Gestisci le policy di accesso

StorageGRID software

NetApp
July 23, 2026

Sommario

Gestisci le policy di accesso

Come StorageGRID utilizza le policy AWS per controllare l'accesso ai bucket e agli oggetti S3

StorageGRID utilizza il linguaggio delle policy di Amazon Web Services (AWS) per consentire ai tenant S3 di controllare l'accesso ai bucket e agli oggetti all'interno di tali bucket. Il sistema StorageGRID implementa un sottoinsieme del linguaggio delle policy dell'API REST S3. Le policy di accesso per l'API S3 sono scritte in JSON.

Panoramica delle policy di accesso

StorageGRID supporta tre tipi di politiche di accesso:

- **Politiche di bucket**, gestite tramite le operazioni API S3 GetBucketPolicy, PutBucketPolicy e DeleteBucketPolicy oppure tramite il Tenant Manager o le API Tenant Management. Le politiche di bucket sono associate ai bucket, quindi sono configurate per controllare l'accesso degli utenti nell'account proprietario del bucket o in altri account al bucket e agli oggetti in esso contenuti. Una politica di bucket si applica a un solo bucket e, eventualmente, a più gruppi.
- Le **policy di gruppo** vengono configurate tramite Tenant Manager o Tenant Management API. Le policy di gruppo sono associate a un gruppo nell'account e sono configurate per consentire a quel gruppo di accedere a risorse specifiche di proprietà di quell'account. Una policy di gruppo si applica a un solo gruppo e, eventualmente, a più bucket.
- Le **politiche di sessione** sono incluse come parte della richiesta AssumeRole. Le politiche di sessione si applicano solo alla sessione in corso e definiscono ulteriormente le autorizzazioni che l'utente possiede, in aggiunta a quelle concesse dalle politiche di gruppo e di bucket.

> Non c'è alcuna differenza di priorità tra le policy di gruppo, di bucket e di sessione.

Le policy di bucket e di gruppo di StorageGRID seguono una grammatica specifica definita da Amazon. All'interno di ciascuna policy c'è un array di istruzioni della policy, e ogni istruzione contiene i seguenti elementi:

- ID della dichiarazione (Sid) (facoltativo)
- Effetto
- Principale/NotPrincipal
- Risorsa/NotResource
- Azione/NotAction
- Condizione (facoltativa)

Le dichiarazioni di policy sono costruite utilizzando questa struttura per specificare le autorizzazioni: Concedi <Effect> per consentire/negare <Principal> di eseguire <Action> su <Resource> quando <Condition> si applica.

Ciascun elemento della policy viene utilizzato per una funzione specifica:

Elemento	Descrizione
Sid	L'elemento Sid è facoltativo. Il Sid ha il solo scopo di fornire una descrizione all'utente. Viene memorizzato ma non interpretato dal sistema StorageGRID.
Effetto	Utilizza l'elemento Effect per stabilire se le operazioni specificate sono consentite o negate. Devi identificare le operazioni che consenti (o neghi) su bucket o oggetti utilizzando le parole chiave supportate dall'elemento Action.
Principale/NotPrincipal	Puoi consentire a utenti, gruppi e account di accedere a risorse specifiche ed eseguire azioni specifiche. Se la richiesta non include una firma S3, l'accesso anonimo è consentito specificando il carattere jolly (*) come principal. Per impostazione predefinita, solo l'account root ha accesso alle risorse di proprietà dell'account. Nelle policy di un bucket è sufficiente specificare l'elemento Principal. Per le policy di gruppo, il gruppo a cui è associata la policy è l'elemento Principal implicito.
Risorsa/NotResource	L'elemento Risorsa identifica bucket e oggetti. Puoi consentire o negare le autorizzazioni a bucket e oggetti utilizzando l'Amazon Resource Name (ARN) per identificare la risorsa.
Azione/NotAction	Gli elementi Azione ed Effetto sono le due componenti delle autorizzazioni. Quando un gruppo richiede una risorsa, l'accesso a tale risorsa può essere concesso o negato. L'accesso viene negato a meno che tu non assegni specificamente delle autorizzazioni, ma puoi usare una negazione esplicita per annullare un'autorizzazione concessa da un'altra policy.
Condizione	L'elemento Condizione è facoltativo. Le condizioni consentono di creare espressioni per determinare quando applicare una policy.

Nell'elemento Action, puoi usare il carattere jolly (*) per specificare tutte le operazioni o un sottoinsieme di operazioni. Ad esempio, questa Action corrisponde a permessi come s3:GetObject, s3:PutObject e s3:DeleteObject.

```
s3:*Object
```

Nell'elemento Resource, puoi usare i caratteri jolly (*) e (?). Mentre l'asterisco (*) corrisponde a 0 o più caratteri, il punto interrogativo (?) corrisponde a qualsiasi singolo carattere.

Nell'elemento Principal, i caratteri jolly non sono supportati, tranne che per impostare l'accesso anonimo, che concede l'autorizzazione a tutti. Ad esempio, imposti il carattere jolly (*) come valore Principal.

