorsi statici 6. Applica modifiche 7. Ping un host 8. Ripristina le impostazioni predefinite
Supporto e diagnostica	1. Accesso alla shell diagnostica 2. Abilita l'accesso diagnostico remoto 3. Fornire le credenziali vCenter per il backup 4. Fai un backup

Configurare l'accesso diagnostico remoto

È possibile configurare gli ONTAP tools for VMware vSphere per abilitare l'accesso SSH per l'utente diag.

Prima di iniziare

L'estensione VASA Provider deve essere abilitata per l'istanza di vCenter Server.

Informazioni su questo compito

L'utilizzo di SSH per accedere all'account utente diag presenta le seguenti limitazioni:

- È consentito un solo account di accesso per ogni attivazione di SSH.
- L'accesso SSH all'account utente diag viene disabilitato quando si verifica una delle seguenti situazioni:
  - Il tempo scade.

    La sessione di accesso rimane valida solo fino alla mezzanotte del giorno successivo.

  - Accedi nuovamente come utente diag tramite SSH.

Passi

1. Dal vCenter Server, aprire una console per VASA Provider.
2. Accedi come utente addetto alla manutenzione.
3. Entra `4` per selezionare Supporto e diagnostica.
4. Entra `2` per selezionare Abilita accesso alla diagnostica remota.
5. Entra `y` nella finestra di dialogo Conferma per abilitare l'accesso diagnostico remoto.
6. Immettere una password per l'accesso alla diagnostica remota.

Avvia SSH su altri nodi

Prima di effettuare l'aggiornamento, è necessario avviare SSH sugli altri nodi.

Prima di iniziare

L'estensione VASA Provider deve essere abilitata per l'istanza di vCenter Server.

Informazioni su questo compito

Eseguire questa procedura su ciascuno dei nodi prima di eseguire l'aggiornamento.

Passi

1. Dal vCenter Server, aprire una console per VASA Provider.
2. Accedi come utente addetto alla manutenzione.
3. Entra `4` per selezionare Supporto e diagnostica.
4. Entra `1` per selezionare Accedi alla shell diagnostica.
5. Entra `y` per procedere.
6. Eseguire il comando *sudo systemctl restart ssh*.

Aggiornare le credenziali di vCenter Server e ONTAP

È possibile aggiornare l'istanza di vCenter Server e le credenziali ONTAP tramite la console di manutenzione.

Prima di iniziare

È necessario disporre delle credenziali di accesso dell'utente addetto alla manutenzione.

Informazioni su questo compito

Se hai modificato le credenziali per vCenter Server, ONTAP o Data LIF dopo la distribuzione, devi aggiornarle utilizzando questa procedura.

Passi

1. Dal vCenter Server, aprire una console per VASA Provider.
2. Accedi come utente addetto alla manutenzione.
3. Entra `2` per selezionare il menu Configurazione di sistema.
4. Entra `9` per modificare le credenziali ONTAP .
5. Entra `10` per modificare le credenziali di vCenter.

Report degli strumenti ONTAP

Il plug-in ONTAP tools for VMware vSphere fornisce report per macchine virtuali e datastore. Quando si seleziona l'icona del plug-in Strumenti NetApp ONTAP tools for VMware vSphere nella sezione dei collegamenti sul client vCenter, l'interfaccia utente passa alla pagina Panoramica. Selezionare la scheda Report per visualizzare il report sulla macchina virtuale e sui datastore.

Il report Macchine virtuali mostra l'elenco delle macchine virtuali rilevate (dovrebbero avere almeno un disco da datastore basati su storage ONTAP) con metriche delle prestazioni. Quando si espande il record della VM, vengono visualizzate tutte le informazioni relative al datastore del disco.

Il report Datastore mostra l'elenco degli ONTAP tools for VMware vSphere , forniti dal backend di archiviazione ONTAP di tutti i tipi con metriche delle prestazioni.

È possibile utilizzare l'opzione Gestisci colonne per nascondere o mostrare colonne diverse.

Raccogliere i file di registro

È possibile raccogliere i file di registro per gli ONTAP tools for VMware vSphere dalle opzioni disponibili nell'interfaccia utente di ONTAP Tools Manager. L'assistenza tecnica potrebbe chiederti di raccogliere i file di registro per aiutarti a risolvere un problema.

> La generazione di log da ONTAP Tools Manager include tutti i log per tutte le istanze di vCenter Server. La generazione di log dall'interfaccia utente del client vCenter è limitata al server vCenter selezionato.

Passi

1. Avviare ONTAP Tools Manager da un browser web:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con le credenziali di amministratore ONTAP tools for VMware vSphere fornite durante la distribuzione.
3. Selezionare **Bundle di log** dalla barra laterale.

   Questa operazione può richiedere diversi minuti.
4. Selezionare **Genera** per generare i file di registro.
5. Inserisci l'etichetta per il pacchetto di log e seleziona **Genera**.

   Scarica il file tar.gz e invialo al supporto tecnico.

Per generare un bundle di log utilizzando l'interfaccia utente del client vCenter, seguire i passaggi indicati di seguito:

Passi

1. Accedi al client vSphere.
2. Dalla home page di vSphere Client, vai a **Supporto** > **Bundle di log** > **Genera**.
3. Specifica l'etichetta del bundle di log e generalo. L'opzione di download verrà visualizzata durante la generazione dei file. Il download potrebbe richiedere del tempo.

> Il bundle di log generato sostituisce il bundle di log generato negli ultimi 3 giorni o 72 ore.

Gestire macchine virtuali

Considerazioni sulla migrazione o la clonazione di macchine virtuali

Durante la migrazione delle macchine virtuali esistenti nel tuo data center, dovresti tenere a mente alcune considerazioni.

Migrare macchine virtuali protette

È possibile migrare le macchine virtuali protette su:

- Stesso datastore vVols in un host ESXi diverso
- Diversi datastore vVols compatibili nello stesso host ESXi
- Diversi datastore vVols compatibili in un host ESXi diverso

Se la macchina virtuale viene migrata su un FlexVol volume diverso, anche il rispettivo file di metadati viene aggiornato con le informazioni sulla macchina virtuale. Se una macchina virtuale viene migrata su un host ESXi diverso ma con lo stesso storage, il file di metadati FlexVol volume sottostante non verrà modificato.

Clona macchine virtuali protette

È possibile clonare macchine virtuali protette nei seguenti modi:

- Stesso contenitore dello stesso FlexVol volume utilizzando il gruppo di replica

  Lo stesso file di metadati del volume FlexVol viene aggiornato con i dettagli della macchina virtuale clonata.

- Stesso contenitore di un FlexVol volume diverso che utilizza il gruppo di replica

  Il file di metadati FlexVol volume in cui è posizionata la macchina virtuale clonata viene aggiornato con i dettagli della macchina virtuale clonata.

- Contenitore diverso o datastore vVols

  Nel FlexVol volume in cui è posizionata la macchina virtuale clonata, il file dei metadati riceve i dettagli aggiornati della macchina virtuale.

Attualmente VMware non supporta macchine virtuali clonate in un modello VM.

È supportato il clone di clone di una macchina virtuale protetta.

Fare riferimento a "Creazione di una macchina virtuale per la clonazione" per maggiori dettagli.

Snapshot della macchina virtuale

Attualmente sono supportati solo gli snapshot di macchine virtuali senza memoria. Se la macchina virtuale ha uno snapshot con memoria, non viene considerata per la protezione.

Non è inoltre possibile proteggere macchine virtuali non protette dotate di snapshot di memoria. Per questa versione, è previsto che tu elimini lo snapshot della memoria prima di abilitare la protezione per la macchina virtuale.

Per le VM Windows con tipo di archiviazione ASA r2, quando si esegue uno snapshot della macchina virtuale, si tratterà di uno snapshot di sola lettura. Quando è richiesta l'alimentazione per la VM, il provider VASA crea

una LUN utilizzando lo snapshot di sola lettura e quindi la abilita per gli IOPS. Durante la richiesta di spegnimento, VASA Provider elimina il LUN creato e quindi disabilita gli IOPS.

Migrare macchine virtuali con datastore NFS e VMFS su datastore vVols

È possibile migrare le macchine virtuali dai datastore NFS e VMFS ai datastore Virtual Volumes (vVols) per sfruttare la gestione delle VM basata su policy e altre funzionalità vVols . I datastore vVols consentono di soddisfare i requisiti di carico di lavoro più elevati.

Prima di iniziare

Assicurarsi che VASA Provider non sia in esecuzione su nessuna delle macchine virtuali che si intende migrare. Se si esegue la migrazione di una macchina virtuale che esegue VASA Provider su un datastore vVols , non è possibile eseguire alcuna operazione di gestione, inclusa l'accensione delle macchine virtuali presenti sui datastore vVols .

Informazioni su questo compito

Quando si esegue la migrazione da un datastore NFS e VMFS a un datastore vVols , vCenter Server utilizza le API vStorage per l'offload di Array Integration (VAAI) quando si spostano i dati dai datastore VMFS, ma non da un file NFS VMDK. Gli offload VAAI normalmente riducono il carico sull'host.

Passi

1. Fare clic con il pulsante destro del mouse sulla macchina virtuale che si desidera migrare e selezionare **Migra**.
2. Selezionare **Modifica solo archiviazione** e quindi selezionare **Avanti**.
3. Selezionare un formato di disco virtuale, una policy di archiviazione VM e un datastore vVol che corrispondano alle funzionalità del datastore che si sta migrando.
4. Rivedi le impostazioni e seleziona **Fine**.

Bonifica VASA

Per eseguire la pulizia VASA, seguire i passaggi descritti in questa sezione.

> Si consiglia di rimuovere tutti gli archivi dati vVols prima di eseguire la pulizia VASA.

Passi

1. Annullare la registrazione del plug-in andando su \ https://OTV_IP:8143/Register.html
2. Verificare che il plug-in non sia più disponibile sul vCenter Server.
3. Arrestare gli ONTAP tools for VMware vSphere VM.
4. Eliminare gli ONTAP tools for VMware vSphere VM.

Collegare o scollegare un disco dati da una macchina virtuale

Collegare un disco dati a una macchina virtuale

Collegare un disco dati a una macchina virtuale per espandere la capacità di archiviazione.

