Procedimientos y ejemplos de API

StorageGRID solutions and resources

NetApp
November 21, 2025

Tabla de contenidos

Procedimientos y ejemplos de API

Pruebe y muestre opciones de cifrado de S3 en StorageGRID

Por Aron Klein

StorageGRID y la API de S3 ofrecen varias formas diferentes de cifrar sus datos en reposo. Para obtener más información, consulte "Consulte los métodos de cifrado de StorageGRID".

En esta guía se mostrarán los métodos de cifrado de la API de S3.

Cifrado del servidor (SSE)

SSE permite al cliente almacenar un objeto y cifrarlo con una clave única gestionada por StorageGRID. Cuando se solicita el objeto, la clave almacenada en StorageGRID descifra el objeto.

Ejemplo de SSE

- PONGA un objeto con SSE

```
aws s3api put-object --bucket <bucket>  --key <file> --body "<file>"
--server-side-encryption AES256 --endpoint-url https://s3.example.com
```

- DIRÍJASE al objeto para verificar el cifrado

```
aws s3api head-object --bucket <bucket>  --key <file>   --endpoint-url
https://s3.example.com
```

```
{
    "AcceptRanges": "bytes",
    "LastModified": "2022-05-02T19:03:03+00:00",
    "ContentLength": 47,
    "ETag": "\"82e8bfb872e778a4687a26e6c0b36bc1\"",
    "ContentType": "text/plain",
    "ServerSideEncryption": "AES256",
    "Metadata": {}
}
```

- OBTENGA el objeto

```
aws s3api get-object --bucket <bucket>  --key <file> <file> --endpoint
-url https://s3.example.com
```

Cifrado del servidor con claves proporcionadas por el cliente (SSE-C)

SSE permite al cliente almacenar un objeto y cifrarlo con una clave única proporcionada por el cliente con el objeto. Cuando se solicita el objeto, se debe proporcionar la misma clave para descifrar y devolver el objeto.

Ejemplo de SSE-C.

- Con fines de prueba o demostración, puede crear una clave de cifrado
  - Cree una clave de cifrado

```
openssl enc -aes-128-cbc -pass pass:secret -P`
```

```
salt=E9DBB6603C7B3D2A
key=23832BAC16516152E560F933F261BF03
iv =71E87C0F6EC3C45921C2754BA131A315
```

- Coloque un objeto con la clave generada

```
aws s3api put-object --bucket <bucket> --key <file> --body "file" --sse
-customer-algorithm AES256 --sse-customer-key
23832BAC16516152E560F933F261BF03 --endpoint-url https://s3.example.com
```

- Dirigir el objeto

```
aws s3api head-object --bucket <bucket> --key <file> --sse-customer
-algorithm AES256 --sse-customer-key 23832BAC16516152E560F933F261BF03
--endpoint-url https://s3.example.com
```

```
{
    "AcceptRanges": "bytes",
    "LastModified": "2022-05-02T19:20:02+00:00",
    "ContentLength": 47,
    "ETag": "\"f92ef20ab87e0e13951d9bee862e9f9a\"",
    "ContentType": "binary/octet-stream",
    "Metadata": {},
    "SSECustomerAlgorithm": "AES256",
    "SSECustomerKeyMD5": "rjGuMdjLpPV1eRuotNaPMQ=="
}
```

Si no proporciona la clave de cifrado, recibirá un error "se ha producido un error (404) al llamar a la operación HeadObject: Not found"

- Obtenga el objeto

```
aws s3api get-object --bucket <bucket> --key <file> <file> --sse
-customer-algorithm AES256 --sse-customer-key
23832BAC16516152E560F933F261BF03 --endpoint-url https://s3.example.com
```

Si no proporciona la clave de cifrado, recibirá un error que indica que se ha producido un error (InvalidRequest) al llamar a la operación GetObject: El objeto se ha almacenado utilizando un formulario de cifrado del lado del servidor. Se deben proporcionar los parámetros correctos para recuperar el objeto."

Cifrado del servidor de bloques (SSE-S3)

SSE-S3 permite al cliente definir un comportamiento de cifrado predeterminado para todos los objetos almacenados en un bloque. Los objetos se cifran con una clave única gestionada por StorageGRID. Cuando se solicita el objeto, éste se descifra mediante una clave almacenada en StorageGRID.

Ejemplo de bloque SSE-S3

- Crear un bloque nuevo y establecer una política de cifrado predeterminada
  - Crear nuevo bloque

```
aws s3api create-bucket --bucket <bucket> --region us-east-1
--endpoint-url https://s3.example.com
```

  - Put bucket Encryption

```
aws s3api put-bucket-encryption --bucket <bucket> --server-side
-encryption-configuration '{"Rules":
[{"ApplyServerSideEncryptionByDefault": {"SSEAlgorithm":
"AES256"}}]}' --endpoint-url https://s3.example.com
```

- Coloque un objeto en el bloque

```
aws s3api put-object --bucket <bucket> --key <file> --body "file"
--endpoint-url https://s3.example.com
```

- Dirigir el objeto

```
aws s3api head-object --bucket <bucket> --key <file> --endpoint-url
https://s3.example.com
```

```
{
"AcceptRanges": "bytes",
"LastModified": "2022-05-02T20:16:23+00:00",
"ContentLength": 47,
"ETag": "\"82e8bfb872e778a4687a26e6c0b36bc1\"",
"ContentType": "binary/octet-stream",
"ServerSideEncryption": "AES256",
"Metadata": {}
}
```

- OBTENGA el objeto

```
aws s3api get-object --bucket <bucket>  --key <file> <file> --endpoint
-url https://s3.example.com
```

Pruebe y muestre el bloqueo de objetos de S3 en StorageGRID

Por Aron Klein

El bloqueo de objetos proporciona un modelo WORM para evitar que los objetos se eliminen o se sobrescriban. La implementación de StorageGRID de un bloqueo de objetos es un activo de valor empresarial que se evalúa para ayudar a cumplir los requisitos normativos, respalda la conservación legal y el modo de cumplimiento de normativas para la retención de objetos y las políticas de retención de bloques predeterminadas.

En esta guía se demostrará la API de bloqueo de objetos S3.