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

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

Nell'esempio seguente, l'istruzione utilizza gli elementi Effect, Principal, Action e Resource. Questo esempio mostra un'istruzione completa di policy per bucket che utilizza l'effetto "Allow" per concedere ai Principal, al gruppo admin `federated-group/admin` e al gruppo finance `federated-group/finance`, le autorizzazioni per eseguire l'azione `s3:ListBucket` sul bucket denominato `mybucket` e l'azione `s3:GetObject` su tutti gli oggetti all'interno di tale bucket.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::mybucket",
        "arn:aws:s3:::mybucket/*"
      ]
    }
  ]
}
```

La policy del bucket ha un limite di dimensione di 20.480 byte e la policy di gruppo ha un limite di dimensione di 5.120 byte.

Coerenza delle policy

Per impostazione predefinita, tutti gli aggiornamenti che apporti alle policy di gruppo sono eventualmente coerenti. Quando una policy di gruppo diventa coerente, le modifiche possono richiedere fino a 15 minuti aggiuntivi per avere effetto, a causa della memorizzazione nella cache delle policy. Per impostazione predefinita, tutti gli aggiornamenti che apporti alle policy dei bucket sono fortemente coerenti.

Se necessario, puoi modificare le garanzie di coerenza per gli aggiornamenti delle policy di bucket. Ad esempio, potresti voler rendere disponibile una modifica a una policy di bucket durante un fuori servizio del sito.

In questo caso, puoi impostare l' `Consistency-Control`intestazione nella richiesta PutBucketPolicy, oppure puoi usare la richiesta PUT Bucket consistency. Quando una policy del bucket diventa coerente, le modifiche possono richiedere fino a 8 secondi aggiuntivi per avere effetto, a causa della memorizzazione nella cache

delle policy.

> Se imposti la coerenza su un valore diverso per aggirare una situazione temporanea, assicurati di riportare l'impostazione a livello di bucket al suo valore originale quando hai finito. Altrimenti, tutte le future richieste di bucket useranno l'impostazione modificata.

Che cos'è la policy di sessione?

Una policy di sessione è una policy di accesso che limita temporaneamente le autorizzazioni disponibili durante una sessione specifica, ad esempio quando un utente assume l'appartenenza a un gruppo. Una policy di sessione può consentire solo un sottoinsieme di autorizzazioni e non può concederne di aggiuntive. Il gruppo stesso potrebbe avere autorizzazioni più ampie.

Usa ARN nelle dichiarazioni di policy

Nelle dichiarazioni delle policy, l'ARN viene utilizzato negli elementi Principal e Resource.

- Utilizza questa sintassi per specificare l'ARN della risorsa S3:

```
arn:aws:s3:::bucket-name
arn:aws:s3:::bucket-name/object_key
```

- Usa questa sintassi per specificare l'ARN della risorsa di identità (utenti e gruppi):

```
arn:aws:iam::account_id:root
arn:aws:iam::account_id:user/user_name
arn:aws:iam::account_id:group/group_name
arn:aws:iam::account_id:federated-user/user_name
arn:aws:iam::account_id:federated-group/group_name
```

${post_edited_translations.segment}

- Puoi usare l'asterisco (*) come carattere jolly per trovare zero o più caratteri all'interno della chiave dell'oggetto.
- I caratteri internazionali, che possono essere specificati nella chiave dell'oggetto, devono essere codificati utilizzando JSON UTF-8 o le sequenze di escape JSON \u. La codifica percentuale non è supportata.

  "Sintassi URN RFC 2141"

  Il corpo della richiesta HTTP per l'operazione PutBucketPolicy deve essere codificato con charset=UTF-8.

Specifica le risorse in una policy

Nelle dichiarazioni di policy, puoi usare l'elemento Resource per specificare il bucket o l'oggetto per cui sono consentite o negate le autorizzazioni.

- Ogni dichiarazione di policy richiede un elemento Resource. In una policy, le risorse sono indicate dall'elemento `Resource`, oppure, in alternativa, `NotResource` per l'esclusione.

- Specifichi le risorse con un ARN di risorsa S3. Per esempio:

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- Puoi anche usare variabili di policy all'interno della chiave dell'oggetto. Ad esempio:

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- Il valore della risorsa può specificare un bucket che non esiste ancora quando viene creata una policy di gruppo.

Specifica i principal in una policy

Usa l'elemento Principal per identificare l'utente, il gruppo o l'account tenant a cui è consentito/negato l'accesso alla risorsa dalla dichiarazione di policy.

- Ogni dichiarazione di policy in una policy a livello di bucket deve includere un elemento Principal. Le dichiarazioni di policy in una policy di gruppo non necessitano dell'elemento Principal perché il gruppo è considerato il principal.
- In una policy, i principal sono indicati dall'elemento "Principal" o, in alternativa, "NotPrincipal" per l'esclusione.
- Le identità basate sull'account devono essere specificate utilizzando un ID o un ARN:

