Anforderungen

Amazon FSx for ONTAP

NetApp
November 17, 2022

Inhaltsverzeichnis

Anforderungen

Einrichten von Berechtigungen für FSX für ONTAP

Um eine Arbeitsumgebung von Amazon FSX für ONTAP zu erstellen oder zu managen, müssen Sie BlueXP Zugangsdaten für AWS Zugangsdaten hinzufügen, indem Sie das ARN einer IAM-Rolle bereitstellen, sodass BlueXP die nötigen Berechtigungen zur Erstellung einer FSX für ONTAP Arbeitsumgebung erteilt.

Einrichten der IAM-Rolle

Richten Sie eine IAM-Rolle ein, mit der BlueXP die Rolle übernehmen kann.

Schritte

1. Wechseln Sie im Zielkonto zur IAM-Konsole.
2. Klicken Sie unter Zugriffsverwaltung auf **Rollen > Rolle erstellen** und befolgen Sie die Schritte zum Erstellen der Rolle.

   Gehen Sie wie folgt vor:

   - Wählen Sie unter **Vertrauenswürdiger Entitätstyp AWS-Konto** aus.
   - Wählen Sie **ein weiteres AWS-Konto** und geben Sie die ID von BlueXP ein.
     - Für BlueXP SaaS: 952013314444
     - Für AWS GovCloud (USA): 033442085313
   - Erstellen Sie eine Richtlinie, die die folgenden Berechtigungen enthält:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "fsx:*",
                "ec2:Describe*",
                "ec2:CreateTags",
                "kms:Describe*",
                "kms:List*",
                "kms:CreateGrant",
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "*"
        }
    ]
}
```

Sehen Sie sich die Richtlinie zur Bereitstellung von Konnektor über die an "Seite „BlueXP Policies“".

3. Kopieren Sie die Rolle ARN der IAM-Rolle, sodass Sie sie im nächsten Schritt in BlueXP einfügen können.

Die IAM-Rolle verfügt nun über die erforderlichen Berechtigungen.