Conservación legal

- La retención legal de bloqueo de objetos es un estado de activación/desactivación simple aplicado a un objeto.

```
aws s3api put-object-legal-hold --bucket <bucket> --key <file> --legal
-hold Status=ON --endpoint-url https://s3.company.com
```

- Verifíquelo mediante una OPERACIÓN DE OBTENER.

```
aws s3api get-object-legal-hold --bucket <bucket> --key <file>
--endpoint-url https://s3.company.com
```

```
{
    "LegalHold": {
        "Status": "ON"
    }
}
```

- Desactivar la conservación legal

```
aws s3api put-object-legal-hold --bucket <bucket> --key <file> --legal
-hold Status=OFF --endpoint-url https://s3.company.com
```

- Verifíquelo mediante una OPERACIÓN DE OBTENER.

```
aws s3api get-object-legal-hold --bucket <bucket> --key <file>
--endpoint-url https://s3.company.com
```

```
{
    "LegalHold": {
        "Status": "OFF"
    }
}
```

Modo de cumplimiento de normativas

- La retención de objetos se realiza con una Marca de tiempo de retención hasta.

```
aws s3api put-object-retention --bucket <bucket> --key <file>
--retention '{"Mode":"COMPLIANCE", "RetainUntilDate": "2025-06-
10T16:00:00"}' --endpoint-url https://s3.company.com
```

- Compruebe el estado de retención

```
aws s3api get-object-retention --bucket <bucket> --key <file> --endpoint
-url https://s3.company.com
+
```

```
{
    "Retention": {
        "Mode": "COMPLIANCE",
        "RetainUntilDate": "2025-06-10T16:00:00+00:00"
    }
}
```

Retención predeterminada

- Establezca el período de retención en días y años en lugar de una fecha de retención hasta definida con la api por objeto.

```
aws s3api put-object-lock-configuration --bucket <bucket> --object-lock
-configuration '{"ObjectLockEnabled": "Enabled", "Rule": {
"DefaultRetention": { "Mode": "COMPLIANCE", "Days": 10 }}}' --endpoint
-url https://s3.company.com
```

- Compruebe el estado de retención

```
aws s3api get-object-lock-configuration --bucket <bucket> --endpoint-url
https://s3.company.com
```

```
{
    "ObjectLockConfiguration": {
        "ObjectLockEnabled": "Enabled",
        "Rule": {
            "DefaultRetention": {
                "Mode": "COMPLIANCE",
                "Days": 10
            }
        }
    }
}
```

- Coloque un objeto en el bloque

```
aws s3api put-object --bucket <bucket> --key <file> --body "file"
--endpoint-url https://s3.example.com
```

- La duración de retención establecida en el bloque se convierte en una Marca de tiempo de retención en el objeto.

```
aws s3api get-object-retention --bucket <bucket> --key <file> --endpoint
-url https://s3.company.com
```

```
{
    "Retention": {
        "Mode": "COMPLIANCE",
        "RetainUntilDate": "2022-03-02T15:22:47.202000+00:00"
    }
}
```

Pruebe a eliminar un objeto con una retención definida

El bloqueo de objetos se crea sobre el control de versiones. La retención se define en una versión del objeto. Si se intenta eliminar un objeto con una retención definida y no se especifica ninguna versión, se crea un marcador de borrado como la versión actual del objeto.

- Elimine el objeto con la retención definida

```
aws s3api delete-object --bucket <bucket> --key <file> --endpoint-url
https://s3.example.com
```

- Enumere los objetos del bloque

```
aws s3api list-objects --bucket <bucket> --endpoint-url
https://s3.example.com
```

  - Observe que el objeto no aparece en la lista.
- Enumere las versiones para ver el marcador de borrado y la versión original bloqueada

```
aws s3api list-object-versions --bucket <bucket> --prefix <file>
--endpoint-url https://s3.example.com
```

```
{
    "Versions": [
        {
            "ETag": "\"82e8bfb872e778a4687a26e6c0b36bc1\"",
            "Size": 47,
            "StorageClass": "STANDARD",
            "Key": "file.txt",
            "VersionId":
"RDVDMjYwMTQtQkNDQS0xMUVDLThGOEUtNjQ3NTAwQzAxQTk1",
            "IsLatest": false,
            "LastModified": "2022-04-15T14:46:29.734000+00:00",
            "Owner": {
                "DisplayName": "Tenant01",
                "ID": "566223993089512949 26"
            }
        }
    ],
    "DeleteMarkers": [
        {
            "Owner": {
                "DisplayName": "Tenant01",
                "ID": "566223993089512949 26"
            },
            "Key": "file01.txt",
            "VersionId":
"QjVDQzgzOTAtQ0FGNi0xMUVDLThFMzgtQ0RGMjAwQjk0MjM1",
            "IsLatest": true,
            "LastModified": "2022-05-03T15:35:50.248000+00:00"
        }
    ]
}
```

- Elimine la versión bloqueada del objeto

```
aws s3api delete-object  --bucket <bucket> --key <file> --version-id
"<VersionId>" --endpoint-url https://s3.example.com
```

```
An error occurred (AccessDenied) when calling the DeleteObject
operation: Access Denied
```

Políticas y permisos en StorageGRID

Aquí hay ejemplos de políticas y permisos en StorageGRID S3.

La estructura de una política

En StorageGRID, las políticas de grupo son las mismas que las políticas de servicio S3 del usuario de AWS (IAM).

Las políticas de grupo son necesarias en StorageGRID. Un usuario con claves de acceso S3 pero no asignadas a un grupo de usuarios, o asignado a un grupo sin una política que otorgue algunos permisos, no podrá acceder a ningún dato.

Las políticas de bloque y de grupo comparten la mayoría de los mismos elementos. Las políticas se crean en formato json y se pueden generar mediante "Generador de políticas de AWS"

Todas las políticas definirán el efecto, las acciones y los recursos. Las políticas de bloque también definirán un principal.

El **efecto** será permitir o denegar la solicitud.

El **Principal**

- Solo se aplica a políticas de bloques.
- El principal es la(s) cuenta(s)/usuario(s) que se está otorgando o denegando los permisos.
- Se puede definir como:
  - Un comodín «*»

```
"Principal":"*"
```

```
"Principal":{"AWS":"*"}
```

  - Un ID de inquilino para todos los usuarios de un inquilino (equivalente a la cuenta de AWS).

```
"Principal": { "AWS": "27233906934684427525" }
```

  - Un usuario (local o federado desde dentro del inquilino que reside el bloque (o bien, otro inquilino en el grid)

```
"Principal": { "AWS":
"arn:aws:iam::76233906934699427431:user/tenant1user1" }
```

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
user/tenant2user1" }
```

- Un grupo (local o federado desde dentro del inquilino que reside el bloque (o bien, otro inquilino en la cuadrícula).

```
"Principal": { "AWS":
"arn:aws:iam::76233906934699427431:group/DevOps"  }
```

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
group/Managers"  }
```

La **Acción** es el conjunto de S3 operaciones que se otorgan o se deniegan al usuario(s).

> Para las políticas de grupo, la acción S3:ListBucket Permitido es necesaria para que los usuarios realicen cualquier acción S3.

El **Recurso** es el cubo o cubetas en los que los principales se otorgan o se les niega la capacidad de realizar las acciones. Opcionalmente puede haber una **condición** para cuando la acción de política es válida.

