



Riferimento

Cloud Manager 3.6

NetApp
March 25, 2024

Sommario

- Riferimento 1
 - Domande frequenti: Integrazione di Cloud Manager con NetApp Cloud Central 1
 - Regole del gruppo di sicurezza per AWS 2
 - Regole del gruppo di sicurezza per Azure 10
 - Autorizzazioni AWS e Azure per Cloud Manager 18
 - Configurazioni predefinite 21
 - Ruoli utente 24
 - Dove trovare assistenza e ulteriori informazioni 25

Riferimento

Domande frequenti: Integrazione di Cloud Manager con NetApp Cloud Central

Durante l'aggiornamento a Cloud Manager 3.5, NetApp sceglierà sistemi Cloud Manager specifici da integrare con NetApp Cloud Central, se non sono già integrati. Queste FAQ possono rispondere alle domande che potresti avere sul processo.

Che cos'è NetApp Cloud Central?

NetApp Cloud Central offre una posizione centralizzata per accedere e gestire i servizi dati cloud di NetApp. Questi servizi ti consentono di eseguire applicazioni critiche nel cloud, creare siti di DR automatizzati, eseguire il backup dei dati SaaS e migrare e controllare in modo efficace i dati su più cloud.

Perché NetApp sta integrando il mio sistema Cloud Manager con Cloud Central?

L'integrazione di Cloud Manager con NetApp Cloud Central offre diversi vantaggi, tra cui un'esperienza di implementazione semplificata, un'unica posizione per visualizzare e gestire più sistemi Cloud Manager e autenticazione utente centralizzata.

Cosa succede durante il processo di integrazione?

NetApp esegue la migrazione di tutti gli account utente locali nel sistema Cloud Manager all'autenticazione utente centralizzata disponibile in Cloud Central.

Come funziona l'autenticazione utente centralizzata?

Con l'autenticazione utente centralizzata, è possibile utilizzare lo stesso set di credenziali nei sistemi Cloud Manager e tra Cloud Manager e altri servizi dati, come Cloud Sync. È anche facile reimpostare la password se la si dimentica.

Devo iscrivermi a un account utente Cloud Central?

NetApp creerà un account utente Cloud Central per te quando integreremo il tuo sistema Cloud Manager con Cloud Central. Per completare il processo di registrazione, è sufficiente reimpostare la password.

Cosa fare se si dispone già di un account utente Cloud Central?

Se l'indirizzo e-mail utilizzato per accedere a Cloud Manager corrisponde all'indirizzo e-mail di un account utente Cloud Central, puoi accedere direttamente al tuo sistema Cloud Manager.

Cosa succede se il sistema Cloud Manager dispone di più account utente?

NetApp esegue la migrazione di tutti gli account utente locali verso gli account utente di Cloud Central. Ogni utente deve reimpostare la propria password.

Cosa succede se si dispone di un account utente che utilizza lo stesso indirizzo e-mail su più sistemi Cloud Manager?

Devi solo reimpostare la password una volta per poter utilizzare lo stesso account utente di Cloud Central per accedere a ciascun sistema Cloud Manager.

Cosa fare se l'account utente locale utilizza un indirizzo e-mail non valido?

La reimpostazione della password richiede un indirizzo e-mail valido. Contattaci tramite l'icona della chat disponibile nell'angolo inferiore destro dell'interfaccia di Cloud Manager.

Cosa succede se si dispone di script di automazione per le API Cloud Manager?

Tutte le API sono compatibili con le versioni precedenti. Sarà necessario aggiornare gli script che utilizzano le password, se si modifica la password al momento della reimpostazione.

Cosa succede se il sistema Cloud Manager utilizza LDAP?

Se il sistema utilizza LDAP, NetApp non può integrare automaticamente il sistema con Cloud Central. È necessario eseguire manualmente i seguenti passaggi:

1. Implementa un nuovo sistema Cloud Manager da ["NetApp Cloud Central"](#).
2. ["Configurare LDAP con il nuovo sistema"](#).
3. ["Scopri i sistemi Cloud Volumes ONTAP esistenti"](#) Dal nuovo sistema Cloud Manager.
4. Eliminare il vecchio sistema Cloud Manager.

È importante dove ho installato il sistema Cloud Manager?

No NetApp integrerà i sistemi con Cloud Central indipendentemente da dove risiedono, sia in AWS, Azure o on-premise.



L'unica eccezione è l'ambiente di servizi cloud commerciali AWS.

Regole del gruppo di sicurezza per AWS

Cloud Manager crea gruppi di sicurezza AWS che includono le regole in entrata e in uscita di cui Cloud Manager e Cloud Volumes ONTAP hanno bisogno per funzionare correttamente. È possibile fare riferimento alle porte a scopo di test o se si preferisce utilizzare i propri gruppi di protezione.

Regole per Cloud Manager

Il gruppo di sicurezza per Cloud Manager richiede regole sia in entrata che in uscita.

Regole in entrata per Cloud Manager

L'origine delle regole in entrata nel gruppo di sicurezza predefinito è 0.0.0.0/0.

Protocollo	Porta	Scopo
SSH	22	Fornisce l'accesso SSH all'host Cloud Manager
HTTP	80	Fornisce l'accesso HTTP dai browser Web client alla console Web di Cloud Manager
HTTPS	443	Fornisce l'accesso HTTPS dai browser Web client alla console Web di Cloud Manager

Regole in uscita per Cloud Manager

Il gruppo di sicurezza predefinito per Cloud Manager apre tutto il traffico in uscita. Se questo è accettabile, attenersi alle regole di base per le chiamate in uscita. Se sono necessarie regole più rigide, utilizzare le regole avanzate in uscita.

Regole di base in uscita

Il gruppo di sicurezza predefinito per Cloud Manager include le seguenti regole in uscita.

Protocollo	Porta	Scopo
Tutti i TCP	Tutto	Tutto il traffico in uscita
Tutti gli UDP	Tutto	Tutto il traffico in uscita

Regole avanzate in uscita

Se sono necessarie regole rigide per il traffico in uscita, è possibile utilizzare le seguenti informazioni per aprire solo le porte richieste per le comunicazioni in uscita da Cloud Manager.



