Riferimento

Cloud Manager 3.7

NetApp
March 25, 2024

Sommario

Riferimento

Domande frequenti: Integrazione di Cloud Manager con NetApp Cloud Central

Quando si esegue l'aggiornamento da Cloud Manager 3.4 o versioni precedenti, 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 accesso HTTP dai browser Web client alla console Web Cloud Manager e connessioni da Cloud Compliance
HTTPS	443	Fornisce l'accesso HTTPS dai browser Web client alla console Web di Cloud Manager
TCP	3128	Fornisce all'istanza Cloud Compliance l'accesso a Internet, se la rete AWS non utilizza un NAT o un proxy

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
	TCP	8088	Backup su S3	API chiama il backup in S3
DNS	UDP	53	DNS	Utilizzato per la risoluzione DNS da parte di Cloud Manager
Conformità al cloud	HTTP	80	Istanza di Cloud Compliance	Conformità del cloud per Cloud Volumes ONTAP

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					

				Directory	
	TCP	389	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	LDAP
Servizio	**Protocollo**	**Porta**	**Origine**	**Destinazione**	**Scopo**
	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)
Backup su S3	TCP	5010	LIF intercluster	Endpoint di backup o endpoint di ripristino	Operazioni di backup e ripristino per la funzione Backup in S3
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.

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

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

Servizio	Porta	Protocollo	Destinazione	Scopo
Chiamate API e AutoSupport	443	HTTPS	LIF gestione cluster ONTAP e Internet in uscita	Chiamate API ad AWS e ONTAP e invio di messaggi AutoSupport a NetApp
Chiamate API	3000	TCP	LIF gestione cluster ONTAP	Chiamate API a ONTAP
DNS	53	UDP	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

Le regole elencate di seguito consentono il traffico, a meno che la descrizione non noti che blocca lo specifico traffico in entrata.

Priorità e nome	Porta e protocollo	Origine e destinazione	Descrizione
1000 inbound_ssh	22 TCP	Qualsiasi a qualsiasi	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 a qualsiasi	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 a qualsiasi	Chiamata a procedura remota per NFS
1003 inbound_111_udp	111 UDP	Qualsiasi a qualsiasi	Chiamata a procedura remota per NFS
1004 inbound_139	139 TCP	Qualsiasi a qualsiasi	Sessione del servizio NetBIOS per CIFS
1005 inbound_161-162 _tcp	161-162 TCP	Qualsiasi a qualsiasi	Protocollo di gestione di rete semplice
1006 inbound_161-162 _udp	161-162 UDP	Qualsiasi a qualsiasi	Protocollo di gestione di rete semplice
1007 inbound_443	443 TCP	Qualsiasi a qualsiasi	Accesso HTTPS alla console Web di System Manager utilizzando l'indirizzo IP della LIF di gestione del cluster

Priorità e nome	Porta e protocollo	Origine e destinazione	Descrizione
1008 inbound_445	445 TCP	Qualsiasi a qualsiasi	Microsoft SMB/CIFS su TCP con frame NetBIOS
1009 inbound_635_tcp	635 TCP	Qualsiasi a qualsiasi	Montaggio NFS
1010 inbound_635_udp	635 UDP	Qualsiasi a qualsiasi	Montaggio NFS
1011 inbound_749	749 TCP	Qualsiasi a qualsiasi	Kerberos
1012 inbound_2049_tcp	2049 TCP	Qualsiasi a qualsiasi	Daemon del server NFS
1013 inbound_2049_udp	2049 UDP	Qualsiasi a qualsiasi	Daemon del server NFS
1014 inbound_3260	3260 TCP	Qualsiasi a qualsiasi	Accesso iSCSI tramite LIF dei dati iSCSI
1015 inbound_4045-4046_tcp	4045-4046 TCP	Qualsiasi a qualsiasi	NFS lock daemon e network status monitor
1016 inbound_4045-4046_udp	4045-4046 UDP	Qualsiasi a qualsiasi	NFS lock daemon e network status monitor
1017 inbound_10000	10000 TCP	Qualsiasi a qualsiasi	Backup con NDMP
1018 inbound_11104-11105	11104-11105 TCP	Qualsiasi a qualsiasi	Trasferimento dei dati SnapMirror
3000 inbound_deny _all_tcp	Qualsiasi porta TCP	Qualsiasi a qualsiasi	Blocca tutto il traffico TCP in entrata
3001 inbound_deny _all_udp	Qualsiasi porta UDP	Qualsiasi a qualsiasi	Blocca tutto il traffico UDP in entrata
65000 AllowVnetInBound	Qualsiasi porta qualsiasi protocollo	Da VirtualNetwork a VirtualNetwork	Traffico in entrata dall'interno di VNET
65001 AllowAzureLoad BalancerInBound	Qualsiasi porta qualsiasi protocollo	AzureLoadBalancer a qualsiasi	Traffico di dati dal bilanciamento del carico standard di Azure
65500 DenyAllInBound	Qualsiasi porta qualsiasi protocollo	Qualsiasi a qualsiasi	Bloccare tutto il traffico in entrata

