



## Requisitos

### Amazon FSx for NetApp ONTAP

NetApp  
August 26, 2024

# Tabla de contenidos

- Requisitos ..... 1
- Configure permisos para FSX para ONTAP ..... 1
- Reglas de grupo de seguridad para FSX para ONTAP ..... 4

# Requisitos

## Configure permisos para FSX para ONTAP

Para crear o gestionar un entorno de trabajo de FSx para ONTAP, debes añadir las credenciales de AWS a BlueXP proporcionando el ARN de un rol de IAM que proporcione a BlueXP los permisos necesarios para crear un entorno de trabajo de FSx para ONTAP.

### Configure el rol IAM

Configure una función de IAM que permita a BlueXP asumir la función.

#### Pasos

1. Vaya a la consola IAM de la cuenta de destino.
2. Otorga acceso de BlueXP a la cuenta de AWS. En Access Management, haga clic en **roles > Crear función** y siga los pasos para crear la función.
  - En **Tipo de entidad de confianza**, seleccione **cuenta de AWS**.
  - Seleccione **Otra cuenta de AWS** e introduzca el **ID de cuenta** de BlueXP:
    - Para BlueXP SaaS: 952013314444
    - Para AWS GovCloud (EE. UU.): 033442085313



Para mayor seguridad, le sugerimos que especifique un "*ID externo*". Para acceder a tu cuenta de AWS, BlueXP tendrá que proporcionar la función ARN (Amazon Resource Name) y el ID externo que especifiques. Esto impide el "[problema de adjunto confuso](#)".

3. Cree una política que incluya los siguientes permisos mínimos requeridos y los permisos opcionales, según sea necesario.

### Permisos necesarios

Se necesitan los siguientes permisos mínimos para permitir que BlueXP cree tu sistema de archivos FSx para ONTAP de NetApp.

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

### Capacidad automática

Los siguientes permisos adicionales son necesarios para habilitarlos ["gestión de la capacidad automática"](#).

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

### Grupos de seguridad

Se necesitan los siguientes permisos adicionales para permitir que BlueXP lo haga ["generar grupos de seguridad"](#).

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

4. Copia el ARN de rol del rol de IAM para poder pegarlo en BlueXP en el siguiente paso.

### Resultado

El rol IAM ahora tiene los permisos necesarios.

## Añada las credenciales

Después de proporcionar la función IAM con los permisos necesarios, agregue el rol ARN a BlueXP.

### Antes de empezar

Si acaba de crear el rol de IAM, espere unos minutos para que las nuevas credenciales estén disponibles.

### Pasos

1. En la parte superior derecha de la consola de BlueXP, haga clic en el icono Configuración y seleccione **credenciales**.



2. Haga clic en **Agregar credenciales** y siga los pasos del asistente.
  - a. **Ubicación de credenciales:** Seleccione **Servicios Web de Amazon > BlueXP**.
  - b. **Definir Credenciales:** Proporciona un **Nombre de Credenciales** y el **Rol ARN** y **ID Externo** (si se especifica) que creaste cuando lo hiciste [Configure el rol IAM](#).

- Si utiliza una cuenta de AWS GovCloud (EE. UU.), marque **utilizo una cuenta de AWS GovCloud (EE. UU.)**.



- La autenticación mediante AWS GovCloud deshabilitará la plataforma SaaS. Este es un cambio permanente en tu cuenta y no se puede deshacer.

c. **Revisión:** Confirme los detalles acerca de las nuevas credenciales y haga clic en **Agregar**.

### Resultado

Ahora puede utilizar las credenciales al crear un entorno de trabajo FSX para ONTAP.

