



Cree el pool de almacenamiento en el cloud

StorageGRID

NetApp
April 10, 2024

Tabla de contenidos

- Cree un pool de almacenamiento en el cloud 1
 - S3: Se especifican detalles de autenticación para un pool de almacenamiento en cloud. 3
 - C2S S3: Especifique los detalles de la autenticación de un pool de almacenamiento en el cloud 7
 - Azure: Especifique detalles de autenticación para un pool de almacenamiento en cloud 10

Cree un pool de almacenamiento en el cloud

Cuando crea un Cloud Storage Pool, debe especificar el nombre y la ubicación del bloque o contenedor externo que StorageGRID utilizará para almacenar objetos, el tipo de proveedor cloud (Amazon S3 o Azure Blob Storage) y la información que StorageGRID necesita para acceder a la bloque o el contenedor externo.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un [navegador web compatible](#).
- Tiene permisos de acceso específicos.
- Ha revisado las directrices para configurar Cloud Storage Pools.
- El bloque o contenedor externo al que hace referencia el Cloud Storage Pool ya existe.
- Tiene toda la información de autenticación necesaria para acceder al bloque o contenedor.

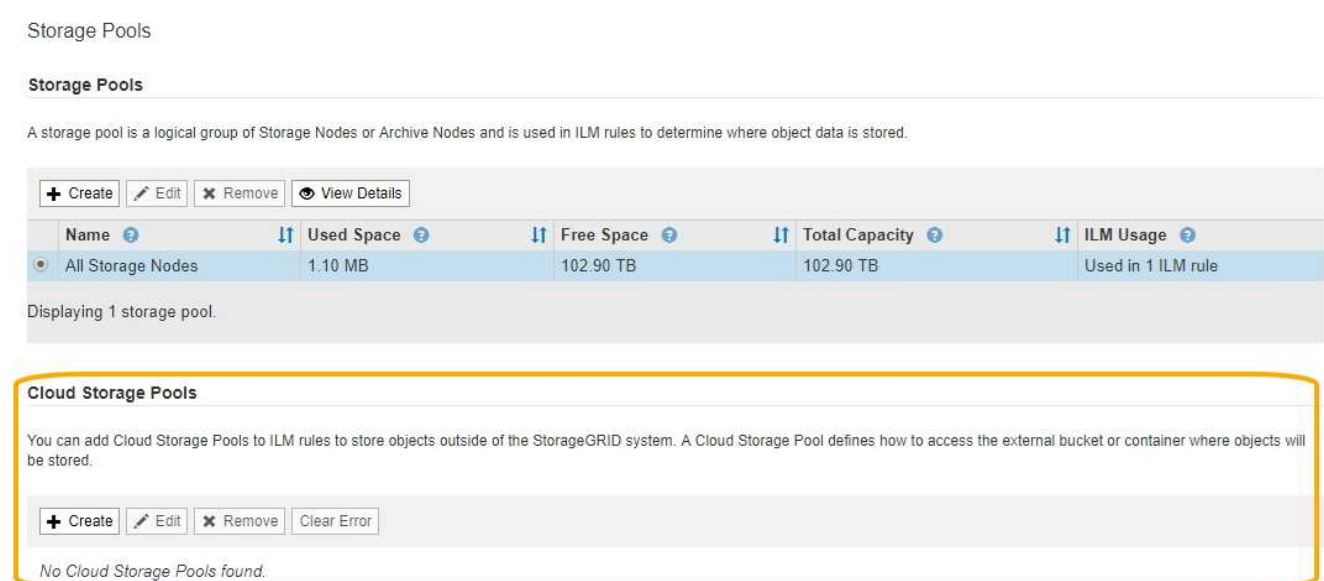
Acerca de esta tarea

Un Cloud Storage Pool especifica un único bloque de almacenamiento S3 externo o Azure Blob. StorageGRID valida el pool de almacenamiento en cloud tan pronto como lo guarde, por lo que debe asegurarse de que existe el bloque o contenedor especificado en el pool de almacenamiento en el cloud y sea posible acceder a él.

Pasos

1. Seleccione **ILM > agrupaciones de almacenamiento**.

Aparece la página Storage Pools. Esta página incluye dos secciones: Pools de almacenamiento y pools de almacenamiento en cloud.



