Criteri di accesso a bucket e gruppi

StorageGRID software

NetApp
December 03, 2025

Sommario

Criteri di accesso a bucket e gruppi

Utilizzare criteri 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 di policy dell'API REST S3. Le policy di accesso per l'API S3 sono scritte in JSON.

Panoramica della politica di accesso

StorageGRID supporta due tipi di criteri di accesso.

- **Politiche bucket**, gestite tramite le operazioni API S3 GetBucketPolicy, PutBucketPolicy e DeleteBucketPolicy oppure tramite l'API Tenant Manager o Tenant Management. I criteri dei bucket sono associati ai bucket e sono quindi configurati per controllare l'accesso degli utenti nell'account proprietario del bucket o di altri account al bucket e agli oggetti in esso contenuti. Una policy basata su bucket si applica a un solo bucket e, possibilmente, a più gruppi.
- **Criteri di gruppo**, configurati tramite Tenant Manager o Tenant Management API. I criteri di gruppo sono associati a un gruppo nell'account e sono quindi configurati per consentire a tale gruppo di accedere a risorse specifiche di proprietà di tale account. Un criterio di gruppo si applica a un solo gruppo e, possibilmente, a più bucket.

Non vi è alcuna differenza di priorità tra i criteri di gruppo e quelli di bucket.

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

- ID dichiarazione (Sid) (facoltativo)
- Effetto
- Principale/Non Principale
- Risorsa/Non Risorsa
- Azione/Non azione
- Condizione (facoltativa)

Le istruzioni di policy vengono create utilizzando questa struttura per specificare le autorizzazioni: Concedi <Effetto> per consentire/negare a <Principale> di eseguire <Azione> su <Risorsa> quando si applica <Condizione>.

Ogni elemento della policy viene utilizzato per una funzione specifica:

Elemento	Descrizione
Sid	L'elemento Sid è facoltativo. Il Sid è inteso solo come descrizione per l'utente. Viene memorizzato ma non interpretato dal sistema StorageGRID .

Elemento	Descrizione
Effetto	Utilizzare l'elemento Effetto per stabilire se le operazioni specificate sono consentite o negate. È necessario identificare le operazioni consentite (o negate) sui bucket o sugli oggetti utilizzando le parole chiave dell'elemento Azione supportate.
Principale/Non Principale	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. È sufficiente specificare l'elemento Principal in un criterio bucket. Per i criteri di gruppo, il gruppo a cui è associato il criterio è l'elemento Principal implicito.
Risorsa/Non Risorsa	L'elemento Risorsa identifica bucket e oggetti. È possibile concedere o negare autorizzazioni a bucket e oggetti utilizzando l'Amazon Resource Name (ARN) per identificare la risorsa.
Azione/Non azione	Gli elementi Azione ed Effetto 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 autorizzazioni specifiche, ma è possibile utilizzare la negazione esplicita per ignorare un'autorizzazione concessa da un altro criterio.
Condizione	L'elemento Condizione è facoltativo. Le condizioni consentono di creare espressioni per determinare quando applicare una policy.

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

```
s3:*Object
```

Nell'elemento Risorsa 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, tranne che per impostare l'accesso anonimo, che concede l'autorizzazione a tutti. Ad esempio, si imposta il carattere jolly (*) come valore Principale.