Passi

1. Accedi al client vSphere.

2. Fare clic con il pulsante destro del mouse su una macchina virtuale nell'inventario e selezionare **Modifica impostazioni**.
3. Nella scheda **Hardware virtuale**, seleziona **Disco rigido esistente**.
4. Selezionare la macchina virtuale in cui si trova il disco.
5. Seleziona il disco che vuoi collegare e seleziona **OK**

Risultato

Il disco rigido viene visualizzato nell'elenco dei dispositivi hardware virtuali.

Scollegare un disco dati dalla macchina virtuale

È possibile scollegare un disco dati collegato a una macchina virtuale quando non è più necessario. Quando si scollega il disco dalla macchina virtuale, questo non viene eliminato automaticamente, ma rimane nel sistema di archiviazione ONTAP .

Passi

1. Accedi al client vSphere.
2. Fare clic con il pulsante destro del mouse su una macchina virtuale nell'inventario e selezionare **Modifica impostazioni**.
3. Sposta il puntatore sul disco e seleziona **Rimuovi**.

> Il disco viene rimosso dalla macchina virtuale. Se altre macchine virtuali condividono il disco, i file del disco non vengono eliminati.

Informazioni correlate

"Aggiungere un nuovo disco rigido a una macchina virtuale"

"Aggiungere un disco rigido esistente a una macchina virtuale"

Scopri i sistemi di archiviazione e gli host

Quando si eseguono per la prima volta gli ONTAP tools for VMware vSphere in un vSphere Client, gli strumenti ONTAP rilevano gli host ESXi, i loro LUN e le esportazioni NFS, nonché i sistemi di storage NetApp che possiedono tali LUN ed esportazioni.

Prima di iniziare

- Tutti gli host ESXi devono essere accesi e connessi.
- Tutte le macchine virtuali di archiviazione (SVM) da rilevare devono essere in esecuzione e ogni nodo del cluster deve avere almeno un LIF dati configurato per il protocollo di archiviazione in uso (NFS o iSCSI).

Informazioni su questo compito

È possibile scoprire nuovi sistemi di archiviazione o aggiornare le informazioni sui sistemi di archiviazione esistenti per ottenere in qualsiasi momento le informazioni più recenti su capacità e configurazione. È anche possibile modificare le credenziali utilizzate ONTAP tools for VMware vSphere per accedere ai sistemi di storage.

Durante la scoperta dei sistemi di storage, gli ONTAP tools for VMware vSphere raccolgono informazioni dagli host ESXi gestiti dall'istanza di vCenter Server.

Passi

1. Dalla home page di vSphere Client, seleziona **Host e cluster**.
2. Fare clic con il pulsante destro del mouse sul data center desiderato e selezionare **Strumenti NetApp ONTAP * > *Aggiorna dati host**.

   Nella finestra di dialogo **Conferma**, conferma la tua scelta.

3. Seleziona i controller di archiviazione rilevati che hanno lo stato `Authentication Failure` e seleziona **Azioni** > **Modifica**.
4. Compilare le informazioni richieste nella finestra di dialogo **Modifica sistema di archiviazione**.
5. Ripetere i passaggi 4 e 5 per tutti i controller di archiviazione con `Authentication Failure` stato.

Una volta completato il processo di individuazione, eseguire le seguenti azioni:

- Utilizzare gli ONTAP tools for VMware vSphere per configurare le impostazioni host ESXi per gli host che visualizzano l'icona di avviso nella colonna delle impostazioni dell'adattatore, nella colonna delle impostazioni MPIO o nella colonna delle impostazioni NFS.
- Fornire le credenziali del sistema di archiviazione.

Modificare le impostazioni dell'host ESXi utilizzando gli strumenti ONTAP

È possibile utilizzare la dashboard degli ONTAP tools for VMware vSphere per modificare le impostazioni dell'host ESXi.

Prima di iniziare

Se si verifica un problema con le impostazioni dell'host ESXi, il problema viene visualizzato nel portlet dei sistemi host ESXi della dashboard. È possibile selezionare il problema per visualizzare il nome host o l'indirizzo IP dell'host ESXi che presenta il problema.

Passi

1. Accedi al client vSphere.
2. Nella pagina dei collegamenti, seleziona *Strumenti NetApp ONTAP * nella sezione plug-in.
3. Accedere al portlet **Conformità host ESXi** nella Panoramica (dashboard) del plug-in ONTAP tools for VMware vSphere .
4. Selezionare il collegamento **Applica impostazioni consigliate**.
5. Nella finestra **Applica impostazioni host consigliate**, seleziona gli host che desideri siano conformi alle impostazioni host consigliate da NetApp e seleziona **Avanti**.

   È possibile espandere l'host ESXi per visualizzare i valori correnti.

6. Nella pagina delle impostazioni, seleziona i valori consigliati in base alle tue esigenze.
7. Nel riquadro di riepilogo, controlla i valori e seleziona **Fine**. È possibile monitorare l'avanzamento nel pannello delle attività recenti.

Informazioni correlate

"Configurare le impostazioni dell'host ESXi"

Gestisci le password

Cambia la password del gestore degli strumenti ONTAP

È possibile modificare la password dell'amministratore utilizzando ONTAP Tools Manager.

Passi

1. Avviare ONTAP Tools Manager da un browser web: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con le credenziali di amministratore ONTAP tools for VMware vSphere fornite durante la distribuzione.
3. Selezionare l'icona **amministratore** nell'angolo in alto a destra dello schermo e selezionare **Cambia password**.
4. Nella finestra pop-up per cambiare la password, inserisci la vecchia password e i dettagli della nuova password. Il vincolo per la modifica della password viene visualizzato nella schermata dell'interfaccia utente.
5. Selezionare **Modifica** per implementare le modifiche.

Reimposta la password del gestore degli strumenti ONTAP

Se hai dimenticato la password di ONTAP Tools Manager, puoi reimpostare le credenziali di amministratore utilizzando il token generato dalla console di manutenzione di ONTAP tools for VMware vSphere .

Passi

1. Avviare ONTAP Tools Manager da un browser web: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Nella schermata di accesso, seleziona l'opzione **Reimposta password**.

   Per reimpostare la password del Manager, è necessario generare il token di reimpostazione utilizzando gli ONTAP tools for VMware vSphere .

   a. Dal vCenter Server, aprire la console di manutenzione
   b. Immettere '2' per selezionare l'opzione Configurazione di sistema
   c. Inserisci '3' per modificare la password utente 'maint'.
3. Nella finestra pop-up per la modifica della password, inserisci il token di reimpostazione della password, il nome utente e i dettagli della nuova password.
4. Selezionare **Reimposta** per implementare le modifiche. Una volta reimpostata la password, potrai utilizzare la nuova password per accedere.

Reimposta la password utente dell'applicazione

La password utente dell'applicazione viene utilizzata per la registrazione di SRA e VASA Provider con vCenter Server.

Passi

1. Avviare ONTAP Tools Manager da un browser web: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con le credenziali di amministratore ONTAP tools for VMware vSphere fornite durante la distribuzione.
3. Seleziona **Impostazioni** dalla barra laterale.
4. Nella schermata **Credenziali VASA/SRA**, seleziona **Reimposta password**.
5. Inserisci una nuova password e conferma i nuovi dati inseriti.
6. Selezionare **Reimposta** per implementare le modifiche.

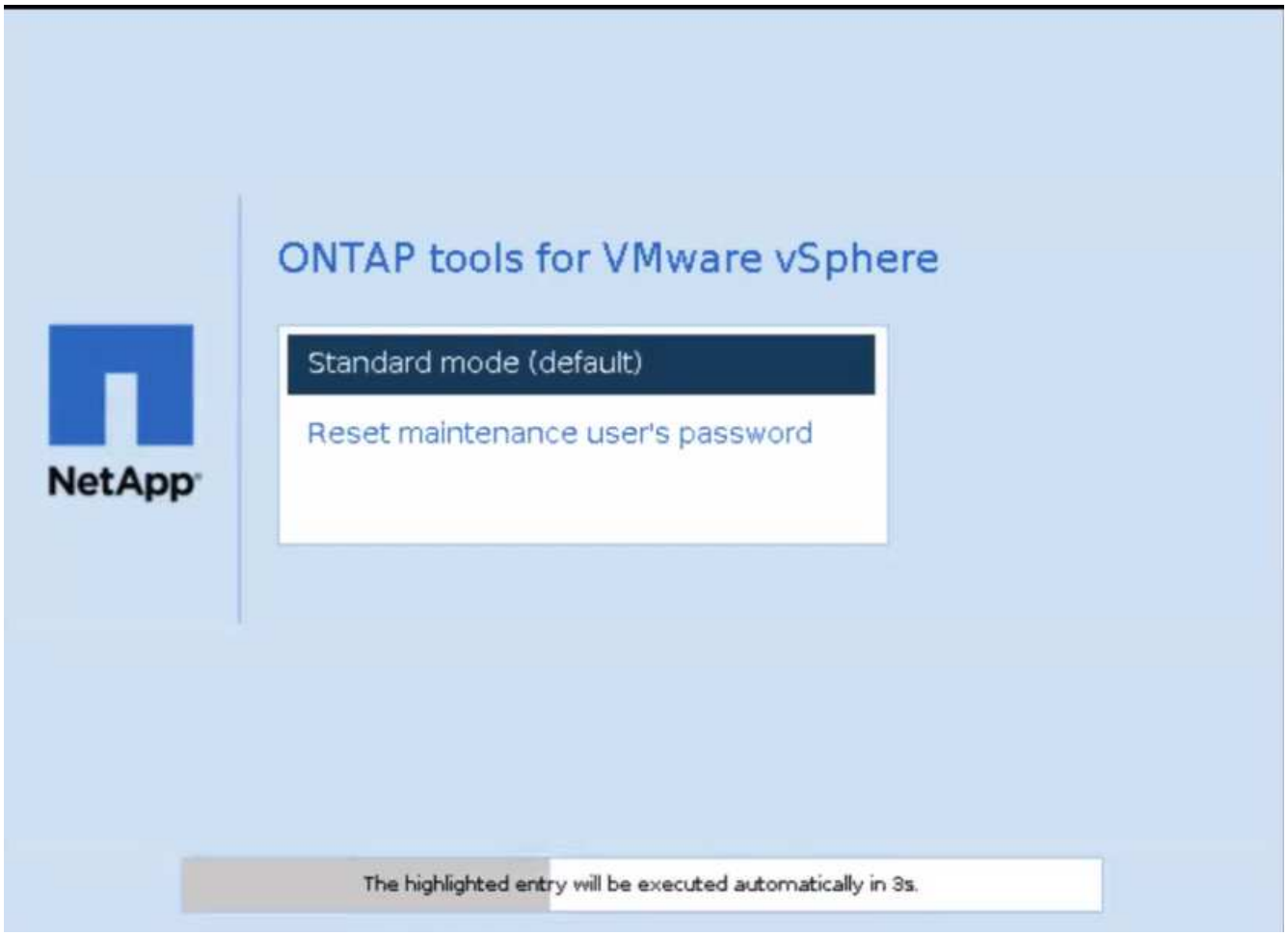
Reimposta la password utente della console di manutenzione

Durante il riavvio del sistema operativo guest, il menu di grub visualizza un'opzione per reimpostare la password utente della console di manutenzione. Questa opzione viene utilizzata per aggiornare la password utente della console di manutenzione presente sulla VM corrispondente. Una volta completata la reimpostazione della password, la VM si riavvia per impostare la nuova password. In uno scenario di distribuzione HA, dopo il riavvio della VM, la password viene aggiornata automaticamente sulle altre due VM.