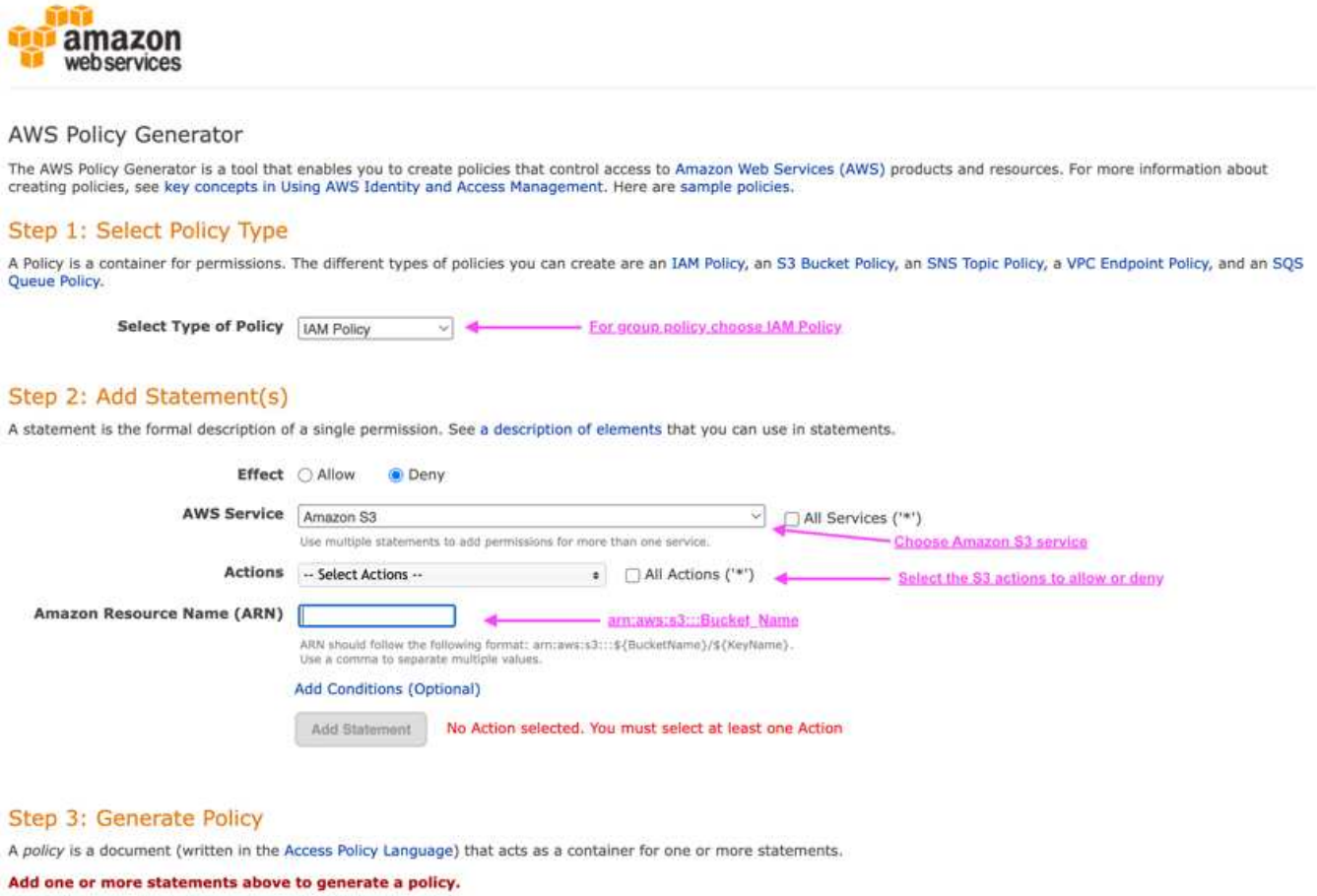
El formato de la política JSON se verá así:

```
{
  "Statement": [
    {
      "Sid": "Custom name for this permission",
      "Effect": "Allow or Deny",
      "Principal": {
        "AWS": [
          "arn:aws:iam::tenant_ID::user/User_Name",
          "arn:aws:iam::tenant_ID::federated-user/User_Name",
          "arn:aws:iam::tenant_ID:group/Group_Name",
          "arn:aws:iam::tenant_ID:federated-group/Group_Name",
          "tenant_ID"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:Other_Action"
      ],
      "Resource": [
        "arn:aws:s3:::Example_Bucket",
        "arn:aws:s3:::Example_Bucket/*"
      ],
    }
  ]
}
```

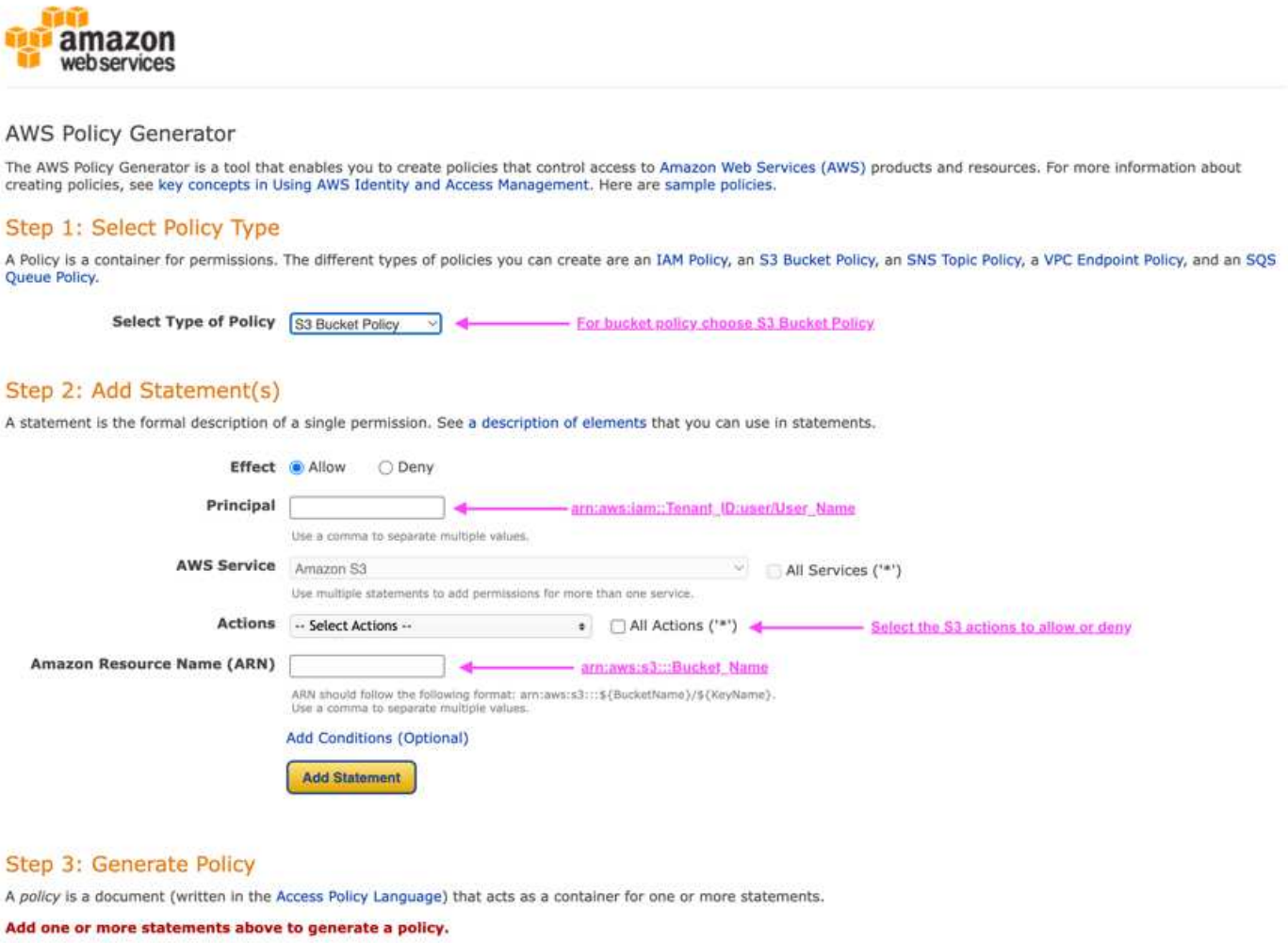
Uso del generador de políticas de AWS

El generador de políticas de AWS es una gran herramienta para ayudar a obtener el código json con el formato correcto y la información que está tratando de implementar.