L'indirizzo IP di origine è l'host Cloud Manager.

Servizio	Protocollo	Porta	Destinazione	Scopo
Active Directory	TCP	88	Insieme di strutture di Active Directory	Autenticazione Kerberos V.
	TCP	139	Insieme di strutture di Active Directory	Sessione del servizio NetBIOS
	TCP	389	Insieme di strutture di Active Directory	LDAP
	TCP	445	Insieme di strutture di Active Directory	Microsoft SMB/CIFS su TCP con frame NetBIOS
	TCP	464	Insieme di strutture di Active Directory	Kerberos V change & set password (SET_CHANGE)
	TCP	749	Insieme di strutture di Active Directory	Modifica e impostazione della password Kerberos V di Active Directory (RPCSEC_GSS)
	UDP	137	Insieme di strutture di Active Directory	Servizio nomi NetBIOS
	UDP	138	Insieme di strutture di Active Directory	Servizio datagramma NetBIOS
	UDP	464	Insieme di strutture di Active Directory	Amministrazione delle chiavi Kerberos
Chiamate API e AutoSupport	HTTPS	443	LIF gestione cluster ONTAP e Internet in uscita	Chiamate API ad AWS e ONTAP e invio di messaggi AutoSupport a NetApp
Chiamate API	TCP	3000	LIF gestione cluster ONTAP	Chiamate API a ONTAP
DNS	UDP	53	DNS	Utilizzato per la risoluzione DNS da parte di Cloud Manager

Regole per Cloud Volumes ONTAP

Il gruppo di sicurezza per Cloud Volumes ONTAP richiede regole sia in entrata che in uscita.

Regole inbound per Cloud Volumes ONTAP

L'origine delle regole in entrata nel gruppo di sicurezza predefinito è 0.0.0.0/0.

Protocollo	Porta	Scopo
Tutti gli ICMP	Tutto	Eseguire il ping dell'istanza
HTTP	80	Accesso HTTP alla console Web di System Manager utilizzando l'indirizzo IP della LIF di gestione del cluster
HTTPS	443	Accesso HTTPS alla console Web di System Manager utilizzando l'indirizzo IP della LIF di gestione del cluster
SSH	22	Accesso SSH all'indirizzo IP della LIF di gestione del cluster o di una LIF di gestione dei nodi
TCP	111	Chiamata a procedura remota per NFS
TCP	139	Sessione del servizio NetBIOS per CIFS
TCP	161-162	Protocollo di gestione di rete semplice
TCP	445	Microsoft SMB/CIFS su TCP con frame NetBIOS
TCP	635	Montaggio NFS
TCP	749	Kerberos
TCP	2049	Daemon del server NFS
TCP	3260	Accesso iSCSI tramite LIF dei dati iSCSI
TCP	4045	Daemon di blocco NFS
TCP	4046	Network status monitor per NFS
TCP	10000	Backup con NDMP
TCP	11104	Gestione delle sessioni di comunicazione tra cluster per SnapMirror
TCP	11105	Trasferimento dei dati SnapMirror con LIF intercluster
UDP	111	Chiamata a procedura remota per NFS
UDP	161-162	Protocollo di gestione di rete semplice
UDP	635	Montaggio NFS
UDP	2049	Daemon del server NFS
UDP	4045	Daemon di blocco NFS
UDP	4046	Network status monitor per NFS
UDP	4049	Protocollo NFS rquotad

Regole in uscita per Cloud Volumes ONTAP

Il gruppo di protezione predefinito per Cloud Volumes ONTAP apre tutto il traffico in uscita. Se questo è accettabile, attenersi alle regole di base per le chiamate in uscita. Se sono necessarie regole più rigide, utilizzare le regole avanzate in uscita.

Regole di base in uscita

Il gruppo di protezione predefinito per Cloud Volumes ONTAP include le seguenti regole in uscita.

Protocollo	Porta	Scopo
Tutti gli ICMP	Tutto	Tutto il traffico in uscita
Tutti i TCP	Tutto	Tutto il traffico in uscita
Tutti gli UDP	Tutto	Tutto il traffico in uscita

Regole avanzate in uscita

Se sono necessarie regole rigide per il traffico in uscita, è possibile utilizzare le seguenti informazioni per aprire solo le porte richieste per le comunicazioni in uscita da Cloud Volumes ONTAP.



L'origine è l'interfaccia (indirizzo IP) del sistema Cloud Volumes ONTAP.

Servizio	Protocollo	Porta	Origine	Destinazione	Scopo
Active Directory					

Servizio	Protocollo	Porta	Origine	Destinazione	Scopo
	TCP	389	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	LDAP
	TCP	445	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Microsoft SMB/CIFS su TCP con frame NetBIOS
	TCP	464	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Kerberos V change & set password (SET_CHANGE)
	UDP	464	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Amministrazione delle chiavi Kerberos
	TCP	749	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Kerberos V change & set password (RPCSEC_GSS)
Cluster	Tutto il traffico	Tutto il traffico	Tutte le LIF su un nodo	Tutte le LIF sull'altro nodo	Comunicazioni tra cluster (solo Cloud Volumes ONTAP ha)
	TCP	3000	LIF di gestione dei nodi	MEDIATORE HA	Chiamate ZAPI (solo Cloud Volumes ONTAP ha)
	ICMP	1	LIF di gestione dei nodi	MEDIATORE HA	Mantieni attivo (solo Cloud Volumes ONTAP ha)
DHCP	UDP	68	LIF di gestione dei nodi	DHCP	Client DHCP per la prima installazione
DHCPS	UDP	67	LIF di gestione dei nodi	DHCP	Server DHCP
DNS	UDP	53	LIF di gestione dei nodi e LIF dei dati (NFS, CIFS)	DNS	DNS
NDMP	TCP	18600–18699	LIF di gestione dei nodi	Server di destinazione	Copia NDMP
SMTP	TCP	25	LIF di gestione dei nodi	Server di posta	Gli avvisi SMTP possono essere utilizzati per AutoSupport
SNMP	TCP	161	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	UDP	161	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	TCP	162	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	UDP	162	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP

Servizio	Protocollo	Porta	Origine	Destinazione	Scopo
SnapMirror	TCP	11104	LIF intercluster	ONTAP Intercluster LIF	Gestione delle sessioni di comunicazione tra cluster per SnapMirror
	TCP	11105	LIF intercluster	ONTAP Intercluster LIF	Trasferimento dei dati SnapMirror
Syslog	UDP	514	LIF di gestione dei nodi	Server syslog	Messaggi di inoltro syslog

Regole per il gruppo di sicurezza esterno del mediatore ha

Il gruppo di sicurezza esterno predefinito per il mediatore Cloud Volumes ONTAP ha include le seguenti regole in entrata e in uscita.

Regole in entrata

L'origine delle regole in entrata è 0.0.0.0/0.

Protocollo	Porta	Scopo
SSH	22	Connessioni SSH al mediatore ha
TCP	3000	Accesso API RESTful da Cloud Manager

Regole in uscita

Il gruppo di sicurezza predefinito per il mediatore ha apre tutto il traffico in uscita. Se questo è accettabile, attenersi alle regole di base per le chiamate in uscita. Se sono necessarie regole più rigide, utilizzare le regole avanzate in uscita.

Regole di base in uscita

Il gruppo di protezione predefinito per il mediatore ha include le seguenti regole in uscita.

Protocollo	Porta	Scopo
Tutti i TCP	Tutto	Tutto il traffico in uscita
Tutti gli UDP	Tutto	Tutto il traffico in uscita

Regole avanzate in uscita

Se sono necessarie regole rigide per il traffico in uscita, è possibile utilizzare le seguenti informazioni per aprire solo le porte necessarie per la comunicazione in uscita dal mediatore ha.

Protocollo	Porta	Destinazione	Scopo
HTTP	80	Indirizzo IP di Cloud Manager	Scarica gli aggiornamenti per il mediatore
HTTPS	443	Servizi API AWS	Assistenza per il failover dello storage
UDP	53	Servizi API AWS	Assistenza per il failover dello storage



Anziché aprire le porte 443 e 53, è possibile creare un endpoint VPC di interfaccia dalla subnet di destinazione al servizio AWS EC2.

Regole per il gruppo di sicurezza interno del mediatore ha

Il gruppo di sicurezza interno predefinito per il mediatore ha Cloud Volumes ONTAP include le seguenti regole. Cloud Manager crea sempre questo gruppo di sicurezza. Non hai la possibilità di utilizzare il tuo.

Regole in entrata

Il gruppo di sicurezza predefinito include le seguenti regole in entrata.

Protocollo	Porta	Scopo
Tutto il traffico	Tutto	Comunicazione tra il mediatore ha e i nodi ha

Regole in uscita

Il gruppo di protezione predefinito include le seguenti regole in uscita.

Protocollo	Porta	Scopo
Tutto il traffico	Tutto	Comunicazione tra il mediatore ha e i nodi ha

Regole del gruppo di sicurezza per Azure

Cloud Manager crea gruppi di sicurezza Azure che includono le regole in entrata e in uscita di cui Cloud Manager e Cloud Volumes ONTAP hanno bisogno per funzionare correttamente. È possibile fare riferimento alle porte a scopo di test o se si preferisce utilizzare i propri gruppi di protezione.

Regole per Cloud Manager

Il gruppo di sicurezza per Cloud Manager richiede regole sia in entrata che in uscita.

Regole in entrata per Cloud Manager

L'origine delle regole in entrata nel gruppo di sicurezza predefinito è 0.0.0.0/0.

Protocollo	Porta	Scopo
SSH	22	Fornisce l'accesso SSH all'host Cloud Manager
HTTP	80	Fornisce l'accesso HTTP dai browser Web client alla console Web di Cloud Manager
HTTPS	443	Fornisce l'accesso HTTPS dai browser Web client alla console Web di Cloud Manager

Regole in uscita per Cloud Manager

Il gruppo di sicurezza predefinito per Cloud Manager apre tutto il traffico in uscita. Se questo è accettabile, attenersi alle regole di base per le chiamate in uscita. Se sono necessarie regole più rigide, utilizzare le regole

avanzate in uscita.

Regole di base in uscita

Il gruppo di sicurezza predefinito per Cloud Manager include le seguenti regole in uscita.

Protocollo	Porta	Scopo
Tutti i TCP	Tutto	Tutto il traffico in uscita
Tutti gli UDP	Tutto	Tutto il traffico in uscita

Regole avanzate in uscita

Se sono necessarie regole rigide per il traffico in uscita, è possibile utilizzare le seguenti informazioni per aprire solo le porte richieste per le comunicazioni in uscita da Cloud Manager.



L'indirizzo IP di origine è l'host Cloud Manager.

Servizio	Protocollo	Porta	Destinazione	Scopo
Active Directory	TCP	88	Insieme di strutture di Active Directory	Autenticazione Kerberos V.
	TCP	139	Insieme di strutture di Active Directory	Sessione del servizio NetBIOS
	TCP	389	Insieme di strutture di Active Directory	LDAP
	TCP	445	Insieme di strutture di Active Directory	Microsoft SMB/CIFS su TCP con frame NetBIOS
	TCP	464	Insieme di strutture di Active Directory	Kerberos V change & set password (SET_CHANGE)
	TCP	749	Insieme di strutture di Active Directory	Modifica e impostazione della password Kerberos V di Active Directory (RPCSEC_GSS)
	UDP	137	Insieme di strutture di Active Directory	Servizio nomi NetBIOS
	UDP	138	Insieme di strutture di Active Directory	Servizio datagramma NetBIOS
	UDP	464	Insieme di strutture di Active Directory	Amministrazione delle chiavi Kerberos

Servizio	Protocollo	Porta	Destinazione	Scopo
Chiamate API e AutoSupport	HTTPS	443	LIF gestione cluster ONTAP e Internet in uscita	Chiamate API ad AWS e ONTAP e invio di messaggi AutoSupport a NetApp
Chiamate API	TCP	3000	LIF gestione cluster ONTAP	Chiamate API a ONTAP
DNS	UDP	53	DNS	Utilizzato per la risoluzione DNS da parte di Cloud Manager

Regole per Cloud Volumes ONTAP

Il gruppo di sicurezza per Cloud Volumes ONTAP richiede regole sia in entrata che in uscita.