> Per gli ONTAP tools for VMware vSphere HA, è necessario modificare la password utente della console di manutenzione sul primo nodo, ovvero node1.

Passi

1. Accedi al tuo vCenter Server
2. Fare clic con il pulsante destro del mouse sulla VM e selezionare **Power** > **Restart Guest OS**. Durante il riavvio del sistema, verrà visualizzata la seguente schermata:



Hai 5 secondi per scegliere la tua opzione. Premere un tasto qualsiasi per interrompere l'avanzamento e bloccare il menu di GRUB.

3. Selezionare l'opzione **Reimposta password utente manutenzione**. Si apre la console di manutenzione.
4. Nella console, inserisci i dettagli della nuova password. Per reimpostare correttamente la password, i dati della nuova password e della nuova password devono corrispondere. Hai tre possibilità per inserire la password corretta. Il sistema si riavvia dopo aver inserito correttamente la nuova password.
5. Premi Invio per continuare. La password viene aggiornata sulla VM.

> Lo stesso menu GRUB viene visualizzato anche durante l'accensione della VM. Tuttavia, dovresti utilizzare l'opzione di reimpostazione della password solo con l'opzione **Riavvia il sistema operativo guest**.

Gestire la protezione del cluster host

Modifica il cluster host protetto

È possibile eseguire le seguenti attività come parte della protezione dalle modifiche. È possibile eseguire tutte le modifiche nello stesso flusso di lavoro.

- Aggiungere nuovi datastore o host al cluster protetto.
- Aggiungere nuove relazioni SnapMirror alle impostazioni di protezione.

- Eliminare le relazioni SnapMirror esistenti dalle impostazioni di protezione.
- Modifica una relazione SnapMirror esistente.

Monitorare la protezione del cluster host

Utilizzare questa procedura per monitorare lo stato della protezione del cluster host. È possibile monitorare ogni cluster host protetto insieme al suo stato di protezione, alle relazioni SnapMirror , ai datastore e allo stato SnapMirror corrispondente.

Passi

1. Accedi al client vSphere.
2. Passare a **Strumenti NetApp ONTAP * > *Protezione** > **Relazioni tra cluster host**.

   L'icona sotto la colonna di protezione mostra lo stato della protezione

3. Passa il mouse sull'icona per visualizzare maggiori dettagli.

Aggiungi nuovi datastore o host

Utilizzare questa procedura per proteggere i datastore o gli host appena aggiunti. È possibile aggiungere nuovi host al cluster protetto o creare nuovi datastore sul cluster host utilizzando l'interfaccia utente nativa di vCenter.

Passi

1. Accedi al client vSphere.
2. Per modificare le proprietà di un cluster protetto, è possibile:
   a. Passare a **Strumenti NetApp ONTAP * > *Protezione** > **Relazioni cluster host**, selezionare il menu con i puntini di sospensione rispetto al cluster e selezionare **Modifica** o
   b. Fare clic con il pulsante destro del mouse su un cluster host e selezionare **Strumenti NetApp ONTAP * > *Proteggi cluster**.
3. Se hai creato un datastore nell'interfaccia utente nativa di vCenter, tale datastore viene visualizzato come non protetto. L'interfaccia utente mostra tutti i datastore nel cluster e il loro stato di protezione in una finestra di dialogo. Selezionare il pulsante **Proteggi** per abilitare la protezione completa.
4. Se hai aggiunto un nuovo host ESXi, lo stato di protezione viene visualizzato come parzialmente protetto. Selezionare il menu con i puntini di sospensione nelle impostazioni SnapMirror e selezionare **Modifica** per impostare la prossimità dell'host ESXi appena aggiunto.

   > In caso di relazione di tipo asincrono, l'azione di modifica non è supportata perché non è possibile aggiungere la SVM di destinazione per il sito terziario alla stessa istanza degli strumenti ONTAP . Tuttavia, è possibile utilizzare il gestore di sistema o l'interfaccia a riga di comando della SVM di destinazione per modificare la configurazione della relazione.

5. Dopo aver apportato le modifiche necessarie, selezionare **Salva**.
6. È possibile visualizzare le modifiche nella finestra **Proteggi cluster**.

Viene creata un'attività vCenter ed è possibile monitorarne l'avanzamento nel pannello **Attività recente**.

Aggiungi una nuova relazione SnapMirror

Passi

1. Accedi al client vSphere.
2. Per modificare le proprietà di un cluster protetto, è possibile:
   a. Passare a **Strumenti NetApp ONTAP * > *Protezione** > **Relazioni cluster host**, selezionare il menu con i puntini di sospensione rispetto al cluster e selezionare **Modifica** o
   b. Fare clic con il pulsante destro del mouse su un cluster host e selezionare **Strumenti NetApp ONTAP * > *Proteggi cluster**.
3. Seleziona **Aggiungi relazione**.
4. Aggiungere una nuova relazione come tipo di policy **Asincrona** o **AutomatedFailOverDuplex**.
5. Seleziona **Proteggi**.

   È possibile visualizzare le modifiche nella finestra **Proteggi cluster**.

Viene creata un'attività vCenter ed è possibile monitorarne l'avanzamento nel pannello **Attività recente**.

Elimina una relazione SnapMirror esistente

Per eliminare una relazione SnapMirror asincrona, è necessario aggiungere un sito secondario SVM o un cluster come backend di archiviazione sugli ONTAP tools for VMware vSphere. Non è possibile eliminare tutte le relazioni SnapMirror . Quando si elimina una relazione, viene rimossa anche la rispettiva relazione sul cluster ONTAP . Quando si elimina una relazione AutomatedFailOverDuplex SnapMirror , i datastore sulla destinazione vengono rimossi e il gruppo di coerenza, i LUN, i volumi e gli igroup vengono rimossi dal cluster ONTAP di destinazione.

L'eliminazione della relazione attiva una nuova scansione sul sito secondario per rimuovere la LUN non mappata come percorso attivo dagli host.

Passi

1. Accedi al client vSphere.
2. Per modificare le proprietà di un cluster protetto, è possibile:
   a. Passare a **Strumenti NetApp ONTAP * > *Protezione** > **Relazioni cluster host**, selezionare il menu con i puntini di sospensione rispetto al cluster e selezionare **Modifica** o
   b. Fare clic con il pulsante destro del mouse su un cluster host e selezionare **Strumenti NetApp ONTAP * > *Proteggi cluster**.
3. Selezionare il menu con i puntini di sospensione nelle impostazioni SnapMirror e selezionare **Elimina**.

Viene creata un'attività vCenter ed è possibile monitorarne l'avanzamento nel pannello **Attività recente**.

Modificare una relazione SnapMirror esistente

Per modificare una relazione SnapMirror asincrona, è necessario aggiungere un sito secondario SVM o un cluster come backend di archiviazione sugli ONTAP tools for VMware vSphere. Se si tratta di una relazione AutomatedFailOverDuplex SnapMirror , è possibile modificare la prossimità dell'host in caso di configurazione uniforme e l'accesso all'host in caso di configurazione non uniforme. Non è possibile scambiare i tipi di policy Asynchronous e AutomatedFailOverDuplex. È possibile impostare la prossimità o l'accesso per gli host appena scoperti sul cluster.

Non è possibile modificare una relazione SnapMirror asincrona esistente.

Passi

1. Accedi al client vSphere.
2. Per modificare le proprietà di un cluster protetto, è possibile:
   a. Passare a **Strumenti NetApp ONTAP * > *Protezione** > **Relazioni cluster host**, selezionare il menu con i puntini di sospensione rispetto al cluster e selezionare **Modifica** o
   b. Fare clic con il pulsante destro del mouse su un cluster host e selezionare **Strumenti NetApp ONTAP * > *Proteggi cluster**.
3. Se è selezionato il tipo di policy AutomatedFailOverDuplex, aggiungere i dettagli di prossimità dell'host o di accesso all'host.
4. Selezionare il pulsante **Proteggi**.

Viene creata un'attività vCenter ed è possibile monitorarne l'avanzamento nel pannello **Attività recente**.

Rimuovere la protezione del cluster host

Quando si rimuove la protezione del cluster host, i datastore non sono più protetti.

Passi

1. Per visualizzare i cluster host protetti, accedere a **Strumenti NetApp ONTAP * > *Protezione** > **Relazioni tra cluster host**.

   In questa pagina è possibile monitorare i cluster host protetti insieme al loro stato di protezione, alla relazione SnapMirror e al corrispondente stato SnapMirror .

2. Nella finestra **Protezione cluster host**, selezionare il menu con i puntini di sospensione in corrispondenza del cluster, quindi selezionare **Rimuovi protezione**.

Disabilita AutoSupport

Quando si configura il sistema di archiviazione per la prima volta, AutoSupport è abilitato per impostazione predefinita. Invia messaggi al supporto tecnico 24 ore dopo l'attivazione. Disattivando AutoSupport, non riceverai più supporto e monitoraggio proattivi.

Si consiglia di mantenere abilitato AutoSupport . Aiuta ad accelerare l'individuazione e la risoluzione dei problemi. Il sistema raccoglie le informazioni AutoSupport e le memorizza localmente, anche quando è disabilitato. Tuttavia, non invia il report ad alcuna rete.