Storage Pools

Storage Pools

A storage pool is a logical group of Storage Nodes or Archive Nodes and is used in ILM rules to determine where object data is stored.

+ Create Edit Remove View Details

Name	Used Space	Free Space	Total Capacity	ILM Usage
All Storage Nodes	1.10 MB	102.90 TB	102.90 TB	Used in 1 ILM rule

Displaying 1 storage pool.

Cloud Storage Pools

You can add Cloud Storage Pools to ILM rules to store objects outside of the StorageGRID system. A Cloud Storage Pool defines how to access the external bucket or container where objects will be stored.

+ Create Edit Remove Clear Error

No Cloud Storage Pools found.

2. En la sección Cloud Storage Pools de la página, seleccione **Crear**.

Se muestra el cuadro de diálogo Crear un pool de almacenamiento en cloud.

Create Cloud Storage Pool

Display Name ?

Provider Type ?

Bucket or Container ?

Cancel

Save

3. Introduzca la siguiente información:

Campo	Descripción
Nombre para mostrar	Un nombre que describe brevemente el pool de almacenamiento en el cloud y su propósito. Utilice un nombre que será fácil de identificar al configurar las reglas de ILM.
Tipo de proveedor	<p>Qué proveedor de cloud utilizará para este pool de almacenamiento en cloud:</p> <ul style="list-style-type: none"> • Amazon S3: Seleccione esta opción para un extremo S3, C2S S3 o Google Cloud Platform (GCP). • Almacenamiento de Azure Blob <p>Nota: cuando selecciona un Tipo de proveedor, las secciones de extremo de servicio, autenticación y verificación de servidor aparecen en la parte inferior de la página.</p>
Cucharón o contenedor	El nombre del bloque de S3 externo o del contenedor de Azure que se creó para el pool de almacenamiento en cloud. Se producirá un error en el nombre que especifique aquí para que coincida exactamente con el nombre del bloque o contenedor, o bien se producirá un error al crear el pool de almacenamiento en cloud. No se puede cambiar este valor después de guardar el pool de almacenamiento en cloud.

4. Complete las secciones Service Endpoint, Authentication and Server Verification de la página, según el tipo de proveedor seleccionado.

- [S3:](#) Especifique los detalles de autenticación para un pool de almacenamiento en cloud
- [C2S S3:](#) Especifique los detalles de la autenticación de un pool de almacenamiento en el cloud
- [Azure:](#) Especifique detalles de autenticación para un pool de almacenamiento en cloud


S3: Se especifican detalles de autenticación para un pool de almacenamiento en cloud


Al crear un Cloud Storage Pool para S3, debe seleccionar el tipo de autenticación requerido para el extremo de Cloud Storage Pool. Puede especificar Anónimo o introducir un ID de clave de acceso y una clave de acceso secreta.


Lo que necesitará

- Ha introducido la información básica para Cloud Storage Pool y ha especificado **Amazon S3** como tipo de proveedor.


Create Cloud Storage Pool


Display Name  S3 Cloud Storage Pool


Provider Type  Amazon S3 ▼


Bucket or Container  my-s3-bucket

Service Endpoint


Protocol  ☐ HTTP ☒ HTTPS

Hostname  example.com or 0.0.0.0

Port (optional)  443

URL Style  Auto-Detect ▼

Authentication

Authentication Type  ▼

Server Verification

Certificate Validation  Use operating system CA certificate ▼

Cancel

Save

- Si utiliza la autenticación de clave de acceso, conoce el identificador de clave de acceso y la clave de acceso secreta del bloque S3 externo.

Pasos

1. En la sección **Service Endpoint**, proporcione la siguiente información:

- a. Seleccione el protocolo que desea utilizar al conectarse al Cloud Storage Pool.

El protocolo predeterminado es HTTPS.

- b. Introduzca el nombre de host o la dirección IP del servidor del grupo de almacenamiento en cloud.

Por ejemplo:

`s3-aws-region.amazonaws.com`



No incluya el nombre del segmento en este campo. Incluye el nombre del segmento en el campo **cucharón o contenedor**.