```
"Principal": { "AWS": "account_id"}
"Principal": { "AWS": "identity_arn" }
```

- Questo esempio utilizza l'ID account tenant 27233906934684427525, che include l'account root e tutti gli utenti dell'account:

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

- Puoi specificare solo l'account root:

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- Puoi specificare un utente federato specifico ("Alex"):

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

- Puoi specificare un gruppo federato specifico ("Managers"):

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

- Puoi specificare un principal anonimo:

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

- Per evitare ambiguità, puoi usare l'UUID dell'utente invece del nome utente:

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-
eb6b9e546013
```

  Ad esempio, supponi che Alex lasci l'organizzazione e il nome utente `Alex` venga eliminato. Se un nuovo Alex entra nell'organizzazione e gli viene assegnato lo stesso `Alex` nome utente, il nuovo utente potrebbe inavvertitamente ereditare le autorizzazioni concesse all'utente originale.

- Il valore principale può specificare un nome di gruppo/utente che non esiste ancora quando viene creata una policy del bucket.

Specifica le autorizzazioni in una policy

In una policy, l'elemento Action viene utilizzato per consentire/negare le autorizzazioni a una risorsa. Esiste un insieme di autorizzazioni che puoi specificare in una policy, indicate dall'elemento "Action" o, in alternativa, da "NotAction" per l'esclusione. Ciascuno di questi elementi corrisponde a specifiche operazioni dell'API REST di S3.

La tabella elenca le autorizzazioni applicabili ai bucket e le autorizzazioni applicabili agli oggetti.

> Amazon S3 ora utilizza l'autorizzazione s3:PutReplicationConfiguration sia per le azioni PutBucketReplication e DeleteBucketReplication. StorageGRID utilizza autorizzazioni separate per ciascuna azione, in linea con le specifiche originali di Amazon S3.

> Un'eliminazione viene eseguita quando usi un'operazione di inserimento per sovrascrivere un valore esistente.

Autorizzazioni applicabili ai bucket

Autorizzazioni	Operazioni API REST S3	Personalizzato per StorageGRID
s3:CreateBucket	CreateBucket	Sì. **Nota**: Da utilizzare solo nelle group policy.

Autorizzazioni	Operazioni API REST S3	Personalizzato per StorageGRID
s3:DeleteBucket	DeleteBucket	
s3:DeleteBucketMetadataNotification	ELIMINA la configurazione della notifica dei metadati del bucket	Sì
s3:DeleteBucketPolicy	DeleteBucketPolicy	
s3:DeleteReplicationConfiguration	DeleteBucketReplication	Sì, autorizzazioni separate per PUT e DELETE
s3:GetBucketAcl	GetBucketAcl	
s3:GetBucketCompliance	GET Bucket compliance (obsoleto)	Sì
s3:GetBucketConsistency	Coerenza GET Bucket	Sì
s3:GetBucketCORS	GetBucketCors	
s3:GetEncryptionConfiguration	GetBucketEncryption	
s3:GetBucketLastAccessTime	Ora dell'ultimo accesso GET Bucket	Sì
s3:GetBucketLocation	GetBucketLocation	
s3:GetBucketMetadataNotification	GET Configurazione della notifica dei metadati del bucket	Sì
s3:GetBucketNotification	GetBucketNotificationConfiguration	
s3:GetBucketObjectLockConfiguration	GetObjectLockConfiguration	
s3:GetBucketPolicy	GetBucketPolicy	
s3:GetBucketTagging	GetBucketTagging	
s3:GetBucketVersioning	GetBucketVersioning	
s3:GetLifecycleConfiguration	GetBucketLifecycleConfiguration	
s3:GetReplicationConfiguration	GetBucketReplication	

Autorizzazioni	Operazioni API REST S3	Personalizzato per StorageGRID
s3:ListAllMyBuckets	• ListBuckets • Ottieni l'utilizzo dello storage	Sì, per GET Storage Usage. **Nota**: Da utilizzare solo nelle group policy.
s3:ListBucket	• ListObjects • HeadBucket • RestoreObject	
s3:ListBucketMultipartUploads	• ListMultipartUploads • RestoreObject	
s3:ListBucketVersions	GET Bucket versions	
s3:PutBucketCompliance	PUT Bucket compliance (obsoleto)	Sì
s3:PutBucketConsistency	Coerenza PUT Bucket	Sì
s3:PutBucketCORS	• DeleteBucketCors† • PutBucketCors	
s3:PutEncryptionConfiguration	• DeleteBucketEncryption • PutBucketEncryption	
s3:PutBucketLastAccessTime	Ora dell'ultimo accesso PUT Bucket	Sì
s3:PutBucketMetadataNotification	Configurazione della notifica dei metadati del bucket PUT	Sì
s3:PutBucketNotification	PutBucketNotificationConfiguration	
s3:PutBucketObjectLockConfiguration	• CreateBucket con l' `x-amz-bucket-object-lock-enabled: true`intestazione della richiesta (richiede anche l'autorizzazione s3:CreateBucket) • PutObjectLockConfiguration	
s3:PutBucketPolicy	PutBucketPolicy	

