Requisiti

Amazon FSx for NetApp ONTAP

NetApp
November 28, 2023

Sommario

Requisiti

Impostare le autorizzazioni per FSX per ONTAP

Per creare o gestire un ambiente di lavoro FSX per ONTAP, devi aggiungere le credenziali AWS a BlueXP fornendo l'ARN di un ruolo IAM che assegna ad BlueXP le autorizzazioni necessarie per creare un ambiente di lavoro FSX per ONTAP.

Impostare il ruolo IAM

Impostare un ruolo IAM che consenta a BlueXP di assumere il ruolo.

Fasi

1. Accedere alla console IAM nell'account di destinazione.
2. Concede l'accesso BlueXP all'account AWS. In Gestione accessi, fare clic su **ruoli > Crea ruolo** e seguire i passaggi per creare il ruolo.
   - In **Trusted entity type**, selezionare **AWS account**.
   - Seleziona **un altro account AWS** e immetti l'ID **account** di BlueXP:
     - Per BlueXP SaaS: 952013314444
     - Per AWS GovCloud (USA): 033442085313

     Per una maggiore protezione, si consiglia di specificare un "*ID esterno*". Per accedere al tuo account AWS, BlueXP dovrà fornire il ruolo ARN (Amazon Resource Name) e l'ID esterno specificato. Questo impedisce "problema del sostituto confuso".
3. Creare un criterio che includa le seguenti autorizzazioni minime richieste e facoltative, in base alle necessità.

Autorizzazioni richieste

Per consentire a BlueXP di creare il file system FSX per NetApp ONTAP, sono necessarie le seguenti autorizzazioni minime.

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

Capacità automatica

Per l'abilitazione sono necessarie le seguenti autorizzazioni aggiuntive "gestione automatica della capacità".

```
"cloudwatch:GetMetricData",
"cloudwatch:GetMetricStatistics"
```

Gruppi di sicurezza

Per consentire a BlueXP di, sono necessarie le seguenti autorizzazioni aggiuntive "generare gruppi di sicurezza".

```
"ec2:AuthorizeSecurityGroupEgress",
"ec2:AuthorizeSecurityGroupIngress",
"ec2:RevokeSecurityGroupEgress",
"ec2:RevokeSecurityGroupIngress",
"ec2:CreateSecurityGroup",
"ec2:DeleteSecurityGroup",
"cloudformation:CreateStack",
"cloudformation:ValidateTemplate",
"cloudformation:DescribeStacks",
"cloudformation:DescribeStackEvents"
```

4. Copia il ruolo ARN del ruolo IAM in modo che sia possibile incollarlo in BlueXP nel passaggio successivo.

Risultato

Il ruolo IAM dispone ora delle autorizzazioni necessarie.

Aggiungere le credenziali

Dopo aver fornito al ruolo IAM le autorizzazioni richieste, aggiungere il ruolo ARN a BlueXP.

Prima di iniziare

Se è stato appena creato il ruolo IAM, attendere alcuni minuti per rendere disponibili le nuove credenziali.

Fasi

1. Nella parte superiore destra della console BlueXP, fare clic sull'icona Impostazioni e selezionare **credenziali**.

2. Fare clic su **Add Credentials** (Aggiungi credenziali) e seguire la procedura guidata.
   a. **Posizione credenziali**: Selezionare **Amazon Web Services > BlueXP**.
   b. **Definisci credenziali**: Fornire un **nome credenziali** e il **ruolo ARN** e **ID esterno** (se specificato) creati al momento Impostare il ruolo IAM.

- Se utilizzi un account AWS GovCloud (US), seleziona **uso un account AWS GovCloud (US)**.

- L'autenticazione con AWS GovCloud disattiva la piattaforma SaaS. Si tratta di una modifica permanente dell'account e non può essere annullata.

c. **Revisione**: Confermare i dettagli relativi alle nuove credenziali e fare clic su **Aggiungi**.

Risultato

È ora possibile utilizzare le credenziali durante la creazione di un ambiente di lavoro FSX per ONTAP.

