



# **Crie Cloud Storage Pool**

## **StorageGRID**

NetApp  
March 12, 2025

# Índice

- Crie um pool de storage em nuvem ..... 1
  - S3: Especificando detalhes de autenticação para um pool de armazenamento em nuvem ..... 2
  - C2S S3: Especificar detalhes de autenticação para um pool de armazenamento em nuvem ..... 7
  - Azure: Especifique os detalhes de autenticação para um pool de armazenamento em nuvem ..... 10

# Crie um pool de storage em nuvem

Ao criar um pool de storage de nuvem, especifique o nome e o local do bucket externo ou do contêiner que o StorageGRID usará para armazenar objetos, o tipo de fornecedor de nuvem (Amazon S3 ou armazenamento de Blob do Azure) e as informações que o StorageGRID precisa para acessar o bucket externo ou o contêiner.

## O que você vai precisar

- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem permissões de acesso específicas.
- Você revisou as diretrizes para a configuração de pools de armazenamento em nuvem.
- O bucket externo ou o contentor referenciado pelo Cloud Storage Pool já existe.
- Você tem todas as informações de autenticação necessárias para acessar o bucket ou o contentor.

## Sobre esta tarefa

Um Cloud Storage Pool especifica um único bucket externo do S3 ou contêiner de storage Azure Blob. O StorageGRID valida o pool de armazenamento em nuvem assim que você o salva, portanto, você deve garantir que o bucket ou o contentor especificado no pool de armazenamento em nuvem existe e está acessível.

## Passos

1. Selecione **ILM > Storage Pools**.

A página conjuntos de armazenamento é exibida. Esta página inclui duas seções: Pools de armazenamento e pools de armazenamento em nuvem.

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. Na seção Cloud Storage Pools da página, selecione **criar**.

A caixa de diálogo criar pool de armazenamento em nuvem é exibida.

### Create Cloud Storage Pool

Display Name ?

Provider Type ?

Bucket or Container ?

Cancel
Save

3. Introduza as seguintes informações:

Campo	Descrição
Nome de exibição	Um nome que descreve brevemente o Cloud Storage Pool e sua finalidade. Use um nome que será fácil de identificar quando você configurar regras ILM.
Tipo de fornecedor	<p>Qual provedor de nuvem você usará para este pool de armazenamento em nuvem:</p> <ul style="list-style-type: none"> <li><b>Amazon S3:</b> Selecione essa opção para um endpoint S3, C2S S3 ou Google Cloud Platform (GCP).</li> <li><b>Armazenamento de Blobs do Azure</b></li> </ul> <p><b>Observação:</b> quando você seleciona um tipo de provedor, as seções ponto final do serviço, Autenticação e Verificação do servidor aparecem na parte inferior da página.</p>
Balde ou recipiente	O nome do bucket externo do S3 ou do contêiner do Azure que foi criado para o Cloud Storage Pool. O nome especificado aqui deve corresponder exatamente ao nome do bucket ou do contentor ou a criação do Cloud Storage Pool falhará. Você não pode alterar esse valor depois que o pool de armazenamento em nuvem for salvo.

4. Preencha as seções Service Endpoint, Authentication e Server Verification da página, com base no tipo de provedor selecionado.

- [S3: Especificar detalhes de autenticação para um pool de armazenamento em nuvem](#)
- [C2S S3: Especificar detalhes de autenticação para um pool de armazenamento em nuvem](#)
- [Azure: Especifique os detalhes de autenticação para um pool de armazenamento em nuvem](#)

## S3: Especificando detalhes de autenticação para um pool de armazenamento em nuvem


Ao criar um pool de armazenamento em nuvem para S3, você deve selecionar o tipo de


autenticação necessário para o ponto de extremidade do pool de armazenamento em nuvem. Você pode especificar anônimo ou inserir um ID de chave de acesso e chave de acesso secreta.


#### **O que você vai precisar**

- Você inseriu as informações básicas do Cloud Storage Pool e especificou **Amazon S3** como o tipo de provedor.

# 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](#)

- Se você estiver usando a autenticação da chave de acesso, você saberá o ID da chave de acesso e a chave de acesso secreta para o bucket externo do S3.

## Passos

1. Na seção **Service Endpoint**, forneça as seguintes informações:

a. Selecione qual protocolo usar ao se conectar ao pool de armazenamento em nuvem.

O protocolo padrão é HTTPS.

b. Insira o nome do host do servidor ou o endereço IP do pool de armazenamento em nuvem.

Por exemplo:

`s3-aws-region.amazonaws.com`



Não inclua o nome do intervalo neste campo. Você inclui o nome do bucket no campo **Bucket ou Container**.

a. Opcionalmente, especifique a porta que deve ser usada ao se conectar ao Cloud Storage Pool.