Passi

1. Avviare ONTAP Tools Manager da un browser web:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con le credenziali di amministratore ONTAP tools for VMware vSphere fornite durante la distribuzione.
3. Selezionare l'opzione **Impostazioni** > **Telemetria** > **Modifica**.
4. Deselezionare l'opzione * AutoSupport* e salvare le modifiche.

Aggiorna l'URL del proxy AutoSupport

Aggiornare l'URL del proxy AutoSupport per garantire il corretto funzionamento della funzionalità AutoSupport negli scenari in cui un server proxy viene utilizzato per il controllo dell'accesso alla rete o per misure di sicurezza. Consente di instradare i dati AutoSupport tramite il proxy appropriato, garantendo la trasmissione sicura e la conformità.

Passi

1. Avviare ONTAP Tools Manager da un browser web: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con le credenziali di amministratore ONTAP tools for VMware vSphere fornite durante la distribuzione.
3. Seleziona **Impostazioni** dalla barra laterale.
4. Selezionare l'opzione **Impostazioni** > **Telemetria** > **Modifica**.
5. Inserisci un **URL proxy** valido e salva le modifiche.

   Se si disabilita AutoSupport, viene disabilitato anche l'URL proxy.

Aggiungi server NTP

Immettere i dettagli del server NTP per sincronizzare gli orologi dell'appliance degli strumenti ONTAP .

Passi

1. Avviare ONTAP Tools Manager da un browser web: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con le credenziali di amministratore ONTAP tools for VMware vSphere fornite durante la distribuzione.
3. Selezionare l'opzione **Impostazioni** > **Server NTP** > **Modifica**.
4. Immettere il nome di dominio completo (FQDN) separato da virgole, gli indirizzi IPv4 o IPv6.

   Aggiorna la schermata per visualizzare i valori aggiornati.

Crea un backup e ripristina la configurazione degli strumenti ONTAP

A partire dagli ONTAP tools for VMware vSphere 10.3, l'appliance utilizza un provisioner di storage dinamico, pertanto non è possibile raggiungere RPO pari a zero. Tuttavia, è possibile raggiungere un RPO prossimo allo zero. Per raggiungere un RPO prossimo allo zero, è necessario creare un backup della configurazione e ripristinarla su una nuova macchina virtuale.

Per migrare ad HA quando è abilitato il backup non HA, disabilitare prima il backup e riabilitarlo dopo la migrazione.

Crea un backup e scarica il file di backup

Passi

1. Dal vCenter Server, aprire la console di manutenzione.
2. Accedi come utente addetto alla manutenzione.
3. Entra `4` per selezionare **Supporto e diagnostica**.
4. Entra `3` per selezionare l'opzione **Abilita backup di sistema**.
5. In caso di non-HA, immettere le credenziali vCenter in cui è distribuita la macchina virtuale degli strumenti ONTAP .
6. Immettere un valore di frequenza di backup compreso tra 5 e 60 minuti.
7. Premi **Invio**

   In questo modo viene creato il backup e lo si invia al datastore della macchina virtuale a intervalli regolari.

8. Per accedere al backup, vai alla sezione di archiviazione e seleziona il datastore della macchina virtuale
9. Selezionare la sezione **File**.

   Nella sezione file puoi vedere la directory. Il nome della directory sarà l'indirizzo IP degli strumenti ONTAP in cui i punti (.) sono sostituiti da caratteri di sottolineatura, con suffisso *backup*.

10. Per ulteriori informazioni sul backup, scaricare il file backup_info.txt da **File** > **Download**.

Recuperare

Per ripristinare la configurazione, spegnere la macchina virtuale esistente e distribuire una nuova macchina virtuale utilizzando l'OVA utilizzato nella distribuzione iniziale.

È necessario utilizzare lo stesso indirizzo IP degli strumenti ONTAP per la nuova macchina virtuale e la configurazione del sistema, ad esempio servizi abilitati, dimensioni del nodo e modalità HA, deve essere la stessa della distribuzione iniziale.

Per ripristinare la configurazione dal file di backup, procedere come segue.

1. Dal vCenter Server, aprire la console di manutenzione.
2. Accedi come utente addetto alla manutenzione.
3. Entra `4` per selezionare **Supporto e diagnostica**.
4. Entra `2` per selezionare l'opzione **Abilita accesso diagnostico remoto** e creare una nuova password per l'accesso diagnostico.
5. Selezionare un backup qualsiasi dalla directory scaricata. Il nome del file di backup più recente è registrato nel file *backup_info.txt*.
6. Eseguire il comando seguente per copiare il backup sulla nuova macchina virtuale e immettere la password di diagnostica quando richiesto.

```
scp <Backup_X.tar.enc> diag@<node_ip>:/home/diag/system_recovery.tar.enc
```

> Non modificare il percorso di destinazione e il nome del file (/home/diag/system_recovery.tar.enc) indicati nel comando.

7. Dopo aver copiato il file di backup, accedi alla shell di diagnostica ed esegui il seguente comando:

```
sudo perl /home/maint/scripts/post-deploy-upgrade.pl -recovery
```

   I log vengono registrati nel file */var/log/post-deploy-upgrade.log*.

8. Dopo il ripristino riuscito, i servizi e gli oggetti vCenter vengono ripristinati.

Disinstallare gli ONTAP tools for VMware vSphere

La disinstallazione degli ONTAP tools for VMware vSphere elimina tutti i dati presenti negli strumenti.

Passi

1. Rimuovere o spostare tutte le macchine virtuali dagli ONTAP tools for VMware vSphere .
   - Per rimuovere le macchine virtuali, fare riferimento a "Rimuovere e registrare nuovamente le VM e i modelli di VM"
   - Per spostarli in un datastore non gestito, fare riferimento a "Come migrare la tua macchina virtuale con Storage vMotion"
2. "Elimina i datastore"creato su ONTAP tools for VMware vSphere.
3. Se hai abilitato il provider VASA, seleziona **Impostazioni** > **Impostazioni provider VASA** > **Annulla registrazione** negli strumenti ONTAP per annullare la registrazione dei provider VASA da tutti i server vCenter.
4. Disassociare tutti i backend di archiviazione dall'istanza di vCenter Server. Fare riferimento a "Dissociare i backend di archiviazione dall'istanza di vCenter Server" .
5. Elimina tutti i backend di archiviazione. Fare riferimento a "Gestire i backend di archiviazione" .
6. Rimuovere l'adattatore SRA da VMware Live Site Recovery:
   a. Accedere come amministratore all'interfaccia di gestione dell'appliance VMware Live Site Recovery utilizzando la porta 5480.
   b. Selezionare **Schede di replicazione dell'archiviazione**.
   c. Selezionare la scheda SRA appropriata e dal menu a discesa selezionare **Elimina**.
   d. Conferma di conoscere i risultati dell'eliminazione dell'adattatore e seleziona **Elimina**.
7. Eliminare le istanze del server vCenter integrate negli ONTAP tools for VMware vSphere. Fare riferimento a "Gestire le istanze di vCenter Server" .
8. Disattivare gli ONTAP tools for VMware vSphere dal vCenter Server ed eliminare le VM.

Cosa succederà adesso?

"Rimuovere i volumi FlexVol"

Rimuovere i volumi FlexVol

Quando si utilizza un cluster ONTAP dedicato per gli strumenti ONTAP per la distribuzione VMware, vengono creati molti volumi FlexVol inutilizzati. Dopo aver rimosso gli ONTAP tools for VMware vSphere, è necessario rimuovere i volumi FlexVol per evitare possibili impatti sulle prestazioni.

Passi

1. Determinare gli ONTAP tools for VMware vSphere dalla prima VM del nodo.

   cat /opt/netapp/meta/ansible_vars.yaml | grep -i protocollo

   Se si tratta di una distribuzione iSCSI, è necessario eliminare anche gli igroup.

2. Ottieni l'elenco dei volumi FlexVol .

   kubectl describe persistentvolumes | grep internalName | awk -F'=' '{print $2}'

3. Rimuovere le VM dal vCenter Server. Fare riferimento a "Rimuovere e registrare nuovamente le VM e i modelli di VM" .
4. Eliminare i volumi FlexVol . Fare riferimento a "Elimina un FlexVol volume" . Nel comando CLI per eliminare un volume, specificare il nome esatto dei volumi FlexVol .
5. Eliminare gli igroup SAN dal sistema di archiviazione ONTAP in caso di distribuzione iSCSI. Fare riferimento a "Visualizza e gestisci gli iniziatori SAN e gli igroup" .

Aggiorna gli ONTAP tools for VMware vSphere

Aggiornamento dagli ONTAP tools for VMware vSphere 10.x alla versione 10.4

È possibile effettuare l'aggiornamento dagli ONTAP tools for VMware vSphere 10.2 o 10.3 alla versione 10.4. Tuttavia, l'aggiornamento diretto dagli strumenti ONTAP 10.0 o 10.1 alla versione 10.4 non è supportato.

NOTA:

- Nei sistemi ASA r2, è necessario eseguire l'aggiornamento agli ONTAP tools for VMware vSphere 10.4 con ONTAP 9.16.1 prima di aggiungere altre zone di disponibilità dello storage (SAZ).
- Se l'aggiornamento dagli ONTAP tools for VMware vSphere 10.2 o 10.3 alla versione 10.4 non riesce, il rollback non è supportato. Per ripristinare la configurazione, utilizzare gli ONTAP tools for VMware vSphere 10.2 e il ripristino RPO prossimo allo zero o tramite snapshot per gli ONTAP tools for VMware vSphere 10.3.

Prima di iniziare

Per un aggiornamento non HA, spegnere la VM degli strumenti ONTAP e, per un aggiornamento HA, spegnere il primo nodo prima di apportare le seguenti modifiche alle impostazioni della macchina virtuale (VM).

Se si esegue l'aggiornamento dagli ONTAP tools for VMware vSphere 10.2 o 10.3, è necessario completare i seguenti passaggi prima di procedere con l'attività di aggiornamento: * Aggiungere un disco rigido aggiuntivo da 100 GB a ciascun nodo, poiché i dati di servizio sono archiviati localmente sulla VM. * Modificare la CPU e la memoria per la VM spenta in base al tipo di distribuzione. Abilitare il plug-in a caldo per CPU e RAM.

