Referenz

Cloud Manager 3.6

NetApp
March 25, 2024

Inhalt

Referenz

Häufig gestellte Fragen: Integration von Cloud Manager in NetApp Cloud Central

Bei einem Upgrade auf Cloud Manager 3.5 wählt NetApp bestimmte Cloud Manager-Systeme zur Integration in NetApp Cloud Central aus, sofern diese noch nicht integriert sind. In dieser FAQ können Sie Fragen zu diesem Prozess beantworten.

Was ist NetApp Cloud Central?

NetApp Cloud Central bietet einen zentralen Standort für den Zugriff auf und das Management von NetApp Cloud Data Services. Mit diesen Services können Sie kritische Applikationen in der Cloud ausführen, automatisierte DR-Standorte erstellen, Ihre SaaS-Daten sichern und Daten effektiv über mehrere Clouds hinweg migrieren und steuern.

Warum integriert NetApp mein Cloud Manager-System in Cloud Central?

Die Integration von Cloud Manager in NetApp Cloud Central bietet verschiedene Vorteile, darunter eine vereinfachte Implementierung, ein zentraler Speicherort zum Anzeigen und Managen mehrerer Cloud Manager-Systeme und eine zentralisierte Benutzerauthentifizierung.

Was passiert während des Integrationsprozesses?

NetApp migriert alle lokalen Benutzerkonten in Ihrem Cloud Manager-System auf die zentralisierte Benutzerauthentifizierung, die in Cloud Central verfügbar ist.

Wie funktioniert die zentralisierte Benutzerauthentifizierung?

Mit der zentralisierten Benutzerauthentifizierung können Sie dieselben Anmeldedaten für Cloud Manager-Systeme und zwischen Cloud Manager und anderen Datenservices wie Cloud Sync verwenden. Sie können Ihr Passwort auch einfach zurücksetzen, wenn Sie es vergessen haben.

Muss ich mich für ein Cloud Central Benutzerkonto anmelden?

NetApp erstellt für Sie ein Cloud Central Benutzerkonto, wenn wir Ihr Cloud Manager System in Cloud Central integrieren. Sie müssen Ihr Passwort zurücksetzen, um die Registrierung abzuschließen.

Was passiert, wenn ich bereits ein Cloud Central Benutzerkonto habe?

Wenn die E-Mail-Adresse, mit der Sie sich bei Cloud Manager anmelden, mit der E-Mail-Adresse für ein Cloud Central-Benutzerkonto übereinstimmt, können Sie sich direkt bei Ihrem Cloud Manager-System anmelden.

Was ist, wenn mein Cloud Manager-System über mehrere Benutzerkonten verfügt?

NetApp migriert alle lokalen Benutzerkonten zu Cloud Central Benutzerkonten. Jeder Benutzer muss sein Passwort zurücksetzen.

Was passiert, wenn ich ein Benutzerkonto habe, das dieselbe E-Mail-Adresse in mehreren Cloud Manager-Systemen verwendet?

Sie müssen Ihr Kennwort nur einmal zurücksetzen. Anschließend können Sie sich über dasselbe Cloud Central-Benutzerkonto bei jedem Cloud Manager-System anmelden.

Was geschieht, wenn mein lokales Benutzerkonto eine ungültige E-Mail-Adresse verwendet?

Zum Zurücksetzen des Passworts ist eine gültige E-Mail-Adresse erforderlich. Kontaktieren Sie uns über das Chat-Symbol unten rechts in der Cloud Manager-Oberfläche.

Was ist, wenn ich Automatisierungsskripts für Cloud Manager-APIs habe?

Alle APIs sind abwärtskompatibel. Sie müssen Skripts aktualisieren, die Kennwörter verwenden, wenn Sie Ihr Kennwort ändern, wenn Sie es zurücksetzen.

Was ist, wenn mein Cloud Manager-System LDAP verwendet?

Wenn Ihr System LDAP verwendet, kann NetApp das System nicht automatisch in Cloud Central integrieren. Sie müssen die folgenden Schritte manuell ausführen:

1. Implementieren Sie ein neues Cloud Manager System von "NetApp Cloud Central".
2. "Richten Sie LDAP mit dem neuen System ein".
3. "Erkennung vorhandener Cloud Volumes ONTAP Systeme" Über das neue Cloud Manager System.
4. Löschen Sie das alte Cloud Manager-System.

Spielt es eine Rolle, wo ich mein Cloud Manager-System installiert habe?

Nein NetApp integriert Systeme in Cloud Central, unabhängig davon, wo sie sich befinden, ob AWS, Azure oder in Ihrem Unternehmen.

Die einzige Ausnahme bildet die AWS Commercial Cloud Services Environment.

Sicherheitsgruppenregeln für AWS

Cloud Manager erstellt AWS-Sicherheitsgruppen, die die ein- und ausgehenden Regeln enthalten, die Cloud Manager und Cloud Volumes ONTAP für einen erfolgreichen Betrieb benötigen. Sie können die Ports zu Testzwecken oder zur Verwendung eigener Sicherheitsgruppen verwenden.

Regeln für Cloud Manager

Für die Sicherheitsgruppe für Cloud Manager sind sowohl eingehende als auch ausgehende Regeln erforderlich.

Eingehende Regeln für Cloud Manager

Die Quelle für eingehende Regeln in der vordefinierten Sicherheitsgruppe ist 0.0.0.0/0.

Protokoll	Port	Zweck
SSH	22	Bietet SSH-Zugriff auf den Cloud Manager-Host
HTTP	80	Bietet HTTP-Zugriff von Client-Webbrowsern auf die Cloud Manager-Webkonsole
HTTPS	443	Bietet HTTPS-Zugriff von Client-Webbrowsern auf die Cloud Manager-Webkonsole

Outbound-Regeln für Cloud Manager

Die vordefinierte Sicherheitsgruppe für Cloud Manager öffnet den gesamten ausgehenden Datenverkehr. Wenn dies akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Anrufe. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Outbound-Regeln.

Grundlegende Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für Cloud Manager enthält die folgenden ausgehenden Regeln.

Protokoll	Port	Zweck
Alle TCP	Alle	Gesamter abgehender Datenverkehr
Alle UDP-Protokolle	Alle	Gesamter abgehender Datenverkehr

Erweiterte Outbound-Regeln

Wenn Sie starre Regeln für ausgehenden Datenverkehr benötigen, können Sie die folgenden Informationen verwenden, um nur die Ports zu öffnen, die für die ausgehende Kommunikation durch Cloud Manager erforderlich sind.