Autorizzazioni	Operazioni API REST S3	Personalizzato per StorageGRID
s3:PutBucketTagging	• DeleteBucketTagging† • PutBucketTagging	
s3:PutBucketVersioning	PutBucketVersioning	
s3:PutLifecycleConfiguration	• DeleteBucketLifecycle† • PutBucketLifecycleConfiguration	
s3:PutReplicationConfiguration	PutBucketReplication	Sì, autorizzazioni separate per PUT e DELETE

${post_edited_translations.segment}

Autorizzazioni	Operazioni API REST S3	Personalizzato per StorageGRID
s3:AbortMultipartUpload	• AbortMultipartUpload • RestoreObject	
s3:BypassGovernanceRetention	• DeleteObject • DeleteObjects • PutObjectRetention	
s3:DeleteObject	• DeleteObject • DeleteObjects • RestoreObject	
s3:DeleteObjectTagging	DeleteObjectTagging	
s3:DeleteObjectVersionTagging	DeleteObjectTagging (una versione specifica dell'oggetto)	
s3:DeleteObjectVersion	DeleteObject (una versione specifica dell'oggetto)	
s3:GetObject	• GetObject • HeadObject • RestoreObject • SelectObjectContent	

Autorizzazioni	Operazioni API REST S3	Personalizzato per StorageGRID
s3:GetObjectAcl	GetObjectAcl	
s3:GetObjectLegalHold	GetObjectLegalHold	
s3:GetObjectRetention	GetObjectRetention	
s3:GetObjectTagging	GetObjectTagging	
s3:GetObjectVersionTagging	GetObjectTagging (una versione specifica dell'oggetto)	
s3:GetObjectVersion	GetObject (una versione specifica dell'oggetto)	
s3:ListMultipartUploadParts	ListParts, RestoreObject	
s3:PutObject	• PutObject • CopyObject • RestoreObject • CreateMultipartUpload • CompleteMultipartUpload • UploadPart • UploadPartCopy	
s3:PutObjectLegalHold	PutObjectLegalHold	
s3:PutObjectRetention	PutObjectRetention	
s3:PutObjectTagging	PutObjectTagging	
s3:PutObjectVersionTagging	PutObjectTagging (una versione specifica dell'oggetto)	
s3:PutOverwriteObject	• PutObject • CopyObject • PutObjectTagging • DeleteObjectTagging • CompleteMultipartUpload	Sì
s3:RestoreObject	RestoreObject	

Utilizza il permesso PutOverwriteObject

L'autorizzazione s3:PutOverwriteObject è un'autorizzazione StorageGRID personalizzata che si applica alle operazioni che creano o aggiornano oggetti. L'impostazione di questa autorizzazione determina se il client può sovrascrivere i dati di un oggetto, i metadati definiti dall'utente o il tagging degli oggetti S3.

Le possibili impostazioni per questa autorizzazione includono:

- **Consenti**: Il client può sovrascrivere un oggetto. Questa è l'impostazione predefinita.
- **Nega**: Il client non può sovrascrivere un oggetto. Quando impostato su Nega, il PutOverwriteObject permission funziona come segue:
  - ${post_edited_translations.segment}
    - I dati dell'oggetto, i metadati definiti dall'utente o i tag degli oggetti S3 non possono essere sovrascritti.
    - Tutte le operazioni di acquisizione in corso vengono annullate e viene restituito un errore.
    - Se il versioning S3 è abilitato, l'impostazione Deny impedisce alle operazioni PutObjectTagging o DeleteObjectTagging di modificare il TagSet per un oggetto e le sue versioni non correnti.
  - Se non viene trovato un oggetto esistente, questa autorizzazione non ha effetto.
- Quando questa autorizzazione non è presente, l'effetto è lo stesso di quando è impostata l'opzione "Consenti".

> Se la policy S3 corrente consente la sovrascrittura e l'autorizzazione PutOverwriteObject è impostata su Nega, il client non può sovrascrivere i dati di un oggetto, i metadati definiti dall'utente o il tagging dell'oggetto. Inoltre, se la casella di controllo **Impedisci modifica client** è selezionata (**Configurazione** > **Impostazioni di sicurezza** > **Rete e oggetti**), tale impostazione prevale sull'impostazione dell'autorizzazione PutOverwriteObject.

${post_edited_translations.segment}

Le condizioni definiscono quando una policy sarà in vigore. Le condizioni sono costituite da operatori e coppie chiave-valore.

