Porte

BlueXP setup and administration

NetApp
September 09, 2024

Sommario

Porte . . . 1
Regole del gruppo di sicurezza del connettore in AWS . . . 1
Regole del gruppo di sicurezza del connettore in Azure . . . 2
Regole del firewall connettore in Google Cloud . . . 4
Porte per il connettore on-premise . . . 5

Porte

Regole del gruppo di sicurezza del connettore in AWS

Il gruppo di sicurezza AWS per il connettore richiede regole sia in entrata che in uscita. BlueXP crea automaticamente questo gruppo di protezione quando si crea un connettore da BlueXP. È necessario impostare questo gruppo di protezione per tutte le altre opzioni di installazione.

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 • Utilizzato durante il processo di aggiornamento di Cloud Volumes ONTAP
HTTPS	443	Fornisce l'accesso HTTPS dai browser Web client all'interfaccia utente locale e le connessioni dall'istanza di classificazione BlueXP
TCP	3128	Fornisce a Cloud Volumes ONTAP l'accesso a Internet per inviare messaggi AutoSupport al supporto NetApp. È necessario aprire manualmente questa porta dopo l'implementazione. "Scopri come il connettore viene utilizzato come proxy per i messaggi AutoSupport"

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
Chiamate API e AutoSupport	HTTPS	443	LIF gestione cluster ONTAP e Internet in uscita	L'API chiama AWS, ONTAP, classificandosi BlueXP e inviando messaggi AutoSupport a NetApp
Chiamate API	TCP	3000	Mediatore ONTAP ha	Comunicazione con il mediatore ONTAP ha
	TCP	8080	Classificazione BlueXP	Eseguire una verifica dell'istanza di classificazione BlueXP durante l'implementazione
DNS	UDP	53	DNS	Utilizzato per la risoluzione DNS di BlueXP

Regole del gruppo di sicurezza del connettore in Azure

Il gruppo di sicurezza Azure per il connettore richiede regole sia in entrata che in uscita. BlueXP crea automaticamente questo gruppo di protezione quando si crea un connettore da BlueXP. È necessario impostare questo gruppo di protezione per tutte le altre opzioni di installazione.

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 • Utilizzato durante il processo di aggiornamento di Cloud Volumes ONTAP
HTTPS	443	Fornisce l'accesso HTTPS dai browser Web client all'interfaccia utente locale e le connessioni dall'istanza di classificazione BlueXP

Protocollo	Porta	Scopo
TCP	3128	Fornisce a Cloud Volumes ONTAP l'accesso a Internet per inviare messaggi AutoSupport al supporto NetApp. È necessario aprire manualmente questa porta dopo l'implementazione. "Scopri come il connettore viene utilizzato come proxy per i messaggi AutoSupport"

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
Chiamate API e AutoSupport	HTTPS	443	LIF gestione cluster ONTAP e Internet in uscita	Le chiamate API ad Azure, a ONTAP, alla classificazione BlueXP e all'invio di messaggi AutoSupport a NetApp
Chiamate API	TCP	8080	Classificazione BlueXP	Eseguire una verifica dell'istanza di classificazione BlueXP durante l'implementazione
DNS	UDP	53	DNS	Utilizzato per la risoluzione DNS di BlueXP

Regole del firewall connettore in Google Cloud

Le regole del firewall Google Cloud per il connettore richiedono regole sia in entrata che in uscita. BlueXP crea automaticamente questo gruppo di protezione quando si crea un connettore da BlueXP. È necessario impostare questo gruppo di protezione per tutte le altre opzioni di installazione.

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 • Utilizzato durante il processo di aggiornamento di Cloud Volumes ONTAP
HTTPS	443	Fornisce l'accesso HTTPS dai browser Web client all'interfaccia utente locale
TCP	3128	Fornisce a Cloud Volumes ONTAP l'accesso a Internet per inviare messaggi AutoSupport al supporto NetApp. È necessario aprire manualmente questa porta dopo l'implementazione. "Scopri come il connettore viene utilizzato come proxy per i messaggi AutoSupport"

Regole in uscita

Le regole firewall predefinite per il connettore 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 il connettore 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 la comunicazione in uscita dal connettore.

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

Servizio	Protocollo	Porta	Destinazione	Scopo
Chiamate API e AutoSupport	HTTPS	443	LIF gestione cluster ONTAP e Internet in uscita	Le chiamate API a Google Cloud, a ONTAP, alla classificazione BlueXP e all'invio di messaggi AutoSupport a NetApp
Chiamate API	TCP	8080	Classificazione BlueXP	Eseguire una verifica dell'istanza di classificazione BlueXP durante l'implementazione
DNS	UDP	53	DNS	Utilizzato per la risoluzione DNS di BlueXP

Porte per il connettore on-premise

Il connettore utilizza porte *inbound* se installato manualmente su un host Linux on-premise. Potrebbe essere necessario fare riferimento a queste porte per scopi di pianificazione.

Queste regole in entrata si applicano a tutti i modelli di implementazione BlueXP.

Protocollo	Porta	Scopo
HTTP	80	• Fornisce l'accesso HTTP dai browser Web client all'interfaccia utente locale • Utilizzato durante il processo di aggiornamento di Cloud Volumes ONTAP
HTTPS	443	Fornisce l'accesso HTTPS dai browser Web client all'interfaccia utente locale