Deixe este campo em branco para usar a porta padrão: Porta 443 para HTTPS ou porta 80 para HTTP.

b. Selecione o estilo de URL do bucket do Cloud Storage Pool:

Opção	Descrição
Virtual Hosted-Style	Use um URL virtual de estilo hospedado para acessar o bucket. URLs de estilo hospedado virtual incluem o nome do intervalo como parte do nome de domínio, por <code>https://bucket-name.s3.company.com/key-name</code> exemplo .
Estilo de caminho	Use um URL de estilo de caminho para acessar o bucket. URLs de estilo de caminho incluem o nome do intervalo no final, por <code>https://s3.company.com/bucket-name/key-name</code> exemplo .  <b>Nota:</b> o URL do estilo de caminho está sendo obsoleto.
Deteção automática	Tente detetar automaticamente qual estilo de URL usar, com base nas informações fornecidas. Por exemplo, se você especificar um endereço IP, o StorageGRID usará um URL estilo caminho. Selecione esta opção somente se você não souber qual estilo específico usar.

2. Na seção **Autenticação**, selecione o tipo de autenticação necessário para o endpoint Cloud Storage Pool.

Opção	Descrição
Chave de acesso	Um ID de chave de acesso e chave de acesso secreta são necessários para acessar o intervalo do pool de armazenamento em nuvem.
Anônimo	Todos têm acesso ao bucket do Cloud Storage Pool. Não é necessário um ID de chave de acesso e uma chave de acesso secreta.

Opção	Descrição
CAP (Portal de Acesso C2S)	Usado apenas para C2S S3. Vá para <a href="#">C2S S3: Especificando detalhes de autenticação para um pool de armazenamento em nuvem</a> .

3. Se tiver selecionado a chave de acesso, introduza as seguintes informações:

Opção	Descrição
ID da chave de acesso	O ID da chave de acesso para a conta que possui o intervalo externo.
Chave de Acesso secreta	A chave de acesso secreto associada.

4. Na seção Verificação do servidor, selecione qual método deve ser usado para validar o certificado para conexões TLS com o pool de armazenamento em nuvem:

Opção	Descrição
Use o certificado CA do sistema operacional	Use os certificados de CA de grade padrão instalados no sistema operacional para proteger conexões.
Use certificado CA personalizado	Use um certificado de CA personalizado. Selecione <b>Selecione novo</b> e carregue o certificado CA codificado em PEM.
Não verifique o certificado	O certificado usado para a conexão TLS não é verificado.

5. Selecione **Guardar**.

Quando você salva um pool de storage de nuvem, o StorageGRID faz o seguinte:

- Valida que o intervalo e o endpoint de serviço existem e que eles podem ser alcançados usando as credenciais que você especificou.
- Grava um arquivo de marcador no bucket para identificar o bucket como um Cloud Storage Pool. Nunca remova esse arquivo, que é `x-ntap-sgws-cloud-pool-uuid` chamado .

Se a validação do Cloud Storage Pool falhar, você receberá uma mensagem de erro que explica por que a validação falhou. Por exemplo, um erro pode ser relatado se houver um erro de certificado ou se o intervalo especificado ainda não existir.



## ! 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 as instruções do [Solução de problemas de Cloud Storage Pools](#), resolva o problema e tente salvar o pool de armazenamento em nuvem novamente.

## C2S S3: Especificar detalhes de autenticação para um pool de armazenamento em nuvem

Para usar o serviço de Serviços comerciais de nuvem (C2S) S3 como um pool de armazenamento em nuvem, você deve configurar o C2S Access Portal (CAP) como o tipo de autenticação, para que a StorageGRID possa solicitar credenciais temporárias para acessar o bucket do S3 na sua conta do C2S.

### O que você vai precisar

- Você inseriu as informações básicas de um pool de armazenamento em nuvem do Amazon S3, incluindo o endpoint do serviço.
- Você sabe o URL completo que o StorageGRID usará para obter credenciais temporárias do SERVIDOR CAP, incluindo todos os parâmetros de API necessários e opcionais atribuídos à sua conta C2S.
- Você tem um certificado de CA de servidor emitido por uma autoridade de certificação governamental (CA) apropriada. O StorageGRID usa esse certificado para verificar a identidade do SERVIDOR CAP. O certificado de CA do servidor deve usar a codificação PEM.
- Você tem um certificado de cliente emitido por uma autoridade de certificação governamental (CA) apropriada. O StorageGRID usa esse certificado para identificar-se para o servidor CAP. O certificado de cliente deve usar codificação PEM e deve ter acesso à sua conta C2S.
- Você tem uma chave privada codificada PEM para o certificado do cliente.
- Se a chave privada do certificado de cliente for encriptada, tem a frase-passe para descriptá-la.

### Passos


1. Na seção **Autenticação**, selecione **CAP (C2S Access Portal)** na lista suspensa **Authentication Type**.

Os campos de autenticação CAP C2S aparecem.

# 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. Forneça as seguintes informações:

- a. Para **URL de credenciais temporárias**, insira o URL completo que o StorageGRID usará para obter credenciais temporárias do SERVIDOR CAP, incluindo todos os parâmetros de API necessários e opcionais atribuídos à sua conta C2S.
- b. Para **certificado CA do servidor**, selecione **Selecionar novo** e carregue o certificado CA codificado em PEM que o StorageGRID usará para verificar o servidor CAP.
- c. Para **certificado de cliente**, selecione **Selecionar novo** e carregue o certificado codificado PEM que o StorageGRID usará para se identificar no servidor CAP.
- d. Para **chave privada do cliente**, selecione **Select New** e carregue a chave privada codificada pelo PEM para o certificado do cliente.