Fügen Sie die Anmeldeinformationen hinzu

Nachdem Sie die IAM-Rolle mit den erforderlichen Berechtigungen angegeben haben, fügen Sie die Rolle ARN zu BlueXP hinzu.

Wenn Sie gerade die IAM-Rolle erstellt haben, kann es ein paar Minuten dauern, bis sie zur Verwendung verfügbar sind. Warten Sie einige Minuten, bevor Sie BlueXP die Anmeldeinformationen hinzufügen.

Schritte

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Symbol Einstellungen und wählen Sie **Anmeldeinformationen**.

2. Klicken Sie auf **Anmeldeinformationen hinzufügen** und befolgen Sie die Schritte im Assistenten.
   a. **Anmeldeort**: Wählen Sie **Amazon Web Services > BlueXP**.
   b. **Anmeldedaten definieren**: Geben Sie den ARN (Amazon Resource Name) der IAM-Rolle an.

- Wenn Sie ein AWS GovCloud (US) Konto nutzen, überprüfen Sie **Ich verwende ein AWS GovCloud (US) Konto**.

- Bei der Authentifizierung mithilfe von AWS GovCloud wird die SaaS-Plattform deaktiviert. Dies ist eine permanente Änderung Ihres Kontos und kann nicht rückgängig gemacht werden.

c. **Review**: Bestätigen Sie die Angaben zu den neuen Anmeldedaten und klicken Sie auf **Hinzufügen**.

Sie können die Anmeldeinformationen jetzt verwenden, wenn Sie eine FSX für ONTAP-Arbeitsumgebung erstellen.

Weiterführende Links

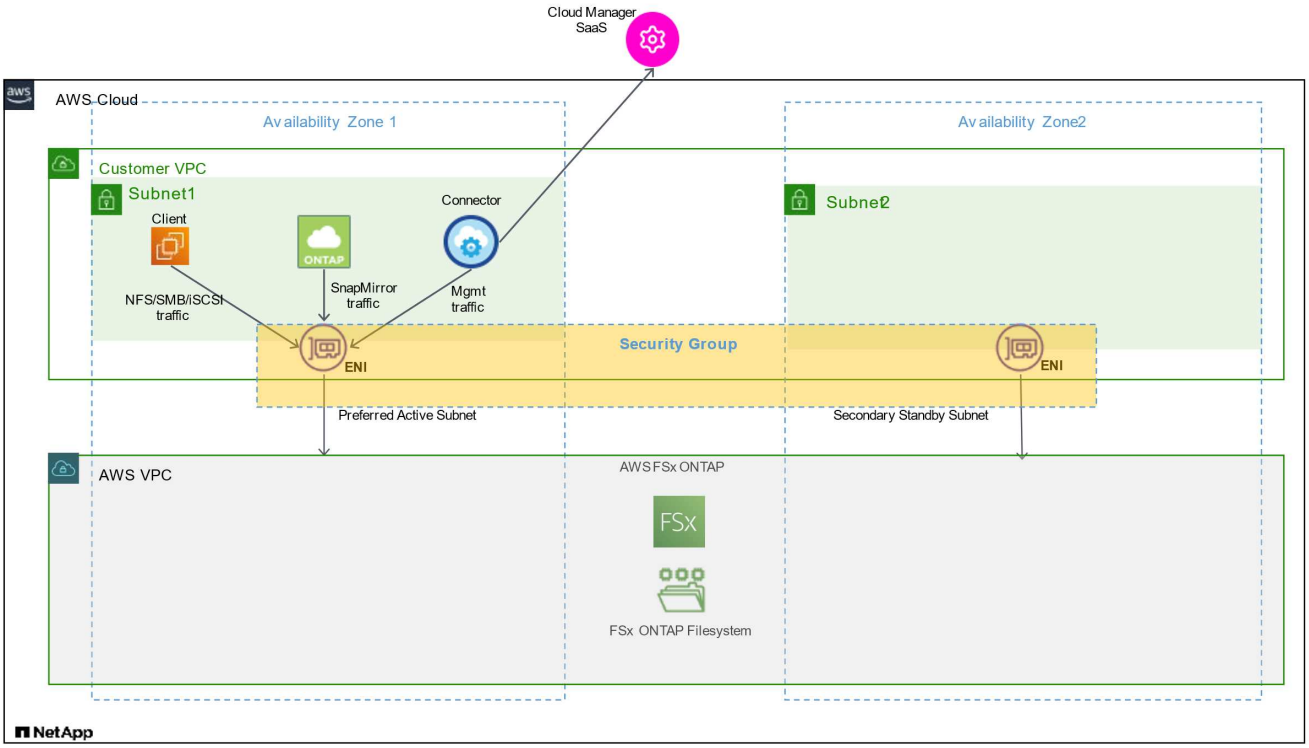
- "AWS Zugangsdaten und Berechtigungen"
- "Management der AWS Credentials für BlueXP"

Sicherheitsgruppenregeln für FSX für ONTAP

BlueXP erstellt AWS Sicherheitsgruppen mit den ein- und ausgehenden Regeln, die für den erfolgreichen Betrieb von BlueXP und FSX für ONTAP erforderlich sind. Möglicherweise möchten Sie zu Testzwecken auf die Ports verweisen oder wenn Sie Ihre eigene verwenden müssen.