Regole in entrata per i sistemi ha

Le regole elencate di seguito consentono il traffico, a meno che la descrizione non noti che blocca lo specifico traffico in entrata.

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 e nome	Porta e protocollo	Origine e destinazione	Descrizione
100 inbound_443	443 qualsiasi protocollo	Qualsiasi a qualsiasi	Accesso HTTPS alla console Web di System Manager utilizzando l'indirizzo IP della LIF di gestione del cluster
101 inbound_111_tcp	111 qualsiasi protocollo	Qualsiasi a qualsiasi	Chiamata a procedura remota per NFS
102 inbound_2049_tcp	2049 qualsiasi protocollo	Qualsiasi a qualsiasi	Daemon del server NFS
111 inbound_ssh	22 qualsiasi protocollo	Qualsiasi a qualsiasi	Accesso SSH all'indirizzo IP della LIF di gestione del cluster o di una LIF di gestione dei nodi
121 inbound_53	53 qualsiasi protocollo	Qualsiasi a qualsiasi	DNS e CIFS
65000 AllowVnetInBound	Qualsiasi porta qualsiasi protocollo	Da VirtualNetwork a VirtualNetwork	Traffico in entrata dall'interno di VNET
65001 AllowAzureLoad BalancerInBound	Qualsiasi porta qualsiasi protocollo	AzureLoadBalancer a qualsiasi	Traffico di dati dal bilanciamento del carico standard di Azure
65500 DenyAllInBound	Qualsiasi porta qualsiasi protocollo	Qualsiasi a qualsiasi	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.

Porta	Protocollo	Scopo
Tutto	Tutti i TCP	Tutto il traffico in uscita
Tutto	Tutti gli UDP	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	Porta	Protocollo	Origine	Destinazione	Scopo
Active Directory					

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

Regole firewall per GCP

Cloud Manager crea regole firewall GCP 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

Le regole firewall per Cloud Manager richiedono regole sia in entrata che in uscita.

Regole in entrata per Cloud Manager

L'origine delle regole in entrata nelle regole firewall predefinite 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

Le regole predefinite del firewall per Cloud Manager aprono 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

Le regole firewall predefinite per Cloud Manager includono 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 a GCP 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

Pagine del marketplace AWS per Cloud Manager e Cloud Volumes ONTAP

Nel marketplace AWS sono disponibili diverse offerte per Cloud Manager e Cloud Volumes ONTAP. Se non sei sicuro di quale pagina devi utilizzare, leggi di seguito e ti indirizzeremo alla pagina giusta in base al tuo obiettivo.

In tutti i casi, non è possibile avviare Cloud Volumes ONTAP in AWS dal marketplace AWS. È necessario avviarlo direttamente da Cloud Manager.

Obiettivo	Pagina AWS Marketplace da utilizzare	Ulteriori informazioni
Abilitare l'implementazione DI Cloud Volumes ONTAP PAYGO per le versioni 9.6 e successive	"Cloud Manager (per Cloud Volumes ONTAP)"	Questa pagina di AWS Marketplace consente di addebitare la versione PAYGO di Cloud Volumes ONTAP 9.6 e versioni successive. Consente inoltre di addebitare le funzioni aggiuntive di Cloud Volumes ONTAP. Questa pagina non consente di avviare Cloud Manager in AWS. Questo dovrebbe essere fatto da "NetApp Cloud Central", O in alternativa utilizzando l'AMI elencato nella riga 4 di questa tabella.
Abilitare le funzionalità add-on per Cloud Volumes ONTAP (PAYGO o BYOL)		
Consentire l'implementazione di Cloud Volumes ONTAP utilizzando una licenza acquistata da NetApp (BYOL)	• "Cloud Volumes ONTAP per AWS (BYOL)" • "Cloud Volumes ONTAP per AWS - alta disponibilità (BYOL)"	Queste pagine del marketplace AWS consentono di iscriversi alle versioni a nodo singolo o ha di Cloud Volumes ONTAP BYOL.
Implementare Cloud Manager da AWS Marketplace utilizzando un AMI	"NetApp Cloud Manager (per NetApp Cloud Volumes ONTAP)"	Si consiglia di avviare Cloud Manager in AWS da "NetApp Cloud Central", Ma è possibile avviarlo da questa pagina di AWS Marketplace, se si preferisce.