Die Quell-IP-Adresse ist der Cloud Manager-Host.

Service	Protokoll	Port	Ziel	Zweck
Active Directory	TCP	88	Active Directory-Gesamtstruktur	Kerberos V-Authentifizierung
	TCP	139	Active Directory-Gesamtstruktur	Sitzung für den NETBIOS-Dienst
	TCP	389	Active Directory-Gesamtstruktur	LDAP
	TCP	445	Active Directory-Gesamtstruktur	Microsoft SMB/CIFS über TCP mit NETBIOS-Framing
	TCP	464	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern und festlegen (SET_CHANGE)
	TCP	749	Active Directory-Gesamtstruktur	Active Directory Kerberos V - Kennwort ändern und festlegen (RPCSEC_GSS)
	UDP	137	Active Directory-Gesamtstruktur	NetBIOS-Namensdienst
	UDP	138	Active Directory-Gesamtstruktur	Netbios Datagramm-Dienst
	UDP	464	Active Directory-Gesamtstruktur	Kerberos-Schlüsselverwaltung
API-Aufrufe und AutoSupport	HTTPS	443	Outbound-Internet und ONTAP Cluster Management LIF	API-Aufrufe an AWS und ONTAP und Senden von AutoSupport Nachrichten an NetApp
API-Aufrufe	TCP	3000	ONTAP Cluster Management LIF	API-Aufrufe für ONTAP
DNS	UDP	53	DNS	Wird für die DNS-Auflösung durch Cloud Manager verwendet

Regeln für Cloud Volumes ONTAP

Die Sicherheitsgruppe für Cloud Volumes ONTAP erfordert sowohl eingehende als auch ausgehende Regeln.

Eingehende Regeln für Cloud Volumes ONTAP

Die Quelle für eingehende Regeln in der vordefinierten Sicherheitsgruppe ist 0.0.0.0/0.

Protokoll	Port	Zweck
Alle ICMP	Alle	Pingen der Instanz
HTTP	80	HTTP-Zugriff auf die System Manager Webkonsole mit der IP-Adresse der Cluster-Management-LIF
HTTPS	443	HTTPS-Zugriff auf die System Manager-Webkonsole unter Verwendung der IP-Adresse der Cluster-Management-LIF
SSH	22	SSH-Zugriff auf die IP-Adresse der Cluster Management LIF oder einer Node Management LIF
TCP	111	Remote-Prozeduraufruf für NFS
TCP	139	NetBIOS-Servicesitzung für CIFS
TCP	161-162	Einfaches Netzwerkverwaltungsprotokoll
TCP	445	Microsoft SMB/CIFS über TCP mit NETBIOS-Framing
TCP	635	NFS-Mount
TCP	749	Kerberos
TCP	2049	NFS-Server-Daemon
TCP	3260	ISCSI-Zugriff über die iSCSI-Daten-LIF
TCP	4045	NFS-Sperr-Daemon
TCP	4046	Netzwerkstatusüberwachung für NFS
TCP	10.000	Backup mit NDMP
TCP	11104	Management von interclusterübergreifenden Kommunikationssitzungen für SnapMirror
TCP	11105	SnapMirror Datenübertragung über Cluster-interne LIFs
UDP	111	Remote-Prozeduraufruf für NFS
UDP	161-162	Einfaches Netzwerkverwaltungsprotokoll
UDP	635	NFS-Mount
UDP	2049	NFS-Server-Daemon
UDP	4045	NFS-Sperr-Daemon
UDP	4046	Netzwerkstatusüberwachung für NFS
UDP	4049	NFS rquotad-Protokoll

Outbound-Regeln für Cloud Volumes ONTAP

Die vordefinierte Sicherheitsgruppe für Cloud Volumes ONTAP öffnet den gesamten ausgehenden Datenverkehr. Wenn dies akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Anrufe. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Outbound-Regeln.

Grundlegende Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für Cloud Volumes ONTAP enthält die folgenden ausgehenden Regeln.

Protokoll	Port	Zweck
Alle ICMP	Alle	Gesamter abgehender Datenverkehr
Alle TCP	Alle	Gesamter abgehender Datenverkehr
Alle UDP-Protokolle	Alle	Gesamter abgehender Datenverkehr

Erweiterte Outbound-Regeln

Wenn Sie strenge Regeln für ausgehenden Datenverkehr benötigen, können Sie mit den folgenden Informationen nur die Ports öffnen, die für die ausgehende Kommunikation durch Cloud Volumes ONTAP erforderlich sind.

Die Quelle ist die Schnittstelle (IP-Adresse) auf dem Cloud Volumes ONTAP System.

Service	Protokoll	Port	Quelle	Ziel	Zweck
Active Directory	TCP	88	Node Management-LIF	Active Directory-Gesamtstruktur	Kerberos V-Authentifizierung
	UDP	137	Node Management-LIF	Active Directory-Gesamtstruktur	NetBIOS-Namensdienst
	UDP	138	Node Management-LIF	Active Directory-Gesamtstruktur	Netbios Datagramm-Dienst
	TCP	139	Node Management-LIF	Active Directory-Gesamtstruktur	Sitzung für den NETBIOS-Dienst
	TCP	389	Node Management-LIF	Active Directory-Gesamtstruktur	LDAP
	TCP	445	Node Management-LIF	Active Directory-Gesamtstruktur	Microsoft SMB/CIFS über TCP mit NETBIOS-Framing
	TCP	464	Node Management-LIF	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern und festlegen (SET_CHANGE)
	UDP	464	Node Management-LIF	Active Directory-Gesamtstruktur	Kerberos-Schlüsselverwaltung
	TCP	749	Node Management-LIF	Active Directory-Gesamtstruktur	Kerberos V - Kennwort ändern und festlegen (RPCSEC_GSS)
	TCP	88	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Kerberos V-Authentifizierung
	UDP	137	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	NetBIOS-Namensdienst
	UDP	138	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Netbios Datagramm-Dienst
	TCP	139	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Sitzung für den NETBIOS-Dienst
	TCP	389	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	LDAP
	TCP	445	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Microsoft SMB/CIFS über TCP mit NETBIOS-Framing
	TCP	464	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern und festlegen (SET_CHANGE)
	UDP	464	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Kerberos-Schlüsselverwaltung
	TCP	749	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Kerberos V - Passwort ändern und festlegen (RPCSEC_GSS)