### Enlaces relacionados

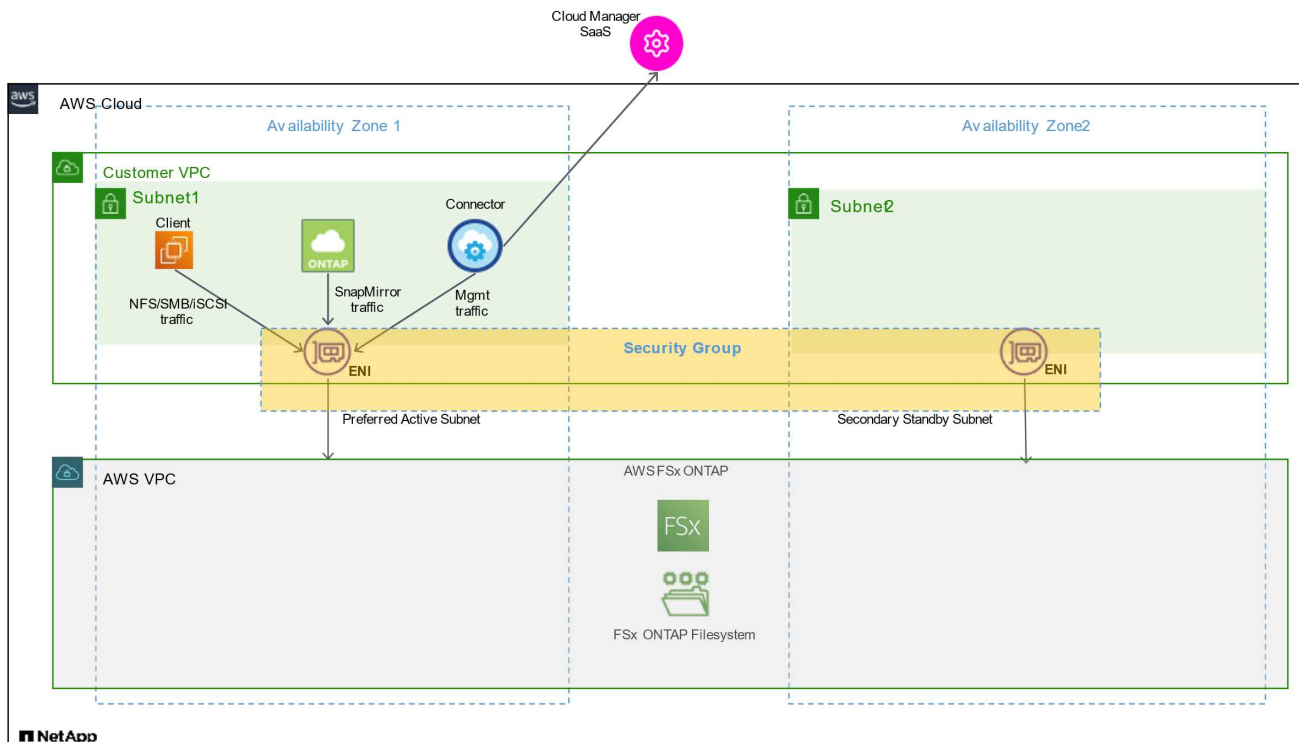
- ["Credenciales y permisos de AWS"](#)
- ["Gestión de credenciales de AWS para BlueXP"](#)

## Reglas de grupo de seguridad para FSX para ONTAP

BlueXP crea grupos de seguridad de AWS que incluyen las reglas de entrada y salida que BlueXP y FSX para ONTAP necesitan para funcionar correctamente. Tal vez desee hacer referencia a los puertos para fines de prueba o si necesita utilizar los suyos propios.

### Reglas para FSX para ONTAP

El grupo de seguridad FSX para ONTAP requiere reglas tanto entrantes como salientes. Este diagrama muestra los requisitos de la configuración de redes y del grupo de seguridad de ONTAP en FSX.

