# Policy di accesso a bucket e gruppi

StorageGRID 11.9

NetApp
November 08, 2024

# Sommario

Policy di accesso a bucket e gruppi . . . . . 1
Utilizza policy di accesso a bucket e gruppi . . . . . 1
Esempio di policy bucket . . . . . 18
Criteri di gruppo di esempio . . . . . 24

# Policy di accesso a bucket e gruppi

## Utilizza policy di accesso a bucket e gruppi

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 dei criteri delle API REST S3. I criteri di accesso per l'API S3 sono scritti in JSON.

### Panoramica dei criteri di accesso

StorageGRID supporta due tipi di policy di accesso.

- **Criteri bucket**, che sono gestiti utilizzando le operazioni API GetBucketPolicy, PutBucketPolicy e DeleteBucketPolicy S3 o l'API Tenant Manager o Tenant Management. Le policy del bucket sono collegate ai bucket, quindi sono configurate per controllare l'accesso degli utenti nell'account del proprietario del bucket o altri account al bucket e agli oggetti in esso contenuti. Una policy di bucket si applica a un solo bucket ed eventualmente a più gruppi.
- **Criteri di gruppo**, configurati utilizzando l'API di gestione tenant Manager o tenant. I criteri di gruppo sono associati a un gruppo dell'account, quindi sono configurati per consentire a tale gruppo di accedere a risorse specifiche di proprietà di tale account. Una policy di gruppo si applica a un solo gruppo e possibilmente a più bucket.

Non vi è alcuna differenza di priorità tra le policy di gruppo e quelle di bucket.

Le policy di gruppo e bucket di StorageGRID seguono una grammatica specifica definita da Amazon. All'interno di ogni policy è presente una serie di dichiarazioni di policy, ciascuna delle quali contiene i seguenti elementi:

- ID dichiarazione (Sid) (opzionale)
- Effetto
- Principal/NotPrincipal
- Risorsa/NotResource
- Azione/Notazione
- Condizione (opzionale)

Le istruzioni dei criteri vengono create utilizzando questa struttura per specificare le autorizzazioni: Grant <Effect> per consentire/negare a <Principal> di eseguire <Action> su <Resource> quando viene applicato <Condition>.

Ciascun elemento di policy viene utilizzato per una funzione specifica:

| Elemento | Descrizione |
| --- | --- |
| SID | L'elemento Sid è opzionale. Il Sid deve essere utilizzato solo come descrizione per l'utente. Viene memorizzato ma non interpretato dal sistema StorageGRID. |

| Elemento | Descrizione |
| --- | --- |
| Effetto | Utilizzare l'elemento Effect per stabilire se le operazioni specificate sono consentite o rifiutate. È necessario identificare le operazioni consentite (o negate) su bucket o oggetti utilizzando le parole chiave dell'elemento Action supportate. |
| Principal/NotPrincipal | È possibile consentire a utenti, gruppi e account di accedere a risorse specifiche ed eseguire azioni specifiche. Se nella richiesta non è inclusa alcuna firma S3, l'accesso anonimo è consentito specificando il carattere jolly (*) come principale. Per impostazione predefinita, solo l'account root ha accesso alle risorse di proprietà dell'account.<br><br>È sufficiente specificare l'elemento Principal in una policy bucket. Per i criteri di gruppo, il gruppo a cui è associato il criterio è l'elemento Principal implicito. |
| Risorsa/NotResource | L'elemento Resource identifica bucket e oggetti. Puoi consentire o negare le autorizzazioni per bucket e oggetti utilizzando il nome risorsa Amazon (ARN) per identificare la risorsa. |
| Azione/Notazione | Gli elementi Action e Effect sono i due componenti delle autorizzazioni. Quando un gruppo richiede una risorsa, gli viene concesso o negato l'accesso alla risorsa. L'accesso viene negato a meno che non si assegnino specificamente autorizzazioni, ma è possibile utilizzare la funzione di negazione esplicita per ignorare un'autorizzazione concessa da un altro criterio. |
| Condizione | L'elemento Condition è opzionale. Le condizioni consentono di creare espressioni per determinare quando applicare un criterio. |

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

```
s3:*Object
```

Nell'elemento Resource, è possibile utilizzare 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, ad eccezione dell'impostazione dell'accesso anonimo, che concede l'autorizzazione a tutti. Ad esempio, impostare il carattere jolly (*) come valore Principal.