Regole in entrata per sistemi a nodo singolo

Priorità	Nome	Porta	Protocollo	Origine	Destinazione	Azione	Descrizione
1000	inbound_ssh	22	TCP	Qualsiasi	Qualsiasi	Consentire	Accesso SSH all'indirizzo IP della LIF di gestione del cluster o di una LIF di gestione dei nodi
1001	inbound_http	80	TCP	Qualsiasi	Qualsiasi	Consentire	Accesso HTTP alla console Web di System Manager utilizzando l'indirizzo IP della LIF di gestione del cluster
1002	inbound_111_tcp	111	TCP	Qualsiasi	Qualsiasi	Consentire	Chiamata a procedura remota per NFS
1003	inbound_111_udp	111	UDP	Qualsiasi	Qualsiasi	Consentire	Chiamata a procedura remota per NFS
1004	inbound_139	139	TCP	Qualsiasi	Qualsiasi	Consentire	Sessione del servizio NetBIOS per CIFS
1005	inbound_161-162_tcp	161-162	TCP	Qualsiasi	Qualsiasi	Consentire	Protocollo di gestione di rete semplice
1006	inbound_161-162_udp	161-162	UDP	Qualsiasi	Qualsiasi	Consentire	Protocollo di gestione di rete semplice
1007	inbound_443	443	TCP	Qualsiasi	Qualsiasi	Consentire	Accesso HTTPS alla console Web di System Manager utilizzando l'indirizzo IP della LIF di gestione del cluster
1008	inbound_445	445	TCP	Qualsiasi	Qualsiasi	Consentire	Microsoft SMB/CIFS su TCP con frame NetBIOS

Priorità	Nome	Porta	Protocollo	Origine	Destinazione	Azione	Descrizione
1009	inbound_635_tcp	635	TCP	Qualsiasi	Qualsiasi	Consentire	Montaggio NFS
1010	inbound_635_udp	635	TCP	Qualsiasi	Qualsiasi	Consentire	Montaggio NFS
1011	inbound_749	749	TCP	Qualsiasi	Qualsiasi	Consentire	Kerberos
1012	inbound_2049_tcp	2049	TCP	Qualsiasi	Qualsiasi	Consentire	Daemon del server NFS
1013	inbound_2049_udp	2049	UDP	Qualsiasi	Qualsiasi	Consentire	Daemon del server NFS
1014	inbound_3260	3260	TCP	Qualsiasi	Qualsiasi	Consentire	Accesso iSCSI tramite LIF dei dati iSCSI
1015	inbound_4045-4046_tcp	4045-4046	TCP	Qualsiasi	Qualsiasi	Consentire	NFS lock daemon e network status monitor
1016	inbound_4045-4046_udp	4045-4046	UDP	Qualsiasi	Qualsiasi	Consentire	NFS lock daemon e network status monitor
1017	inbound_10000	10000	TCP	Qualsiasi	Qualsiasi	Consentire	Backup con NDMP
1018	inbound_11104-11105	11104-11105	TCP	Qualsiasi	Qualsiasi	Consentire	Trasferimento dei dati SnapMirror
3000	inbound_deny_all_tcp	Qualsiasi	TCP	Qualsiasi	Qualsiasi	Negare	Blocca tutto il traffico TCP in entrata
3001	inbound_deny_all_udp	Qualsiasi	UDP	Qualsiasi	Qualsiasi	Negare	Blocca tutto il traffico UDP in entrata
65000	AllowVnetInBound	Qualsiasi	Qualsiasi	VirtualNetwork	VirtualNetwork	Consentire	Traffico in entrata dall'interno di VNET
65001	AllowAzureLoadBalancerInBound	Qualsiasi	Qualsiasi	AzureLoadBalancer	Qualsiasi	Consentire	Traffico di dati dal bilanciamento del carico standard di Azure
65500	DenyAllInBound	Qualsiasi	Qualsiasi	Qualsiasi	Qualsiasi	Negare	Bloccare tutto il traffico in entrata

Regole in entrata per i sistemi ha



I sistemi HA hanno meno regole in entrata rispetto ai sistemi a nodo singolo perché il traffico dati in entrata passa attraverso il bilanciamento del carico standard di Azure. Per questo motivo, il traffico proveniente dal bilanciamento del carico deve essere aperto, come mostrato nella regola "AllowAzureLoadBalancerInBound".

Priorità	Nome	Porta	Protocollo	Origine	Destinazione	Azione	Descrizione
100	inbound_443	443	Qualsiasi	Qualsiasi	Qualsiasi	Consentire	Accesso HTTPS alla console Web di System Manager utilizzando l'indirizzo IP della LIF di gestione del cluster
101	inbound_111_tcp	111	Qualsiasi	Qualsiasi	Qualsiasi	Consentire	Chiamata a procedura remota per NFS
102	inbound_2049_tcp	2049	Qualsiasi	Qualsiasi	Qualsiasi	Consentire	Daemon del server NFS
111	inbound_ssh	22	Qualsiasi	Qualsiasi	Qualsiasi	Consentire	Accesso SSH all'indirizzo IP della LIF di gestione del cluster o di una LIF di gestione dei nodi
121	inbound_53	53	Qualsiasi	Qualsiasi	Qualsiasi	Consentire	DNS e CIFS
65000	AllowVnetInbound	Qualsiasi	Qualsiasi	VirtualNetwork	VirtualNetwork	Consentire	Traffico in entrata dall'interno di VNET
65001	AllowAzureLoadBalancerInbound	Qualsiasi	Qualsiasi	AzureLoadBalancer	Qualsiasi	Consentire	Traffico di dati dal bilanciamento del carico standard di Azure
65500	DenyAllInbound	Qualsiasi	Qualsiasi	Qualsiasi	Qualsiasi	Negare	Bloccare tutto il traffico in entrata

Regole in uscita per Cloud Volumes ONTAP

Il gruppo di protezione predefinito per Cloud Volumes ONTAP apre tutto il traffico in uscita. Se questo è accettabile, attenersi alle regole di base per le chiamate in uscita. Se sono necessarie regole più rigide, utilizzare le regole avanzate in uscita.