Service	Protokoll	Port	Quelle	Ziel	Zweck
Cluster	Gesamter Datenverkehr	Gesamter Datenverkehr	Alle LIFs auf einem Node	Alle LIFs auf dem anderen Node	Kommunikation zwischen Clustern (nur Cloud Volumes ONTAP HA)
	TCP	3000	Node Management-LIF	Ha Mediator	ZAPI-Aufrufe (nur Cloud Volumes ONTAP HA)
	ICMP	1	Node Management-LIF	Ha Mediator	Bleiben Sie am Leben (nur Cloud Volumes ONTAP HA)
DHCP	UDP	68	Node Management-LIF	DHCP	DHCP-Client für die erstmalige Einrichtung
DHCPS	UDP	67	Node Management-LIF	DHCP	DHCP-Server
DNS	UDP	53	Node Management LIF und Daten LIF (NFS, CIFS)	DNS	DNS
NDMP	TCP	18600-18699	Node Management-LIF	Zielserver	NDMP-Kopie
SMTP	TCP	25	Node Management-LIF	Mailserver	SMTP-Warnungen können für AutoSupport verwendet werden
SNMP	TCP	161	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps
	UDP	161	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps
	TCP	162	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps
	UDP	162	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps
SnapMirror	TCP	11104	Intercluster-LIF	ONTAP Intercluster-LIFs	Management von interclusterübergreifenden Kommunikationssitzungen für SnapMirror
	TCP	11105	Intercluster-LIF	ONTAP Intercluster-LIFs	SnapMirror Datenübertragung
Syslog	UDP	514	Node Management-LIF	Syslog-Server	Syslog-Weiterleitungsmeldungen

Regeln für die externe Sicherheitsgruppe des HA Mediators

Die vordefinierte externe Sicherheitsgruppe für den Cloud Volumes ONTAP HA Mediator enthält die folgenden Regeln für ein- und ausgehende Anrufe.

Regeln für eingehende Anrufe

Die Quelle für eingehende Regeln ist 0.0.0.0/0.

Protokoll	Port	Zweck
SSH	22	SSH-Verbindungen zum HA-Vermittler
TCP	3000	Ruhiger API-Zugriff über Cloud Manager

Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für den HA-Vermittler öffnet den gesamten ausgehenden Datenverkehr. Wenn dies akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Anrufe. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Outbound-Regeln.

Grundlegende Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für den HA-Vermittler enthält die folgenden Regeln für ausgehende Anrufe.

Protokoll	Port	Zweck
Alle TCP	Alle	Gesamter abgehender Datenverkehr
Alle UDP-Protokolle	Alle	Gesamter abgehender Datenverkehr

Erweiterte Outbound-Regeln

Wenn Sie starre Regeln für ausgehenden Datenverkehr benötigen, können Sie die folgenden Informationen verwenden, um nur die Ports zu öffnen, die für die ausgehende Kommunikation durch den HA-Vermittler erforderlich sind.

Protokoll	Port	Ziel	Zweck
HTTP	80	IP-Adresse von Cloud Manager	Lade Upgrades für den Mediator herunter
HTTPS	443	AWS API-Services	Unterstützung bei Storage Failover
UDP	53	AWS API-Services	Unterstützung bei Storage Failover

Anstatt die Ports 443 und 53 zu öffnen, können Sie einen VPC-Endpunkt des Zielsubnetzen zum AWS EC2 Service erstellen.

Regeln für die interne Sicherheitsgruppe des HA-Vermittlers

Die vordefinierte interne Sicherheitsgruppe für den Cloud Volumes ONTAP HA Mediator enthält die folgenden Regeln. Cloud Manager erstellt immer diese Sicherheitsgruppe. Sie haben nicht die Möglichkeit, Ihre eigenen zu verwenden.

Regeln für eingehende Anrufe

Die vordefinierte Sicherheitsgruppe enthält die folgenden Regeln für eingehende Anrufe.

Protokoll	Port	Zweck
Gesamter Datenverkehr	Alle	Kommunikation zwischen HA-Mediator und HA-Knoten

Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe enthält die folgenden ausgehenden Regeln.

Protokoll	Port	Zweck
Gesamter Datenverkehr	Alle	Kommunikation zwischen HA-Mediator und HA-Knoten

Sicherheitsgruppenregeln für Azure

Cloud Manager erstellt Azure Sicherheitsgruppen, die die ein- und ausgehenden Regeln enthalten, die Cloud Manager und Cloud Volumes ONTAP für einen erfolgreichen Betrieb benötigen. Sie können die Ports zu Testzwecken oder zur Verwendung eigener Sicherheitsgruppen verwenden.

Regeln für Cloud Manager

Für die Sicherheitsgruppe für Cloud Manager sind sowohl eingehende als auch ausgehende Regeln erforderlich.

Eingehende Regeln für Cloud Manager

Die Quelle für eingehende Regeln in der vordefinierten Sicherheitsgruppe ist 0.0.0.0/0.

Protokoll	Port	Zweck
SSH	22	Bietet SSH-Zugriff auf den Cloud Manager-Host
HTTP	80	Bietet HTTP-Zugriff von Client-Webbrowsern auf die Cloud Manager-Webkonsole
HTTPS	443	Bietet HTTPS-Zugriff von Client-Webbrowsern auf die Cloud Manager-Webkonsole

Outbound-Regeln für Cloud Manager

Die vordefinierte Sicherheitsgruppe für Cloud Manager öffnet den gesamten ausgehenden Datenverkehr. Wenn dies akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Anrufe. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Outbound-Regeln.

Grundlegende Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für Cloud Manager enthält die folgenden ausgehenden Regeln.

Protokoll	Port	Zweck
Alle TCP	Alle	Gesamter abgehender Datenverkehr
Alle UDP-Protokolle	Alle	Gesamter abgehender Datenverkehr

Erweiterte Outbound-Regeln

Wenn Sie starre Regeln für ausgehenden Datenverkehr benötigen, können Sie die folgenden Informationen verwenden, um nur die Ports zu öffnen, die für die ausgehende Kommunikation durch Cloud Manager erforderlich sind.

Die Quell-IP-Adresse ist der Cloud Manager-Host.