Se a chave privada for criptografada, o formato tradicional deve ser usado. (O formato criptografado PKCS nº 8 não é suportado.)

- e. Se a chave privada do cliente estiver encriptada, introduza a frase-passe para descriptar a chave privada do cliente. Caso contrário, deixe o campo **frase-passe de chave privada do cliente** em branco.

3. Na seção Verificação do servidor, forneça as seguintes informações:

- a. Para **Validação de certificado**, selecione **usar certificado CA personalizado**.
- b. Selecione **Selecione novo** e carregue o certificado CA codificado em PEM.

4. Selecione **Guardar**.

Quando você salva um pool de storage de nuvem, o StorageGRID faz o seguinte:

- Valida que o intervalo e o endpoint de serviço existem e que eles podem ser alcançados usando as credenciais que você especificou.
- Grava um arquivo de marcador no bucket para identificar o bucket como um Cloud Storage Pool. Nunca remova esse arquivo, que é `x-ntap-sgws-cloud-pool-uuid` chamado .

Se a validação do Cloud Storage Pool falhar, você receberá uma mensagem de erro que explica por que a validação falhou. Por exemplo, um erro pode ser relatado se houver um erro de certificado ou se o intervalo especificado ainda não existir.

## ! 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 as instruções do [Solução de problemas de Cloud Storage Pools](#), resolva o problema e tente salvar o pool de armazenamento em nuvem novamente.

# Azure: Especifique os detalhes de autenticação para um pool de armazenamento em nuvem

Ao criar um pool de storage de nuvem para storage de Blobs do Azure, você deve especificar um nome de conta e uma chave de conta para o contêiner externo que o StorageGRID usará para armazenar objetos.

## O que você vai precisar

- Você inseriu as informações básicas do Cloud Storage Pool e especificou **armazenamento de Blobs do Azure** como tipo de provedor. **Chave compartilhada** aparece no campo **tipo de autenticação**.

### Create Cloud Storage Pool

Display Name	<input type="text" value="Azure Cloud Storage Pool"/>
Provider Type	<input type="text" value="Azure Blob Storage"/>
Bucket or Container	<input type="text" value="my-azure-container"/>

### Service Endpoint

URI	<input type="text" value="https://myaccount.blob.core.windows.net"/>
-----	--

### Authentication

Authentication Type	Shared Key
Account Name	<input type="text"/>
Account Key	<input type="text"/>

### Server Verification

Certificate Validation	<input type="text" value="Use operating system CA certificate"/>
------------------------	--

- Você conhece o URI (Uniform Resource Identifier) usado para acessar o contentor de armazenamento de Blob usado para o Cloud Storage Pool.

- Você sabe o nome da conta de armazenamento e a chave secreta. Você pode usar o portal do Azure para encontrar esses valores.

## Passos

1. Na seção **Service Endpoint**, insira o URI (Uniform Resource Identifier) usado para acessar o contentor de armazenamento de Blob usado para o Cloud Storage Pool.

Especifique o URI em um dos seguintes formatos:

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

Se você não especificar uma porta, por padrão, a porta 443 será usada para URIs HTTPS e a porta 80 será usada para URIs HTTP. \* Exemplo de URI para o contentor de armazenamento Blob do Azure\*  
`https://myaccount.blob.core.windows.net`

2. Na seção **Autenticação**, forneça as seguintes informações:
  - a. Para **Nome da conta**, insira o nome da conta de armazenamento Blob que possui o contentor de serviço externo.
  - b. Para **chave de conta**, insira a chave secreta da conta de armazenamento Blob.



Para endpoints do Azure, você deve usar a autenticação chave compartilhada.

3. Na seção **Verificação do servidor**, selecione qual método deve ser usado para validar o certificado para conexões TLS ao pool de armazenamento em nuvem:

Opção	Descrição
Use o certificado CA do sistema operacional	Use os certificados Grid CA instalados no sistema operacional para proteger conexões.
Use certificado CA personalizado	Use um certificado de CA personalizado. Selecione <b>Selecione novo</b> e carregue o certificado codificado em PEM.
Não verifique o certificado	O certificado usado para a conexão TLS não é verificado.

4. Selecione **Guardar**.

Quando você salva um pool de storage de nuvem, o StorageGRID faz o seguinte:

- Valida que o contentor e o URI existem e que eles podem ser alcançados usando as credenciais que você especificou.
- Grava um arquivo de marcador no contentor para identificá-lo como um Cloud Storage Pool. Nunca remova esse arquivo, que é `x-ntap-sgws-cloud-pool-uuid` chamado .

Se a validação do Cloud Storage Pool falhar, você receberá uma mensagem de erro que explica por que a validação falhou. Por exemplo, um erro pode ser relatado se houver um erro de certificado ou se o contentor especificado ainda não existir.

Consulte as instruções do [Solução de problemas de Cloud Storage Pools](#), resolva o problema e tente salvar o pool de armazenamento em nuvem novamente.

## Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

## Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.