- a. Opcionalmente, especifique el puerto que se debe utilizar al conectarse al Cloud Storage Pool.

Deje este campo vacío para utilizar el puerto predeterminado: Puerto 443 para HTTPS o puerto 80 para HTTP.

- b. Seleccione el estilo de la URL para el bucket de Cloud Storage Pool:

Opción	Descripción
Estilo de alojamiento virtual	Utilice una URL de estilo alojado virtual para acceder al bloque. Las URL de estilo alojado virtual incluyen el nombre de bloque como parte del nombre de dominio, por ejemplo <code>https://bucket-name.s3.company.com/key-name</code> .
Estilo de trazado	Utilice una dirección URL de estilo de ruta para acceder al bloque. Las direcciones URL de estilo de ruta incluyen el nombre de bloque al final, por ejemplo <code>https://s3.company.com/bucket-name/key-name</code> . Nota: la dirección URL de estilo de ruta está en desuso.
Detección automática	Intente detectar automáticamente qué estilo de URL usar, en función de la información proporcionada. Por ejemplo, si especifica una dirección IP, StorageGRID utilizará una dirección URL de tipo path. Seleccione esta opción sólo si no conoce el estilo específico que desea utilizar.

2. En la sección **autenticación**, seleccione el tipo de autenticación que se requiere para el extremo de Cloud Storage Pool.

Opción	Descripción
Clave de acceso	Se requiere un identificador de clave de acceso y una clave de acceso secreta para acceder al bloque del pool de almacenamiento en cloud.

Opción	Descripción
Anónimo	Todos tienen acceso al bloque de pools de almacenamiento en cloud. No se requieren un identificador de clave de acceso ni una clave de acceso secreta.
CAP (Portal de acceso C2S)	Se utiliza únicamente para C2S S3. Vaya a. C2S S3: Especificar detalles de autenticación de un pool de almacenamiento en el cloud.

3. Si seleccionó Access Key, introduzca la siguiente información:

Opción	Descripción
ID de clave de acceso	El ID de clave de acceso de la cuenta a la que pertenece el bloque externo.
Clave de acceso secreta	La clave de acceso secreta asociada.

4. En la sección Server Verification, seleccione el método que debe utilizarse para validar el certificado de conexiones TLS con el pool de almacenamiento de cloud:

Opción	Descripción
Utilizar certificado de CA del sistema operativo	Utilice los certificados de CA de cuadrícula predeterminados instalados en el sistema operativo para asegurar las conexiones.
Utilizar certificado de CA personalizado	Usar un certificado de CA personalizado. Seleccione Seleccionar nuevo y cargue el certificado de CA codificado con PEM.
No verifique el certificado	El certificado utilizado para la conexión TLS no se verifica.

5. Seleccione **Guardar**.

Cuando guarda un pool de almacenamiento en cloud, StorageGRID hace lo siguiente:

- Valida que el bloque y el extremo de servicio existen y que se pueden alcanzar utilizando las credenciales especificadas.
- Escribe un archivo de marcador en el bloque para identificar el bloque como un pool de almacenamiento en el cloud. No elimine nunca este archivo, que se denomina `x-ntap-sgws-cloud-pool-uuid`.

Si la validación de Cloud Storage Pool falla, recibirá un mensaje de error que explica por qué falló la validación. Por ejemplo, se puede informar un error si existe un error de certificado o si el bloque especificado no existe todavía.

! Error

422: Unprocessable Entity

Validation failed. Please check the values you entered for errors.

Cloud Pool test failed. Could not create or update Cloud Pool. Error from endpoint: NoSuchBucket:
The specified bucket does not exist. status code: 404, request id: 4211567681, host id:

OK

Consulte las instrucciones para [Solución de problemas de Cloud Storage Pools](#), Resuelva el problema e intente volver a guardar el grupo de almacenamiento en la nube.

C2S S3: Especifique los detalles de la autenticación de un pool de almacenamiento en el cloud

Para utilizar el servicio S3 de Commercial Cloud Services (C2S) como un Pool de almacenamiento en cloud, debe configurar C2S Access Portal (CAP) como el tipo de autenticación, de modo que StorageGRID pueda solicitar credenciales temporales para acceder al bloque de S3 de su cuenta C2S.