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

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

Nell'esempio seguente, l'istruzione utilizza gli elementi Effetto, Principale, Azione e Risorsa. Questo esempio mostra un'istruzione completa della policy del bucket che utilizza l'effetto "Consenti" per fornire ai Principals, il gruppo di amministrazione `federated-group/admin` e il gruppo finanziario `federated-group/finance` , autorizzazioni per eseguire l'azione `s3:ListBucket` sul secchio denominato `mybucket` e l'azione `s3:GetObject` su tutti gli oggetti all'interno di quel contenitore.

```
{
  "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 del bucket ha un limite di dimensione di 20.480 byte, mentre il criterio del gruppo ha un limite di dimensione di 5.120 byte.

Coerenza per le politiche

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

Se necessario, è possibile modificare le garanzie di coerenza per gli aggiornamenti dei criteri dei bucket. Ad esempio, potresti voler rendere disponibile una modifica ai criteri di un bucket durante un'interruzione del sito.

In questo caso, è possibile impostare il `Consistency-Control` intestazione nella richiesta PutBucketPolicy oppure puoi utilizzare la richiesta di coerenza PUT Bucket. Quando un criterio di bucket diventa coerente, le modifiche potrebbero richiedere altri 8 secondi per diventare effettive, a causa della memorizzazione nella cache dei criteri.

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

Utilizzare ARN nelle dichiarazioni di policy

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

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

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

- Utilizzare questa sintassi per specificare l'ARN della risorsa 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 trovare la corrispondenza con 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 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.

Specificare le risorse in una policy

Nelle istruzioni dei criteri, è possibile utilizzare l'elemento Risorsa per specificare il bucket o l'oggetto per cui sono concesse o negate le autorizzazioni.

- Ogni dichiarazione di policy richiede un elemento Risorsa. In una policy, le risorse sono indicate dall'elemento `Resource` , o in alternativa, `NotResource` per l'esclusione.
- È possibile specificare le risorse con un ARN di risorsa S3. Per esempio:

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

- È anche possibile utilizzare variabili di policy all'interno della chiave dell'oggetto. Per esempio:

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

- Il valore della risorsa può specificare un bucket che non esiste ancora al momento della creazione di un criterio di gruppo.

Specificare i principi in una policy

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

- Ogni istruzione di policy in una policy di bucket deve includere un elemento Principal. Le istruzioni di policy in un criterio di gruppo non necessitano dell'elemento Principal perché il gruppo è considerato il principale.
- In una policy, i mandanti sono indicati dall'elemento "Manager" o, in alternativa, "NotManager" 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 nell'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 un gruppo federato specifico ("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 dell'utente anziché il nome utente:

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

  Ad esempio, supponiamo che Alex lasci l'organizzazione e il nome utente `Alex` viene eliminato. Se un nuovo Alex si unisce all'organizzazione e gli viene assegnato lo stesso `Alex` nome utente, il nuovo utente potrebbe ereditare involontariamente i permessi concessi all'utente originale.

- Il valore principale può specificare un nome di gruppo/utente che non esiste ancora al momento della creazione di un criterio bucket.

Specificare le autorizzazioni in una policy

In una policy, l'elemento Azione viene utilizzato per concedere/negare le autorizzazioni a una risorsa. Esiste una serie di autorizzazioni che è possibile specificare in una policy, contrassegnate dall'elemento "Azione" o, in alternativa, "NonAzione" per l'esclusione. Ciascuno di questi elementi è mappato a specifiche operazioni dell'API REST S3.

Nelle tabelle sono elencate le autorizzazioni che si applicano ai bucket e le autorizzazioni che si applicano agli oggetti.

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

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

Autorizzazioni applicabili ai bucket

Permessi	Operazioni API REST S3	Personalizzato per StorageGRID
s3:CreaBucket	CreaBucket	Sì. **Nota**: utilizzare solo nei criteri di gruppo.
s3:EliminaBucket	EliminaBucket	
s3:DeleteBucketMetadataNotification	ELIMINA la configurazione della notifica dei metadati del bucket	SÌ
s3:EliminaBucketPolicy	DeleteBucketPolicy	

Permessi	Operazioni API REST S3	Personalizzato per StorageGRID
s3:EliminaConfigurazioneReplicazione	DeleteBucketReplication	Sì, autorizzazioni separate per PUT e DELETE
s3:GetBucketAcl	OttieniBucketAcl	
s3:GetBucketCompliance	Conformità GET Bucket (obsoleto)	SÌ
s3:GetBucketConsistency	OTTIENI la coerenza del bucket	SÌ
s3:GetBucketCORS	GetBucketCors	
s3:Ottieni configurazione crittografia	Ottieni crittografia dei bucket	
s3:GetBucketLastAccessTime	GET Ora dell'ultimo accesso al bucket	SÌ
s3:OttieniPosizioneBucket	OttieniPosizioneBucket	
s3:GetBucketMetadataNotification	Configurazione della notifica dei metadati del bucket GET	SÌ
s3:OttieniNotificaBucket	Configurazione di notifica di GetBucket	
s3:GetBucketObjectLockConfiguration	Ottieni configurazione blocco oggetto	
s3:GetBucketPolicy	OttieniPoliticaBucket	
s3:OttieniTaggingBucket	OttieniBucketTagging	
s3:GetBucketVersioning	GetBucketVersioning	