Para generar los permisos para una directiva de grupo de StorageGRID: * Seleccione la política de IAM para el tipo de política. * Seleccione el botón para el efecto deseado - Permitir o Denegar. Es recomendable iniciar las directivas con los permisos de denegación y, a continuación, agregar los permisos de permiso * en el menú desplegable de acciones. Haga clic en el cuadro junto a tantas acciones de S3 que desee incluir en este permiso o en el cuadro Todas las acciones. * Escriba las rutas de acceso del depósito en el cuadro Nombre del recurso de Amazon (arn). Incluya “arn:aws:S3::” antes del nombre del depósito. «arn:aws:s3:::example_bucket»

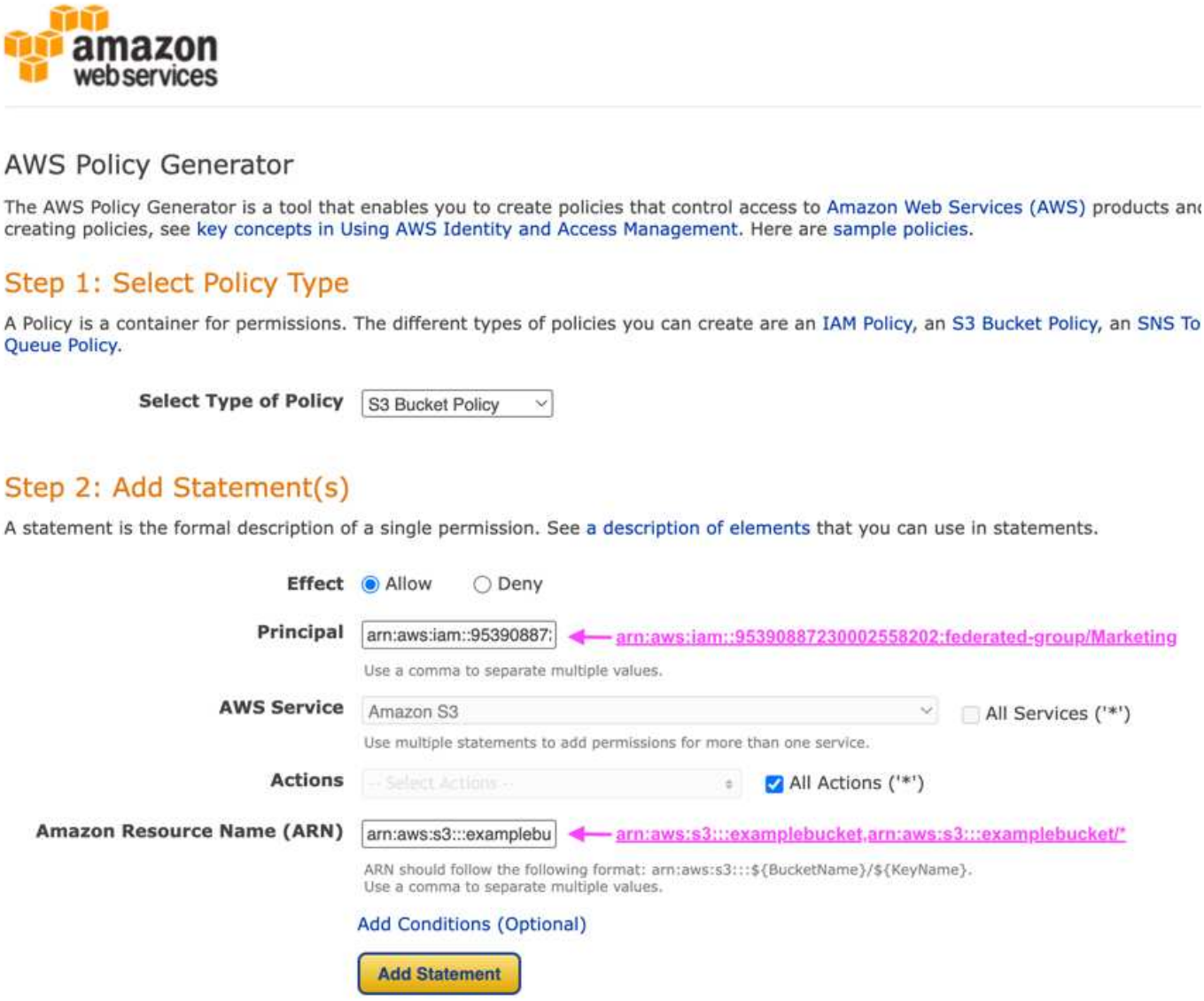


Para generar los permisos para una política de depósito: * Elija la política de bloques de S3 para el tipo de política. * Seleccione el botón para el efecto deseado - Permitir o Denegar. Es una buena práctica iniciar las políticas con los permisos de denegación y, a continuación, agregar los permisos de permiso * Tipo en la información de usuario o grupo para el Principal. * En el menú desplegable de acciones haz clic en el cuadro junto a tantas de las S3 acciones que quieras incluir en este permiso o en el cuadro “Todas las acciones”. * Escriba las rutas de acceso del depósito en el cuadro Nombre del recurso de Amazon (arn). Incluya “arn:aws:S3::” antes del nombre del depósito. «arn:aws:s3:::example_bucket»