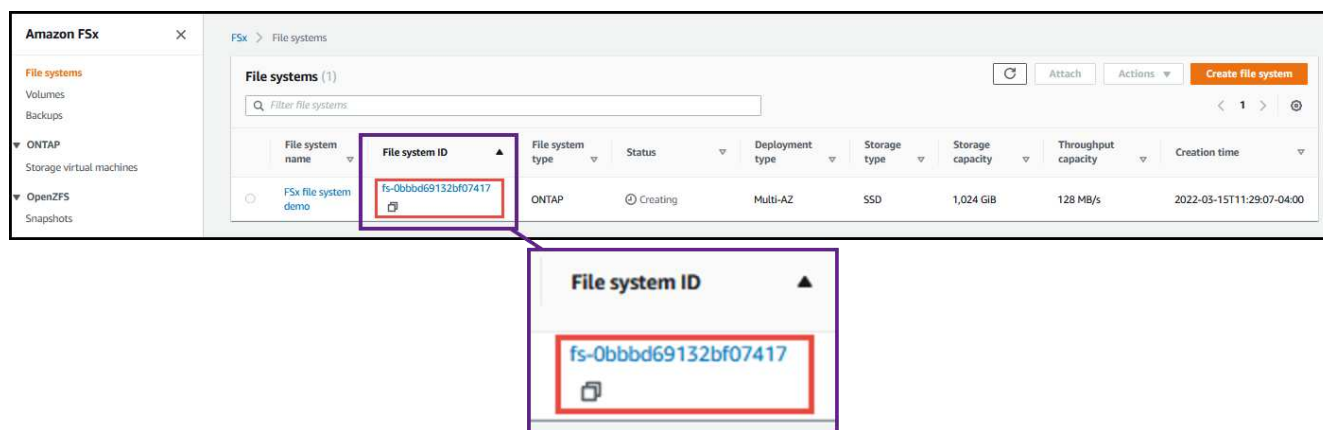


## Antes de empezar

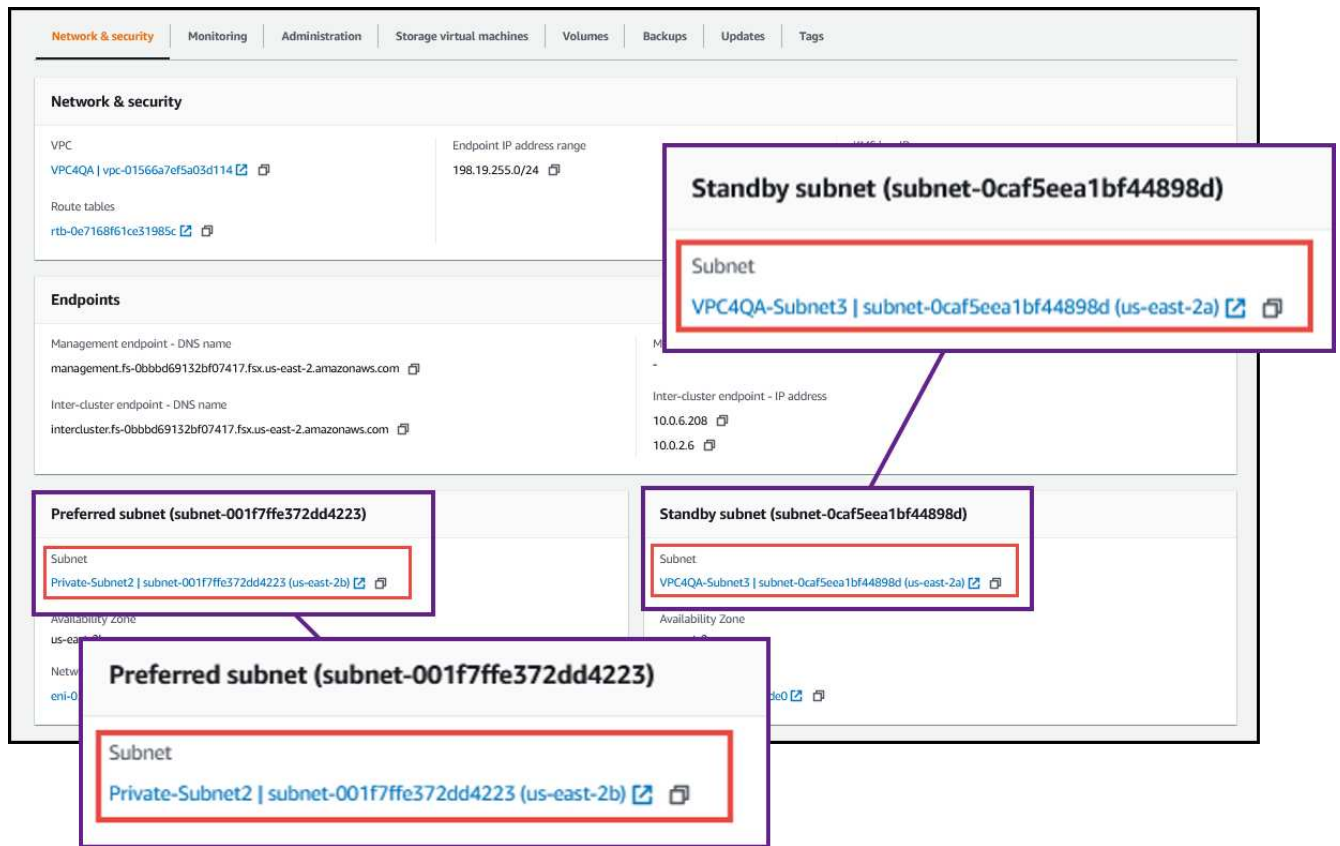
Debe localizar los grupos de seguridad asociados con el sistema Enis mediante la Consola de administración de AWS.