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

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

Nell'esempio seguente, l'istruzione utilizza gli elementi Effect, Principal, Action e Resource. In questo esempio viene illustrata un'istruzione completa dei criteri bucket che utilizza l'effetto "Consenti" per assegnare ai Principals, 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/*"
      ]
    }
  ]
}
```

Il criterio bucket ha un limite di dimensione di 20,480 byte e il criterio di gruppo ha un limite di dimensione di 5,120 byte.

## Coerenza delle policy

Per impostazione predefinita, gli aggiornamenti apportati ai criteri di gruppo sono coerenti. Quando un criterio di gruppo diventa coerente, le modifiche possono richiedere altri 15 minuti, a causa della memorizzazione nella cache dei criteri. Per impostazione predefinita, tutti gli aggiornamenti apportati ai criteri bucket sono fortemente coerenti.

Come richiesto, è possibile modificare le garanzie di coerenza per gli aggiornamenti delle policy bucket. Ad esempio, è possibile rendere disponibile una modifica a un criterio bucket in caso di fuori servizio di un sito.

In questo caso, è possibile impostare l' `Consistency-Control`intestazione nella richiesta PutBucketPolicy oppure utilizzare la richiesta di coerenza PUT Bucket. Quando un criterio bucket diventa coerente, le modifiche possono richiedere altri 8 secondi per diventare effettive, a causa del caching delle policy.

Se si imposta la coerenza su un valore diverso per risolvere una situazione temporanea, assicurarsi di riportare l'impostazione del livello del bucket al valore originale al termine dell'operazione. In caso contrario, tutte le richieste bucket future utilizzeranno l'impostazione modificata.

## Utilizzare ARN nelle dichiarazioni delle policy

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

- Utilizzare questa sintassi per specificare la risorsa S3 ARN:

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

- Utilizzare 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
```

Altre considerazioni:

- È possibile utilizzare l'asterisco (*) come carattere jolly per far corrispondere zero o più caratteri all'interno della chiave oggetto.
- I caratteri internazionali, che possono essere specificati nella chiave oggetto, devono essere codificati utilizzando JSON UTF-8 o le sequenze di escape JSON. La codifica in percentuale non è supportata.

  "Sintassi URN RFC 2141"

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

## Specificare le risorse in un criterio

Nelle istruzioni policy, è possibile utilizzare l'elemento Resource per specificare il bucket o l'oggetto per cui le autorizzazioni sono consentite o negate.

- Ogni dichiarazione di policy richiede un elemento Resource. In un criterio, le risorse sono indicate dall'elemento `Resource`, o in alternativa, `NotResource` per esclusione.
- Specificare le risorse con un ARN di risorsa S3. Ad esempio:

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

- È inoltre possibile utilizzare le variabili dei criteri all'interno della chiave a oggetti. 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.

## Specificare le entità in un criterio

Utilizzare l'elemento Principal per identificare l'account utente, gruppo o tenant a cui è consentito/negato l'accesso alla risorsa dall'istruzione policy.