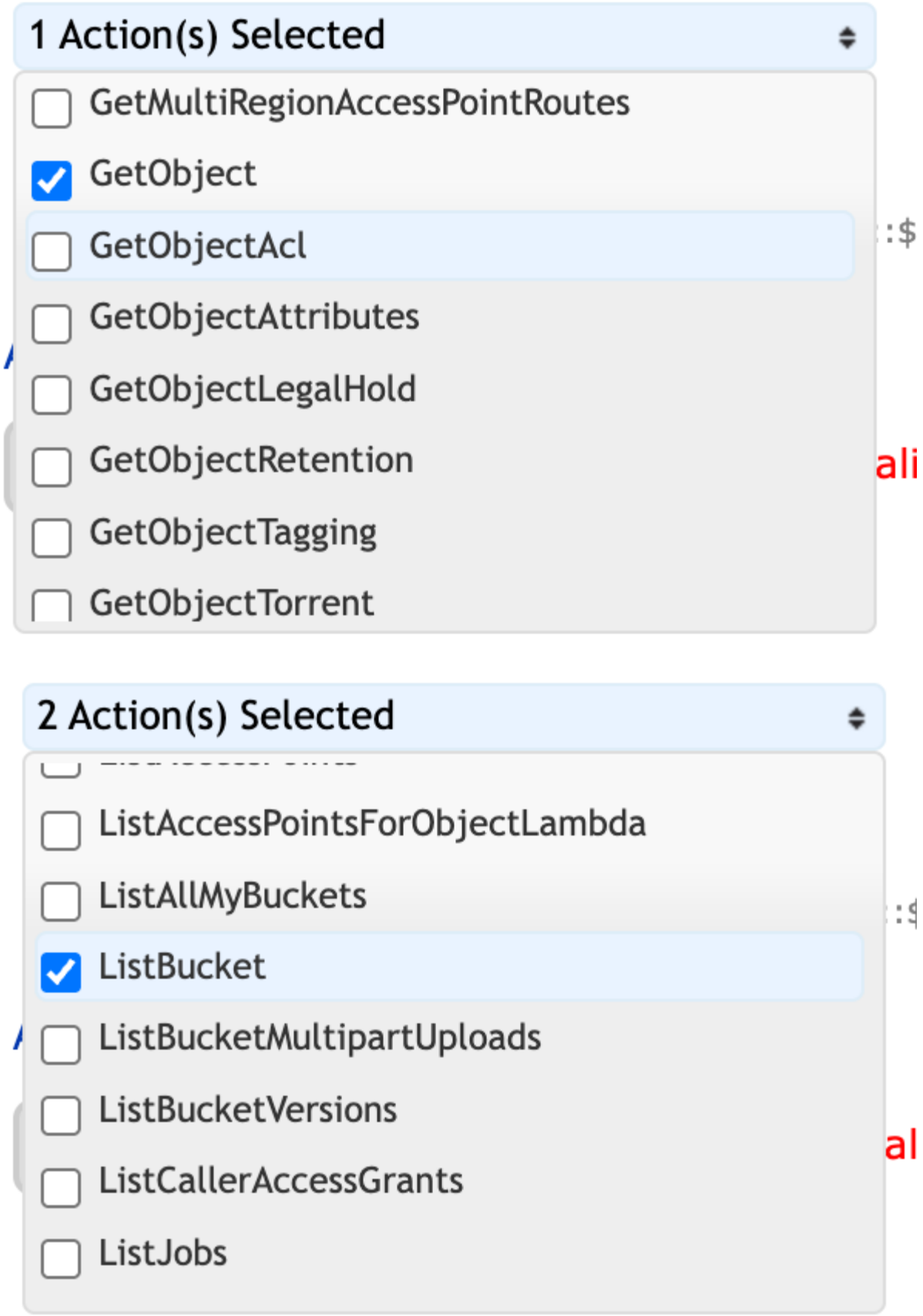
Por ejemplo, si desea generar una política de depósito para permitir que todos los usuarios realicen operaciones GetObject en todos los objetos del depósito, mientras que solo los usuarios que pertenecen al grupo Marketing en la cuenta especificada tienen acceso completo.

- Seleccione S3 Bucket Policy como tipo de política.
- Elija el efecto Permitir
- Introduzca la información del grupo de Marketing: arn:aws:iam::95390887230002558202:federated-group/Marketing
- Haga clic en la casilla de «Todas las acciones»
- Introduzca la información del bloque: arn:aws:S3:::example_bucket,arn:aws:S3:::example_bucket/*

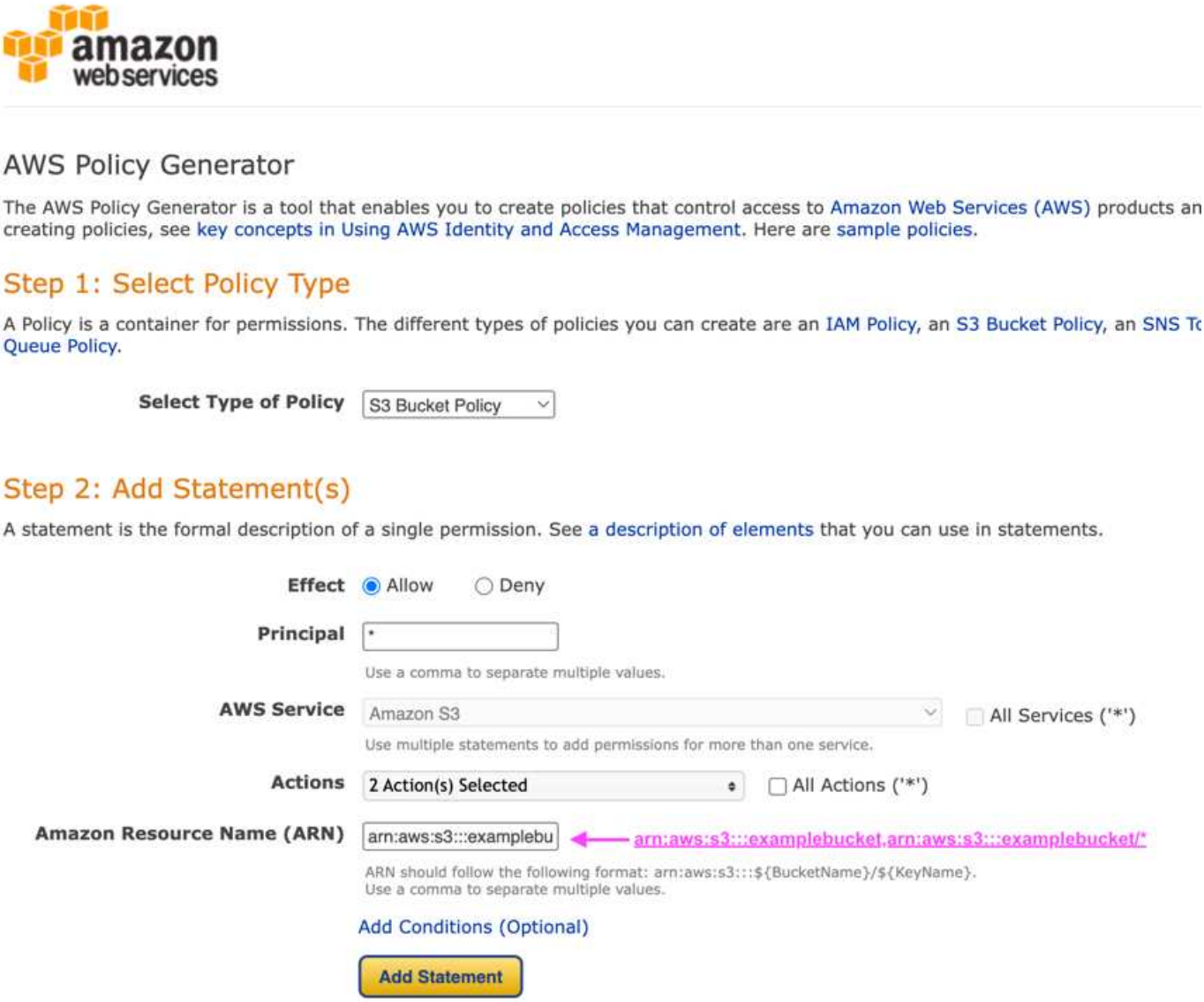


- Haga clic en el botón «Agregar declaración»

- Elija el efecto Permitir
- Introduzca el asterisco * para todos
- Haga clic en el cuadro junto a las acciones GetObject y ListBucket.