Regeln für FSX für ONTAP

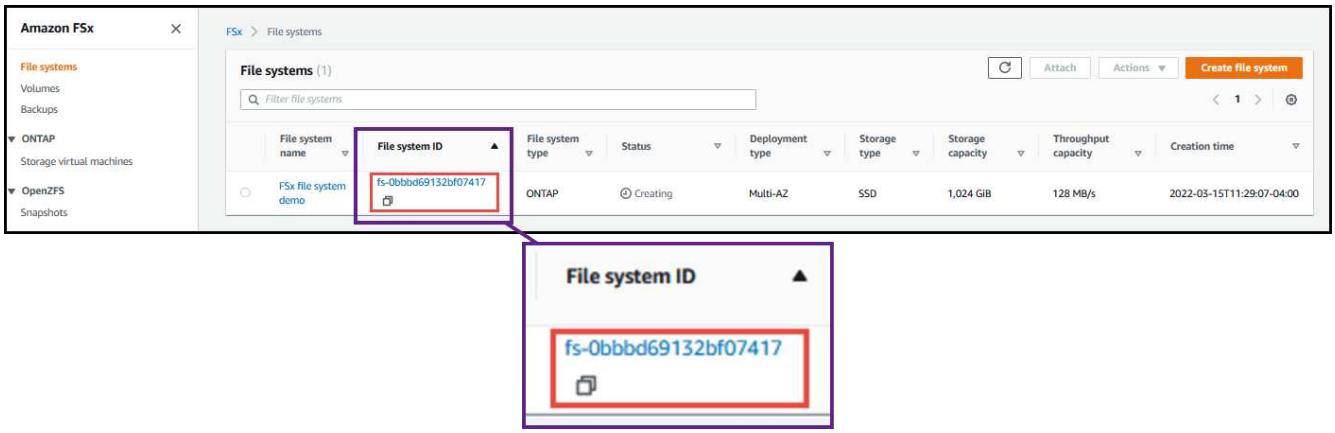
Die Sicherheitsgruppe FSX für ONTAP erfordert sowohl ein- als auch ausgehende Regeln. Dieses Diagramm zeigt FSX für ONTAP die Netzwerkkonfiguration und die Anforderungen an Sicherheitsgruppen.



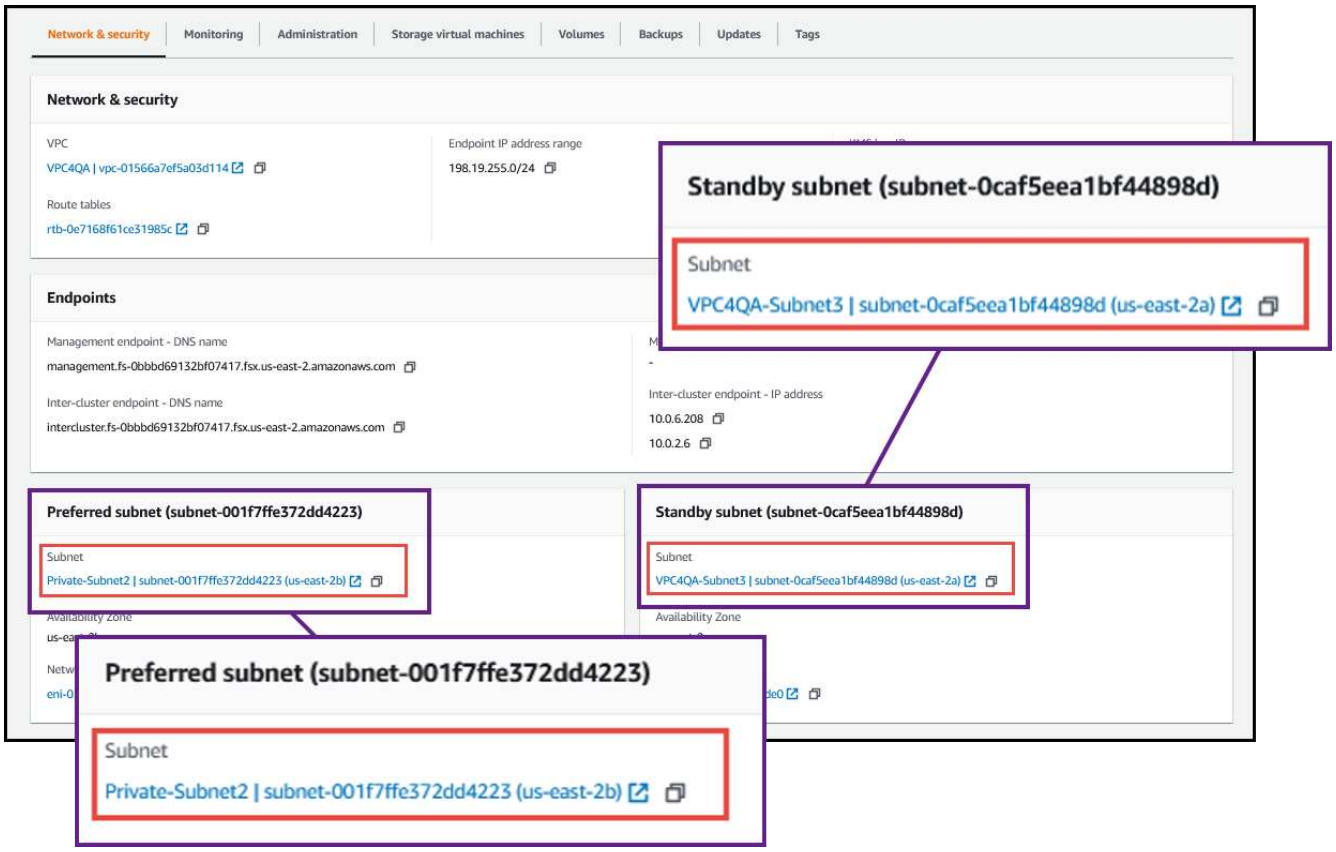
Sie müssen die mit dem Enis verbundenen Sicherheitsgruppen über die AWS Management Console suchen.

Schritte

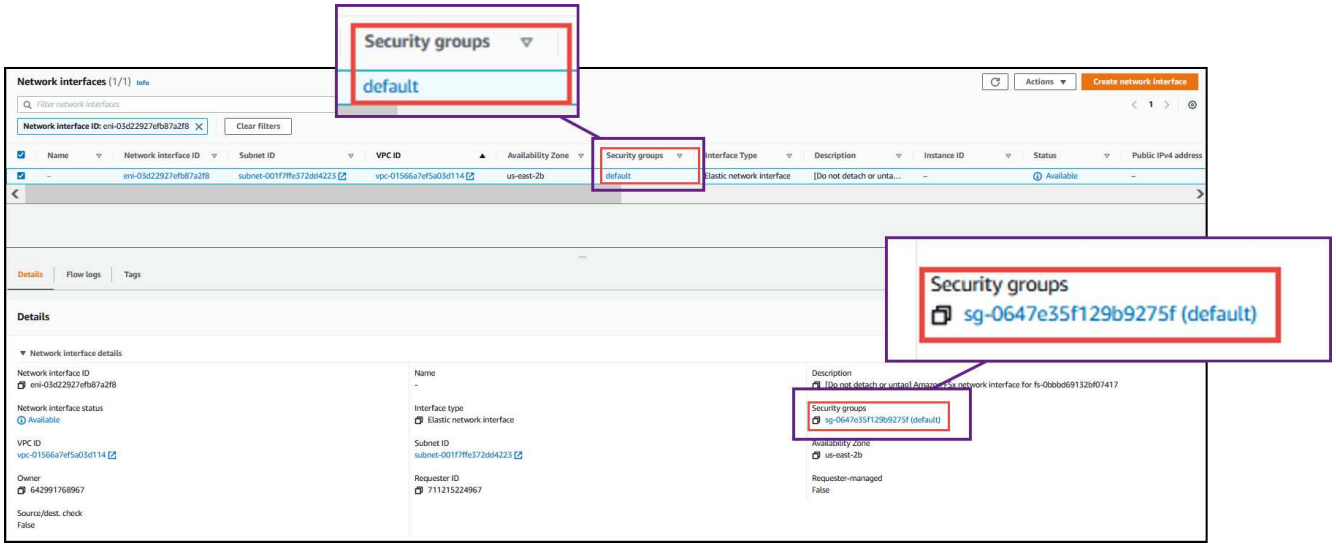
1. Öffnen Sie das Dateisystem FSX für ONTAP in der AWS-Verwaltungskonsole und klicken Sie auf den Link Dateisystem-ID.



2. Klicken Sie auf der Registerkarte **Netzwerk & Sicherheit** auf die Netzwerkschnittstelle-ID für das bevorzugte oder Standby-Subnetz.



3. Klicken Sie in der Netzwerkschnittstellentabelle auf die Sicherheitsgruppe oder auf den Abschnitt **Details** für die Netzwerkschnittstelle.



Regeln für eingehende Anrufe

Protokoll	Port	Zweck
Alle ICMP	Alle	Pingen der Instanz
HTTPS	443	Zugriff vom Connector auf die Verwaltungsschnittstelle fsxadmin, um API-Aufrufe an FSX zu senden

Protokoll	Port	Zweck
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

Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für FSX für 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 FSX für ONTAP umfasst die folgenden ausgehende 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

Es müssen keine spezifischen Ports für den Mediator oder zwischen Nodes in FSX für ONTAP geöffnet werden.