Obiettivo	Pagina AWS Marketplace da utilizzare	Ulteriori informazioni
Implementazione di Cloud Volumes ONTAP PAYGO (9.5 o precedente)	• "Cloud Volumes ONTAP per AWS" • "Cloud Volumes ONTAP per AWS - alta disponibilità"	Queste pagine di AWS Marketplace consentono di sottoscrivere le versioni a nodo singolo o ha di Cloud Volumes ONTAP PAYGO per le versioni 9.5 e precedenti. A partire dalla versione 9.6, è necessario iscriversi alla pagina AWS Marketplace elencata nella riga 1 di questa tabella per le implementazioni PAYGO.

In che modo Cloud Manager utilizza le autorizzazioni del cloud provider

Cloud Manager richiede autorizzazioni per eseguire azioni nel tuo cloud provider. 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:DescripbeInstances", "ec2:DescripbeInstanceStatus", "ec2:RunInstances", "ec2:TerminateInstances", "ec2:ModifyInstanceAttribute",	Avvia un'istanza di Cloud Volumes ONTAP e interrompe, avvia e monitora l'istanza.
"ec2:DescripbeInstanceAttribute",	Verifica che la rete avanzata sia abilitata per i tipi di istanze supportati.
"ec2:DescripbeRouteTable", "ec2:DescripbeImages",	Avvia una configurazione Cloud Volumes ONTAP ha.
"ec2:CreateTags",	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:DescripbeVolumes", "ec2:ModifyVolumeAttribute", "ec2:AttachVolume", "ec2:DeleteVolume", "ec2:DetachVolume",	Gestisce i volumi EBS utilizzati da Cloud Volumes ONTAP come storage back-end.

Azioni	Scopo
"ec2:CreateSecurityGroup", "ec2:DeleteSecurityGroup", "ec2:DescripbeSecurityGroups", "ec2:RevokeSecurityGroupErgress", "ec2:AuthorizeSecurityGroupErgress", "ec2:AuthorizeSecurityGroupIngress", "ec2:RevokeSecurityGroupIngress",	Crea gruppi di protezione predefiniti per Cloud Volumes ONTAP.
"ec2:CreateNetworkInterface", "ec2:DescripbeNetworkInterfaces", "ec2:DeleteNetworkInterface", "ec2:ModifyNetworkInterfaceAttribute",	Crea e gestisce le interfacce di rete per Cloud Volumes ONTAP nella subnet di destinazione.
"ec2:DescripbeSubnet", "ec2:DescripbeVpcs",	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:DescripbeDhcpOptions",	Determina i server DNS e il nome di dominio predefinito quando si avviano le istanze di Cloud Volumes ONTAP.
"ec2:CreateSnapshot", "ec2:DeleteSnapshot", "ec2:DescripbeSnapshot",	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:DescripbeKeyPairs",	Ottiene l'elenco delle coppie di chiavi disponibili quando si avviano le istanze.
"ec2:DescripbeRegions",	Ottiene un elenco delle regioni AWS disponibili.
"ec2:DeleteTags", "ec2:DescripteTags",	Gestisce i tag per le risorse associate alle istanze di Cloud Volumes ONTAP.
"Cloudformation:CreateStack", "Cloudformation:DeleteStack", "Cloudformation:DescripbeStack", "Cloudformation:DescripbeStackEvents", "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:DescripbeIamInstanceProfileAssociations", "ec2:DisassociateIamInstanceProfile",	Gestisce i profili di istanza per le istanze di Cloud Volumes ONTAP.

Azioni	Scopo
"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:descrivi*"	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/rigeneratekey/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.

Azioni	Scopo
"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/checkIpAddressAvailability/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.
"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.

Azioni	Scopo
"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.