+

Tipo di distribuzione	CPU (core) per nodo	Memoria (GB) per nodo	Spazio su disco (GB) per nodo	CPU totale (core)	Memoria (GB)	Spazio totale su disco (GB)
Non-HA Piccolo	9	18	350	9	18	350
Mezzo non HA	13	26	350	13	26	350
HA Piccolo	9	18	350	27	54	1050
HA Medio	13	26	350	39	78	1050
HA Grande	17	34	350	51	102	1050

- Una volta apportate le modifiche, accendere la macchina virtuale e attendere che i servizi siano in esecuzione.
- In caso di distribuzione HA, apportare le modifiche alle risorse, abilitare il plug-in a caldo per CPU e RAM e aggiungere dischi rigidi da 100 GB anche per il secondo e il terzo nodo. Non è necessario riavviare questi nodi.
- Se l'appliance è stata distribuita come percorso locale (distribuzione semplice) con gli strumenti ONTAP 10.2, è necessario eseguire uno snapshot di quiesce prima dell'aggiornamento.

Se si esegue l'aggiornamento dagli ONTAP tools for VMware vSphere 10.0 alla versione 10.1, è necessario completare i seguenti passaggi prima di procedere con l'attività di aggiornamento: **Abilita diagnostica**

1. Dal vCenter Server, aprire una console per gli strumenti ONTAP .
2. Accedi come utente addetto alla manutenzione.
3. Immettere **4** per selezionare **Supporto e diagnostica**.
4. Immettere **2** per selezionare **Abilita accesso diagnostico remoto**.
5. Inserisci **y** per impostare la password che preferisci.
6. Accedere all'indirizzo IP della VM dal terminale/putty con l'utente 'diag' e la password impostata nel passaggio precedente.

Esegui un backup di MongoDB

Eseguire i seguenti comandi per eseguire un backup di MongoDB:

- kn exec -it ntv-mongodb-0 sh - kn è un alias di kubectl -n ntv-system.
- Eseguire il comando *env | grep MONGODB_ROOT_PASSWORD* all'interno del pod.
- Eseguire il comando *exit* per uscire dal pod.
- Eseguire il comando *kn exec ntv-mongodb-0 --mongodump -u root -p MONGODB_ROOT_PASSWORD --archive=/tmp/mongodb-backup.gz --gzip* per sostituire il set MONGO_ROOT_PASSWORD dal comando precedente.
- Eseguire il comando *kn cp ntv-mongodb-0:/tmp/mongodb-backup.gz ./mongodb-backup.gz* per copiare il backup di Mongodb creato utilizzando il comando precedente dal pod all'host.

Fai una foto istantanea di tutti i volumi

- Eseguire il comando 'kn get pvc' e salvare l'output del comando.
- Eseguire snapshot di tutti i volumi uno alla volta utilizzando uno dei seguenti metodi:
  - Da CLI, eseguire il comando *volume snapshot create -vserver <nome_vserver> -volume <nome_volume> -snapshot <nome_snapshot>*
  - Dall'interfaccia utente di ONTAP System Manager, cercare il volume in base al suo nome nella barra di ricerca, quindi aprire il volume selezionando il nome. Vai allo snapshot e aggiungi lo snapshot di quel volume.

Eseguire l'istantanea degli ONTAP tools for VMware vSphere in vCenter (3 VM in caso di distribuzione HA, 1 VM in caso di distribuzione non HA)

- Nell'interfaccia utente del client vSphere, selezionare la VM.
- Vai alla scheda snapshot e seleziona il pulsante **Scatta snapshot**. Acquisisci uno snapshot inattivo della VM. Fare riferimento a "Scatta un'istantanea di una macchina virtuale" per i dettagli.

Prima di eseguire l'aggiornamento, eliminare i pod completati dal bundle di log con il prefisso "generate-support-bundle-job". Se è in corso la generazione del bundle di supporto, attendere il completamento, quindi eliminare il pod.

Per qualsiasi tipo di aggiornamento, è necessario aggiungere un ulteriore disco rigido (HDD) da 100 GB. Per aggiungere un HDD, eseguire la seguente operazione.

1. Selezionare la VM nella configurazione a nodo singolo o tutte e tre le VM nella configurazione HA.

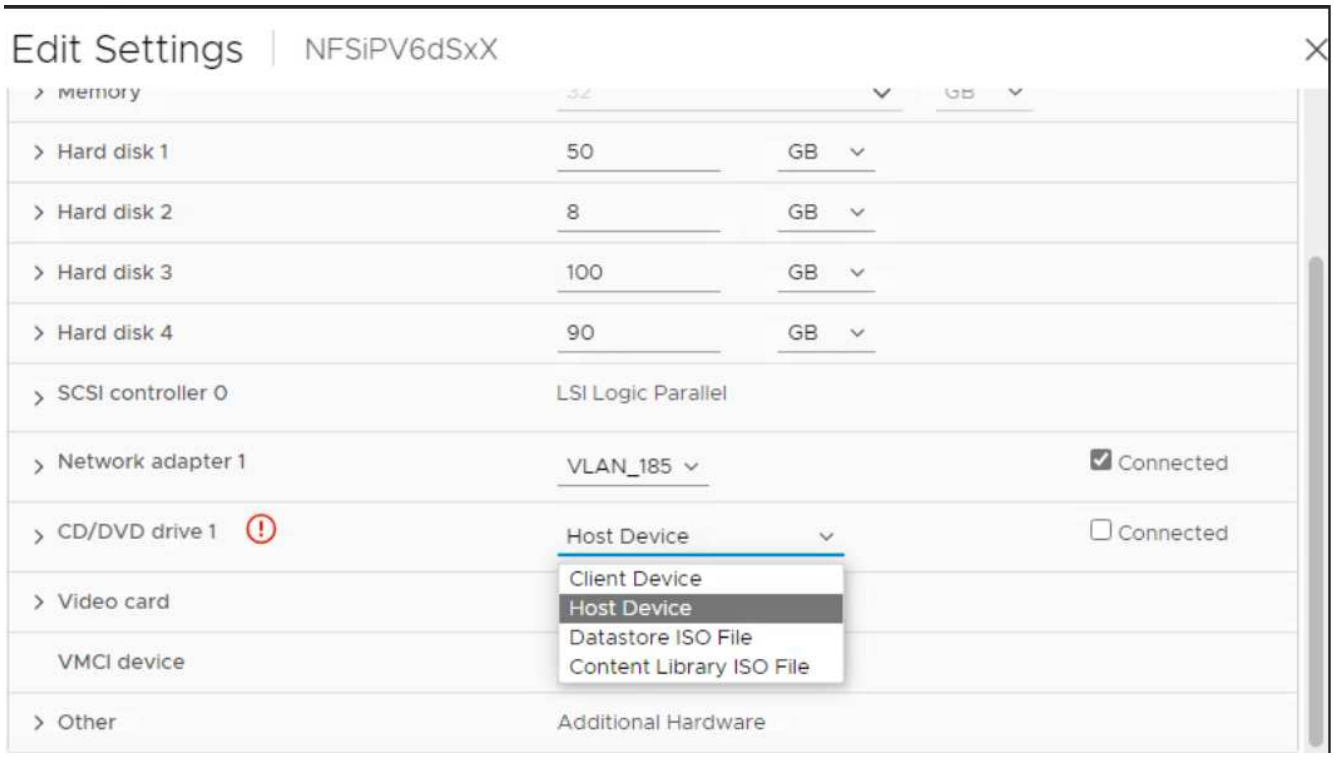
2. Fare clic con il pulsante destro del mouse sulla/e VM e selezionare **Aggiungi nuovo dispositivo** > **Disco rigido**
3. Aggiungere un HDD da 100 GB nel campo **Nuovo disco rigido**.
4. Seleziona **Applica**

Dopo aver aggiunto il disco rigido, aggiornare le risorse della VM per le rispettive configurazioni e riavviare la VM primaria.

Verrà creato un nuovo HDD. Il provisioner di archiviazione dinamica utilizza questo HDD per generare o replicare i volumi.

Passi

1. Carica gli ONTAP tools for VMware vSphere nella libreria dei contenuti.
2. Nella pagina della VM primaria, seleziona **Azioni** > **Modifica impostazioni**
3. Selezionare il file ISO della libreria di contenuti nella finestra di modifica delle impostazioni nel campo **Unità CD/DVD**.
4. Selezionare il file ISO e fare clic su **OK**. Selezionare la casella di controllo Connesso nel campo **Unità CD/DVD**.



5. Dal vCenter Server, aprire una console per gli strumenti ONTAP .
6. Accedi come utente addetto alla manutenzione.
7. Immettere **3** per selezionare il menu Configurazione di sistema.
8. Immettere **7** per selezionare l'opzione di aggiornamento.
9. Quando esegui l'aggiornamento, vengono eseguite automaticamente le seguenti azioni:
   a. Aggiornamento del certificato
   b. Aggiornamento remoto del plug-in

Dopo aver eseguito l'aggiornamento agli ONTAP tools for VMware vSphere 10.4, è possibile:

- Disabilitare i servizi dall'interfaccia utente del gestore
- Passare da una configurazione non HA a una configurazione HA
- Passare da una configurazione non-HA piccola a una configurazione non-HA media o a una configurazione HA media o grande.
- In caso di aggiornamento non HA, riavviare la VM degli strumenti ONTAP per riflettere le modifiche. In caso di aggiornamento HA, riavviare il primo nodo per riflettere le modifiche sul nodo.

Cosa c'è dopo?

Dopo aver eseguito l'aggiornamento dalle versioni precedenti degli ONTAP tools for VMware vSphere alla versione 10.4, eseguire nuovamente la scansione degli adattatori SRA per verificare che i dettagli siano aggiornati nella pagina Adattatori VMware Live Site Recovery Storage Replication.

Dopo aver eseguito correttamente l'aggiornamento, eliminare manualmente i volumi Trident da ONTAP utilizzando la seguente procedura:

> Questi passaggi non sono necessari se gli ONTAP tools for VMware vSphere 10.1 o 10.2 erano in configurazioni non HA di piccole o medie dimensioni (percorso locale).

1. Dal vCenter Server, aprire una console per gli strumenti ONTAP .
2. Accedi come utente addetto alla manutenzione.
3. Immettere **4** per selezionare il menu **Supporto e diagnostica**.
4. Immettere **1** per selezionare l'opzione **Accesso alla shell di diagnostica**.
5. Esegui il seguente comando

```
sudo python3 /home/maint/scripts/ontap_cleanup.py
```

6. Inserisci il nome utente e la password ONTAP

In questo modo vengono eliminati tutti i volumi Trident in ONTAP utilizzati negli ONTAP tools for VMware vSphere 10.1/10.2.