Service	Protokoll	Port	Ziel	Zweck
Active Directory	TCP	88	Active Directory-Gesamtstruktur	Kerberos V-Authentifizierung
	TCP	139	Active Directory-Gesamtstruktur	Sitzung für den NETBIOS-Dienst
	TCP	389	Active Directory-Gesamtstruktur	LDAP
	TCP	445	Active Directory-Gesamtstruktur	Microsoft SMB/CIFS über TCP mit NETBIOS-Framing
	TCP	464	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern und festlegen (SET_CHANGE)
	TCP	749	Active Directory-Gesamtstruktur	Active Directory Kerberos V - Kennwort ändern und festlegen (RPCSEC_GSS)
	UDP	137	Active Directory-Gesamtstruktur	NetBIOS-Namensdienst
	UDP	138	Active Directory-Gesamtstruktur	Netbios Datagramm-Dienst
	UDP	464	Active Directory-Gesamtstruktur	Kerberos-Schlüsselverwaltung
API-Aufrufe und AutoSupport	HTTPS	443	Outbound-Internet und ONTAP Cluster Management LIF	API-Aufrufe an AWS und ONTAP und Senden von AutoSupport Nachrichten an NetApp
API-Aufrufe	TCP	3000	ONTAP Cluster Management LIF	API-Aufrufe für ONTAP
DNS	UDP	53	DNS	Wird für die DNS-Auflösung durch Cloud Manager verwendet

Regeln für Cloud Volumes ONTAP

Die Sicherheitsgruppe für Cloud Volumes ONTAP erfordert sowohl eingehende als auch ausgehende Regeln.

Eingehende Regeln für Single-Node-Systeme

Priorität	Name	Port	Protokoll	Quelle	Ziel	Aktion	Beschreibung
1000	Inbound_SSH	22	TCP	Alle	Alle	Zulassen	SSH-Zugriff auf die IP-Adresse der Cluster Management LIF oder einer Node Management LIF
1001	Eingehend_http	80	TCP	Alle	Alle	Zulassen	HTTP-Zugriff auf die System Manager Webkonsole mit der IP-Adresse der Cluster-Management-LIF
1002	Inbound_111_tcp	111	TCP	Alle	Alle	Zulassen	Remote-Prozeduraufruf für NFS
1003	Eingehend_111_udp	111	UDP	Alle	Alle	Zulassen	Remote-Prozeduraufruf für NFS
1004	Eingehend_139	139	TCP	Alle	Alle	Zulassen	NetBIOS-Servicesitzung für CIFS
1005	Inbound_161-162_tcp	161-162	TCP	Alle	Alle	Zulassen	Einfaches Netzwerkverwaltungsprotokoll
1006	Inbound_161-162_udp	161-162	UDP	Alle	Alle	Zulassen	Einfaches Netzwerkverwaltungsprotokoll
1007	Eingehend_443	443	TCP	Alle	Alle	Zulassen	HTTPS-Zugriff auf die System Manager-Webkonsole unter Verwendung der IP-Adresse der Cluster-Management-LIF
1008	Eingehend_445	445	TCP	Alle	Alle	Zulassen	Microsoft SMB/CIFS über TCP mit NETBIOS-Framing
1009	Inbound_635_tcp	635	TCP	Alle	Alle	Zulassen	NFS-Mount
1010	Eingehend_635_udp	635	TCP	Alle	Alle	Zulassen	NFS-Mount
1011	Eingehend_749	749	TCP	Alle	Alle	Zulassen	Kerberos
1012	Inbound_2049_tcp	2049	TCP	Alle	Alle	Zulassen	NFS-Server-Daemon
1013	Eingehend_2049_udp	2049	UDP	Alle	Alle	Zulassen	NFS-Server-Daemon

Priorität	Name	Port	Protokoll	Quelle	Ziel	Aktion	Beschreibung
1014	Eingehend_3260	3260	TCP	Alle	Alle	Zulassen	ISCSI-Zugriff über die iSCSI-Daten-LIF
1015	Inbound_4045-4046_tcp	4045-4046	TCP	Alle	Alle	Zulassen	NFS Lock Daemon und Network Status Monitor
1016	Inbound_4045-4046_udp	4045-4046	UDP	Alle	Alle	Zulassen	NFS Lock Daemon und Network Status Monitor
1017	Eingehend_10000	10.000	TCP	Alle	Alle	Zulassen	Backup mit NDMP
1018	Eingehend_11104-11105	11104-11105	TCP	Alle	Alle	Zulassen	SnapMirror Datenübertragung
3000	Inbound_Deny_all_tcp	Alle	TCP	Alle	Alle	Ablehnen	Blockieren Sie den gesamten anderen TCP-eingehenden Datenverkehr
3001	Inbound_Deny_all_udp	Alle	UDP	Alle	Alle	Ablehnen	Alle anderen UDP-eingehenden Datenverkehr blockieren
65000	AllowVnetInBound	Alle	Alle	VirtualNetwork	VirtualNetwork	Zulassen	Eingehender Verkehr aus dem vnet
65001	AllowAzureLoad BalancerInBound	Alle	Alle	AzureLoadBalancer	Alle	Zulassen	Datenverkehr vom Azure Standard Load Balancer
65500	DenyAllInBound	Alle	Alle	Alle	Alle	Ablehnen	Alle anderen eingehenden Datenverkehr blockieren

Eingehende Regeln für HA-Systeme

HA-Systeme weisen weniger eingehende Regeln als Systeme mit einzelnen Nodes auf, da eingehender Datenverkehr durch den Azure Standard Load Balancer geleitet wird. Aus diesem Grund sollte der Verkehr aus dem Load Balancer geöffnet sein, wie in der Regel "AllowAzureLoadBalancerInBound" gezeigt.