Lo que necesitará

- Introdujo la información básica de un pool de almacenamiento en cloud de Amazon S3, incluido el extremo de servicio.
- Conoce la dirección URL completa que StorageGRID utilizará para obtener credenciales temporales del servidor CAP, incluidos todos los parámetros API necesarios y opcionales asignados a su cuenta C2S.
- Tiene un certificado de CA de servidor emitido por una entidad de certificación gubernamental (CA) correspondiente. StorageGRID utiliza este certificado para comprobar la identidad del servidor CAP. El certificado de CA del servidor debe utilizar la codificación PEM.
- Tiene un certificado de cliente emitido por una autoridad de certificación gubernamental (CA) correspondiente. StorageGRID utiliza este certificado para identificarse al servidor CAP. El certificado de cliente debe utilizar la codificación PEM y debe tener acceso a su cuenta C2S.
- Tiene una clave privada codificada en PEM para el certificado de cliente.
- Si la clave privada del certificado de cliente está cifrada, tendrá la frase de contraseña para descifrarla.

Pasos


1. En la sección **autenticación**, seleccione **CAP (Portal de acceso de C2S)** en el menú desplegable **Tipo de autenticación**.

Aparecen los campos de autenticación CAP C2S.

Create Cloud Storage Pool

Display Name  C2S Cloud Storage Pool

Provider Type  Amazon S3 ▼

Bucket or Container  my-c2s-bucket

Service Endpoint

Protocol  ☐ HTTP ☒ HTTPS

Hostname  s3-aws-region.amazonaws.com

Port (optional)  443

URL Style  Auto-Detect ▼

Authentication

Authentication Type  CAP (C2S Access Portal) ▼

Temporary Credentials URL  https://example.com/CAP/api/v1/cred


Server CA Certificate  [Select New](#)

Client Certificate  [Select New](#)

Client Private Key  [Select New](#)

Client Private Key
Passphrase (optional) 

Server Verification

Certificate Validation  Use operating system CA certificate ▼

Cancel

Save

2. Proporcione la siguiente información:

- a. Para **URL de credenciales temporales**, introduzca la dirección URL completa que StorageGRID utilizará para obtener credenciales temporales del servidor CAP, incluidos todos los parámetros API necesarios y opcionales asignados a su cuenta C2S.
- b. Para **Certificado CA de servidor**, seleccione **Seleccionar nuevo** y cargue el certificado de CA codificado con PEM que StorageGRID utilizará para verificar el servidor CAP.
- c. Para **Certificado de cliente**, seleccione **Seleccionar nuevo** y cargue el certificado codificado con PEM que StorageGRID utilizará para identificarse al servidor CAP.
- d. Para **clave privada de cliente**, seleccione **Seleccionar nuevo** y cargue la clave privada codificada con PEM para el certificado de cliente.

Si la clave privada está cifrada, se debe utilizar el formato tradicional. (No se admite el formato cifrado PKCS #8).

- e. Si la clave privada del cliente está cifrada, introduzca la frase de acceso para descifrar la clave privada del cliente. De lo contrario, deje en blanco el campo **frase de paso de clave privada cliente**.

3. En la sección Server Verification, introduzca la siguiente información:

- a. Para **validación de certificados**, seleccione **utilizar certificado de CA personalizado**.
- b. Seleccione **Seleccionar nuevo** y cargue el certificado de CA codificado con PEM.

4. Seleccione **Guardar**.

Cuando guarda un pool de almacenamiento en cloud, StorageGRID hace lo siguiente:

- Valida que el bloque y el extremo de servicio existen y que se pueden alcanzar utilizando las credenciales especificadas.
- Escribe un archivo de marcador en el bloque para identificar el bloque como un pool de almacenamiento en el cloud. No elimine nunca este archivo, que se denomina `x-ntap-sgws-cloud-pool-uuid`.

Si la validación de Cloud Storage Pool falla, recibirá un mensaje de error que explica por qué falló la validación. Por ejemplo, se puede informar un error si existe un error de certificado o si el bloque especificado no existe todavía.

! Error

422: Unprocessable Entity

Validation failed. Please check the values you entered for errors.