Link correlati

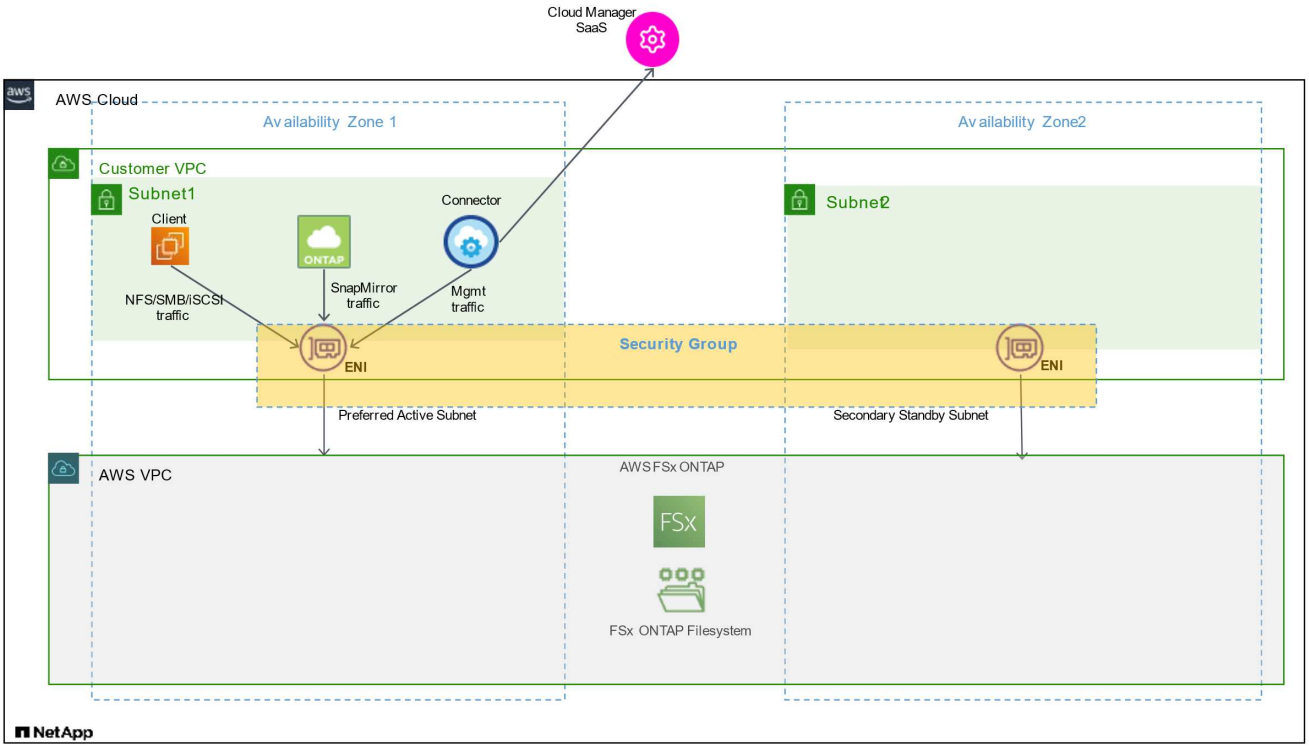
- "Credenziali e autorizzazioni AWS"
- "Gestione delle credenziali AWS per BlueXP"

Regole del gruppo di sicurezza per FSX per ONTAP

BlueXP crea gruppi di sicurezza AWS che includono le regole in entrata e in uscita di cui BlueXP e FSX per ONTAP hanno bisogno per funzionare correttamente. Potrebbe essere necessario fare riferimento alle porte per eseguire test o se è necessario utilizzare il proprio.

Regole per FSX per ONTAP

Il gruppo di sicurezza FSX per ONTAP richiede regole sia in entrata che in uscita. Questo diagramma illustra la configurazione di rete e i requisiti del gruppo di protezione di FSX per ONTAP.