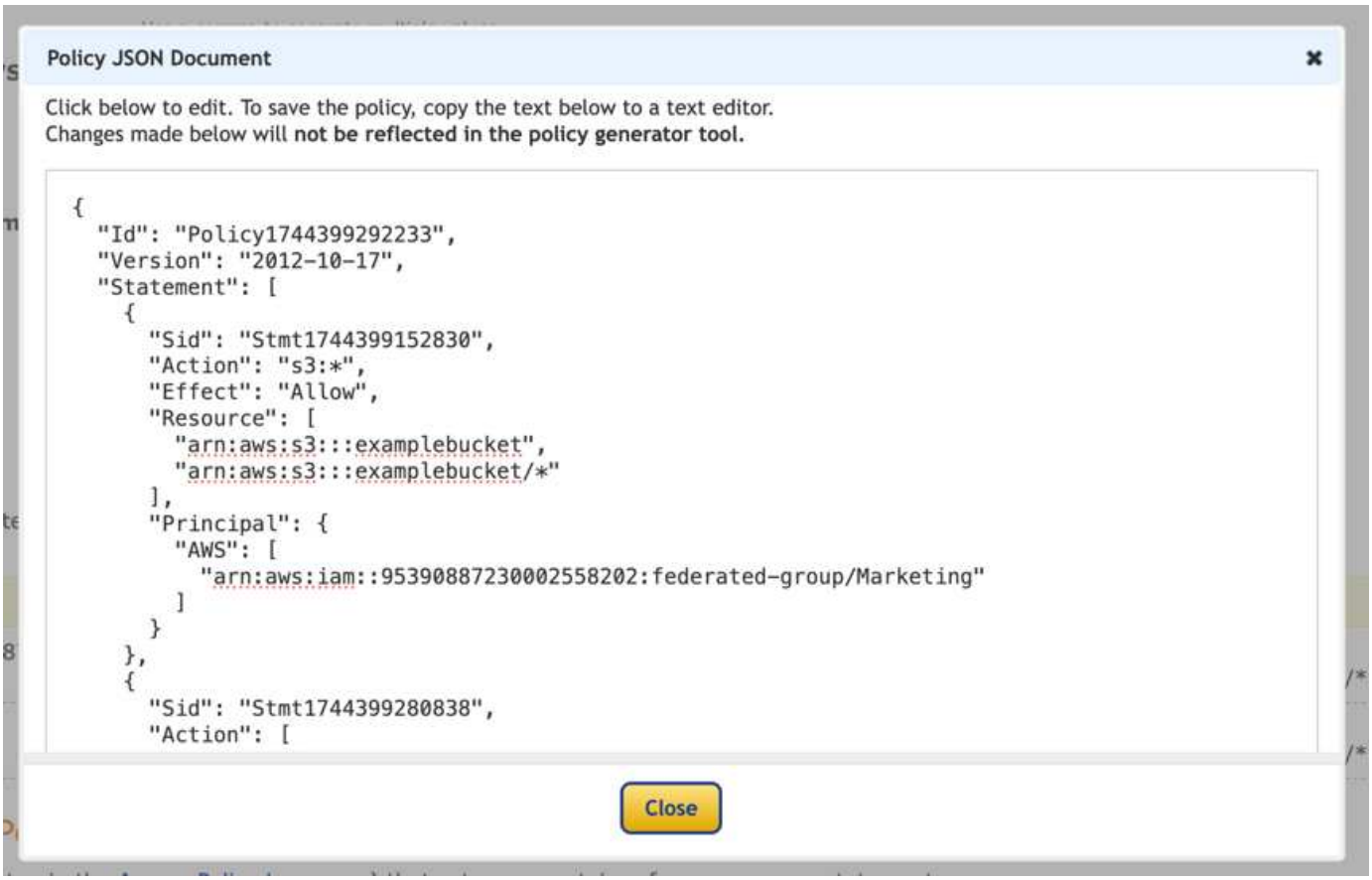


- Introduzca la información del bloque: arn:aws:S3:::example_bucket,arn:aws:S3:::example_bucket/*



- Haga clic en el botón «Agregar declaración»

- Haga clic en el botón “Generar Política” y aparecerá una ventana emergente con su política generada.



- Copie el texto json completo que debería tener el siguiente aspecto:

```
{
  "Id": "Policy1744399292233",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1744399152830",
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::example_bucket",
        "arn:aws:s3:::example_bucket/*"
      ],
      "Principal": {
        "AWS": [
          "arn:aws:iam::95390887230002558202:federated-group/Marketing"
        ]
      }
    },
    {
      "Sid": "Stmt1744399280838",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::example_bucket",
        "arn:aws:s3:::example_bucket/*"
      ],
      "Principal": "*"
    }
  ]
}
```

Este json se puede utilizar tal cual, o puede eliminar las líneas de ID y versión encima de la línea de “Declaración” y puede personalizar el Sid para cada permiso con un título más significativo para cada permiso o también se pueden eliminar.

Por ejemplo:

```
{
  "Statement": [
    {
      "Sid": "MarketingAllowFull",
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::example_bucket",
        "arn:aws:s3:::example_bucket/*"
      ],
      "Principal": {
        "AWS": [
          "arn:aws:iam::95390887230002558202:federated-group/Marketing"
        ]
      }
    },
    {
      "Sid": "EveryoneReadOnly",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::example_bucket",
        "arn:aws:s3:::example_bucket/*"
      ],
      "Principal": "*"
    }
  ]
}
```

Políticas de grupo (IAM)

Acceso a bloque de estilo de directorio de casa

Esta política de grupo sólo permitirá a los usuarios acceder a los objetos del depósito denominado nombre de usuario de los usuarios.

```
{
"Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::home",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::home/?/?/${aws:username}/*"
    }

  ]
}
```

Denegar creación de bloque de bloqueo de objetos

Esta política de grupo restringirá a los usuarios a crear un bloque con el bloqueo de objeto habilitado en el bloque.

> Esta política no se aplica en la interfaz de usuario de StorageGRID, sino que solo se aplica mediante la API de S3.

```
{
    "Statement": [
        {
            "Action": "s3:*",
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Action": [
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutBucketVersioning"
            ],
            "Effect": "Deny",
            "Resource": "arn:aws:s3:::*"
        }
    ]
}
```

Límite de retención de bloqueo de objetos

Esta política de depósito restringirá la duración de la retención de bloqueo de objetos a 10 días o menos

```
{
 "Version":"2012-10-17",
 "Id":"CustSetRetentionLimits",
 "Statement": [
   {
    "Sid":"CustSetRetentionPeriod",
    "Effect":"Deny",
    "Principal":"*",
    "Action": [
      "s3:PutObjectRetention"
    ],
    "Resource":"arn:aws:s3:::testlock-01/*",
    "Condition": {
      "NumericGreaterThan": {
        "s3:object-lock-remaining-retention-days":"10"
      }
    }
   }
  ]
}
```