Le condizioni utilizzano coppie chiave-valore per la valutazione. Un elemento Condition può contenere più condizioni e ogni condizione può contenere più coppie chiave-valore. Il blocco condition utilizza il seguente formato:

```
Condition: {
     condition_type: {
          condition_key: condition_values
```

Nell'esempio seguente, la condizione IpAddress utilizza la chiave condizione SourceIp.

```
"Condition": {
    "IpAddress": {
      "aws:SourceIp": "54.240.143.0/24"
        ...
},
        ...
```

Operatori di condizione supportati

Gli operatori condizionali sono classificati come segue:

- Stringa
- ${post_edited_translations.segment}
- Booleano
- indirizzo IP
- ${post_edited_translations.segment}

Operatori di condizione	Descrizione
StringEquals	${post_edited_translations.segment}
StringNotEquals	${post_edited_translations.segment}
StringEqualsIgnoreCase	Confronta una chiave con un valore stringa in base alla corrispondenza esatta (ignora la distinzione tra maiuscole e minuscole).
StringNotEqualsIgnoreCase	${post_edited_translations.segment}
StringLike	Confronta una chiave con un valore stringa in base alla corrispondenza esatta (sensibile alle maiuscole/minuscole). Può includere i caratteri jolly * e ?.
StringNotLike	Confronta una chiave con un valore stringa in base alla corrispondenza negata (case sensitive). Può includere i caratteri jolly * e ?.
NumericEquals	${post_edited_translations.segment}
NumericNotEquals	${post_edited_translations.segment}
NumericGreaterThan	Confronta una chiave con un valore numerico in base alla corrispondenza "maggiore di".
NumericGreaterThanEquals	Confronta una chiave con un valore numerico in base alla corrispondenza "maggiore o uguale a".

Operatori di condizione	Descrizione
NumericLessThan	Confronta una chiave con un valore numerico in base alla corrispondenza "minore di".
NumericLessThanEquals	Confronta una chiave con un valore numerico in base alla corrispondenza "minore o uguale".
${post_edited_translations.segment}	${post_edited_translations.segment}
IpAddress	${post_edited_translations.segment}
NotIpAddress	Confronta una chiave con un indirizzo IP o un intervallo di indirizzi IP in base alla corrispondenza negata.
Null	${post_edited_translations.segment}
IfExists	Aggiunto in coda a qualsiasi operatore di condizione, eccetto la condizione Null, per verificare l'assenza di tale chiave di condizione. Restituisce TRUE se la chiave di condizione non è presente.

${post_edited_translations.segment}

${post_edited_translations.segment}	Azioni	Descrizione
aws:SourceIp	${post_edited_translations.segment}	Verrà confrontato con l'indirizzo IP da cui è stata inviata la richiesta. Può essere utilizzato per operazioni su bucket o oggetti. **Nota:** Se la richiesta S3 è stata inviata tramite il servizio Load Balancer sui nodi Admin e Gateway, questa verrà confrontata con l'indirizzo IP a monte del servizio Load Balancer. **Nota**: se utilizzi un bilanciatore di carico non trasparente di terze parti, questo verrà confrontato con l'indirizzo IP di tale bilanciatore di carico. Qualsiasi header `X-Forwarded-For` verrà ignorato perché non è possibile verificarne la validità.
${post_edited_translations.segment}	${post_edited_translations.segment}	Verrà confrontato con il nome utente del mittente da cui è stata inviata la richiesta. Può essere utilizzato per operazioni su bucket o oggetti.

${post_edited_translations.segment}	Azioni	Descrizione
${post_edited_translations.segment}	s3:ListBucket e autorizzazioni s3:ListBucketVersions	Verrà confrontato con il parametro delimitatore specificato in una richiesta ListObjects o ListObjectVersions.
s3:ExistingObjectTag/<tag-key>	s3:DeleteObjectTagging s3:DeleteObjectVersionTagging s3:GetObject s3:GetObjectAcl 3:GetObjectTagging s3:GetObjectVersion s3:GetObjectVersionAcl s3:GetObjectVersionTagging s3:PutObjectAcl s3:PutObjectTagging s3:PutObjectVersionAcl s3:PutObjectVersionTagging	Sarà necessario che l'oggetto esistente abbia la chiave e il valore del tag specifici.
s3:max-keys	s3:ListBucket e autorizzazioni s3:ListBucketVersions	Verrà confrontato con il parametro max-keys specificato in una richiesta ListObjects o ListObjectVersions.
s3:object-lock-mode	s3:PutObject	Confronta con l' `object-lock-mode` espanso dall'intestazione della richiesta nelle richieste PutObject, CopyObject e CreateMultipartUpload.
s3:object-lock-mode	s3:PutObjectRetention	Confronta con l' `object-lock-mode`espansione dal corpo XML nella richiesta PutObjectRetention.