Priorität	Name	Port	Protokoll	Quelle	Ziel	Aktion	Beschreibung
100	Eingehend_443	443	Alle	Alle	Alle	Zulassen	HTTPS-Zugriff auf die System Manager-Webkonsole unter Verwendung der IP-Adresse der Cluster-Management-LIF
101	Inbound_111_tcp	111	Alle	Alle	Alle	Zulassen	Remote-Prozeduraufruf für NFS
102	Inbound_2049_tcp	2049	Alle	Alle	Alle	Zulassen	NFS-Server-Daemon

Priorität	Name	Port	Protokoll	Quelle	Ziel	Aktion	Beschreibung
111	Inbound_SSH	22	Alle	Alle	Alle	Zulassen	SSH-Zugriff auf die IP-Adresse der Cluster Management LIF oder einer Node Management LIF
121	Eingehend_53	53	Alle	Alle	Alle	Zulassen	DNS und CIFS
65000	AllowVnetInBound	Alle	Alle	VirtualNetwork	VirtualNetwork	Zulassen	Eingehender Verkehr aus dem vnet
65001	AllowAzureLoad BalancerInBound	Alle	Alle	AzureLoadBalancer	Alle	Zulassen	Datenverkehr vom Azure Standard Load Balancer
65500	DenyAllInBound	Alle	Alle	Alle	Alle	Ablehnen	Alle anderen eingehenden Datenverkehr blockieren

Outbound-Regeln für Cloud Volumes ONTAP

Die vordefinierte Sicherheitsgruppe für Cloud Volumes ONTAP öffnet den gesamten ausgehenden Datenverkehr. Wenn dies akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Anrufe. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Outbound-Regeln.

Grundlegende Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für Cloud Volumes ONTAP enthält die folgenden ausgehenden Regeln.

Protokoll	Port	Zweck
Alle TCP	Alle	Gesamter abgehender Datenverkehr
Alle UDP-Protokolle	Alle	Gesamter abgehender Datenverkehr

Erweiterte Outbound-Regeln

Wenn Sie strenge Regeln für ausgehenden Datenverkehr benötigen, können Sie mit den folgenden Informationen nur die Ports öffnen, die für die ausgehende Kommunikation durch Cloud Volumes ONTAP erforderlich sind.

Die Quelle ist die Schnittstelle (IP-Adresse) auf dem Cloud Volumes ONTAP System.

Service	Protokoll	Port	Quelle	Ziel	Zweck
Active Directory	TCP	88	Node Management-LIF	Active Directory-Gesamtstruktur	Kerberos V-Authentifizierung
	UDP	137	Node Management-LIF	Active Directory-Gesamtstruktur	NetBIOS-Namensdienst
	UDP	138	Node Management-LIF	Active Directory-Gesamtstruktur	Netbios Datagramm-Dienst
	TCP	139	Node Management-LIF	Active Directory-Gesamtstruktur	Sitzung für den NETBIOS-Dienst
	TCP	389	Node Management-LIF	Active Directory-Gesamtstruktur	LDAP
	TCP	445	Node Management-LIF	Active Directory-Gesamtstruktur	Microsoft SMB/CIFS über TCP mit NETBIOS-Framing
	TCP	464	Node Management-LIF	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern und festlegen (SET_CHANGE)
	UDP	464	Node Management-LIF	Active Directory-Gesamtstruktur	Kerberos-Schlüsselverwaltung
	TCP	749	Node Management-LIF	Active Directory-Gesamtstruktur	Kerberos V - Kennwort ändern und festlegen (RPCSEC_GSS)
	TCP	88	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Kerberos V-Authentifizierung
	UDP	137	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	NetBIOS-Namensdienst
	UDP	138	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Netbios Datagramm-Dienst
	TCP	139	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Sitzung für den NETBIOS-Dienst
	TCP	389	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	LDAP
	TCP	445	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Microsoft SMB/CIFS über TCP mit NETBIOS-Framing
	TCP	464	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern und festlegen (SET_CHANGE)
	UDP	464	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Kerberos-Schlüsselverwaltung
	TCP	749	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Kerberos V - Passwort ändern und festlegen (RPCSEC_GSS)
DHCP	UDP	68	Node Management-LIF	DHCP	DHCP-Client für die erstmalige Einrichtung
DHCPS	UDP	67	Node Management-LIF	DHCP	DHCP-Server

Service	Protokoll	Port	Quelle	Ziel	Zweck
DNS	UDP	53	Node Management LIF und Daten LIF (NFS, CIFS)	DNS	DNS
NDMP	TCP	18600-18699	Node Management-LIF	Zielserver	NDMP-Kopie
SMTP	TCP	25	Node Management-LIF	Mailserver	SMTP-Warnungen können für AutoSupport verwendet werden
SNMP	TCP	161	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps
	UDP	161	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps
	TCP	162	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps
	UDP	162	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps
SnapMirror	TCP	11104	Intercluster-LIF	ONTAP Intercluster-LIFs	Management von interclusterübergreifenden Kommunikationssitzungen für SnapMirror
	TCP	11105	Intercluster-LIF	ONTAP Intercluster-LIFs	SnapMirror Datenübertragung
Syslog	UDP	514	Node Management-LIF	Syslog-Server	Syslog-Weiterleitungsmeldungen

AWS- und Azure-Berechtigungen für Cloud Manager

Cloud Manager benötigt Berechtigungen, um Aktionen in AWS und Azure in Ihrem Namen auszuführen. Diese Berechtigungen sind in enthalten "Die von NetApp bereitgestellten Richtlinien". Sie möchten vielleicht wissen, was Cloud Manager mit diesen Berechtigungen macht.

Was Cloud Manager mit AWS-Berechtigungen macht

Cloud Manager verwendet ein AWS-Konto, um API-Aufrufe an mehrere AWS-Services durchzuführen, darunter EC2, S3, CloudFormation, IAM, den Security Token Service (STS) und den Key Management Service (KMS).