- Ogni dichiarazione di policy in una policy 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 principale.
- In un criterio, 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" }
```

- In questo esempio viene utilizzato l'ID account tenant 27233906934684427525, che include l'account root e tutti gli utenti dell'account:

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

- È possibile specificare solo l'account root:

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

- È possibile specificare un utente federato specifico ("Alex"):

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

- È possibile specificare uno specifico gruppo federated ("Manager"):

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

- È possibile specificare un'entità anonima:

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

- Per evitare ambiguità, è possibile utilizzare l'UUID utente invece del nome utente:

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

  Ad esempio, supponiamo che Alex abbandoni l'organizzazione e che il nome utente `Alex` venga eliminato. Se un nuovo Alex entra a far parte dell'organizzazione e 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 utente/gruppo che non esiste ancora quando viene creata una policy bucket.

## Specificare le autorizzazioni in un criterio

In un criterio, l'elemento Action viene utilizzato per consentire/negare le autorizzazioni a una risorsa. È possibile specificare una serie di autorizzazioni in un criterio, indicate dall'elemento "Action" o, in alternativa, "NotAction" per l'esclusione. Ciascuno di questi elementi viene associato a specifiche operazioni REST API S3.

Le tabelle elencano le autorizzazioni applicabili ai bucket e le autorizzazioni applicabili agli oggetti.

> Amazon S3 ora utilizza l'autorizzazione S3:PutReplicationConfiguration per entrambe le azioni PutBucketReplication e DeleteBucketReplication. StorageGRID utilizza autorizzazioni separate per ciascuna azione, che corrispondono alla specifica originale di Amazon S3.

> Un'eliminazione viene eseguita quando si utilizza un put per sovrascrivere un valore esistente.

**Autorizzazioni applicabili ai bucket**

| Permessi | OPERAZIONI REST API S3 | Personalizzato per StorageGRID |
|---|---|---|
| s3:CreateBucket | CreateBucket | Sì.<br><br>**Nota**: Utilizzare solo nei criteri di gruppo. |
| s3:Deletebucket | DeleteBucket | |
| s3:DeleteBucketMetadataNotification | ELIMINA la configurazione di notifica dei metadati del bucket | Sì |
| s3:DeleteBucketPolicy | DeleteBucketPolicy | |

| Permessi | OPERAZIONI REST API S3 | Personalizzato per StorageGRID |
| --- | --- | --- |
| s3:DeleteReplicationConfiguration | DeleteBucketReplication | Sì, separare le autorizzazioni per PUT ed DELETE |
| s3:GetBucketAcl | GetBucketAcl | |
| s3:GetBucketCompliance | OTTIENI compliance bucket (obsoleta) | Sì |
| s3:GetBucketConsistency | COERENZA del bucket | Sì |
| s3:GetBucketCORS | GetBucketCors | |
| s3:GetEncryptionConfiguration | GetBucketEncryption | |
| s3:GetBucketLastAccessTime | OTTIENI l'ultimo tempo di accesso a bucket | Sì |
| s3:GetBucketLocation | GetBucketLocation | |
| s3:GetBucketMetadataNotification | OTTIENI la 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 | |
| s3:ListAllMyBucket | • ListBucket<br>• OTTIENI l'utilizzo dello storage | Sì, per OTTIENI utilizzo storage.<br>**Nota**: Utilizzare solo nei criteri di gruppo. |

| Permessi | OPERAZIONI REST API S3 | Personalizzato per StorageGRID |
| --- | --- | --- |
| s3:ListBucket | • ListObjects (oggetti elenco)<br>• HeadBucket<br>• RestoreObject | |
| s3:ListBucketMultipartUploads | • ListMultipartUploads<br>• RestoreObject | |
| s3:ListBucketVersions | SCARICA le versioni di bucket | |
| s3:PutBucketCompliance | METTERE la compliance del bucket (obsoleta) | Sì |
| s3:PutBucketConsistency | METTI la coerenza del bucket | Sì |
| s3:PutBucketCORS | • DeleteBucketCors†<br>• PutBucketCors | |
| s3:PutEncryptionConfiguration | • DeleteBucketEncryption<br>• PutBucketEncryption | |
| s3:PutBucketLastAccessTime | TEMPO ULTIMO accesso bucket | Sì |
| s3:PutBucketMetadataNotification | INSERIRE la configurazione della notifica dei metadati del bucket | 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)<br>• PutObjectLockConfiguration | |
| s3:PutBucketPolicy | PutBucketPolicy | |
| s3:PutBucketTagging | • DeleteBucketTagging†<br>• PutBucketTagging | |
| s3:PutBucketVersioning | PutBucketVersioning | |

| Permessi | OPERAZIONI REST API S3 | Personalizzato per StorageGRID |
| --- | --- | --- |
| s3:PutLifecycleConfiguration | • DeleteBucketLifecycle†<br>• PutBucketLifecycleConfiguration | |
| s3:PutReplicationConfiguration | PutBucketReplication | Sì, separare le autorizzazioni per PUT ed DELETE |

**Autorizzazioni applicabili agli oggetti**

| Permessi | OPERAZIONI REST API S3 | Personalizzato per StorageGRID |
| --- | --- | --- |
| s3:AbortMultipartUpload | • AbortMultipartUpload<br>• RestoreObject | |