${post_edited_translations.segment}	Azioni	Descrizione
s3:object-lock-remaining-retention-days	s3:PutObject	Confronta con la retain-until-date specificata nell' `x-amz-object-lock-retain-until-date`intestazione della richiesta o calcolata dal periodo di conservazione predefinito del bucket per assicurarti che questi valori siano all'interno dell'intervallo consentito per le seguenti richieste: • PutObject • CopyObject • CreateMultipartUpload
s3:object-lock-remaining-retention-days	s3:PutObjectRetention	Confronta la data di conservazione specificata nella richiesta PutObjectRetention per assicurarti che rientri nell'intervallo consentito.
s3:prefix	s3:ListBucket e autorizzazioni s3:ListBucketVersions	Verrà confrontato con il parametro prefisso specificato in una richiesta ListObjects o ListObjectVersions.
s3:RequestObjectTag/<tag-key>	s3:PutObject s3:PutObjectTagging s3:PutObjectVersionTagging	Richiederà una chiave e un valore di tag specifici quando la richiesta dell'oggetto include il tagging.
s3:x-amz-server-side-encryption-customer-algorithm	s3:PutObject	Confronta con `sse-customer-algorithm` o con `copy-source-sse-customer-algorithm` espanso dall'intestazione della richiesta nella PutObject, CopyObject, CreateMultipartUpload, UploadPart, UploadPartCopy e CompleteMultipartUpload request.

Specifica le variabili in una policy

Puoi usare variabili nelle policy per popolare le informazioni sulla policy quando sono disponibili. Puoi usare variabili di policy nell'elemento `Resource` e nei confronti di stringhe nell'elemento `Condition`.

In questo esempio, la variabile `${aws:username}` è parte dell'elemento Resource:

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

In questo esempio, la variabile `${aws:username}` fa parte del valore della condizione nel blocco di condizione:

```
"Condition": {
    "StringLike": {
      "s3:prefix": "${aws:username}/*"
        ...
},
        ...
```

Variabile	Descrizione
`${aws:SourceIp}`	Utilizza la chiave SourceIp come variabile fornita.
`${aws:username}`	Utilizza la chiave username come variabile fornita.
`${s3:prefix}`	Utilizza la chiave del prefisso specifico del servizio come variabile fornita.
`${s3:max-keys}`	Utilizza la chiave max-keys specifica del servizio come variabile fornita.
`${*}`	Carattere speciale. Usa il carattere come un carattere * letterale.
`${?}`	Carattere speciale. Usa il carattere come un carattere ? letterale.
`${$}`	Carattere speciale. Usa il carattere come simbolo $ letterale.

Crea policy che richiedono una gestione speciale

A volte una policy può concedere autorizzazioni pericolose per la sicurezza o per la continuità operativa, come ad esempio bloccare l'utente root dell'account. L'implementazione dell'API REST S3 di StorageGRID è meno restrittiva durante la convalida delle policy rispetto ad Amazon, ma altrettanto rigorosa durante la valutazione delle policy.

Descrizione della policy	Tipo di policy	Comportamento Amazon	Comportamento di StorageGRID
Negati qualsiasi autorizzazione per l'account root	Bucket	Valido e applicato, ma l'utente root mantiene l'autorizzazione per tutte le operazioni sulle policy dei bucket S3	Stesso
Nega a te stesso qualsiasi autorizzazione per l'utente/gruppo	Gruppo	Valido e applicato	Stesso

Descrizione della policy	Tipo di policy	Comportamento Amazon	Comportamento di StorageGRID
Consenti a un gruppo di account esteri qualsiasi autorizzazione	Bucket	Principal non valido	Valido, ma le autorizzazioni per tutte le operazioni della policy del bucket S3 restituiscono un errore 405 Method Not Allowed quando consentito da una policy
Consenti a un account root o utente straniero qualsiasi autorizzazione	Bucket	Valido, ma le autorizzazioni per tutte le operazioni della policy del bucket S3 restituiscono un errore 405 Method Not Allowed quando consentito da una policy	Stesso
Consenti a tutti di eseguire tutte le azioni	Bucket	Valido, ma le autorizzazioni per tutte le operazioni della policy del bucket S3 restituiscono un errore 405 Method Not Allowed per l'account root esterno e gli utenti	Stesso
Nega a tutti i permessi per tutte le azioni	Bucket	Valido e applicato, ma l'utente root mantiene l'autorizzazione per tutte le operazioni sulle policy dei bucket S3	Stesso
Principal è un utente o un gruppo inesistente	Bucket	Principal non valido	Valido
La risorsa è un bucket S3 inesistente	Gruppo	Valido	Stesso
Principal è un gruppo locale	Bucket	Principal non valido	Valido
La policy concede a un account non proprietario (inclusi gli account anonimi) le autorizzazioni per inserire oggetti.	Bucket	Valido. Gli oggetti sono di proprietà dell'account creatore e la policy del bucket non si applica. L'account creatore deve concedere le autorizzazioni di accesso per l'oggetto utilizzando gli ACL dell'oggetto.	Valido. Gli oggetti sono di proprietà dell'account proprietario del bucket. Si applica la policy del bucket.