Aktionen	Zweck
„ec2:StartInstances“, „ec2:StopInstances“, „ec2:DescribeInstances“, „ec2:DescribeInstanceStatus“, „ec2:RunInstances“, „ec2:TerminateInstances“, „ec2:ModifyInstanceAttribut“,	Startet eine Cloud Volumes ONTAP Instanz und stoppt, startet und überwacht die Instanz.
"EC2:DescribeInstanceAttribute",	Überprüft, ob das erweiterte Netzwerk für unterstützte Instanztypen aktiviert ist.
„ec2:DescribeRouteTables“, „ec2:DescribeImages“,	Startet eine Cloud Volumes ONTAP HA-Konfiguration.
"EC2:CreateTags",	Kennzeichnet jede Ressource, die Cloud Manager erstellt, mit den Tags "workingenvironment" und "WorkingEnvironmentId". Cloud Manager verwendet diese Tags für Wartung und Kostenzuordnung.
„ec2:CreateVolume“, „ec2:DescribeVolumes“, „ec2:ModifyVolumeAttribute“, „ec2:AttachVolume“, „ec2:DeleteVolume“, „ec2:DetachVolume“,	Managt die EBS Volumes, die Cloud Volumes ONTAP als Back-End Storage verwendet.
„ec2:CreateSecurityGroup“, „ec2:DeleteSecurityGroup“, „ec2:DescribeSecurityGroups“, „ec2:RevokeSecurityGroupEgress“, „ec2:AuthoriseSecurityGroupEgress“, „ec2:AuthoriseSecurityGroupIngress“, „ec2:RevokeSecurityGroupIngress“,	Erstellt vordefinierte Sicherheitsgruppen für Cloud Volumes ONTAP.
„ec2:CreateNetworkInterface“, „ec2:DescribeNetworkInterfaces“, „ec2:DeleteNetworkInterface“, „ec2:ModifyNetworkInterface“,	Erstellt und managt Netzwerkschnittstellen für Cloud Volumes ONTAP im Ziel-Subnetz.
„ec2:DescribeSubnets“, „ec2:DescribeVpcs“,	Ruft die Liste der Zielsubnetze und Sicherheitsgruppen ab, die beim Erstellen einer neuen Arbeitsumgebung für Cloud Volumes ONTAP benötigt wird.
"EC2:DescribeDhcpOptions",	Bestimmt DNS-Server und den Standarddomänennamen beim Starten von Cloud Volumes ONTAP Instanzen.
„ec2:CreateSnapshot“, „ec2:DeleteSnapshot“, „ec2:DescribeSnapshots“,	Erstellt Snapshots von EBS Volumes während der Ersteinrichtung und bei jedem Anhalten einer Cloud Volumes ONTAP Instanz.
"EC2:GetConsoleOutput",	Erfasst die Cloud Volumes ONTAP Konsole, die an AutoSupport Nachrichten angehängt ist.
"EC2:DescribeKeyPairs",	Ruft beim Starten von Instanzen die Liste der verfügbaren Schlüsselpaare ab.
"EC2:DescribeRegions",	Ruft eine Liste der verfügbaren AWS-Regionen ab.
„ec2:DeleteTags“, „ec2:DescribeTags“,	Managt Tags für Ressourcen, die mit Cloud Volumes ONTAP Instanzen verbunden sind.

Aktionen	Zweck
„Cloudformation:CreateStack“, „Cloudformation:DeleteStack“, „Cloudformation:DescribeStacks“, „Cloudformation:DescribeStackEvents“, „Cloudformation:ValidateTemplate“,	Startet Cloud Volumes ONTAP Instanzen.
„iam:PassRollenole“, „iam:CreateRollenole“, „iam:DeleteRollenole“, „iam:PutRolePolicy“, „iam:CreateInstanceProfil“, „iam:DeleteRolePolicy“, „iam:AddRoleToInstanceProfile“, „iam:RemoveRoleFromInstanceProfile“, „iam:DeleteInstanceProfile“,	Startet eine Cloud Volumes ONTAP HA-Konfiguration.
„iam:ListInstanceProfiles“, „STS:DecodeAuthorisationMessage“, „ec2:AssociateIamInstanceProfil“, „ec2:DescribeIamInstanceProfilAssociations“, „ec2:DisassotionIamInstanceProfile“,	Managt Instanzprofile für Cloud Volumes ONTAP Instanzen.
„s3:GetBucketTagging“, „s3:GetBucketLocation“, „s3:ListAllMyBuckets“, „s3:ListBucket“	Informationen zu AWS S3-Buckets, damit Cloud Manager in den NetApp Data Fabric Cloud Sync Service integriert werden kann
„s3:CreateBucket“, „s3:DeleteBucket“, „s3:GetLifecycleConfiguration“, „s3:PutLifecycleConfiguration“, „s3:PutBucketTagging“, „s3:ListBucketVersions“,	Managt den S3-Bucket, den ein Cloud Volumes ONTAP System als Kapazitäts-Tier verwendet.
„Kms:Liste*“, „Kms:Beschreiben*“	Ruft Informationen zu Schlüsseln vom AWS Key Management Service ab.
„ce:GetReservationUtilisation“, „ce:GetDimensionValues“, „ce:GetCostAndUsage“, „ce:GetTags“	Abrufen von AWS-Kostendaten für Cloud Volumes ONTAP
„ec2:CreatePlacementGroup“, „ec2:DeletePlacementGroup“	Wenn Sie eine HA-Konfiguration in einer einzigen AWS Availability Zone implementieren, startet Cloud Manager die beiden HA-Nodes und den Mediator in einer AWS Spread-Placement-Gruppe.

Was Cloud Manager mit Azure-Berechtigungen tut

Die Cloud Manager Azure Policy enthält die Berechtigungen, die Cloud Manager für die Bereitstellung und das Management von Cloud Volumes ONTAP in Azure benötigt.

Aktionen	Zweck
„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",	Erstellt Cloud Volumes ONTAP und beendet, startet, löscht und erhält den Status des Systems.
„Microsoft.Compute/images/write", „Microsoft.Compute/images/read",	Ermöglicht die Implementierung von Cloud Volumes ONTAP über eine 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/Retgeneratekey/Action“, „Microsoft.Storage/storageAccounts/write“, „Microsoft.Storage/storageAccounts/delete“, „Microsoft.Storage/Nutzungs/Lesevorgang“,	Verwaltet Azure Storage-Konten und -Festplatten und hängt die Festplatten an Cloud Volumes ONTAP an.
„Microsoft.Network/networkInterfaces/read", „Microsoft.Network/networkInterfaces/write", „Microsoft.Network/networkInterfaces/join/action",	Erstellt und managt Netzwerkschnittstellen für Cloud Volumes ONTAP im Ziel-Subnetz.
„Microsoft.Network/networkSecurityGroups/read", „Microsoft.Network/networkSecurityGroups/write", „Microsoft.Network/networkSecurityGroups/join/action",	Erstellt vordefinierte Netzwerksicherheitsgruppen für Cloud Volumes ONTAP.
„Microsoft.Ressourcen/Abonnements/Standorte/gelesen“, „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",	Ruft Netzwerkinformationen zu Regionen, dem Ziel-VNet und dem Subnetz ab und fügt Cloud Volumes ONTAP VNets hinzu.
„Microsoft.Network/virtualNetworks/subnets/write", „Microsoft.Network/routeTables/join/action",	Aktiviert VNet Service-Endpunkte für das Daten-Tiering.