| s3:BypassGovernanceRetention | • DeleteObject (Elimina oggetto)<br>• DeleteObjects<br>• PutObjectRetention | |
| s3:DeleteObject | • DeleteObject (Elimina oggetto)<br>• DeleteObjects<br>• RestoreObject | |
| s3:DeleteObjectTagging | DeleteObjectTagging | |
| s3:DeleteObjectVersionTagging | DeleteObjectTagging (una versione specifica dell'oggetto) | |
| s3:DeleteObjectVersion | DeleteObject (una versione specifica dell'oggetto) | |
| s3:GetObject | • GetObject<br>• HeadObject (oggetto intestazione)<br>• RestoreObject<br>• SelectObjectContent | |
| s3:GetObjectAcl | GetObjectAcl | |
| s3:GetObjectLegalHold | GetObjectLegalHold | |
| s3:GetObjectRetention | GetObjectRetention | |

| Permessi | OPERAZIONI REST API S3 | Personalizzato per StorageGRID |
|---|---|---|
| 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<br>• Oggetto CopyObject<br>• RestoreObject<br>• CreateMultipartUpload<br>• CompleteMultipartUpload<br>• UploadPart<br>• UploadPartCopy | |
| s3:PutObjectLegalHold | PutObjectLegalHold | |
| s3:PutObjectRetention | PutObjectRetention | |
| s3:PutObjectTagging | PutObjectTagging | |
| s3:PutObjectVersionTagging | PutObjectTagging (una versione specifica dell'oggetto) | |
| s3:PutOverwriteObject | • PutObject<br>• Oggetto CopyObject<br>• PutObjectTagging<br>• DeleteObjectTagging<br>• CompleteMultipartUpload | Sì |
| s3:RestoreObject (Riavvia oggetto) | RestoreObject | |

## Utilizza l'autorizzazione 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 impostazioni possibili per questa autorizzazione includono:

- **Allow**: Il client può sovrascrivere un oggetto. Questa è l'impostazione predefinita.
- **Nega**: Il client non può sovrascrivere un oggetto. Se impostata su Nega, l'autorizzazione PutOverwriteObject funziona come segue:
  - Se un oggetto esistente viene trovato nello stesso percorso:
    - I dati dell'oggetto, i metadati definiti dall'utente o il tag S3 non possono essere sovrascritti.
    - Tutte le operazioni di acquisizione in corso vengono annullate e viene restituito un errore.
    - Se è attivata la versione S3, l'impostazione Nega impedisce alle operazioni PutObjectTagging o DeleteObjectTagging di modificare il TagSet per un oggetto e le relative 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 se Allow è stato impostato.

> Se il criterio 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 degli oggetti. Inoltre, se la casella di controllo **Impedisci modifica client** è selezionata (**CONFIGURAZIONE** > **Impostazioni di sicurezza** > **rete e oggetti**), tale impostazione sovrascrive l'impostazione dell'autorizzazione PutOverwriteObject.

## Specificare le condizioni in un criterio

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 ciascuna 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 SourceIp Condition.

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

### Operatori delle condizioni supportati

Gli operatori delle condizioni sono classificati come segue:

- Stringa
- Numerico

- Booleano
- Indirizzo IP
- Controllo nullo

| Condizionare gli operatori | Descrizione |
|---|---|
| StringEquals | Confronta una chiave con un valore stringa in base alla corrispondenza esatta (distinzione tra maiuscole e minuscole). |
| StringNotEquals | Confronta una chiave con un valore stringa in base alla corrispondenza negata (distinzione tra maiuscole e minuscole). |
| StringEqualsIgnoreCase | Confronta una chiave con un valore stringa in base alla corrispondenza esatta (ignora maiuscole/minuscole). |
| StringNotEqualsIgnoreCase | Confronta una chiave con un valore stringa in base alla corrispondenza negata (ignora maiuscole/minuscole). |
| StringLike | Confronta una chiave con un valore stringa in base alla corrispondenza esatta (distinzione tra maiuscole e minuscole). Può includere caratteri jolly * e ?. |
| StringNotLike | Confronta una chiave con un valore stringa in base alla corrispondenza negata (distinzione tra maiuscole e minuscole). Può includere caratteri jolly * e ?. |
| Valori numerici Equals | Confronta una chiave con un valore numerico in base alla corrispondenza esatta. |
| NumericNotEquals | Confronta una chiave con un valore numerico in base alla corrispondenza negata. |
| NumericGreaterThan | Confronta un tasto con un valore numerico basato sulla corrispondenza "maggiore di". |
| NumericGreaterThanEquals | Confronta una chiave con un valore numerico basato sulla corrispondenza "maggiore o uguale". |
| NumericLessThan | Confronta una chiave con un valore numerico basato sulla corrispondenza "minore di". |
| NumericLessThanEquals | Confronta una chiave con un valore numerico basato sulla corrispondenza "minore di o uguale". |
| Bool | Confronta una chiave con un valore booleano basato sulla corrispondenza "true o false". |

| Condizionare gli operatori | Descrizione |
| --- | --- |
| Indirizzo IP | Confronta una chiave con un indirizzo IP o un intervallo di indirizzi IP. |