Regole di base in uscita

Il gruppo di protezione predefinito per Cloud Volumes ONTAP include le seguenti regole in uscita.

Protocollo	Porta	Scopo
Tutti i TCP	Tutto	Tutto il traffico in uscita
Tutti gli UDP	Tutto	Tutto il traffico in uscita

Regole avanzate in uscita

Se sono necessarie regole rigide per il traffico in uscita, è possibile utilizzare le seguenti informazioni per aprire solo le porte richieste per le comunicazioni in uscita da Cloud Volumes ONTAP.



L'origine è l'interfaccia (indirizzo IP) del sistema Cloud Volumes ONTAP.

Servizio	Protocollo	Porta	Origine	Destinazione	Scopo
Active Directory					

Servizio	Protocollo	Porta	Origine	Destinazione	Scopo
	TCP	389	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	LDAP
	TCP	445	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Microsoft SMB/CIFS su TCP con frame NetBIOS
	TCP	464	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Kerberos V change & set password (SET_CHANGE)
	UDP	464	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Amministrazione delle chiavi Kerberos
	TCP	749	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Kerberos V change & set password (RPCSEC_GSS)
DHCP	UDP	68	LIF di gestione dei nodi	DHCP	Client DHCP per la prima installazione
DHCPS	UDP	67	LIF di gestione dei nodi	DHCP	Server DHCP
DNS	UDP	53	LIF di gestione dei nodi e LIF dei dati (NFS, CIFS)	DNS	DNS
NDMP	TCP	18600–18699	LIF di gestione dei nodi	Server di destinazione	Copia NDMP
SMTP	TCP	25	LIF di gestione dei nodi	Server di posta	Gli avvisi SMTP possono essere utilizzati per AutoSupport
SNMP	TCP	161	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	UDP	161	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	TCP	162	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	UDP	162	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
SnapMirror	TCP	11104	LIF intercluster	ONTAP Intercluster LIF	Gestione delle sessioni di comunicazione tra cluster per SnapMirror
	TCP	11105	LIF intercluster	ONTAP Intercluster LIF	Trasferimento dei dati SnapMirror
Syslog	UDP	514	LIF di gestione dei nodi	Server syslog	Messaggi di inoltro syslog

Autorizzazioni AWS e Azure per Cloud Manager

Cloud Manager richiede autorizzazioni per eseguire azioni in AWS e Azure per conto dell'utente. Queste autorizzazioni sono incluse in ["Le policy fornite da NetApp"](#). Potresti voler capire cosa fa Cloud Manager con queste autorizzazioni.

Cosa fa Cloud Manager con le autorizzazioni AWS

Cloud Manager utilizza un account AWS per effettuare chiamate API a diversi servizi AWS, tra cui EC2, S3, CloudFormation, IAM, Il servizio token di protezione (STS) e il servizio di gestione delle chiavi (KMS).

Azioni	Scopo
"ec2:StartInstances", "ec2:StopInstances", "ec2:DescribeInstances", "ec2:DescribeInstanceStatus", "ec2:RunInstances", "ec2:TerminateInstances", "ec2:ModifyInstanceAttribute",	Avvia un'istanza di Cloud Volumes ONTAP e interrompe, avvia e monitora l'istanza.
"ec2:DescribeInstanceAttribute",	Verifica che la rete avanzata sia abilitata per i tipi di istanze supportati.
"ec2:DescribeRouteTable", "ec2:DescribeImages", "ec2:CreateTags",	Avvia una configurazione Cloud Volumes ONTAP ha. Contrassegna ogni risorsa creata da Cloud Manager con i tag "WorkingEnvironment" e "WorkingEnvironmentId". Cloud Manager utilizza questi tag per la manutenzione e l'allocazione dei costi.
"ec2:CreateVolume", "ec2:DescribeVolumes", "ec2:ModifyVolumeAttribute", "ec2:AttachVolume", "ec2>DeleteVolume", "ec2:DetachVolume",	Gestisce i volumi EBS utilizzati da Cloud Volumes ONTAP come storage back-end.
"ec2:CreateSecurityGroup", "ec2>DeleteSecurityGroup", "ec2:DescribeSecurityGroups", "ec2:RevokeSecurityGroupEgress", "ec2:AuthorizeSecurityGroupEgress", "ec2:AuthorizeSecurityGroupIngress", "ec2:RevokeSecurityGroupIngress",	Crea gruppi di protezione predefiniti per Cloud Volumes ONTAP.
"ec2:CreateNetworkInterface", "ec2:DescribeNetworkInterfaces", "ec2>DeleteNetworkInterface", "ec2:ModifyNetworkInterfaceAttribute",	Crea e gestisce le interfacce di rete per Cloud Volumes ONTAP nella subnet di destinazione.
"ec2:DescribeSubnet", "ec2:DescribeVpcs",	Ottiene l'elenco delle subnet di destinazione e dei gruppi di protezione necessari per la creazione di un nuovo ambiente di lavoro per Cloud Volumes ONTAP.
"ec2:DescribeDhcpOptions",	Determina i server DNS e il nome di dominio predefinito quando si avviano le istanze di Cloud Volumes ONTAP.