Cosa fa Cloud Manager con le autorizzazioni GCP

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

Azioni	Scopo
- Compute.disks.create - compute.disks.createSnapshot - compute.disks.delete - compute.disks.get - compute.disks.list - compute.disks.setLabels - compute.disks.use	Per creare e gestire dischi per Cloud Volumes ONTAP.
- compute.firewalls.create - compute.firewalls.delete - compute.firewalls.get - compute.firewalls.list	Per creare regole firewall per Cloud Volumes ONTAP.
- Compute.globalOperations.get	Per ottenere lo stato delle operazioni.
- Compute.images.get - compute.images.getFromFamily - compute.images.list - compute.images.useReadOnly	Per ottenere immagini per istanze di macchine virtuali.
- compute.instances.attachDisk - compute.instances.detachDisk	Per collegare e scollegare i dischi a Cloud Volumes ONTAP.
- compute.instances.create - compute.instances.delete	Per creare ed eliminare istanze di Cloud Volumes ONTAP VM.
- compute.instances.get	Per elencare le istanze di macchine virtuali.
- compute.instances.getSerialPortOutput	Per ottenere i log della console.
- compute.instances.list	Per recuperare l’elenco di istanze in una zona.
- compute.instances.setDeletionProtection	Per impostare la protezione di eliminazione sull’istanza.
- compute.instances.setLabels	Per aggiungere etichette.

Azioni	Scopo
- compute.instances.setMachineType	Per modificare il tipo di macchina per Cloud Volumes ONTAP.
- compute.instances.setMetadata	Per aggiungere metadati.
- compute.instances.setTags	Per aggiungere tag per le regole del firewall.
- compute.instances.start - compute.instances.stop - compute.instances.updateDisplayDevice	Per avviare e arrestare Cloud Volumes ONTAP.
- Compute.machineTypes.get	Per ottenere il numero di core per controllare le qoutas.
- compute.projects.get	Per supportare progetti multipli.
- Compute.Snapshot.create - compute.snapshots.delete - compute.Snapshot.get - compute.Snapshot.list - compute.snapshots.setLabels	Per creare e gestire snapshot di dischi persistenti.
- compute.networks.get - compute.networks.list - compute.regions.get - compute.regions.list - compute.subnetworks.get - compute.subnetworks.list - compute.zoneOperations.get - compute.zones.get - compute.zone.list	Per ottenere le informazioni di rete necessarie per creare una nuova istanza di macchina virtuale Cloud Volumes ONTAP.
- deploymentmanager.compositeTypes.get - deploymentmanager.compositeTypes.list - deploymentmanager.deployments.create - deploymentmanager.deployments.delete - deploymentmanager.deployments.get - deploymentmanager.deployments.list - deploymentmanager.manifests.get - deploymentmanager.manifests.list - deploymentmanager.Operations.get - deploymentmanager.Operations.list - deploymentmanager.resources.get - deploymentmanager.typeProviders.get - deploymentmanager.typeProviders.list - deploymentmanager.typeopers.get.get.get - deploymentmanager.get.list	Per implementare l'istanza della macchina virtuale Cloud Volumes ONTAP utilizzando Google Cloud Deployment Manager.
- Logging.logEntries.list - logging.privateLogEntries.list	Per ottenere unità di log stack.
- resourcemanager.projects.get	Per supportare progetti multipli.
- storage.bucket.create - storage.buckets.delete - storage.bucket.get - storage.bucket.list	Per creare e gestire un bucket di storage Google Cloud per il tiering dei dati.
- cloudkms.cryptoKeyVersions.useToEncrypt - cloudkms.cryptKeys.get - cloudkms.cryptKeys.list - cloudkms.keyrings.list	Per utilizzare le chiavi di crittografia gestite dal cliente dal servizio di gestione delle chiavi cloud con Cloud Volumes ONTAP.

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 dal mercato di un cloud provider), prendi nota di quanto segue:
  - In AWS, il nome utente per l'istanza EC2 Linux è ec2-user.
  - 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 in AWS, Azure e GCP e come coppia ha in AWS e Azure.
- Cloud Manager crea una SVM per il servizio dei dati quando implementa Cloud Volumes ONTAP. Non è supportato l'utilizzo di più SVM per la distribuzione dei dati.
- Cloud Manager installa automaticamente le seguenti licenze ONTAP Feature su Cloud Volumes ONTAP:
  - CIFS
  - FlexCache

- FlexClone
- ISCSI
- NetApp Volume Encryption (solo per sistemi BYOL o PAYGO registrati)
- NFS
- SnapMirror
- SnapRestore
- SnapVault

- Per impostazione predefinita, vengono create diverse interfacce di rete:
  - Una LIF di gestione del cluster
  - Un LIF intercluster
  - LIF di gestione SVM su sistemi ha in Azure, sistemi a nodo singolo in AWS e, facoltativamente, su sistemi ha in più zone di disponibilità AWS
  - 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 dell'account può modificare questo valore dalla pagina Impostazioni.
Stile di sicurezza	NTFS per CIFS Volumes UNIX per NFS Volumes
Stile garanzia di spazio	nessuno