Restringir a los usuarios la supresión de objetos por versionID

Esta política de grupo restringirá a los usuarios la supresión de objetos versionados por versionID

```
{
    "Statement": [
        {
            "Action": [
                "s3:DeleteObjectVersion"
            ],
            "Effect": "Deny",
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Action": "s3:*",
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::*"
        }
    ]
}
```

Restrinja un grupo a un único subdirectorio (prefijo) con acceso de solo lectura

Esta política permite a los miembros del grupo tener acceso de solo lectura a un subdirectorio (prefijo) dentro de un bloque. El nombre del depósito es «study» y el subdirectorio es «study01».

```
{
    "Statement": [
        {
            "Sid": "AllowUserToSeeBucketListInTheConsole",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::*"
            ]
        },
        {
            "Sid": "AllowRootAndstudyListingOfBucket",
            "Action": [
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3::: study"
```

```
            ],
            "Condition": {
                "StringEquals": {
                    "s3:prefix": [
                        "",
                        "study01/"
                    ],
                    "s3:delimiter": [
                        "/"
                    ]
                }
            }
        },
        {
            "Sid": "AllowListingOfstudy01",
            "Action": [
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::study"
            ],
            "Condition": {
                "StringLike": {
                    "s3:prefix": [
                        "study01/*"
                    ]
                }
            }
        },
        {
            "Sid": "AllowAllS3ActionsInstudy01Folder",
            "Effect": "Allow",
            "Action": [
                "s3:Getobject"
            ],
            "Resource": [
                "arn:aws:s3:::study/study01/*"
            ]
        }
    ]
}
```

Políticas de bloques

Restringir bloque a un solo usuario con acceso de sólo lectura

Esta directiva permite a un solo usuario tener acceso de sólo lectura a un bloque y denys explícitamente acceso a todos los demás usuarios. La agrupación de las declaraciones denegadas en la parte superior de la directiva es una buena práctica para una evaluación más rápida.

```
{
    "Statement": [
        {
            "Sid": "Deny non user1",
            "Effect": "Deny",
            "NotPrincipal": {
                "AWS": "arn:aws:iam::349215141330028336 65:user/user1"
            },
            "Action": [
                "s3:*"
            ],
            "Resource": [
                "arn:aws:s3:::bucket1",
                "arn:aws:s3:::bucket1/*"
            ]
        },
        {
            "Sid": "Allow user1 read access to bucket bucket1",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::349215141330028336 65:user/user1"
            },
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::bucket1",
                "arn:aws:s3:::bucket1/*"
            ]
        }
    ]
}
```

restringe un bloque a algunos usuarios con acceso de solo lectura.

```
{
    "Statement": [
      {
        "Sid": "Deny all S3 actions to employees 002-005",
        "Effect": "deny",
        "Principal": {
          "AWS": [
            "arn:aws:iam::465215141330027038882:user/employee-002",
            "arn:aws:iam::465215141330027038882:user/employee-003",
            "arn:aws:iam::465215141330027038882:user/employee-004",
            "arn:aws:iam::465215141330027038882:user/employee-005"
          ]
        },
        "Action": "*",
        "Resource": [
          "arn:aws:s3:::databucket1",
          "arn:aws:s3:::databucket1/*"
        ]
      },
      {
        "Sid": "Allow read-only access for employees 002-005",
        "Effect": "Allow",
        "Principal": {
          "AWS": [
            "arn:aws:iam::465215141330027038882:user/employee-002",
            "arn:aws:iam::465215141330027038882:user/employee-003",
            "arn:aws:iam::465215141330027038882:user/employee-004",
            "arn:aws:iam::465215141330027038882:user/employee-005"
          ]
        },
        "Action": [
          "s3:GetObject",
          "s3:GetObjectTagging",
          "s3:GetObjectVersion"
        ],
        "Resource": [
          "arn:aws:s3:::databucket1",
          "arn:aws:s3:::databucket1/*"
        ]
      }
    ]
}
```

Restringir las eliminaciones de objetos versionados por el usuario en un depósito

Esta política de depósito restringirá a un usuario (identificado por el ID de usuario «56622399308951294926») de eliminar objetos versionados por versionID

```
{
  "Statement": [
    {
      "Action": [
        "s3:DeleteObjectVersion"
      ],
      "Effect": "Deny",
      "Resource": "arn:aws:s3:::verdeny/*",
      "Principal": {
        "AWS": [
          "56622399308951294926"
        ]
      }
    },
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::verdeny/*",
      "Principal": {
        "AWS": [
          "56622399308951294926"
        ]
      }
    }
  ]
}
```

Ciclo de vida de un bucket en StorageGRID

Puede crear una configuración del ciclo de vida de S3 para controlar cuándo se eliminan objetos específicos del sistema StorageGRID.

¿Qué es una configuración de ciclo de vida?

Una configuración de ciclo de vida es un conjunto de reglas que se aplican a los objetos en bloques de S3 específicos. Cada regla especifica qué objetos se ven afectados y cuándo caducarán dichos objetos (en una fecha específica o después de un número determinado de días).

Cada objeto sigue la configuración de retención de un ciclo de vida de bloques de S3 o una política de ILM. Cuando se configura el ciclo de vida de un bloque de S3, las acciones de caducidad del ciclo de vida anulan la política de ILM de los objetos que coinciden con el filtro de ciclo de vida del bloque. Los objetos que no coinciden con el filtro de ciclo de vida del bloque utilizan la configuración de retención de la política de ILM. Si

un objeto coincide con un filtro de ciclo de vida del bloque y no se especifica ninguna acción de caducidad explícitamente, no se utiliza la configuración de retención de la política de ILM y se implica que las versiones de los objetos se retienen permanentemente.

Como resultado, es posible que se elimine un objeto de la cuadrícula aunque las instrucciones de colocación de una regla de ILM aún se apliquen al objeto. O bien, un objeto podría conservarse en la cuadrícula incluso después de que hayan transcurrido las instrucciones de ubicación de ILM para el objeto.

StorageGRID admite hasta 1,000 reglas de ciclo de vida en una configuración del ciclo de vida. Cada regla puede incluir los siguientes elementos XML:

- Caducidad: Elimine un objeto cuando se alcance una fecha especificada o cuando se alcance un número especificado de días, empezando desde el momento en que se ingirió el objeto.
- NoncurrentVersionExpiration: Elimine un objeto cuando se alcance un número especificado de días, empezando desde el momento en que el objeto se volvió no actual.
- Filtro (prefijo, etiqueta)
- Estado *ID

StorageGRID admite el uso de las siguientes operaciones de bloques para gestionar las configuraciones del ciclo de vida:

- DeleteBucketLifecycle
- GetBucketLifecycleConfiguration
- PutBucketLifecycleConfiguration

Estructura de una política de ciclo de vida

Como primer paso en la creación de una configuración de ciclo de vida, se crea un archivo JSON que incluye una o varias reglas. Por ejemplo, este archivo JSON incluye tres reglas, de la siguiente manera:

1. La regla 1 solo se aplica a los objetos que coinciden con el prefijo category1/ y cuyo valor de clave2 es tag2. El parámetro Expiration especifica que los objetos que coinciden con el filtro caducarán a la medianoche del 22 de agosto de 2020.
2. La regla 2 solo se aplica a los objetos que coinciden con el prefijo category2/. El parámetro Expiración especifica que los objetos que coinciden con el filtro expirarán 100 días después de su ingesta.