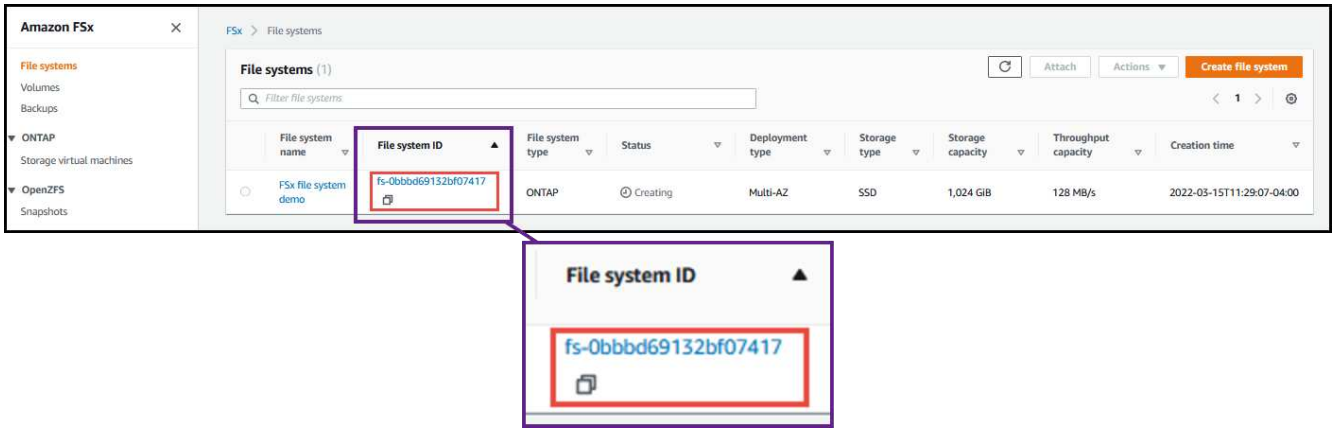


Prima di iniziare

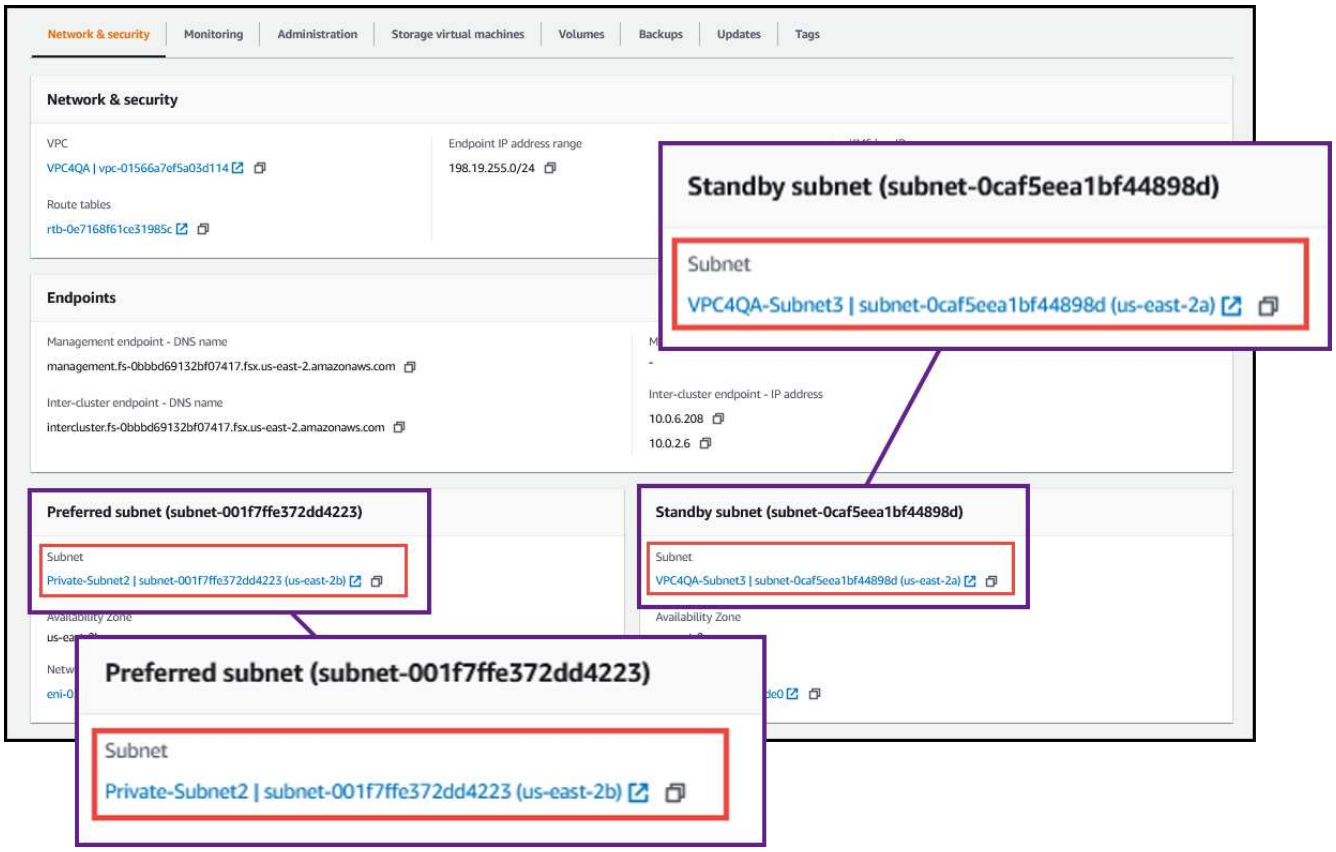
È necessario individuare i gruppi di protezione associati a Enis utilizzando AWS Management Console.