Azioni	Scopo
"ec2:CreateSnapshot", "ec2:DeleteSnapshot", "ec2:DescribeSnapshot",	Esegue snapshot dei volumi EBS durante la configurazione iniziale e ogni volta che un'istanza di Cloud Volumes ONTAP viene arrestata.
"ec2:GetConsoleOutput",	Acquisisce la console Cloud Volumes ONTAP, che è collegata ai messaggi AutoSupport.
"ec2:DescribeKeyPairs",	Ottiene l'elenco delle coppie di chiavi disponibili quando si avviano le istanze.
"ec2:DescribeRegions",	Ottiene un elenco delle regioni AWS disponibili.
"ec2:DeleteTags", "ec2:DescribeTags",	Gestisce i tag per le risorse associate alle istanze di Cloud Volumes ONTAP.
"Cloudformation:CreateStack", "Cloudformation:DeleteStack", "Cloudformation:DescribeStack", "Cloudformation:DescribeStackEvents", "Cloudformation:ValidateTemplate",	Avvia le istanze di Cloud Volumes ONTAP.
"iam:PassRole", "iam:CreateRole", "iam:DeleteRole", "iam:PutRolePolicy", "iam:CreateInstanceProfile", "iam:DeleteRolePolicy", "iam:AddRoleToInstanceProfile", "iam:RemoveRoleFromInstanceProfile", "iam:DeleteInstanceProfile",	Avvia una configurazione Cloud Volumes ONTAP ha.
"iam:ListInstanceProfiles", "sts:DecodeAuthorizationMessage", "ec2:AssociateIamInstanceProfile", "ec2:DescribeIamInstanceProfileAssociations", "ec2:DisassociateIamInstanceProfile",	Gestisce i profili di istanza per le istanze di Cloud Volumes ONTAP.
"s3:GetBucketTagging", "s3:GetBucketLocation", "s3:ListAllMyBucket", "s3:ListBucket"	Ottiene informazioni sui bucket AWS S3 in modo che Cloud Manager possa integrarsi con il servizio NetApp Data Fabric Cloud Sync.
"s3:Createbucket", "s3:Deletebucket", "s3:GetLifecycleConfiguration", "s3:PutLifecycleConfiguration", "s3:PutBucketTagging", "s3:ListBucketVersions",	Gestisce il bucket S3 utilizzato da un sistema Cloud Volumes ONTAP come Tier di capacità.
"Kms:List*", "kms:descriv**"	Ottiene informazioni sulle chiavi da AWS Key Management Service.
"ce:GetReservationUtilization", "ce:GetDimensionValues", "ce:GetCostAndUsage", "ce:GetTags"	Ottiene i dati dei costi AWS per Cloud Volumes ONTAP.
"ec2:CreatePlacementGroup", "ec2:DeletePlacementGroup"	Quando si implementa una configurazione ha in una singola AWS Availability zone, Cloud Manager lancia i due nodi ha e il mediatore in un gruppo di posizionamento AWS Spread.

Cosa fa Cloud Manager con le autorizzazioni Azure

La policy di Cloud Manager Azure include le autorizzazioni necessarie per implementare e gestire Cloud Volumes ONTAP in Azure.

Azioni	Scopo
"Microsoft.Compute/locations/operations/read", "Microsoft.Compute/locations/vmSizes/read", "Microsoft.Compute/operations/read", "Microsoft.Compute/virtualMachines/instanceView/read", "Microsoft.Compute/virtualMachines/powerOff/action", "Microsoft.Compute/virtualMachines/read", "Microsoft.Compute/virtualMachines/restart/action", "Microsoft.Compute/virtualMachines/start/action", "Microsoft.Compute/virtualMachines/deallocate/action", "Microsoft.Compute/virtualMachines/vmSizes/read", "Microsoft.Compute/virtualMachines/write",	Crea Cloud Volumes ONTAP e arresta, avvia, elimina e ottiene lo stato del sistema.
"Microsoft.Compute/images/write", "Microsoft.Compute/images/read",	Consente l'implementazione di Cloud Volumes ONTAP da un VHD.
"Microsoft.Compute/disks/delete", "Microsoft.Compute/disks/read", "Microsoft.Compute/disks/write", "Microsoft.Storage/checknameAvailability/Read", "Microsoft.Storage/Operations/Read", "Microsoft.Storage/storageAccounts/listkeys/action", "Microsoft.Storage/storageAccounts/Read", "Microsoft.Storage/storageAccounts/regeneratekey/action", "Microsoft.Storage/storageAccounts/write", "Microsoft.Storage/uses/Read",	Gestisce gli account e i dischi dello storage Azure e li collega a Cloud Volumes ONTAP.
"Microsoft.Network/networkInterfaces/read", "Microsoft.Network/networkInterfaces/write", "Microsoft.Network/networkInterfaces/join/action",	Crea e gestisce le interfacce di rete per Cloud Volumes ONTAP nella subnet di destinazione.
"Microsoft.Network/networkSecurityGroups/read", "Microsoft.Network/networkSecurityGroups/write", "Microsoft.Network/networkSecurityGroups/join/action",	Crea gruppi di sicurezza di rete predefiniti per Cloud Volumes ONTAP.
"Microsoft.Resources/subscriptions/locations/Read", "Microsoft.Network/locations/operationResults/read", "Microsoft.Network/locations/operations/read", "Microsoft.Network/virtualNetworks/read", "Microsoft.Network/virtualNetworks/checkIpAvailability/read", "Microsoft.Network/virtualNetworks/subnets/read", "Microsoft.Network/virtualNetworks/subnets/virtualMachines/read", "Microsoft.Network/virtualNetworks/virtualMachines/read", "Microsoft.Network/virtualNetworks/subnets/join/action",	Ottiene informazioni di rete relative alle regioni, alla rete virtuale di destinazione e alla subnet e aggiunge Cloud Volumes ONTAP ai reti virtuali.