| NotIpAddress | Confronta una chiave con un indirizzo IP o un intervallo di indirizzi IP in base alla corrispondenza negata. |
| Nullo | Controlla se è presente una chiave di condizione nel contesto della richiesta corrente. |

**Chiavi di condizione supportate**

| Tasti Condition | Azioni | Descrizione |
| --- | --- | --- |
| aws: SourceIp | Operatori IP | Viene confrontato con l'indirizzo IP da cui è stata inviata la richiesta. Può essere utilizzato per operazioni bucket o a oggetti.<br><br>**Nota:** se la richiesta S3 è stata inviata tramite il servizio Load Balancer sui nodi Admin e Gateway, viene confrontato con l'indirizzo IP a monte del servizio Load Balancer.<br><br>**Nota**: Se si utilizza un bilanciamento del carico non trasparente di terze parti, questo viene confrontato con l'indirizzo IP del bilanciamento del carico. Qualsiasi `X-Forwarded-For` intestazione verrà ignorata perché la sua validità non può essere accertata. |
| aws:nome utente | Risorsa/identità | Viene confrontato con il nome utente del mittente da cui è stata inviata la richiesta. Può essere utilizzato per operazioni bucket o a oggetti. |
| s3:delimitatore | s3:ListBucket e.<br><br>s3:autorizzazioni ListBucketVersions | Verrà eseguito un confronto con il parametro delimitatore specificato in una richiesta ListObjects o ListObjectVersions. |

| Tasti Condition | Azioni | Descrizione |
| --- | --- | --- |
| S3:ExistingObjectTag/<tag-key> | s3:DeleteObjectTagging<br><br>s3:DeleteObjectVersionTagging<br><br>s3:GetObject<br><br>s3:GetObjectAcl<br><br>3:GetObjectTagging<br><br>s3:GetObjectVersion<br><br>s3:GetObjectVersionAcl<br><br>s3:GetObjectVersionTagging<br><br>S3:PutObjectAcl<br><br>s3:PutObjectTagging<br><br>S3:PutObjectVersionAcl<br><br>s3:PutObjectVersionTagging | Richiede che l'oggetto esistente abbia la chiave e il valore tag specifici. |
| s3: tasti max | s3:ListBucket e.<br><br>s3:autorizzazioni ListBucketVersions | Verrà eseguito un confronto con il parametro max-keys specificato in una richiesta ListObjects o ListObjectVersions. |
| s3:giorni-rimanenti-conservazione-blocco-oggetto | s3:PutObject | Viene confrontato con la data di scadenza specificata nell' `x-amz-object-lock-retain-until-date`intestazione della richiesta o calcolata dal periodo di conservazione predefinito del bucket per assicurarsi che questi valori rientrino nell'intervallo consentito per le seguenti richieste:<br><br>• PutObject<br>• Oggetto CopyObject<br>• CreateMultipartUpload |
| s3:giorni-rimanenti-conservazione-blocco-oggetto | s3:PutObjectRetention | Viene confrontato con la data di scadenza specificata nella richiesta PutObjectRetention per garantire che rientri nell'intervallo consentito. |

| Tasti Condition | Azioni | Descrizione |
|---|---|---|
| s3:prefisso | s3:ListBucket e.<br><br>s3:autorizzazioni ListBucketVersions | Verrà eseguito un confronto con il parametro prefix specificato in una richiesta ListObjects o ListObjectVersions. |
| S3:RequestObjectTag/<tag-key> | s3:PutObject<br><br>s3:PutObjectTagging<br><br>s3:PutObjectVersionTagging | Richiede una chiave e un valore tag specifici quando la richiesta dell'oggetto include il tagging. |

## Specificare le variabili in un criterio

È possibile utilizzare le variabili nei criteri per popolare le informazioni sui criteri quando sono disponibili. È possibile utilizzare le variabili dei criteri nell' `Resource`elemento e nei confronti delle stringhe nell' `Condition`elemento.

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

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

In questo esempio, la variabile `${aws:username}` fa parte del valore di 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. |
| `${s3:prefix}` | Utilizza la chiave di prefisso specifica del servizio come variabile fornita. |
| `${s3:max-keys}` | Utilizza la chiave max-keys specifica del servizio come variabile fornita. |
| `${*}` | Carattere speciale. Utilizza il carattere come carattere * letterale. |

| Variabile | Descrizione |
| --- | --- |
| `${?}` | Carattere speciale. Utilizza il carattere come carattere letterale ?. |
| `${$}` | Carattere speciale. Utilizza il carattere come carattere letterale. |

## Creare policy che richiedono una gestione speciale

A volte un criterio può concedere autorizzazioni pericolose per la sicurezza o pericolose per operazioni continue, come il blocco dell'utente root dell'account. L'implementazione dell'API REST di StorageGRID S3 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 di Amazon | Comportamento di StorageGRID |
| --- | --- | --- | --- |
| Negare automaticamente le autorizzazioni all'account root | Bucket | Valido e applicato, ma l'account utente root conserva l'autorizzazione per tutte le operazioni di policy del bucket S3 | Stesso |
| Negare automaticamente le autorizzazioni all'utente/gruppo | Gruppo | Valido e applicato | Stesso |