Informazioni correlate

"Migrazione dagli ONTAP tools for VMware vSphere 9.xx a 10.4"

Codici di errore di aggiornamento

Potrebbero verificarsi codici di errore durante l'operazione di aggiornamento ONTAP tools for VMware vSphere . I codici di errore sono lunghi cinque cifre: le prime due rappresentano lo script che ha riscontrato il problema, mentre le ultime tre rappresentano il flusso di lavoro specifico all'interno di quello script.

Tutti i log degli errori vengono registrati nel file ansible-perl-errors.log per facilitare il monitoraggio e la risoluzione dei problemi. Questo file di registro contiene il codice di errore e l'attività Ansible non riuscita.

> I codici di errore forniti in questa pagina sono solo a scopo di riferimento. Se l'errore persiste o se non viene indicata alcuna soluzione, contattare il team di supporto.

Nella tabella seguente sono elencati i codici di errore e i nomi dei file corrispondenti.

Codice di errore	Nome dello script
00	firstboot-network-config.pl, modalità di distribuzione
01	firstboot-network-config.pl, aggiornamento della modalità
02	firstboot-inputs-validation.pl
03	firstboot-deploy-otv-ng.pl, distribuzione, HA
04	firstboot-deploy-otv-ng.pl, distribuzione, non HA
05	firstboot-deploy-otv-ng.pl, riavvio
06	firstboot-deploy-otv-ng.pl, aggiornamento, HA
07	firstboot-deploy-otv-ng.pl, aggiornamento, non-HA
08	firstboot-otv-recovery.pl
09	post-deploy-upgrade.pl

Le ultime tre cifre del codice di errore indicano l'errore specifico del flusso di lavoro all'interno dello script:

Codice di errore di aggiornamento	Flusso di lavoro	Risoluzione
052	L'ISO potrebbe essere uguale alla versione corrente o due release superiori rispetto alla versione corrente.	Utilizza una versione ISO compatibile per effettuare l'aggiornamento dalla tua versione attuale.
068	Il rollback dei pacchetti Debian non è riuscito	Utilizzare il ripristino basato su RPO zero o snapshot e riprovare l'aggiornamento.
069	Ripristino dei file non riuscito	Utilizzare il ripristino basato su RPO zero o snapshot e riprovare l'aggiornamento.
070	Eliminazione del backup non riuscita	-
071	Il cluster Kubernetes non era in buone condizioni	-
074	Il montaggio ISO non è riuscito	Controllare /var/log/upgrade-run.log e riprovare l'aggiornamento.
075	I controlli preliminari dell'aggiornamento non sono riusciti	Riprovare l'aggiornamento.
076	L'aggiornamento del registro non è riuscito	Utilizzare il ripristino basato su RPO zero o snapshot e riprovare l'aggiornamento.

Codice di errore di aggiornamento	Flusso di lavoro	Risoluzione
077	Il rollback del registro non è riuscito	Utilizzare il ripristino basato su RPO zero o snapshot e riprovare l'aggiornamento.
078	L'aggiornamento dell'operatore non è riuscito	Utilizzare il ripristino basato su RPO zero o snapshot e riprovare l'aggiornamento.
079	Il rollback dell'operatore non è riuscito	Utilizzare il ripristino basato su RPO zero o snapshot e riprovare l'aggiornamento.
080	L'aggiornamento dei servizi non è riuscito	Utilizzare il ripristino basato su RPO zero o snapshot e riprovare l'aggiornamento.
081	Il rollback dei servizi non è riuscito	Utilizzare il ripristino basato su RPO zero o snapshot e riprovare l'aggiornamento.
082	Eliminazione delle vecchie immagini dal contenitore non riuscita	Utilizzare il ripristino basato su RPO zero o snapshot e riprovare l'aggiornamento.
083	L'eliminazione del backup non è riuscita	Utilizzare il ripristino basato su RPO zero o snapshot e riprovare l'aggiornamento.
084	Impossibile ripristinare JobManager su Produzione	Per ripristinare/completare l'aggiornamento, seguire i passaggi indicati di seguito. 1. Abilita Diagnostic Shell 2. Eseguire il comando: *sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postupgrade* 3. Controllare i registri in /var/log/post-deploy-upgrade.log
087	I passaggi successivi all'aggiornamento non sono riusciti.	Per ripristinare/completare l'aggiornamento, procedere come segue. 1. Abilita Diagnostic Shell 2. Eseguire il comando *sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postupgrade* 3. Controllare i registri in /var/log/post-deploy-upgrade.log
088	La configurazione della rotazione dei log per journald non è riuscita	Verificare che le impostazioni di rete della VM siano compatibili con l'host su cui è ospitata la VM. Puoi provare a migrare la VM su un altro host e riavviare.

Codice di errore di aggiornamento	Flusso di lavoro	Risoluzione
089	La modifica della proprietà del file di configurazione di rotazione del registro di riepilogo non è riuscita	Riprovare l'aggiornamento.
095	Aggiornamento del sistema operativo non riuscito	Nessun ripristino per l'aggiornamento del sistema operativo. I servizi degli strumenti ONTAP vengono aggiornati e saranno operativi nuovi pod.
096	Installa il provisioner di archiviazione dinamica	Controllare i registri di aggiornamento e riprovare l'aggiornamento.
097	La disinstallazione dei servizi per l'aggiornamento non è riuscita	Utilizzare un ripristino basato su RPO zero o snapshot e riprovare l'aggiornamento.
098	la copia del segreto dockercred da ntv-system allo spazio dei nomi del provisioner di archiviazione dinamica non è riuscita	Controllare i registri di aggiornamento e riprovare l'aggiornamento.
099	Impossibile convalidare l'aggiunta del nuovo HDD	Aggiungere il nuovo HDD a tutti i nodi in caso di HA e a un nodo in caso di distribuzione non HA.
108	Script di seeding non riuscito	-
109	il backup dei dati del volume persistente non è riuscito	Controllare i registri di aggiornamento e riprovare l'aggiornamento.
110	il ripristino dei dati del volume persistente non è riuscito	Utilizzare il ripristino basato su RPO zero o snapshot e riprovare l'aggiornamento.
111	L'aggiornamento dei parametri di timeout etcd per RKE2 non è riuscito	Controllare i registri di aggiornamento e riprovare l'aggiornamento.
112	La disinstallazione del provisioner di archiviazione dinamica non è riuscita	-
113	L'aggiornamento delle risorse sui nodi secondari non è riuscito	Controllare i registri di aggiornamento e riprovare l'aggiornamento.
104	Il riavvio del nodo secondario non è riuscito	Riavviare manualmente i nodi uno per uno
100	il rollback del kernel non è riuscito	-
051	l'aggiornamento del provisioner di archiviazione dinamica non è riuscito	Controllare i registri di aggiornamento e riprovare l'aggiornamento.

Codice di errore di aggiornamento	Flusso di lavoro	Risoluzione
056	l'eliminazione del backup della migrazione non è riuscita	N / A

A partire dagli ONTAP tools for VMware vSphere 10.3, l'RPO zero non è supportato.

Scopri di più su "Come ripristinare gli ONTAP tools for VMware vSphere se l'aggiornamento dalla versione 10.0 alla 10.1 non riesce"

Migrare gli ONTAP tools for VMware vSphere 9.xx a 10.4

Migrazione dagli ONTAP tools for VMware vSphere 9.xx a 10.4

Lo spostamento degli strumenti NetApp ONTAP tools for VMware vSphere dalla versione 9.xx alla 10.x richiede un processo di migrazione a causa degli aggiornamenti e dei miglioramenti significativi del prodotto nelle diverse versioni.

È possibile migrare dagli ONTAP tools for VMware vSphere 9.12D1, 9.13D2 e 9.13P2 agli ONTAP tools for VMware vSphere 10.4.

Se nella configurazione sono presenti datastore NFS e VMFS e nessun datastore vVols , è sufficiente disinstallare ONTAP Tools 9.xx e distribuire ONTAP Tools 10.x. Tuttavia, se la configurazione contiene datastore vVols , sarà necessario eseguire un processo di migrazione del provider VASA e dell'SRA.

La tabella seguente descrive il processo di migrazione in questi due diversi scenari.

*Se la configurazione ha datastore vVols *	Se la configurazione contiene solo datastore NFS e VMFS
Passaggi: 1. "Migrare il provider VASA" 2. "Creare criteri di archiviazione VM"	Passaggi: 1. Rimuovere gli strumenti ONTAP 9.xx dal proprio ambiente. Fare riferimento a "Come rimuovere OTV 9.xx dal tuo ambiente" Articolo della Knowledge Base NetApp . 2. "Distribuisci e configura gli ONTAP tools for VMware vSphere 10.4" 3. "Aggiorna l'SRA" 4. "Creare criteri di archiviazione VM"

Dopo la migrazione dagli ONTAP tools for VMware vSphere 9.xx alla versione 10.4, i datastore vVols che utilizzano il protocollo NVMe/FC diventano non operativi perché gli strumenti ONTAP 10.4 supportano il protocollo NVMe-oF solo con i datastore VMFS.

Migrare il provider VASA e aggiornare l'SRA

Passaggi per migrare il provider VASA

1. Per abilitare Derby PORT 1527 sugli ONTAP tools for VMware vSphere, abilitare l'utente root e accedere alla CLI tramite SSH. Quindi, esegui il seguente comando:

   ```
   iptables -I INPUT 1 -p tcp --dport 1527 -j ACCEPT
   ```

2. Distribuisci OVA per gli ONTAP tools for VMware vSphere 10.4.
3. Aggiungere l'istanza di vCenter Server che si desidera migrare agli ONTAP tools for VMware vSphere 10.4. Fare riferimento a "Aggiungi un'istanza di vCenter Server" per maggiori informazioni.
4. Integrare localmente il backend di archiviazione dalle API del server vCenter per il plug-in degli strumenti ONTAP .