## Pasos

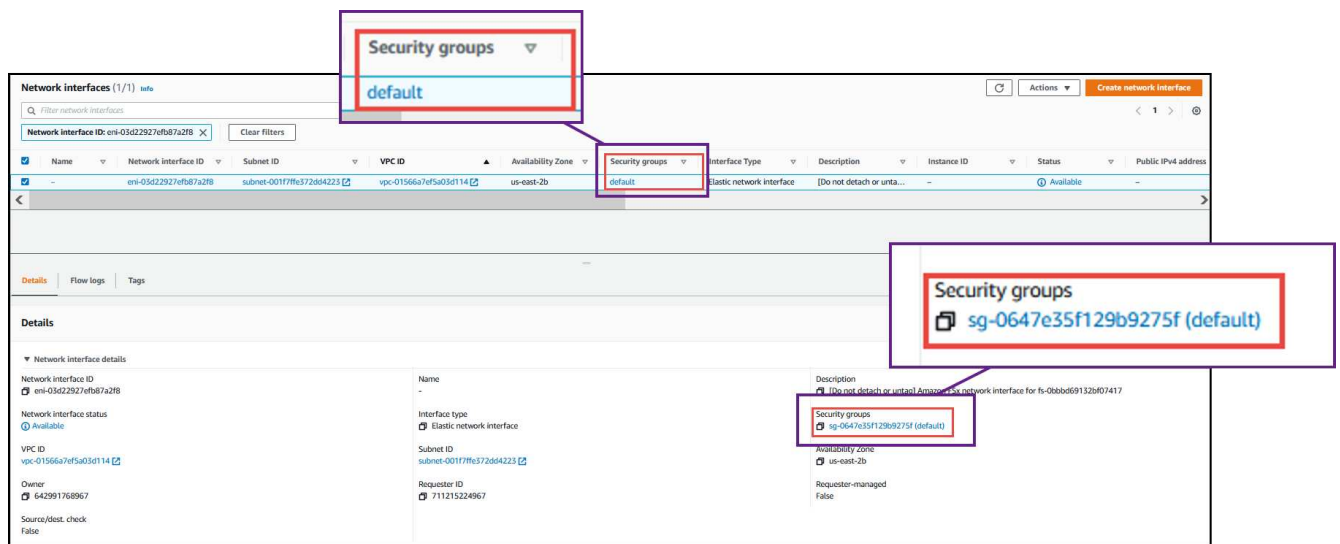
1. Abra el FSx para el sistema de archivos ONTAP en la consola de gestión de AWS y haga clic en el enlace del ID del sistema de archivos.



2. En la ficha **Red y seguridad**, haga clic en el identificador de interfaz de red de la subred preferida o en espera.



3. Haga clic en el grupo de seguridad de la tabla de interfaz de red o en la sección **Detalles** de la interfaz de red.



## Reglas de entrada

Protocolo	Puerto	Específico
ICMP	Todo	Hacer ping a la instancia



Protocolo	Puerto	Específico
HTTPS	443	Acceso desde la LIF de gestión de Connector to fsxadmin para enviar llamadas API a FSX
SSH	22	Acceso SSH a la dirección IP de administración del clúster LIF o una LIF de gestión de nodos
TCP	111	Llamada a procedimiento remoto para NFS
TCP	139	Sesión de servicio NetBIOS para CIFS
TCP	161-162	Protocolo simple de gestión de red
TCP	445	Microsoft SMB/CIFS sobre TCP con trama NetBIOS
TCP	635	Montaje NFS
TCP	749	Kerberos
TCP	2049	Daemon del servidor NFS
TCP	3260	Acceso iSCSI mediante la LIF de datos iSCSI
TCP	4045	Daemon de bloqueo NFS
TCP	4046	Supervisor de estado de red para NFS
TCP	10000	Backup con NDMP
TCP	11104	Gestión de sesiones de comunicación de interconexión de clústeres para SnapMirror
TCP	11105	Transferencia de datos de SnapMirror mediante LIF de interconexión de clústeres
UDP	111	Llamada a procedimiento remoto para NFS
UDP	161-162	Protocolo simple de gestión de red
UDP	635	Montaje NFS
UDP	2049	Daemon del servidor NFS
UDP	4045	Daemon de bloqueo NFS
UDP	4046	Supervisor de estado de red para NFS
UDP	4049	Protocolo rquotad NFS