Fasi

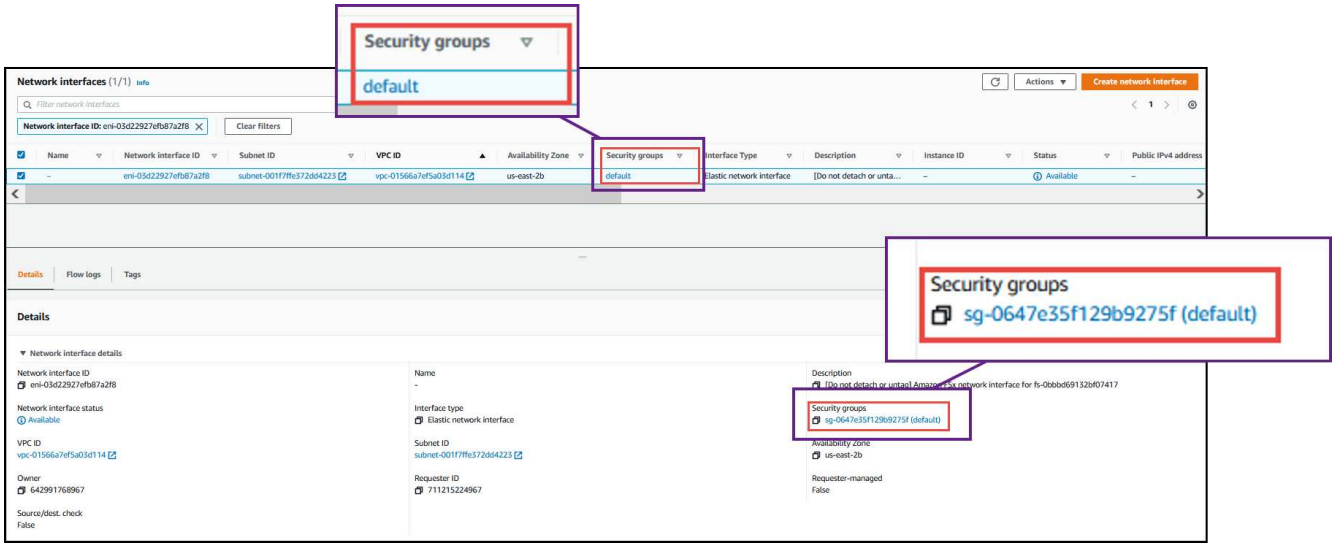
1. Aprire il file system FSX per ONTAP nella console di gestione AWS e fare clic sul collegamento ID file system.



2. Nella scheda **Network & Security** (rete e sicurezza), fare clic sull'ID dell'interfaccia di rete per la subnet preferita o di standby.



3. Fare clic sul gruppo di protezione nella tabella dell'interfaccia di rete o nella sezione **Dettagli** dell'interfaccia di rete.