Azioni	Scopo
"Microsoft.Network/virtualNetworks/subnets/write", "Microsoft.Network/routeTables/join/action",	Attiva gli endpoint del servizio VNET per il tiering dei dati.
"Microsoft.Resources/Deployments/Operations/Read", "Microsoft.Resources/Deployments/Read", "Microsoft.Resources/Deployments/write",	Implementa Cloud Volumes ONTAP da un modello.
"Microsoft.Resources/Deployments/Operations/Read", "Microsoft.Resources/Deployments/Read", "Microsoft.Resources/Read", "Microsoft.Resources/subscriptions/operationresults/Read", "Microsoft.Resources/subscriptions/resourceGroups/delete", "Microsoft.Resources/subscriptions/resourceGroups/Read", "Microsoft.Resources/subscriptions/resourceGroups/write",	Crea e gestisce gruppi di risorse per Cloud Volumes ONTAP.
"Microsoft.Compute/snapshots/write", "Microsoft.Compute/snapshots/read", "Microsoft.Compute/disks/beginGetAccess/action"	Crea e gestisce snapshot gestite da Azure.
"Microsoft.Compute/availabilitySets/write", "Microsoft.Compute/availabilitySets/read",	Crea e gestisce i set di disponibilità per Cloud Volumes ONTAP.
"Microsoft.MarketplaceOrdering/offers/publisher/offers/plans/agreements/Read", "Microsoft.MarketplaceOrdering/offers/plans/agreements/write"	Consente implementazioni programmatiche da Azure Marketplace.
"Microsoft.Network/loadBalancers/read", "Microsoft.Network/loadBalancers/write", "Microsoft.Network/loadBalancers/delete", "Microsoft.Network/loadBalancers/backendAddressPools/read", "Microsoft.Network/loadBalancers/backendAddressPools/join/action", "Microsoft.Network/loadBalancers/frontendIPConfigurations/read", "Microsoft.Network/loadBalancers/loadBalancingRules/read", "Microsoft.Network/loadBalancers/probes/read", "Microsoft.Network/loadBalancers/probes/join/action",	Gestisce un bilanciamento del carico Azure per le coppie ha.
"Microsoft.Authorization/Blocks/*"	Consente la gestione dei blocchi sui dischi Azure.
"Microsoft.Authorization/roleDefinitions/write", "Microsoft.Authorization/roleAssignments/write", "Microsoft.Web/sites/*"	Gestisce il failover per le coppie ha.

Configurazioni predefinite

I dettagli sulla configurazione predefinita di Cloud Manager e Cloud Volumes ONTAP

possono aiutare l'amministratore dei sistemi.

Configurazione predefinita per Cloud Manager su Linux

Se hai bisogno di risolvere i problemi di Cloud Manager o del tuo host Linux, potrebbe aiutarti a capire come è configurato Cloud Manager.

- Se hai implementato Cloud Manager da NetApp Cloud Central (o direttamente da AWS Marketplace o Azure Marketplace), tieni presente quanto segue:
 - In AWS, il nome utente per l'istanza EC2 Linux è `ec2-user`.
 - Per AWS e Azure, il sistema operativo per l'immagine Cloud Manager è Red Hat Enterprise Linux 7.4 (HVM).

Il sistema operativo non include una GUI. Per accedere al sistema, è necessario utilizzare un terminale.

- La cartella di installazione di Cloud Manager si trova nella seguente posizione:

```
/opt/application/netapp/cloudmanager
```

- I file di log sono contenuti nella seguente cartella:

```
/opt/application/netapp/cloudmanager/log
```

- Il servizio Cloud Manager è denominato `occm`.
- Il servizio `occm` dipende dal servizio MySQL.

Se il servizio MySQL non è attivo, anche il servizio `occm` è inattivo.

- Cloud Manager installa i seguenti pacchetti sull'host Linux, se non sono già installati:
 - 7zip
 - AWSCLI
 - Java
 - Kubectl
 - MySQL
 - Tridentctl
 - Wget

Configurazione predefinita per Cloud Volumes ONTAP

La configurazione predefinita di Cloud Volumes ONTAP consente di configurare e amministrare i sistemi, in particolare se si conosce ONTAP perché la configurazione predefinita di Cloud Volumes ONTAP è diversa da ONTAP.

- Cloud Volumes ONTAP è disponibile come sistema a nodo singolo e come coppia ha in AWS e Azure.
- Cloud Manager crea una SVM per il servizio dei dati quando implementa Cloud Volumes ONTAP. Anche se è possibile creare un'altra SVM per la gestione dei dati da System Manager o CLI, l'utilizzo di più SVM per la gestione dei dati non è supportato.
- Per impostazione predefinita, vengono create diverse interfacce di rete:

- Una LIF di gestione del cluster
- Un LIF intercluster
- Una LIF di gestione dei nodi
- Una LIF di dati iSCSI
- Una LIF di dati CIFS e NFS



Il failover LIF è disattivato per impostazione predefinita per Cloud Volumes ONTAP a causa dei requisiti EC2. La migrazione di una LIF a una porta diversa interrompe la mappatura esterna tra gli indirizzi IP e le interfacce di rete sull'istanza, rendendo la LIF inaccessibile.

- Cloud Volumes ONTAP invia i backup della configurazione a Cloud Manager utilizzando HTTPS.
- Una volta effettuato l'accesso a Cloud Manager, i backup sono accessibili da <https://ipaddress/occm/offboxconfig/>
- Cloud Manager imposta alcuni attributi di volume in modo diverso rispetto ad altri strumenti di gestione (ad esempio, System Manager o CLI).

La tabella seguente elenca gli attributi del volume impostati da Cloud Manager in modo diverso dai valori predefiniti:

Attributo	Valore stabilito da Cloud Manager
Modalità di dimensionamento automatico	crescere
Dimensionamento automatico massimo	1,000% L'amministratore di Cloud Manager può modificare questo valore dalla pagina Impostazioni.
Stile di sicurezza	NTFS per CIFS Volumes UNIX per NFS Volumes
Stile garanzia di spazio	nessuno
Autorizzazioni UNIX (solo NFS)	777

Per informazioni su questi attributi, consulta la pagina man *volume create*.