   > Las reglas que especifican un número de días son relativas al momento en que se ingirió el objeto. Si la fecha actual supera la fecha de ingesta más el número de días, es posible que algunos objetos se eliminen del bloque en cuanto se aplique la configuración del ciclo de vida.

3. La regla 3 solo se aplica a los objetos que coinciden con el prefijo category3/. El parámetro Expiración especifica que cualquier versión no vigente de los objetos coincidentes caducará 50 días después de que dejen de estar vigentes.

```
{
    "Rules": [
        {
            "ID": "rule1",
            "Filter": {
                "And": {
                    "Prefix": "category1/",
                    "Tags": [
                        {
                            "Key": "key2",
                            "Value": "tag2"
                        }
                    ]
                }
            },
            "Expiration": {
                "Date": "2020-08-22T00:00:00Z"
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule2",
            "Filter": {
                "Prefix": "category2/"
            },
            "Expiration": {
                "Days": 100
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule3",
            "Filter": {
                "Prefix": "category3/"
            },
            "NoncurrentVersionExpiration": {
                "NoncurrentDays": 50
            },
            "Status": "Enabled"
        }
    ]
}
```

Aplicar la configuración del ciclo de vida al bloque

Después de crear el archivo de configuración de ciclo de vida, se aplica a un depósito emitiendo una solicitud PutBucketLifecycleConfiguration.

Esta solicitud aplica la configuración del ciclo de vida en el archivo de ejemplo a los objetos de un depósito denominado `testbucket`.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-
configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

Para validar que una configuración del ciclo de vida se ha aplicado correctamente al bloque, emita una solicitud GetBucketLifecycleConfiguration. Por ejemplo:

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-
configuration
 --bucket testbucket
```

Ejemplo de políticas de ciclo de vida para depósitos estándar (sin versiones)

Eliminar objetos después de 90 días

Caso de uso: Esta política es ideal para gestionar datos relevantes por tiempo limitado, como archivos temporales, registros o datos de procesamiento intermedio. Beneficio: Reduce los costos de almacenamiento y garantiza que el bucket esté ordenado.

```
{
    "Rules": [
      {
        "ID": "Delete after 90 day rule",
        "Filter": {},
        "Status": "Enabled",
          "Expiration": {
              "Days": 90
        }
      }
    ]
}
```

Ejemplo de políticas de ciclo de vida para depósitos versionados

Eliminar versiones no actuales después de 10 días

Caso de uso: Esta política ayuda a gestionar el almacenamiento de objetos con versiones no actuales, que pueden acumularse con el tiempo y consumir un espacio considerable. Beneficio: Optimiza el uso del

almacenamiento conservando solo la versión más reciente.

```
{
    "Rules": [
            {
        "ID": "NoncurrentVersionExpiration 10 day rule",
        "Filter": {},
        "Status": "Enabled",
          "NoncurrentVersionExpiration": {
              "NoncurrentDays": 10
        }
    }
    ]
}
```

Mantener 5 versiones no actuales

Caso de uso: útil cuando desea conservar una cantidad limitada de versiones anteriores para fines de recuperación o auditoría. Beneficio: conserve suficientes versiones no actuales para garantizar un historial y puntos de recuperación suficientes.

```
{
    "Rules": [
      {
        "ID": "NewerNoncurrentVersions 5 version rule",
        "Filter": {},
        "Status": "Enabled",
        "NoncurrentVersionExpiration": {
            "NewerNoncurrentVersions": 5
        }
    }
    ]
}
```

Eliminar marcadores de eliminación cuando no existan otras versiones

Caso de uso: Esta política ayuda a gestionar los marcadores de eliminación que quedan después de eliminar todas las versiones no actuales, los cuales pueden acumularse con el tiempo. Beneficio: Reduce el desorden innecesario.

```
{
    "Rules": [
    {
        "ID": "Delete marker cleanup rule",
        "Filter": {},
        "Status": "Enabled",
        "Expiration": {
        "ExpiredObjectDeleteMarker": true
        }
    }
    ]
}
```

Eliminar versiones actuales después de 30 días, eliminar versiones no actuales después de 60 días y eliminar los marcadores de eliminación creados por la eliminación de la versión actual una vez que no existan otras versiones.

Caso de uso: Proporcionar un ciclo de vida completo para las versiones actuales y no actuales, incluyendo los marcadores de eliminación. Beneficio: Reducir los costos de almacenamiento y garantizar que el depósito esté ordenado, conservando suficientes puntos de recuperación e historial.

```
{
  "Rules": [
    {
      "ID": "Delete current version",
      "Filter": {},
      "Status": "Enabled",
      "Expiration": {
        "Days": 30
      }
    },
    {
      "ID": "noncurrent version retention",
      "Filter": {},
      "Status": "Enabled",
      "NoncurrentVersionExpiration": {
        "NoncurrentDays": 60
      }
    },
    {
      "ID": "Markers",
      "Filter": {},
      "Status": "Enabled",
      "Expiration": {
        "ExpiredObjectDeleteMarker": true
      }
    }
  ]
}
```

eliminar marcadores de eliminación que no tengan otras versiones, conservar 4 versiones no actuales y al menos 30 días de historial para objetos con el "prefijo account_" y mantener 2 versiones y al menos 10 días de historial para todas las demás versiones de objetos.

Caso de uso: Proporcionar reglas únicas para objetos específicos, junto con otros objetos, para gestionar el ciclo de vida completo de las versiones actuales y futuras, incluyendo los marcadores de eliminación. Beneficio: Reducir los costos de almacenamiento y garantizar que el depósito esté ordenado, conservando suficientes puntos de recuperación e historial para satisfacer diversas necesidades del cliente.

```
{
  "Rules": [
    {
      "ID": "Markers",
      "Filter": {},
      "Status": "Enabled",
      "Expiration": {
        "ExpiredObjectDeleteMarker": true
      }
    },
    {
      "ID": "accounts version retention",
      "Filter": {"Prefix":"account_"},
      "Status": "Enabled",
      "NoncurrentVersionExpiration": {
        "NewerNoncurrentVersions": 4,
        "NoncurrentDays": 30
      }
    },
    {
      "ID": "noncurrent version retention",
      "Filter": {},
      "Status": "Enabled",
      "NoncurrentVersionExpiration": {
        "NewerNoncurrentVersions": 2,
        "NoncurrentDays": 10
      }
    }
  ]
}
```

Conclusión

- Revise y actualice periódicamente las políticas del ciclo de vida y alinéelas con los objetivos de ILM y gestión de datos.
- Pruebe las políticas en un entorno o contenedor que no sea de producción antes de aplicarlas ampliamente para garantizar que funcionen según lo previsto
- Utilice identificaciones descriptivas para las reglas para que sea más intuitivo, ya que la estructura lógica puede volverse compleja.
- Supervise el impacto de estas políticas de ciclo de vida del depósito en el uso y el rendimiento del almacenamiento para realizar los ajustes necesarios.

Información de copyright

Información de la marca comercial