### Reglas de salida

El grupo de seguridad predefinido para FSX para ONTAP abre todo el tráfico saliente. Si eso es aceptable, siga las reglas básicas de la salida. Si necesita más reglas rígidas, utilice las reglas avanzadas de salida.

### Reglas de salida básicas

El grupo de seguridad predefinido para FSX para ONTAP incluye las siguientes reglas de salida.

Protocolo	Puerto	Específico
Todos los ICMP	Todo	Todo el tráfico saliente
Todos los TCP	Todo	Todo el tráfico saliente

Protocolo	Puerto	Específico
Todas las UDP	Todo	Todo el tráfico saliente

#### Reglas salientes avanzadas

No necesita abrir puertos específicos para el mediador o entre nodos de FSX para ONTAP.



El origen es la interfaz (dirección IP) en el FSX para el sistema ONTAP.

<b>Servicio</b>	<b>Protocolo</b>	<b>Puerto</b>	<b>Origen</b>	<b>Destino</b>	<b>Específico</b>	
Active Directory	TCP	88	LIF de gestión de nodos	Bosque de Active Directory	Autenticación Kerberos V.	
	UDP	137	LIF de gestión de nodos	Bosque de Active Directory	Servicio de nombres NetBIOS	
	UDP	138	LIF de gestión de nodos	Bosque de Active Directory	Servicio de datagramas NetBIOS	
	TCP	139	LIF de gestión de nodos	Bosque de Active Directory	Sesión de servicio NetBIOS	
	TCP Y UDP	389	LIF de gestión de nodos	Bosque de Active Directory	LDAP	
	TCP	445	LIF de gestión de nodos	Bosque de Active Directory	Microsoft SMB/CIFS sobre TCP con trama NetBIOS	
	TCP	464	LIF de gestión de nodos	Bosque de Active Directory	Kerberos V cambiar y establecer contraseña (SET_CHANGE)	
	UDP	464	LIF de gestión de nodos	Bosque de Active Directory	Administración de claves Kerberos	
	TCP	749	LIF de gestión de nodos	Bosque de Active Directory	Contraseña de Kerberos V Change & Set (RPCSEC_GSS)	
	TCP	88	LIF de datos (NFS, CIFS e iSCSI)	Bosque de Active Directory	Autenticación Kerberos V.	
	UDP	137	LIF DE DATOS (NFS, CIFS)	Bosque de Active Directory	Servicio de nombres NetBIOS	
	UDP	138	LIF DE DATOS (NFS, CIFS)	Bosque de Active Directory	Servicio de datagramas NetBIOS	
	TCP	139	LIF DE DATOS (NFS, CIFS)	Bosque de Active Directory	Sesión de servicio NetBIOS	
	TCP Y UDP	389	LIF DE DATOS (NFS, CIFS)	Bosque de Active Directory	LDAP	
	TCP	445	LIF DE DATOS (NFS, CIFS)	Bosque de Active Directory	Microsoft SMB/CIFS sobre TCP con trama NetBIOS	
	TCP	464	LIF DE DATOS (NFS, CIFS)	Bosque de Active Directory	Kerberos V cambiar y establecer contraseña (SET_CHANGE)	
	UDP	464	LIF DE DATOS (NFS, CIFS)	Bosque de Active Directory	Administración de claves Kerberos	
	TCP	749	LIF DE DATOS (NFS, CIFS)	Bosque de Active Directory	Contraseña de Kerberos V change & set (RPCSEC_GSS)	
	Backup en S3	TCP	5010	LIF entre clústeres	Extremo de backup o extremo de restauración	Realizar backups y restaurar operaciones para el backup en S3 función