Dati di boot e root per Cloud Volumes ONTAP

Oltre allo storage per i dati degli utenti, Cloud Manager acquista anche lo storage cloud per i dati di boot e root su ogni sistema Cloud Volumes ONTAP.

AWS

- Un disco SSD IOPS con provisioning per i dati di avvio Cloud Volumes ONTAP, che è di circa 45 GB e 1,250 PIOPS
- Un disco SSD General Purpose per i dati root Cloud Volumes ONTAP, che è di circa 140 GB
- Un'istantanea EBS per ogni disco di boot e disco root

In una coppia ha, entrambi i nodi Cloud Volumes ONTAP replicano il proprio disco root nel nodo partner.

Azure

- Un disco SSD Premium Storage per i dati di avvio Cloud Volumes ONTAP, pari a circa 73 GB
- Un disco SSD Premium Storage per i dati root Cloud Volumes ONTAP, pari a circa 140 GB
- Uno snapshot Azure per ogni disco di boot e disco root

Dove risiedono i dischi

Cloud Manager definisce lo storage di AWS e Azure come segue:

- I dati di avvio risiedono su un disco collegato all'istanza EC2 o alla macchina virtuale Azure.

Questo disco, che contiene l'immagine di avvio, non è disponibile per Cloud Volumes ONTAP.

- I dati root, che contengono la configurazione del sistema e i log, risiedono in aggr0.
- Il volume root della macchina virtuale di storage (SVM) risiede in aggr1.
- I volumi di dati risiedono anche in aggr1.

Ruoli utente

A ciascun account utente di Cloud Manager viene assegnato un ruolo che definisce le autorizzazioni.

Attività	Amministratore di Cloud Manager	Amministratore tenant	Amministratore dell'ambiente di lavoro
Gestire i tenant	Sì	No	No
Gestire gli ambienti di lavoro	Sì	Sì, per il tenant assegnato	Sì, per ambienti di lavoro assegnati
Integra un ambiente di lavoro con Cloud Sync	Sì	Sì	No
Visualizzare lo stato della replica dei dati	Sì	Sì, per il tenant assegnato	Sì, per ambienti di lavoro assegnati
Visualizza la timeline	Sì	Sì	Sì
Creare ed eliminare gli account utente	Sì	Sì, per il tenant assegnato	No
Modificare gli account utente	Sì	Sì, per il tenant assegnato	Sì, per il proprio account

Attività	Amministratore di Cloud Manager	Amministratore tenant	Amministratore dell'ambiente di lavoro
Gestire le impostazioni dell'account	Sì	No	No
Configurare Kubernetes	Sì	No	No
Passare dalla visualizzazione del sistema di storage a quella del volume	Sì	No	No
Modificare le impostazioni	Sì	No	No
Visualizza e gestisci la dashboard di supporto	Sì	No	No
Backup e ripristino di Cloud Manager	Sì	No	No
Rimuovere un ambiente di lavoro	Sì	No	No
Aggiorna Cloud Manager	Sì	No	No
Installare un certificato HTTPS	Sì	No	No
Configurare Active Directory	Sì	No	No
Attiva il Cloud Storage Automation Report	Sì	No	No

Dove trovare assistenza e ulteriori informazioni

Puoi ottenere aiuto e ottenere ulteriori informazioni su Cloud Manager e Cloud Volumes ONTAP attraverso varie risorse, tra cui video, forum e supporto.

- ["Video per Cloud Manager e Cloud Volumes ONTAP"](#)

Guarda i video che mostrano come implementare e gestire Cloud Volumes ONTAP in AWS e Azure e come replicare i dati nel tuo cloud ibrido.

- ["Policy per Cloud Manager"](#)

Scarica i file JSON che includono le autorizzazioni necessarie a Cloud Manager per eseguire azioni in AWS e Azure.

- ["Guida per sviluppatori API di Cloud Manager"](#)

Leggi una panoramica delle API, esempi di come utilizzarle e un riferimento API.

- Training per Cloud Volumes ONTAP
 - ["Nozioni di base su Cloud Volumes ONTAP"](#)

- ["Implementazione e gestione di Cloud Volumes ONTAP per Azure"](#)

- Report tecnici

- ["Report tecnico di NetApp 4383: Caratterizzazione delle performance di Cloud Volumes ONTAP nei servizi Web Amazon con carichi di lavoro delle applicazioni"](#)

- ["Report tecnico di NetApp 4671: Caratterizzazione delle performance di Cloud Volumes ONTAP in Azure con carichi di lavoro applicativi"](#)

- ["Guida rapida alla preparazione del disaster recovery per Cloud Volumes ONTAP 9 SVM"](#)

Descrive come configurare rapidamente una SVM di destinazione in preparazione al disaster recovery.

- ["Guida rapida al disaster recovery di Cloud Volumes ONTAP 9 SVM"](#)

Descrive come attivare rapidamente una SVM di destinazione dopo un disastro e riattivare la SVM di origine.

- ["Centro documentazione di ONTAP 9"](#)

Accedi alla documentazione del prodotto per ONTAP, che può aiutarti a utilizzare Cloud Volumes ONTAP.

- ["Supporto NetApp Cloud Volumes ONTAP"](#)

Accedi alle risorse di supporto per ottenere assistenza e risolvere i problemi relativi a Cloud Volumes ONTAP.

- ["Community NetApp: Servizi dati cloud"](#)

Connettiti con i colleghi, fai domande, scambia idee, trova risorse e condividi le Best practice.

- ["NetApp Cloud Central"](#)

Informazioni su ulteriori prodotti e soluzioni NetApp per il cloud.

- ["Documentazione sui prodotti NetApp"](#)

Cerca nella documentazione dei prodotti NetApp istruzioni, risorse e risposte.

Informazioni sul copyright

Copyright © 2024 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 COMMERCIALIZZABILITÀ 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 CONSEGUENZIALE (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.