| Consenti a un gruppo di account esterno qualsiasi autorizzazione | Bucket | Principal non valido | Valido, ma le autorizzazioni per tutte le operazioni dei criteri del bucket S3 restituiscono un errore 405 Method Not Allowed (metodo non consentito) quando consentito da un criterio |
| Consentire a un account root esterno o a un utente qualsiasi autorizzazione | Bucket | Valido, ma le autorizzazioni per tutte le operazioni dei criteri del bucket S3 restituiscono un errore 405 Method Not Allowed (metodo non consentito) quando consentito da un criterio | Stesso |
| Consenti a tutti i permessi per tutte le azioni | Bucket | Valido, ma le autorizzazioni per tutte le operazioni dei criteri del bucket S3 restituiscono un errore 405 Method Not Allowed (metodo non consentito) per l'account root esterno e gli utenti | Stesso |

| Descrizione della policy | Tipo di policy | Comportamento di Amazon | Comportamento di StorageGRID |
|---|---|---|---|
| Negare a Everyone le autorizzazioni per tutte le azioni | Bucket | Valido e applicato, ma l'account utente root conserva l'autorizzazione per tutte le operazioni di policy del 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 |
| Il criterio concede a un account non proprietario (inclusi gli account anonimi) le autorizzazioni per l'inserimento degli oggetti. | Bucket | Valido. Gli oggetti sono di proprietà dell'account creatore e la policy bucket non si applica. L'account creatore deve concedere le autorizzazioni di accesso per l'oggetto utilizzando gli ACL a oggetti. | Valido. Gli oggetti sono di proprietà dell'account proprietario del bucket. Si applica la policy bucket. |

## Protezione WORM (Write-Once-Read-Many)

È possibile creare bucket WORM (write-once-Read-many) per proteggere i dati, i metadati degli oggetti definiti dall'utente e il tagging degli oggetti S3. I bucket WORM vengono configurati in modo da consentire la creazione di nuovi oggetti e impedire la sovrascrittura o l'eliminazione del contenuto esistente. Utilizzare uno degli approcci descritti di seguito.

Per garantire che le sovrascritture vengano sempre negate, è possibile:

- Da Grid Manager, selezionare **CONFIGURATION** > **Security** > **Security settings** > **Network and Objects**, quindi selezionare la casella di controllo **Impedisci modifica client**.
- Applicare le seguenti regole e criteri S3:
  - Aggiungere un'operazione di NEGAZIONE PutOverwriteObject al criterio S3.
  - Aggiungere un'operazione di NEGAZIONE DeleteObject al criterio S3.
  - Aggiungere un'operazione PutObject ALLOW al criterio S3.

> L'impostazione di DeleteObject su NEGA in un criterio S3 non impedisce a ILM di eliminare oggetti quando esiste una regola come "zero copie dopo 30 giorni".

> Anche quando tutte queste regole e policy vengono applicate, non si proteggono dalle scritture simultanee (vedi situazione A). Si proteggono dalle sovrascritture sequenziali completate (vedere situazione B).

**Situazione A**: Scritture simultanee (non protette)

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

**Situazione B**: Sovrascritture sequenziali completate (con protezione)

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

**Informazioni correlate**

- "Modalità di gestione degli oggetti da parte delle regole ILM di StorageGRID"
- "Esempio di policy bucket"
- "Criteri di gruppo di esempio"
- "Gestire gli oggetti con ILM"
- "Utilizzare un account tenant"

# Esempio di policy bucket

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

I criteri del bucket specificano le autorizzazioni di accesso per il bucket a cui è associata la policy. È possibile configurare un criterio bucket utilizzando l'API S3 PutBucketPolicy tramite uno dei seguenti strumenti:

- "Manager tenant".
- AWS CLI utilizzando il seguente comando (vedere la "Operazioni sui bucket"):

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

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

In questo esempio, a tutti, incluso anonimo, è consentito elencare gli oggetti nel bucket ed eseguire operazioni GetObject su tutti gli oggetti nel bucket. Tutte le altre operazioni verranno negate. Si noti che questo criterio potrebbe non essere particolarmente utile perché nessuno, ad eccezione dell'account root, dispone delle autorizzazioni di scrittura nel bucket.

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

## Esempio: Consentire a tutti gli utenti di un account l'accesso completo e a tutti gli utenti di 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 elencare il bucket ed eseguire operazioni GetObject sugli oggetti 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 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: Consentire a tutti l'accesso in sola lettura a un bucket e l'accesso completo per gruppo specificato

In questo esempio, a tutti gli utenti, incluso anonimo, è consentito elencare il bucket ed eseguire operazioni GetObject su tutti gli oggetti nel bucket, mentre solo gli utenti appartenenti al gruppo `Marketing` nell'account specificato possono accedere completamente.