Protezione WORM (Write-once-read-many)

Puoi creare bucket WORM (write-once-read-many) per proteggere dati, metadati degli oggetti definiti

dall'utente e il tagging degli oggetti S3. Configura i bucket WORM per consentire la creazione di nuovi oggetti e per impedire la sovrascrittura o l'eliminazione dei contenuti esistenti. Usa uno degli approcci descritti qui.

Per garantire che le sovrascritture vengano sempre negate, puoi:

- Dal Grid Manager, vai su **Configurazione** > **Sicurezza** > **Impostazioni di sicurezza** > **Rete e oggetti** e seleziona la casella di controllo **Impedisci la modifica del client**.
- Applica le seguenti regole e policy S3:
  - Aggiungi un'operazione DENY PutOverwriteObject alla policy S3.
  - Aggiungi un'operazione DENY DeleteObject alla policy S3.
  - Aggiungi un'operazione ALLOW PutObject alla policy S3.

> Impostare DeleteObject su DENY in una policy S3 non impedisce a ILM di eliminare gli oggetti quando esiste una regola come "zero copie dopo 30 giorni".

> Anche quando tutte queste regole e politiche sono applicate, non ti proteggono dalle scritture simultanee (vedi Situazione A). Ti proteggono invece dalle sovrascritture sequenziali completate (vedi Situazione B).

Situazione A: Scritture simultanee (non protette)

```
/mybucket/important.doc
PUT#1 ---> OK
PUT#2 -------> OK
```

Situazione B: Sovrascritture sequenziali completate (protette)

```
/mybucket/important.doc
PUT#1 -------> PUT#2 ---X (denied)
```

Informazioni correlate

- "Come le regole ILM di StorageGRID gestiscono gli oggetti"
- "Esempi di policy dei bucket"
- "Esempi di criteri di gruppo"
- "Esempio di policy di sessione"
- "Gestisci gli oggetti con ILM"
- "Usa un tenant account"

Esempio di policy di sessione dell'API REST S3 di StorageGRID

Usa il seguente esempio per creare una policy di sessione StorageGRID.

Esempio: imposta una policy di sessione che consente il recupero degli oggetti

In questo esempio, al principale della sessione è consentito solo recuperare oggetti da bucket1. Tutte le altre azioni sono implicitamente negate, ad eccezione delle azioni specifiche di StorageGRID, come l'utilizzo dell'autorizzazione "s3:PutOverwriteObject". La policy di sessione può essere fornita come file JSON durante la chiamata all'API AssumeRole.

```
{
  "Statement": [
    {
      "Action": "s3:GetObject",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::bucket1/*"
    }
  ]
}
```

Esempi di policy bucket S3 REST API di StorageGRID

Utilizza gli esempi in questa sezione per creare policy di accesso a StorageGRID per i bucket.

Le policy dei bucket specificano le autorizzazioni di accesso per il bucket a cui sono associate. Configuri una policy per un bucket utilizzando l'API S3 PutBucketPolicy tramite uno di questi strumenti:

- "${post_edited_translations.segment}".
- AWS CLI utilizzando questo comando (consulta "Operazioni sui bucket"):

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
file://policy.json
```

Esempio: consenti a tutti l'accesso in sola lettura a un bucket

In questo esempio, a tutti, incluso l'anonimo, è consentito elencare gli oggetti nel bucket ed eseguire operazioni GetObject su tutti gli oggetti nel bucket. Tutte le altre operazioni saranno negate. Nota che questa policy potrebbe non essere particolarmente utile perché nessuno, tranne l'utente root dell'account, ha i permessi per scrivere nel bucket.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:GetObject", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"]
    }
  ]
}
```

Esempio: consenti a tutti in un account l'accesso completo e a tutti in un altro account l'accesso in sola lettura a un bucket

In questo esempio, a tutti gli utenti di un account specificato è consentito l'accesso completo a un bucket, mentre a tutti gli utenti di un altro account specificato è consentito solo visualizzare il contenuto del bucket ed eseguire GetObject operazioni sugli oggetti presenti nel bucket che iniziano con il `shared/` prefisso della chiave dell'oggetto.

> In StorageGRID, gli oggetti creati da un account non proprietario (inclusi gli account anonimi) sono di proprietà dell'account proprietario del bucket. La policy del bucket si applica a questi oggetti.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "95390887230002558202"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/shared/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::examplebucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "shared/*"
        }
      }
    }
  ]
}
```

Esempio: consenti a tutti l'accesso in sola lettura a un bucket e l'accesso completo a un gruppo specificato

In questo esempio, chiunque, incluso l'utente anonimo, può elencare il bucket ed eseguire operazioni GetObject su tutti gli oggetti nel bucket, mentre solo gli utenti appartenenti al gruppo `Marketing` nello specifico account hanno accesso completo.

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

Esempio: consenti a tutti l'accesso in lettura e scrittura a un bucket se il client si trova nell'intervallo IP

In questo esempio, chiunque, incluso l'anonimo, può elencare il bucket ed eseguire qualsiasi operazione sugli oggetti presenti nel bucket, a condizione che le richieste provengano da un intervallo IP specificato (54.240.143.0 a 54.240.143.255, tranne 54.240.143.188). Tutte le altre operazioni saranno negate e tutte le richieste al di fuori dell'intervallo IP saranno negate.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadWriteAccessIfInSourceIpRange",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:*Object", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"],
      "Condition": {
        "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},
        "NotIpAddress": {"aws:SourceIp": "54.240.143.188"}
      }
    }
  ]
}
```