Servicio	Protocolo	Puerto	Origen	Destino	Específico
DHCP	UDP	68	LIF de gestión de nodos	DHCP	Cliente DHCP para la configuración inicial
DHCPS	UDP	67	LIF de gestión de nodos	DHCP	Servidor DHCP
DNS	UDP	53	LIF de gestión de nodos y LIF de datos (NFS, CIFS)	DNS	DNS
NDMP	TCP	1860-18699	LIF de gestión de nodos	Servidores de destino	Copia NDMP
SMTP	TCP	25	LIF de gestión de nodos	Servidor de correo	Alertas SMTP, que se pueden utilizar para AutoSupport
SNMP	TCP	161	LIF de gestión de nodos	Servidor de supervisión	Supervisión mediante capturas SNMP
	UDP	161	LIF de gestión de nodos	Servidor de supervisión	Supervisión mediante capturas SNMP
	TCP	162	LIF de gestión de nodos	Servidor de supervisión	Supervisión mediante capturas SNMP
	UDP	162	LIF de gestión de nodos	Servidor de supervisión	Supervisión mediante capturas SNMP
SnapMirror	TCP	11104	LIF entre clústeres	LIF de interconexión de clústeres de ONTAP	Gestión de sesiones de comunicación de interconexión de clústeres para SnapMirror
	TCP	11105	LIF entre clústeres	LIF de interconexión de clústeres de ONTAP	Transferencia de datos de SnapMirror
Syslog	UDP	514	LIF de gestión de nodos	Servidor de syslog	Mensajes de syslog Reenviar

## Reglas para el conector

El grupo de seguridad del conector requiere reglas entrantes y salientes.

### Reglas de entrada

Protocolo	Puerto	Específico
SSH	22	Proporciona acceso SSH al host de Connector
HTTP	80	Proporciona acceso HTTP desde los navegadores web del cliente a la interfaz de usuario local y las conexiones desde la instancia de clasificación de BlueXP
HTTPS	443	Proporciona acceso HTTPS desde exploradores web de cliente al local interfaz de usuario

Protocolo	Puerto	Específico
TCP	3128	Proporciona acceso a Internet a la instancia de clasificación de BlueXP si la red AWS no utiliza un NAT o un proxy

### Reglas de salida

El grupo de seguridad predefinido para el conector abre todo el tráfico saliente. Si eso es aceptable, siga las reglas básicas de la salida. Si necesita más reglas rígidas, utilice las reglas avanzadas de salida.

#### Reglas de salida básicas

El grupo de seguridad predefinido para el conector incluye las siguientes reglas de salida.

Protocolo	Puerto	Específico
Todos los TCP	Todo	Todo el tráfico saliente
Todas las UDP	Todo	Todo el tráfico saliente

#### Reglas salientes avanzadas

Si necesita reglas rígidas para el tráfico saliente, puede utilizar la siguiente información para abrir sólo los puertos necesarios para la comunicación saliente por parte del conector.



La dirección IP de origen es el host del conector.

<b>Servicio</b>	<b>Protocolo</b>	<b>Puerto</b>	<b>Destino</b>	<b>Específico</b>
Active Directory	TCP	88	Bosque de Active Directory	Autenticación Kerberos V.
	TCP	139	Bosque de Active Directory	Sesión de servicio NetBIOS
	TCP	389	Bosque de Active Directory	LDAP
	TCP	445	Bosque de Active Directory	Microsoft SMB/CIFS sobre TCP con trama NetBIOS
	TCP	464	Bosque de Active Directory	Kerberos V cambiar y establecer contraseña (SET_CHANGE)
	TCP	749	Bosque de Active Directory	Contraseña de modificación y definición de Kerberos V de Active Directory (RPCSEC_GSS)
	UDP	137	Bosque de Active Directory	Servicio de nombres NetBIOS
	UDP	138	Bosque de Active Directory	Servicio de datagramas NetBIOS
	UDP	464	Bosque de Active Directory	Administración de claves Kerberos
Llamadas API y AutoSupport	HTTPS	443	LIF de gestión de clústeres de ONTAP y Internet saliente	API llama a AWS y ONTAP y envía mensajes de AutoSupport a NetApp
Llamadas API	TCP	8088	Backup en S3	Llamadas API a Backup en S3
DNS	UDP	53	DNS	Utilizado para resolver DNS por BlueXP
Clasificación de BlueXP	HTTP	80	Clasificación de BlueXP	Clasificación de BlueXP para Cloud Volumes ONTAP

## Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPTIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

## Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.