```
{
  "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: Consentire a tutti l'accesso in lettura e scrittura a un bucket se il client si trova nell'intervallo IP

In questo esempio, Everyone, incluso l'anonimato, è autorizzato a elencare il bucket ed eseguire qualsiasi operazione oggetto su tutti gli oggetti nel bucket, a condizione che le richieste provengano da un intervallo IP specificato (da 54.240.143.0 a 54.240.143.255, eccetto 54.240.143.188). Tutte le altre operazioni verranno rifiutate e tutte le richieste al di fuori dell'intervallo IP verranno rifiutate.

```
{
  "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: Consentire l'accesso completo a un bucket esclusivamente da un utente federato specificato

In questo esempio, all'utente federato Alex è consentito l'accesso completo al `examplebucket` bucket e ai relativi oggetti. A tutti gli altri utenti, tra cui 'root', vengono esplicitamente negate tutte le operazioni. Si noti tuttavia che a 'root' non vengono mai negate le autorizzazioni per 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: Autorizzazione PutOverwriteObject

In questo esempio, l' `Deny`effetto di PutOverwriteObject e DeleteObject garantisce che nessuno possa sovrascrivere o eliminare i dati dell'oggetto, i metadati definiti dall'utente e l'etichettatura 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/*"
    }
  ]
}
```