Esempio: consenti l'accesso completo a un bucket esclusivamente a un utente federato specificato

In questo esempio, all'utente federato Alex è consentito l'accesso completo al `examplebucket` bucket e ai suoi oggetti. A tutti gli altri utenti, incluso 'root', sono esplicitamente negate tutte le operazioni. Nota però che a 'root' non vengono mai negati i permessi di Put/Get/DeleteBucketPolicy.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

Esempio: permesso PutOverwriteObject

In questo esempio, l' `Deny`effetto per PutOverwriteObject e DeleteObject garantisce che nessuno possa sovrascrivere o eliminare i dati dell'oggetto, i metadati definiti dall'utente e i tag degli oggetti S3.

```
{
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:PutOverwriteObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::wormbucket/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::wormbucket"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::wormbucket/*"
    }
  ]
}
```

Esempi di criteri di gruppo dell'API REST S3 di StorageGRID

Utilizza gli esempi in questa sezione per creare criteri di accesso StorageGRID per i gruppi.

Le policy di gruppo specificano le autorizzazioni di accesso per il gruppo a cui sono associate. Non c'è elemento `Principal` nella policy perché è implicito. Le policy di gruppo si configurano usando il Tenant Manager o l'API.

Esempio: imposta i criteri di gruppo tramite Tenant Manager

Quando aggiungi o modifichi un gruppo in Tenant Manager, puoi selezionare un criterio di gruppo per determinare quali autorizzazioni di accesso S3 avranno i membri di questo gruppo. Vedi "Crea gruppi per un tenant S3".

- **Nessun accesso a S3**: opzione predefinita. Gli utenti di questo gruppo non hanno accesso alle risorse S3, a meno che l'accesso non venga concesso tramite una bucket policy. Se selezioni questa opzione, solo l'utente root avrà accesso alle risorse S3 per impostazione predefinita.
- **Accesso di sola lettura**: Gli utenti di questo gruppo hanno accesso di sola lettura alle risorse S3. Ad esempio, gli utenti di questo gruppo possono elencare gli oggetti e leggere i dati degli oggetti, i metadati e i tag. Quando selezioni questa opzione, la stringa JSON per un criterio di gruppo di sola lettura appare nella casella di testo. Non puoi modificare questa stringa.
- **Accesso completo**: Gli utenti di questo gruppo hanno accesso completo alle risorse S3, inclusi i bucket. Quando selezioni questa opzione, la stringa JSON per un criterio di gruppo con accesso completo appare nella casella di testo. Non puoi modificare questa stringa.
- **Mitigazione del ransomware**: Questa policy di esempio si applica a tutti i bucket per questo tenant. Gli utenti di questo gruppo possono eseguire azioni comuni, ma non possono eliminare definitivamente oggetti dai bucket che hanno il versioning degli oggetti abilitato.

  Gli utenti di Tenant Manager che dispongono dell'autorizzazione "Gestisci tutti i bucket" possono ignorare questo criterio di gruppo. Limita l'autorizzazione "Gestisci tutti i bucket" agli utenti attendibili e usa l'autenticazione a più fattori (MFA) dove disponibile.

- **Personalizzato**: Agli utenti del gruppo concedi le autorizzazioni che specifichi nella casella di testo.

Esempio: Consenti al gruppo l'accesso completo a tutti i bucket

In questo esempio, a tutti i membri del gruppo è consentito l'accesso completo a tutti i bucket di proprietà dell'account del tenant, a meno che non sia esplicitamente negato dalla policy del bucket.

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

Esempio: Consenti l'accesso di sola lettura del gruppo a tutti i bucket

In questo esempio, tutti i membri del gruppo hanno accesso in sola lettura alle risorse S3, a meno che non sia esplicitamente negato dalla policy del bucket. Ad esempio, gli utenti di questo gruppo possono elencare gli oggetti e leggere i dati, i metadati e i tag degli oggetti.

```
{
  "Statement": [
    {
      "Sid": "AllowGroupReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Esempio: consenti ai membri del gruppo l'accesso completo solo alla loro "cartella" in un bucket

In questo esempio, i membri del gruppo sono autorizzati a visualizzare e accedere solo alla propria cartella specifica (prefisso chiave) nel bucket specificato. Nota che, per determinare la privacy di queste cartelle, devi considerare anche le autorizzazioni di accesso di altri criteri di gruppo e del criterio del bucket.

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

Informazioni sul copyright

Informazioni sul marchio commerciale