Attributo	Valore stabilito da Cloud Manager
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

- Due dischi SSD General Purpose:
  - Un disco da 140 GB per i dati root (uno per nodo)
  - 9.6 e versioni successive: Un disco da 86 GB per i dati di avvio (uno per nodo)
  - 9.5 e versioni precedenti: Un disco da 45 GB per i dati di avvio (uno per nodo)
- Un'istantanea EBS per ogni disco di boot e disco root
- Per le coppie ha, un volume EBS per l'istanza Mediator, che è di circa 8 GB

Azure (nodo singolo)

- Due dischi SSD Premium:
  - Un disco da 90 GB per i dati di avvio
  - Un disco da 140 GB per i dati root
- Uno snapshot Azure per ogni disco di boot e disco root

Azure (coppie ha)

- Due dischi SSD Premium da 90 GB per il volume di boot (uno per nodo)
- Due blob di pagina Premium Storage da 140 GB per il volume root (uno per nodo)
- Due dischi HDD standard da 128 GB per il risparmio di core (uno per nodo)
- Uno snapshot Azure per ogni disco di boot e disco root

GCP

- Un disco persistente standard da 10 GB per i dati di avvio
- Un disco persistente standard da 64 GB per i dati root
- Un disco persistente standard da 500 GB per NVRAM
- Un disco persistente standard da 216 GB per il risparmio dei core
- Uno snapshot GCP per il disco di boot e il disco root

Dove risiedono i dischi

Cloud Manager definisce lo storage come segue:

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

  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.

Crittografia

I dischi di boot e root sono sempre crittografati in Azure e Google Cloud Platform perché la crittografia è attivata per impostazione predefinita in tali provider cloud.

Quando si attiva la crittografia dei dati in AWS utilizzando il servizio di gestione delle chiavi (KMS), vengono crittografati anche i dischi di avvio e i dischi root per Cloud Volumes ONTAP. Questo include il disco di boot per l'istanza del mediatore in una coppia ha. I dischi vengono crittografati utilizzando la CMK selezionata quando si crea l'ambiente di lavoro.

Ruoli

I ruoli account Admin (Amministratore account) e Workspace Admin (Amministratore area di lavoro) forniscono autorizzazioni specifiche agli utenti.

Attività	Amministratore account	Amministratore dello spazio di lavoro
Gestire gli ambienti di lavoro	Sì	Sì, per le aree di lavoro associate
Visualizzare lo stato della replica dei dati	Sì	Sì, per le aree di lavoro associate
Visualizza la timeline	Sì	Sì, per le aree di lavoro associate
Eliminare gli ambienti di lavoro	Sì	No
Connettere i cluster Kubernetes a Cloud Volumes ONTAP	Sì	No
Ricevere il report Cloud Volumes ONTAP	Sì	No
Gestire gli account Cloud Central	Sì	No
Gestire gli account dei cloud provider	Sì	No
Modificare le impostazioni di Cloud Manager	Sì	No
Visualizza e gestisci la dashboard di supporto	Sì	No

Attività	Amministratore account	Amministratore dello spazio di lavoro
Rimuovere gli ambienti di lavoro da Cloud Manager	Sì	No
Aggiorna Cloud Manager	Sì	No
Installare un certificato HTTPS	Sì	No
Configurare Active Directory	Sì	No

Link correlati

- "Impostazione di aree di lavoro e utenti nell'account Cloud Central"
- "Gestione degli spazi di lavoro e degli utenti nell'account Cloud Central"

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 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 un cloud provider.

- "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"
  - "Implementazione e gestione di Cloud Volumes ONTAP per AWS"
- 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"
- Disaster recovery SVM

  Il disaster recovery SVM è il mirroring asincrono dei dati SVM e della configurazione da una SVM di origine a una SVM di destinazione. È possibile attivare rapidamente una SVM di destinazione per l'accesso ai dati se la SVM di origine non è più disponibile.

  - "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.

- "Guida all'alimentazione di FlexCache Volumes per un accesso più rapido ai dati"

  Viene descritto come creare e gestire volumi FlexCache nello stesso cluster o in un cluster diverso del volume di origine per accelerare i dati access.es come attivare rapidamente una SVM di destinazione dopo un disastro, quindi riattivare la SVM di origine.

- "Avvisi di sicurezza"

  Identificare le vulnerabilità note (CVE) per i prodotti NetApp, incluso ONTAP. Si noti che è possibile correggere le vulnerabilità di sicurezza per Cloud Volumes ONTAP seguendo la documentazione di ONTAP.

- "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

Informazioni sul marchio commerciale