Aktionen	Zweck
„Microsoft.Ressourcen/Implementierungen/Betrieb/Lesen“, „Microsoft.Resources/Deployments/read“, „Microsoft.Resources/Deployments/write“,	Implementierung von Cloud Volumes ONTAP anhand einer Vorlage
„Microsoft.Resources/Deployments/Operations/read“, „Microsoft.Resources/Deployments/read“, „Microsoft.Resources/Deployments/write“, „Microsoft.Resources/Resources/read“, „Microsoft.Resources/Subscriptions/Operationresults/read“, „Microsoft.Resources/subskriptions/resourceGroups/delete“, „Microsoft.Resources/Subskriptions/resourceGroups/read“, „Microsoft.Resources/subskriptions/resourcegruppen/Resources/read“, „Microsoft.Resources/subskriptions/resourceGroups/write“,	Erstellt und managt Ressourcengruppen für Cloud Volumes ONTAP.
„Microsoft.Compute/snapshots/write", „Microsoft.Compute/snapshots/read", „Microsoft.Compute/disks/beginGetAccess/action"	Erstellt und managt von Azure verwaltete Snapshots.
„Microsoft.Compute/availabilitySets/write", „Microsoft.Compute/availabilitySets/read",	Erstellt und managt Verfügbarkeitssätze für Cloud Volumes ONTAP.
„Microsoft.MarketplaceOrdering/offertypes/Publisher/offerers/Plans/Agreements/read“, „Microsoft.MarketplaceOrdering/offertypes/Publisher/Offerers/Plans/Agreements/write“	Ermöglicht programmatische Implementierungen über 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",	Managt einen Azure Load Balancer für HA-Paare.
"Microsoft.Authorization/locks/*"	Ermöglicht das Management von Sperren auf Azure Festplatten.
„Microsoft.Authorization/roleDefinitions/write“, „Microsoft.Authorization/roleAssignments/write“, „Microsoft.Web/sites/*“	Managt Failover für HA-Paare

Standardkonfigurationen

Details zur Konfiguration von Cloud Manager und Cloud Volumes ONTAP können Ihnen bei der Administration der Systeme helfen.

Standardkonfiguration für Cloud Manager unter Linux

Wenn Sie eine Fehlerbehebung für Cloud Manager oder Ihren Linux-Host durchführen müssen, kann dies dazu beitragen, die Konfiguration von Cloud Manager zu verstehen.

- Wenn Sie Cloud Manager über NetApp Cloud Central (oder direkt über den AWS Marketplace oder Azure Marketplace) bereitgestellt haben, beachten Sie Folgendes:
  - In AWS lautet der Benutzername für die EC2 Linux-Instanz ec2-user.
  - Für AWS und Azure ist das Betriebssystem für das Cloud Manager-Image Red Hat Enterprise Linux 7.4 (HVM).

    Das Betriebssystem enthält keine GUI. Sie müssen ein Terminal verwenden, um auf das System zuzugreifen.
- Der Installationsordner von Cloud Manager befindet sich am folgenden Speicherort:

  /opt/application/netapp/cloudmanager
- Protokolldateien befinden sich im folgenden Ordner:

  /opt/application/netapp/cloudmanager/log
- Der Cloud Manager Service heißt occm.
- Der occm-Dienst ist vom MySQL-Dienst abhängig.

  Wenn der MySQL-Dienst nicht verfügbar ist, ist auch der occm-Dienst nicht verfügbar.
- Cloud Manager installiert die folgenden Pakete auf dem Linux-Host, sofern sie noch nicht installiert sind:
  - 7-Zip
  - AWSCLI
  - Java
  - Kubectl
  - MySQL
  - Tridentctl
  - Wget

Standardkonfiguration für Cloud Volumes ONTAP

Wenn Sie verstehen, wie Cloud Volumes ONTAP standardmäßig konfiguriert ist, können Sie Ihre Systeme einrichten und verwalten. Dies gilt insbesondere, wenn Sie mit ONTAP vertraut sind, da sich das Standard-Setup für Cloud Volumes ONTAP von ONTAP unterscheidet.

- Cloud Volumes ONTAP ist als Single-Node-System und als HA-Paar in AWS und Azure verfügbar.

- Cloud Manager erstellt bei der Implementierung von Cloud Volumes ONTAP eine Data Serving SVM. Sie können zwar über System Manager oder die CLI eine weitere SVM mit Datenbereitstellung erstellen, jedoch wird die Verwendung mehrerer SVMs mit Datenbereitstellung nicht unterstützt.
- Standardmäßig werden mehrere Netzwerkschnittstellen erstellt:
  - Eine Cluster Management-LIF
  - Eine Intercluster-LIF
  - Eine Node Management-LIF
  - Eine iSCSI-Daten-LIF
  - Eine CIFS- und NFS-Daten-LIF

  Aufgrund der EC2-Anforderungen ist das LIF-Failover für Cloud Volumes ONTAP standardmäßig deaktiviert. Durch die Migration einer LIF auf einen anderen Port wird die externe Zuordnung zwischen IP-Adressen und Netzwerkschnittstellen in der Instanz aufgehoben, sodass der LIF nicht mehr zugänglich ist.

- Cloud Volumes ONTAP sendet Konfigurations-Backups über HTTPS an Cloud Manager.
- Wenn Sie sich bei Cloud Manager anmelden, können Sie über die Backup-Daten darauf zugreifen https://ipaddress/occm/offboxconfig/
- Cloud Manager legt einige Volume-Attribute anders fest als andere Management-Tools (z. B. System Manager oder CLI).

  In der folgenden Tabelle sind die Volume-Attribute aufgeführt, die Cloud Manager anders als die Standardeinstellungen festlegt:

Attribut	Vom Cloud Manager festgelegter Wert
AutoSize Modus	Wachsen
Maximale automatische Größe	1.000 Prozent Der Cloud Manager Admin kann diesen Wert auf der Seite Einstellungen ändern.
Sicherheitsstil	NTFS für CIFS-Volumes UNIX für NFS-Volumes
Platz garantiert Stil	Keine
UNIX-Berechtigungen (nur NFS)	777

  Informationen zu diesen Attributen finden Sie auf der Seite „*Volume create* man“.

Boot- und Root-Daten für Cloud Volumes ONTAP

Zusätzlich zum Storage für Benutzerdaten erwirbt Cloud Manager auch Cloud Storage für Boot- und Root-Daten auf jedem Cloud Volumes ONTAP System.