Cloud Pool test failed. Could not create or update Cloud Pool. Error from endpoint: NoSuchBucket:
The specified bucket does not exist. status code: 404, request id: 4211567681, host id:

OK

Consulte las instrucciones para [Solución de problemas de Cloud Storage Pools](#), Resuelva el problema e intente volver a guardar el grupo de almacenamiento en la nube.

Azure: Especifique detalles de autenticación para un pool de almacenamiento en cloud

Cuando crea un Cloud Storage Pool para el almacenamiento BLOB de Azure, debe especificar un nombre de cuenta y una clave de cuenta para el contenedor externo que StorageGRID utilizará para almacenar objetos.

Lo que necesitará

- Ha introducido la información básica para Cloud Storage Pool y ha especificado **Azure Blob Storage** como tipo de proveedor. **Clave compartida** aparece en el campo **Tipo de autenticación**.

Create Cloud Storage Pool

Display Name ⓘ

Azure Cloud Storage Pool

Provider Type ⓘ

Azure Blob Storage ▼

Bucket or Container ⓘ

my-azure-container

Service Endpoint

URI ⓘ

https://myaccount.blob.core.windows.net

Authentication

Authentication Type ⓘ

Shared Key

Account Name ⓘ

Account Key ⓘ

Server Verification

Certificate Validation ⓘ

Use operating system CA certificate ▼

Cancel

Save

- Conoce el identificador uniforme de recursos (URI) que se utiliza para acceder al contenedor de almacenamiento BLOB que se utiliza para el pool de almacenamiento cloud.

- Conoce el nombre de la cuenta de almacenamiento y la clave secreta. Puede usar el portal de Azure para encontrar estos valores.

Pasos

1. En la sección **Service Endpoint**, introduzca el Identificador uniforme de recursos (URI) que se utiliza para acceder al contenedor de almacenamiento BLOB utilizado para el Pool de almacenamiento en la nube.

Especifique el URI en uno de los siguientes formatos:

- `https://host:port`
- `http://host:port`

Si no especifica un puerto, el puerto 443 se utiliza de manera predeterminada para los URI HTTPS y el puerto 80 se utiliza para los URI HTTP. + + **ejemplo URI para el contenedor de almacenamiento Azure Blob:**

`https://myaccount.blob.core.windows.net`

2. En la sección **autenticación**, proporcione la siguiente información:
 - a. Para **Nombre de cuenta**, introduzca el nombre de la cuenta de almacenamiento Blob que posee el contenedor de servicios externo.
 - b. Para **clave de cuenta**, introduzca la clave secreta de la cuenta de almacenamiento Blob.



Para los extremos de Azure, se debe usar la autenticación de clave compartida.

3. En la sección **verificación del servidor**, seleccione el método que debe utilizarse para validar el certificado para las conexiones TLS con el grupo de almacenamiento en la nube:

Opción	Descripción
Utilizar certificado de CA del sistema operativo	Utilice los certificados de CA de cuadrícula instalados en el sistema operativo para asegurar las conexiones.
Utilizar certificado de CA personalizado	Usar un certificado de CA personalizado. Seleccione Seleccionar nuevo y cargue el certificado codificado con PEM.
No verifique el certificado	El certificado utilizado para la conexión TLS no se verifica.

4. Seleccione **Guardar**.

Cuando guarda un pool de almacenamiento en cloud, StorageGRID hace lo siguiente:

- Valida que el contenedor y el URI existen y que se puede alcanzar utilizando las credenciales especificadas.
- Escribe un archivo marcador en el contenedor para identificarlo como un pool de almacenamiento en el cloud. No elimine nunca este archivo, que se denomina `x-ntap-sgws-cloud-pool-uuid`.

Si la validación de Cloud Storage Pool falla, recibirá un mensaje de error que explica por qué falló la validación. Por ejemplo, es posible que se notifique un error si existe un error de certificado o el contenedor especificado no existe todavía.

Consulte las instrucciones para [Solución de problemas de Cloud Storage Pools](#), Resuelva el problema e

intente volver a guardar el grupo de almacenamiento en la nube.

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 INTERRUPCIÓN 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.