Regole in entrata

Protocollo	Porta	Scopo
Tutti gli ICMP	Tutto	Eseguire il ping dell'istanza
HTTPS	443	Accesso dal connettore alla LIF di gestione di fsxadmin per inviare chiamate API a FSX

Protocollo	Porta	Scopo
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

Il gruppo di sicurezza predefinito per FSX per 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 FSX per 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

Non è necessario aprire porte specifiche per il mediatore o tra i nodi in FSX per ONTAP.

> L'origine è l'interfaccia (indirizzo IP) sul sistema FSX per ONTAP.

Servizio	Protocollo	Porta	Origine	Destinazione	Scopo
Active Directory	TCP	88	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Autenticazione Kerberos V.
	UDP	137	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Servizio nomi NetBIOS
	UDP	138	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Servizio datagramma NetBIOS
	TCP	139	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Sessione del servizio NetBIOS
	TCP E UDP	389	LIF di gestione dei nodi	Insieme di strutture di Active Directory	LDAP
	TCP	445	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Microsoft SMB/CIFS su TCP con frame NetBIOS
	TCP	464	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Kerberos V change & set password (SET_CHANGE)
	UDP	464	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Amministrazione delle chiavi Kerberos
	TCP	749	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Kerberos V change & set Password (RPCSEC_GSS)
	TCP	88	Data LIF (NFS, CIFS, iSCSI)	Insieme di strutture di Active Directory	Autenticazione Kerberos V.
	UDP	137	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Servizio nomi NetBIOS
	UDP	138	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Servizio datagramma NetBIOS
	TCP	139	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Sessione del servizio NetBIOS
	TCP E UDP	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)
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
DHCP	UDP	68	LIF di gestione dei nodi	DHCP	Client DHCP per la prima installazione

Servizio	Protocollo	Porta	Origine	Destinazione	Scopo
DHCPS	UDP	67	LIF di gestione dei nodi	DHCP	Server DHCP
DNS	UDP	53	LIF di gestione dei nodi e LIF dei dati (NFS, CIFS)	DNS	DNS
NDMP	TCP	18600–18699	LIF di gestione dei nodi	Server di destinazione	Copia NDMP
SMTP	TCP	25	LIF di gestione dei nodi	Server di posta	Gli avvisi SMTP possono essere utilizzati per AutoSupport
SNMP	TCP	161	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	UDP	161	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	TCP	162	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	UDP	162	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
SnapMirror	TCP	11104	LIF intercluster	ONTAP Intercluster LIF	Gestione delle sessioni di comunicazione tra cluster per SnapMirror
	TCP	11105	LIF intercluster	ONTAP Intercluster LIF	Trasferimento dei dati SnapMirror
Syslog	UDP	514	LIF di gestione dei nodi	Server syslog	Messaggi di inoltro syslog

Regole per il connettore

Il gruppo di protezione per il connettore richiede regole sia in entrata che in uscita.

Regole in entrata

Protocollo	Porta	Scopo
SSH	22	Fornisce l’accesso SSH all’host del connettore
HTTP	80	Fornisce l’accesso HTTP dai browser Web client all’interfaccia utente locale e alle connessioni dall’istanza di classificazione BlueXP
HTTPS	443	Fornisce l’accesso HTTPS dai browser Web client all’interfaccia utente locale
TCP	3128	Fornisce l’istanza di classificazione BlueXP con accesso a Internet, se la rete AWS non utilizza un NAT o un proxy

Regole in uscita

Il gruppo di protezione predefinito per il connettore 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 connettore 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 la comunicazione in uscita dal connettore.

L'indirizzo IP di origine è l'host del connettore.

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

Servizio	Protocollo	Porta	Destinazione	Scopo
Chiamate API e AutoSupport	HTTPS	443	LIF gestione cluster ONTAP e Internet in uscita	Chiamate API ad AWS e ONTAP e invio di messaggi AutoSupport a NetApp
Chiamate API	TCP	8088	Backup su S3	API chiama il backup in S3
DNS	UDP	53	DNS	Utilizzato per la risoluzione DNS di BlueXP
Classificazione BlueXP	HTTP	80	Classificazione BlueXP	Classificazione BlueXP per Cloud Volumes ONTAP