5. Per effettuare la migrazione, emettere la seguente API da Swagger o in Postman.

   arricciatura -X POST `https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/{vcguid}/migration-jobs`

   Puoi accedere a Swagger tramite questo URL: `https://$FQDN_IP_PORT/', for example: `\https://10.67.25.33:8443 .`

   Metodo HTTP ed endpoint

   Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Sentiero
INVIARE	/api/v1

   Tipo di elaborazione

   Asincrono

   Esempio di ricciolo

   curl -X POST'https://<OTV-NG-IP>:8443/virtualization/api/v1/vcenters/<vcguid>/migration-jobs' \ --header 'x-auth: <auth_token>' \ --header 'Content-Type: application/json' \ --data '{ "otv_ip": "xx.xx.xx.xx", "vasa_provider_credentials": { "username": "xxxxx", "password": "" }, "database_password": "" }'

   Corpo della richiesta per la migrazione di altre versioni:

   { "otv_ip": "xx.xx.xx.xx", "vasa_provider_credentials": { "username": "xxxxx", "password": "*" } }

   Esempio di output JSON

   Viene restituito un oggetto lavoro. Dovresti salvare l'identificativo del lavoro per utilizzarlo nel passaggio successivo.

   { "id": 123, "migration_id": "d50073ce-35b4-4c51-9d2e-4ce66f802c35", "status": "in esecuzione" }

6. Per verificare lo stato, utilizzare il seguente URI in Swagger:

   ```
   curl `\https://xx.xx.xx.xxx:8443/virtualization/api/jobmanager/v2/jobs/<JobID>?includeSubJobsAndTasks=true`
   ```

   Dopo aver completato il lavoro, rivedere il report di migrazione. Questo report è incluso nei dati del lavoro ed è accessibile dalla risposta al lavoro.

7. Aggiungere gli ONTAP tools for VMware vSphere al vCenter Server e"Registra il fornitore VASA" con ONTAP tools for VMware vSphere.

8. "Abilita il provider VASA"servizio sugli ONTAP tools for VMware vSphere 10.4.
9. Arrestare gli ONTAP tools for VMware vSphere Storage Provider 9.10/9.11/9.12/9.13 VASA Provider dalla console di manutenzione.

   Non eliminare il fornitore VASA.

   Dopo l'arresto del vecchio provider VASA, il vCenter Server esegue il failover sugli ONTAP tools for VMware vSphere. Tutti i datastore e le VM diventano accessibili e vengono gestiti dagli ONTAP tools for VMware vSphere.

10. I datastore NFS e VMFS migrati dagli ONTAP tools for VMware vSphere 9.xxx sono visibili negli ONTAP tools for VMware vSphere 10.4 solo dopo l'attivazione del processo di individuazione del datastore, che potrebbe richiedere fino a 30 minuti. Verificare che i datastore siano visibili nella pagina di panoramica degli strumenti ONTAP per la pagina dell'interfaccia utente del plugin VMware vSphere.
11. Eseguire la migrazione delle patch utilizzando la seguente API in Swagger o in Postman:

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Sentiero
TOPPA	/api/v1

Tipo di elaborazione

Asincrono

Esempio di ricciolo

arricciatura -X PATCH `https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/56d373bd-4163-44f9-a872-9adabb008ca9/migration-jobs/84dr73bd-9173-65r7-w345-8ufdbb887d43`

Esempio di output JSON

Viene restituito un oggetto lavoro. Dovresti salvare l'identificativo del lavoro per utilizzarlo nel passaggio successivo.

{ "id": 123, "migration_id": "d50073ce-35b4-4c51-9d2e-4ce66f802c35", "status": "in esecuzione" }

Il corpo della richiesta è vuoto per l'operazione di patch.

> UUID è l'UUID di migrazione restituito in risposta all'API post-migrazione.

Dopo aver eseguito l'API di migrazione delle patch, tutte le VM saranno conformi ai criteri di archiviazione.

Cosa c'è dopo?

Dopo aver completato la migrazione e registrato gli strumenti ONTAP 10.4 su vCenter Server, seguire questi passaggi:

- Attendi il completamento di **Discovery**, i certificati verranno aggiornati automaticamente su tutti gli host.
- Attendere un tempo sufficiente prima di avviare le operazioni del datastore e della macchina virtuale. Il periodo di attesa richiesto varia in base al numero di host, datastore e macchine virtuali nella configurazione. La mancata attesa potrebbe causare errori operativi intermittenti.

Dopo l'aggiornamento, se lo stato di conformità della macchina virtuale non è aggiornato, riapplicare i criteri di archiviazione seguendo i passaggi seguenti:

1. Accedere al datastore e selezionare **Riepilogo** > **Criteri di archiviazione VM**.

   Lo stato di conformità in **Conformità ai criteri di archiviazione delle VM** è **Obsoleto**.

2. Selezionare il criterio VM di archiviazione e la VM corrispondente
3. Seleziona **Applica**

   Lo stato di conformità in **Conformità ai criteri di archiviazione delle VM** ora viene visualizzato come conforme.

Informazioni correlate

- "Scopri di più sugli ONTAP tools for VMware vSphere 10 RBAC"
- "Aggiornamento dagli ONTAP tools for VMware vSphere 10.x alla versione 10.4"

Passaggi per aggiornare l'adattatore di replicazione dello storage (SRA)

Prima di iniziare

Nel piano di ripristino, il sito protetto si riferisce alla posizione in cui le VM sono attualmente in esecuzione, mentre il sito di ripristino è quello in cui le VM verranno ripristinate. L'interfaccia SRM visualizza lo stato del piano di ripristino con dettagli sui siti protetti e di ripristino. Nel piano di ripristino, i pulsanti **CleanupP** e **Reprotect** sono disabilitati, mentre i pulsanti TEST ed ESEGUI rimangono abilitati. Ciò indica che il sito è pronto per il ripristino dei dati. Prima di migrare l'SRA, verificare che un sito sia in stato protetto e l'altro in stato di ripristino.

> Non avviare la migrazione se il failover è stato completato ma la nuova protezione è in sospeso. Assicurarsi che il processo di riprotezione sia completato prima di procedere con la migrazione. Se è in corso un failover di prova, pulire il failover di prova e avviare la migrazione.

1. Seguire questi passaggi per eliminare l'adattatore SRA degli strumenti ONTAP per VMware vSphere 9.xx in VMware Site Recovery:
   a. Vai alla pagina di gestione della configurazione di VMware Live Site Recovery
   b. Vai alla sezione **Storage Replication Adapter**.
   c. Dal menu con i puntini di sospensione selezionare **Reimposta configurazione**.
   d. Dal menu con i puntini di sospensione selezionare **Elimina**.
2. Eseguire questi passaggi sia sui siti di protezione che su quelli di ripristino.
   a. "Abilita gli ONTAP tools for VMware vSphere"
   b. Installare gli ONTAP tools for VMware vSphere 10.4 SRA seguendo i passaggi in"Configurare SRA sull'appliance VMware Live Site Recovery" .
   c. Nella pagina dell'interfaccia utente di VMware Live Site Recovery, eseguire le operazioni **Discover Arrays** e **Discover Devices** e confermare che i dispositivi siano visualizzati come prima della

migrazione.

Automatizzare utilizzando l’API REST

Scopri di più sugli ONTAP tools for VMware vSphere 10 REST API

ONTAP tools for VMware vSphere 10 è un set di strumenti per la gestione del ciclo di vita delle macchine virtuali. Include una solida API REST che puoi utilizzare come parte dei tuoi processi di automazione.

Fondazione dei servizi web REST

Representational State Transfer (REST) è uno stile per la creazione di applicazioni web distribuite, inclusa la progettazione di API di servizi web. Stabilisce una serie di tecnologie per esporre le risorse basate su server e gestirne gli stati.

Risorse e rappresentanza statale

Le risorse sono i componenti fondamentali di un’applicazione di servizi Web REST. Quando si progetta un’API REST, ci sono due importanti attività iniziali:

- Identificare le risorse basate sul sistema o sul server
- Definire gli stati delle risorse e le operazioni di transizione di stato associate

Le applicazioni client possono visualizzare e modificare gli stati delle risorse tramite flussi di messaggi ben definiti.

Messaggi HTTP

Hypertext Transfer Protocol (HTTP) è il protocollo utilizzato dal client e dal server dei servizi Web per scambiare messaggi sulle risorse. Segue il modello CRUD basato sulle operazioni generiche di creazione, lettura, aggiornamento ed eliminazione. Il protocollo HTTP include intestazioni di richiesta e risposta, nonché codici di stato della risposta.

Formattazione dei dati JSON

Sebbene siano disponibili diversi formati di messaggio, l’opzione più diffusa è JavaScript Object Notation (JSON). JSON è uno standard industriale per la rappresentazione di strutture dati semplici in testo normale e viene utilizzato per trasferire informazioni sullo stato che descrivono le risorse e le azioni desiderate.

Sicurezza

La sicurezza è un aspetto importante di una API REST. Oltre al protocollo Transport Layer Security (TLS) utilizzato per proteggere il traffico HTTP sulla rete, gli ONTAP tools for VMware vSphere 10 REST API utilizzano anche token di accesso per l’autenticazione. È necessario acquisire un token di accesso e utilizzarlo nelle successive chiamate API.

Supporto per richieste asincrone

Gli ONTAP tools for VMware vSphere 10 REST API eseguono la maggior parte delle richieste in modo sincrono, restituendo un codice di stato al termine dell’operazione. Supporta anche l’elaborazione asincrona per le attività che richiedono più tempo per essere completate.

Ambiente di gestione degli strumenti ONTAP

Ci sono diversi aspetti dell’ambiente ONTAP Tools Manager che dovresti prendere in considerazione.

Macchina virtuale

Gli ONTAP tools for VMware vSphere 10 vengono distribuiti utilizzando l'architettura del plug-in remoto vSphere. Il software, incluso il supporto per l'API REST, viene eseguito in una macchina virtuale separata.

Indirizzo IP degli strumenti ONTAP

Gli ONTAP tools for VMware vSphere 10 espongono un singolo indirizzo IP che fornisce un gateway per le funzionalità della macchina virtuale. È necessario fornire l'indirizzo durante la configurazione iniziale e questo viene assegnato a un componente di bilanciamento del carico interno. L'indirizzo viene utilizzato dall'interfaccia utente di ONTAP Tools Manager e per accedere direttamente alla pagina della documentazione di Swagger e all'API REST.

Due API REST

Oltre agli ONTAP tools for VMware vSphere 10 REST API, il cluster ONTAP dispone di una propria REST API. ONTAP Tools Manager utilizza l'API REST ONTAP come client per eseguire attività relative all'archiviazione. È importante tenere presente che queste due API sono separate e distinte. Per ulteriori informazioni, consulta "Automazione ONTAP" .