Die Quelle ist die Schnittstelle (IP-Adresse) auf dem FSX für 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 UND UDP	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	Daten-LIF (NFS, CIFS, iSCSI)	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 UND UDP	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)
Backup auf S3	TCP	5010	Intercluster-LIF	Backup-Endpunkt oder Wiederherstellungsendpunkt	Backup- und Restore-Vorgänge für die Funktion „Backup in S3“

Service	Protokoll	Port	Quelle	Ziel	Zweck
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 den Konnektor

Die Sicherheitsgruppe für den Konnektor erfordert sowohl ein- als auch ausgehende Regeln.

Regeln für eingehende Anrufe

Protokoll	Port	Zweck
SSH	22	Bietet SSH-Zugriff auf den Connector-Host
HTTP	80	Bietet HTTP-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche und Verbindungen von Cloud Data Sense
HTTPS	443	Bietet HTTPS-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche
TCP	3128	Bietet die Cloud Data Sense-Instanz einen Internetzugriff, wenn Ihr AWS-Netzwerk keine NAT oder Proxy verwendet

Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für den Konnektor 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 Connector 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 den Konnektor erforderlich sind.

Die Quell-IP-Adresse ist der Connector-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

Service	Protokoll	Port	Ziel	Zweck
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	8088	Backup auf S3	API-Aufrufe zur Sicherung in S3
DNS	UDP	53	DNS	Wird für DNS Resolve von BlueXP verwendet
Cloud-Daten Sinnvoll	HTTP	80	Cloud Data Sense Instanz	Cloud-Daten sinnvoll für Cloud Volumes ONTAP