# Criteri di gruppo di esempio

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

I criteri di gruppo specificano le autorizzazioni di accesso per il gruppo a cui è associato il criterio. Non vi è alcun `Principal` elemento nella politica perché è implicita. I criteri di gruppo vengono configurati utilizzando il tenant Manager o l'API.

## Esempio: Impostare i criteri di gruppo utilizzando Tenant Manager

Quando si aggiunge o si modifica un gruppo in Tenant Manager, è possibile selezionare una policy di gruppo per determinare quali autorizzazioni di accesso S3 avranno i membri di questo gruppo. Vedere "Creare gruppi per un tenant S3".

- **Nessun accesso S3**: Opzione predefinita. Gli utenti di questo gruppo non hanno accesso alle risorse S3, a meno che l'accesso non sia concesso con una policy bucket. Se si seleziona 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 si seleziona questa opzione, nella casella di testo viene visualizzata la stringa JSON per un criterio di gruppo di sola lettura. Impossibile modificare questa stringa.
- **Accesso completo**: Gli utenti di questo gruppo hanno accesso completo alle risorse S3, inclusi i bucket. Quando si seleziona questa opzione, nella casella di testo viene visualizzata la stringa JSON per un criterio di gruppo ad accesso completo. Impossibile modificare questa stringa.
- **Ransomware Mitigation**: 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 in modo permanente gli oggetti dai bucket che hanno attivato la versione degli oggetti.

  Gli utenti di tenant Manager che dispongono dell'autorizzazione Gestisci tutti i bucket possono eseguire l'override di questa policy di gruppo. Limitare l'autorizzazione Manage All bucket (Gestisci tutti i bucket) agli utenti attendibili e utilizzare l'autenticazione multifattore (MFA), se disponibile.

- **Personalizzato**: Agli utenti del gruppo vengono concesse le autorizzazioni specificate nella casella di testo.

## Esempio: Consentire l'accesso completo del gruppo 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 tenant, a meno che non sia esplicitamente negato dalla policy bucket.

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

## Esempio: Consentire l'accesso di gruppo in sola lettura 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 degli oggetti, i metadati e i tag.

```
{
  "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 di accedere completamente solo alla loro "cartella" in un bucket

In questo esempio, i membri del gruppo possono solo elencare e accedere alla propria cartella specifica (prefisso chiave) nel bucket specificato. Tenere presente che le autorizzazioni di accesso da altre policy di gruppo e la policy del bucket devono essere prese in considerazione quando si determina la privacy di queste cartelle.

```
{
  "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