Dettagli di implementazione per gli ONTAP tools for VMware vSphere 10 REST API

Sebbene REST stabilisca un insieme comune di tecnologie e best practice, l'implementazione esatta di ciascuna API può variare in base alle scelte di progettazione. Prima di utilizzare gli ONTAP tools for VMware vSphere 10 REST API, è necessario avere familiarità con la progettazione.

L'API REST include diverse categorie di risorse, come vCenter e Aggregati. Rivedere il"Riferimento API" per maggiori informazioni.

Come accedere alla REST API

È possibile accedere agli ONTAP tools for VMware vSphere 10 REST API tramite l'indirizzo IP degli strumenti ONTAP insieme alla porta. L'URL completo è composto da diverse parti, tra cui:

- Indirizzo IP e porta degli strumenti ONTAP
- Versione API
- Categoria di risorse
- Risorsa specifica

È necessario configurare l'indirizzo IP durante la configurazione iniziale, mentre la porta rimane fissa a 8443. La prima parte dell'URL è coerente per ogni istanza ONTAP tools for VMware vSphere 10; cambiano solo la categoria della risorsa e la risorsa specifica tra gli endpoint.

> I valori dell'indirizzo IP e della porta negli esempi seguenti sono solo a scopo illustrativo. È necessario modificare questi valori per il proprio ambiente.

Esempio per accedere ai servizi di autenticazione

```
https://10.61.25.34:8443/virtualization/api/v1/auth/login
```

Questo URL può essere utilizzato per richiedere un token di accesso tramite il metodo POST.

Esempio per elencare i server vCenter

```
https://10.61.25.34:8443/virtualization/api/v1/vcenters
```

Questo URL può essere utilizzato per richiedere un elenco delle istanze del server vCenter definite utilizzando il metodo GET.

Dettagli HTTP

Gli ONTAP tools for VMware vSphere 10 REST API utilizzano HTTP e parametri correlati per agire sulle istanze e sulle raccolte di risorse. Di seguito vengono presentati i dettagli dell'implementazione HTTP.

Metodi HTTP

I metodi o verbi HTTP supportati dall'API REST sono presentati nella tabella seguente.

Metodo	CRUD	Descrizione
OTTENERE	Leggere	Recupera le proprietà dell'oggetto per un'istanza o una raccolta di risorse. Questa operazione è considerata un'operazione di elenco quando utilizzata con una raccolta.
INVIARE	Creare	Crea una nuova istanza di risorsa in base ai parametri di input.
METTERE	Aggiornamento	Aggiorna un'intera istanza di risorsa con il corpo della richiesta JSON fornito. I valori chiave non modificabili dall'utente vengono mantenuti.
TOPPA	Aggiornamento	Richiede che un insieme di modifiche selezionate nella richiesta vengano applicate all'istanza della risorsa.
ELIMINARE	Eliminare	Elimina un'istanza di risorsa esistente.

Intestazioni di richiesta e risposta

La tabella seguente riassume le intestazioni HTTP più importanti utilizzate con l'API REST.

Intestazione	Tipo	Note sull'utilizzo
Accettare	Richiesta	Questo è il tipo di contenuto che l'applicazione client può accettare. I valori validi includono '*/*` o `application/json`.
x-auth	Richiesta	Contiene un token di accesso che identifica l'utente che invia la richiesta tramite l'applicazione client.
Tipo di contenuto	Risposta	Restituito dal server in base al `Accept` intestazione della richiesta.

Codici di stato HTTP

Di seguito sono descritti i codici di stato HTTP utilizzati dall'API REST.

Codice	Senso	Descrizione
200	OK	Indica il successo delle chiamate che non creano una nuova istanza di risorsa.

Codice	Senso	Descrizione
201	Creato	È stato creato correttamente un oggetto con un identificatore univoco per l'istanza della risorsa.
202	Accettato	La richiesta è stata accettata ed è stato creato un processo in background per eseguirla.
204	Nessun contenuto	La richiesta è stata accettata, anche se non è stato restituito alcun contenuto.
400	Brutta richiesta	L'input della richiesta non è riconosciuto o è inappropriato.
401	Non autorizzato	L'utente non è autorizzato e deve autenticarsi.
403	Vietato	L'accesso è negato a causa di un errore di autorizzazione.
404	Non trovato	La risorsa a cui si fa riferimento nella richiesta non esiste.
409	Conflitto	Il tentativo di creare un oggetto non è riuscito perché l'oggetto esiste già.
500	Errore interno	Si è verificato un errore interno generale sul server.

Autenticazione

L'autenticazione di un client all'API REST viene eseguita tramite un token di accesso. Le caratteristiche rilevanti del token e del processo di autenticazione includono:

- Il client deve richiedere un token utilizzando le credenziali di amministratore di ONTAP Tools Manager (nome utente e password).
- I token sono formattati come JSON Web Token (JWT).
- Ogni token scade dopo 60 minuti.
- Le richieste API da un client devono includere il token nel `x-auth` intestazione della richiesta.

Fare riferimento a"La tua prima chiamata API REST" per un esempio di richiesta e utilizzo di un token di accesso.

Richieste sincrone e asincrone

La maggior parte delle chiamate API REST vengono completate rapidamente e pertanto vengono eseguite in modo sincrono. Ciò significa che restituiscono un codice di stato (ad esempio 200) dopo che una richiesta è stata completata. Le richieste che richiedono più tempo per essere completate vengono eseguite in modo asincrono tramite un processo in background.

Dopo aver emesso una chiamata API eseguita in modo asincrono, il server restituisce un codice di stato HTTP 202. Indica che la richiesta è stata accettata ma non ancora completata. È possibile interrogare il processo in background per determinarne lo stato, incluso se è riuscito o meno.

L'elaborazione asincrona viene utilizzata per diversi tipi di operazioni di lunga durata, tra cui le operazioni datastore e vVol. Per ulteriori informazioni, fare riferimento alla categoria Job Manager dell'API REST nella pagina Swagger.

La tua prima chiamata API REST ONTAP tools for VMware vSphere 10

È possibile effettuare una chiamata API tramite curl per iniziare a utilizzare gli ONTAP tools for VMware vSphere 10 REST API.

Prima di iniziare

Dovresti rivedere le informazioni e i parametri richiesti negli esempi curl.

Informazioni richieste

Ti occorre quanto segue:

- ONTAP tools for VMware vSphere 10 e la porta
- Credenziali per l'amministratore del gestore degli strumenti ONTAP (nome utente e password)

Parametri e variabili

Gli esempi curl presentati di seguito includono variabili in stile Bash. È possibile impostare queste variabili nell'ambiente Bash oppure aggiornarle manualmente prima di impartire i comandi. Se si impostano le variabili, la shell sostituirà i valori in ciascun comando prima che venga eseguito. Le variabili sono descritte nella tabella seguente.

Variabile	Descrizione
$FQDN_IP_PORT	Il nome di dominio completo o l'indirizzo IP del gestore degli strumenti ONTAP insieme al numero di porta.
$MYUSER	Nome utente per l'account del gestore degli strumenti ONTAP .
$MIAPASSWORD	Password associata al nome utente del gestore degli strumenti ONTAP .
$ACCESS_TOKEN	Il token di accesso emesso dal gestore degli strumenti ONTAP .

I seguenti comandi e output nella CLI di Linux illustrano come impostare e visualizzare una variabile:

```
FQDN_IP_PORT=172.14.31.224:8443
echo $FQDN_IP
172.14.31.224:8443
```

Passaggio 1: acquisire un token di accesso

Per utilizzare l'API REST è necessario acquisire un token di accesso. Di seguito è riportato un esempio di come richiedere un token di accesso. Dovresti sostituire i valori appropriati per il tuo ambiente.

```
curl --request POST \
--location "https://$FQDN_IP_PORT/virtualization/api/v1/auth/login” \
--header "Content-Type: application/json" \
--header "Accept: */*" \
-d "{"username": "$MYUSER", "password": "$MYPASSWORD"}"
```

Copia e salva il token di accesso fornito nella risposta.

Passaggio 2: emettere la chiamata API REST

Dopo aver ottenuto un token di accesso, puoi utilizzare curl per emettere una chiamata API REST. Includi il token di accesso acquisito nel primo passaggio.

Esempio di ricciolo

```
curl --request GET \
--location "https://$FQDN_IP_PORT/virtualization/api/v1/vcenters" \
--header "Accept: */*" \
--header "x-auth: $ACCESS_TOKEN"
```

La risposta JSON include un elenco delle istanze VMware vCenter configurate in ONTAP Tools Manager.

Riferimento API per gli ONTAP tools for VMware vSphere 10 REST API

Il riferimento API REST ONTAP tools for VMware vSphere 10 contiene dettagli su tutte le chiamate API. Questo riferimento è utile quando si sviluppano applicazioni di automazione.

È possibile accedere alla documentazione degli ONTAP tools for VMware vSphere 10 REST API online tramite l’interfaccia utente Swagger. Sono necessari l’indirizzo IP o il nome di dominio completo degli ONTAP tools for VMware vSphere 10, nonché la porta.

Passi

1. Digita il seguente URL nel tuo browser sostituendo la variabile con la combinazione appropriata di indirizzo IP e porta e premi **Invio**.

   `https://$FQDN_IP_PORT/`

   Esempio

   `https://10.61.25.33:8443/`

2. Come esempio di una chiamata API individuale, scorri verso il basso fino alla categoria **vCenters** e seleziona **GET** accanto all’endpoint `/virtualization/api/v1/vcenters`

Note legali

Le note legali forniscono accesso a dichiarazioni di copyright, marchi commerciali, brevetti e altro ancora.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marchi

NETAPP, il logo NETAPP e i marchi elencati nella pagina Marchi NetApp sono marchi di NetApp, Inc. Altri nomi di aziende e prodotti possono essere marchi dei rispettivi proprietari.

"https://www.netapp.com/company/legal/trademarks/"

Brevetti

Un elenco aggiornato dei brevetti di proprietà di NetApp è disponibile all'indirizzo:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Politica sulla riservatezza

"https://www.netapp.com/company/legal/privacy-policy/"

Open source

I file di avviso forniscono informazioni sui diritti d'autore e sulle licenze di terze parti utilizzati nel software NetApp .

"Avviso per gli ONTAP tools for VMware vSphere 10.4"

Informazioni sul copyright

Copyright © 2025 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.