AWS

- Eine bereitgestellte IOPS SSD-Festplatte für Cloud Volumes ONTAP Boot-Daten, die ca. 45 GB und 1.250 Piops betragen
- Eine universelle SSD-Festplatte für Cloud Volumes ONTAP Root-Daten mit ca. 140 GB
- Ein EBS-Snapshot für jede Boot- und Root-Festplatte

In einem HA-Paar replizieren beide Cloud Volumes ONTAP Nodes ihre Root-Festplatte auf den Partner-Node.

Azure

- Eine Premium Storage SSD-Festplatte für Cloud Volumes ONTAP Bootdaten, die ca. 73 GB betragen
- Eine Premium Storage SSD-Festplatte für Cloud Volumes ONTAP Root-Daten, die ca. 140 GB betragen
- Ein Azure Snapshot für jedes Boot- und Root-Laufwerk

Wo sich die Festplatten befinden

Cloud Manager legt den Storage von AWS und Azure wie folgt fest:

- Startdaten befinden sich auf einer Festplatte, die mit der EC2-Instanz oder der Azure Virtual Machine verbunden ist.

  Diese Festplatte, die das Boot-Image enthält, steht Cloud Volumes ONTAP nicht zur Verfügung.

- Die Stammdaten, die die Systemkonfiguration und die Protokolle enthalten, befinden sich in aggr0.
- Das Root-Volume der Storage Virtual Machine (SVM) befindet sich in aggr1.
- Daten-Volumes befinden sich auch in aggr1.

Benutzerrollen

Jedem Cloud Manager-Benutzerkonto wird eine Rolle zugewiesen, die Berechtigungen definiert.

Aufgabe	Cloud Manager Admin	Mandantenverwaltung	Administrator der Arbeitsumgebung
Verwalten von Mandanten	Ja.	Nein	Nein
Verwalten von Arbeitsumgebungen	Ja.	Ja, für den zugewiesenen Mandanten	Ja, für zugewiesene Arbeitsumgebungen
Integrieren Sie eine Arbeitsumgebung in Cloud Sync	Ja.	Ja.	Nein
Anzeigen des Status der Datenreplizierung	Ja.	Ja, für den zugewiesenen Mandanten	Ja, für zugewiesene Arbeitsumgebungen
Zeitachse anzeigen	Ja.	Ja.	Ja.
Erstellen und Löschen von Benutzerkonten	Ja.	Ja, für den zugewiesenen Mandanten	Nein

Aufgabe	Cloud Manager Admin	Mandantenverwaltung	Administrator der Arbeitsumgebung
Benutzerkonten ändern	Ja.	Ja, für den zugewiesenen Mandanten	Ja, für ihren eigenen Account
Kontoeinstellungen verwalten	Ja.	Nein	Nein
Einrichtung Von Kubernetes	Ja.	Nein	Nein
Wechseln Sie zwischen der Storage System View und der Volume View	Ja.	Nein	Nein
Einstellungen ändern	Ja.	Nein	Nein
Anzeigen und Verwalten des Support-Dashboards	Ja.	Nein	Nein
Backup und Wiederherstellung von Cloud Manager	Ja.	Nein	Nein
Entfernen Sie eine Arbeitsumgebung	Ja.	Nein	Nein
Aktualisieren Sie Cloud Manager	Ja.	Nein	Nein
Installieren Sie ein HTTPS-Zertifikat	Ja.	Nein	Nein
Einrichten von Active Directory	Ja.	Nein	Nein
Aktivieren Sie den Cloud Storage Automation Report	Ja.	Nein	Nein

Wo Sie Hilfe und weitere Informationen erhalten

Über verschiedene Ressourcen, darunter Videos, Foren und Support, erhalten Sie Hilfe und weitere Informationen zu Cloud Manager und Cloud Volumes ONTAP.

- "Videos für Cloud Manager und Cloud Volumes ONTAP"

  Sehen Sie sich Videos an, die Ihnen zeigen, wie Sie Cloud Volumes ONTAP in AWS und Azure implementieren und managen und wie Sie Daten in Ihrer Hybrid Cloud replizieren können.

- "Richtlinien für Cloud Manager"

  Laden Sie JSON-Dateien herunter, die die Berechtigungen enthalten, die Cloud Manager zum Ausführen von Aktionen in AWS und Azure benötigt.

- "Cloud Manager API-Entwicklerleitfaden"

Lesen Sie einen Überblick über die APIs, Beispiele für deren Verwendung und eine API-Referenz.

- Training für Cloud Volumes ONTAP
  - "Grundlagen von Cloud Volumes ONTAP"
  - "Implementierung und Management von Cloud Volumes ONTAP für Azure"
- Technische Berichte
  - "NetApp Technical Report 4383: Performance Characterization of Cloud Volumes ONTAP in Amazon Web Services with Application Workloads"
  - "Technischer Bericht von NetApp 4671: Performance-Charakterisierung von Cloud Volumes ONTAP in Azure mit Applikations-Workloads"
- "Cloud Volumes ONTAP 9 SVM Disaster Recovery Preparation Express-Leitfaden"

  Beschreibt, wie eine Ziel-SVM zur Vorbereitung auf die Disaster Recovery schnell konfiguriert wird.
- "Cloud Volumes ONTAP 9 SVM Disaster Recovery Express Guide"

  Beschreibt, wie Sie eine Ziel-SVM nach einem Notfall schnell aktivieren und dann die Quell-SVM erneut aktivieren.
- "ONTAP 9 Dokumentationszentrum"

  Greifen Sie auf die Produktdokumentation für ONTAP zu, die Ihnen bei der Verwendung von Cloud Volumes ONTAP helfen kann.
- "NetApp Cloud Volumes ONTAP Support"

  Greifen Sie auf Support-Ressourcen zu, um Hilfe zu erhalten und Probleme mit Cloud Volumes ONTAP zu beheben.
- "NetApp Community: Cloud Data Services"

  Tauschen Sie sich mit Kollegen aus, stellen Sie Fragen, tauschen Sie Ideen aus, suchen Sie nach Ressourcen und tauschen Sie Best Practices aus.
- "NetApp Cloud Central"

  Hier finden Sie weitere Informationen zu NetApp Produkten und Lösungen für die Cloud.
- "NetApp Produktdokumentation"

  In der NetApp Produktdokumentation finden Sie Anleitungen, Ressourcen und Antworten.