s3:GetLifecycleConfiguration	GetBucketLifecycleConfiguration	
s3:OttieniConfigurazioneReplicazione	OttieniReplicazioneBucket	
s3:ElencaTuttiIMieBucket	• ListBuckets • Utilizzo dello spazio di archiviazione GET	Sì, per l'utilizzo dello spazio di archiviazione GET. **Nota**: utilizzare solo nei criteri di gruppo.

Permessi	Operazioni API REST S3	Personalizzato per StorageGRID
s3:ElencoBucket	• ElencoOggetti • HeadBucket • Ripristina oggetto	
s3:ListBucketMultipartUploads	• Caricamenti multiparte di List • Ripristina oggetto	
s3:ListBucketVersions	Versioni GET Bucket	
s3:PutBucketCompliance	Conformità al bucket PUT (obsoleto)	SÌ
s3:PutBucketConsistency	PUT Consistenza del secchio	SÌ
s3:PutBucketCORS	• DeleteBucketCors† • PutBucketCors	
s3:PutEncryptionConfiguration	• DeleteBucketEncryption • PutBucketEncryption	
s3:PutBucketLastAccessTime	Ora dell'ultimo accesso al bucket PUT	SÌ
s3:PutBucketMetadataNotification	Configurazione della notifica dei metadati del bucket PUT	SÌ
s3:PutBucketNotification	Configurazione della notifica PutBucket	
s3:PutBucketObjectLockConfiguration	• CreateBucket con il `x-amz-bucket-object-lock-enabled: true` intestazione della richiesta (richiede anche l'autorizzazione s3:CreateBucket) • PutObjectLockConfiguration	
s3:PoliticaPutBucket	PutBucketPolicy	
s3:PutBucketTagging	• EliminaBucketTagging† • PutBucketTagging	
s3:PutBucketVersioning	PutBucketVersioning	

Permessi	Operazioni API REST S3	Personalizzato per StorageGRID
s3:PutLifecycleConfiguration	• DeleteBucketLifecycle† • Configurazione del ciclo di vita di PutBucket	
s3:PutReplicationConfiguration	PutBucketReplication	Sì, autorizzazioni separate per PUT e DELETE

Autorizzazioni applicabili agli oggetti

Permessi	Operazioni API REST S3	Personalizzato per StorageGRID
s3:AnnullaCaricamentoMultipart	• Annulla caricamento multiparte • Ripristina oggetto	
s3:BypassGovernanceRetention	• EliminaOggetto • EliminaOggetti • PutObjectRetention	
s3:EliminaOggetto	• EliminaOggetto • EliminaOggetti • Ripristina oggetto	
s3:EliminaTaggingOggetto	DeleteObjectTagging	
s3:EliminaObjectVersionTagging	DeleteObjectTagging (una versione specifica dell'oggetto)	
s3:EliminaVersioneOggetto	DeleteObject (una versione specifica dell'oggetto)	
s3:OttieniOggetto	• OttieniOggetto • HeadObject • Ripristina oggetto • SelezionaOggettoContenuto	
s3:GetObjectAcl	OttieniOggettoAcl	
s3:GetObjectLegalHold	OttieniOggettoLegaleHold	

Permessi	Operazioni API REST S3	Personalizzato per StorageGRID
s3:OttieniRitenzioneOggetto	Ottieni conservazione oggetto	
s3:OttieniTaggingOggetto	OttieniTaggingOggetto	
s3:GetObjectVersionTagging	GetObjectTagging (una versione specifica dell'oggetto)	
s3:GetObjectVersion	GetObject (una versione specifica dell'oggetto)	
s3:ListMultipartUploadParts	ListParts, RestoreObject	
s3:PutObject	• MettiOggetto • CopiaOggetto • Ripristina oggetto • CreaCaricamentoMultiparte • Caricamento multiparte completo • CaricaParte • CaricaParteCopia	
s3:PutObjectLegalHold	PutObjectLegalHold	
s3:PutObjectRetention	PutObjectRetention	
s3:PutObjectTagging	PutObjectTagging	
s3:PutObjectVersionTagging	PutObjectTagging (una versione specifica dell'oggetto)	
s3:PutOverwriteObject	• MettiOggetto • CopiaOggetto • PutObjectTagging • DeleteObjectTagging • Caricamento multiparte completo	SÌ
s3:RipristinaOggetto	Ripristina oggetto	

Utilizzare 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 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. Se impostato 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 i tag degli oggetti S3 non possono essere sovrascritti.
    - Tutte le operazioni di acquisizione in corso vengono annullate e viene restituito un errore.
    - Se è abilitato il controllo delle versioni S3, l'impostazione Nega 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 che si avrebbe se fosse impostato Consenti.

> Se l'attuale policy S3 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 i tag degli oggetti. Inoltre, se è selezionata la casella di controllo **Impedisci modifica client** (**CONFIGURAZIONE** > **Impostazioni di sicurezza** > **Rete e oggetti**), tale impostazione sostituisce l'impostazione dell'autorizzazione PutOverwriteObject.

Specificare le condizioni in una policy

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

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

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

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

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

Operatori di condizione supportati

Gli operatori condizionali sono classificati come segue:

- Corda
- Numerico
- Booleano
- indirizzo IP
- Controllo nullo

Operatori di condizione	Descrizione
StringEquals	Confronta una chiave con un valore stringa in base alla corrispondenza esatta (con distinzione tra maiuscole e minuscole).
Stringa non uguale	Confronta una chiave con un valore stringa in base alla corrispondenza negata (sensibile alle maiuscole e alle minuscole).
StringEqualsIgnoreCase	Confronta una chiave con un valore stringa in base alla corrispondenza esatta (ignora la distinzione tra maiuscole e minuscole).
StringNotEqualsIgnoreCase	Confronta una chiave con un valore stringa in base alla corrispondenza negata (ignora la distinzione tra maiuscole e minuscole).
StringLike	Confronta una chiave con un valore stringa in base alla corrispondenza esatta (con distinzione tra maiuscole e minuscole). Può includere i caratteri jolly * e ?.
Stringa non piace	Confronta una chiave con un valore stringa in base alla corrispondenza negata (sensibile alle maiuscole e alle minuscole). Può includere i caratteri jolly * e ?.
NumericEquals	Confronta una chiave con un valore numerico in base alla corrispondenza esatta.
NumericoNonUguale	Confronta una chiave con un valore numerico in base alla corrispondenza negata.
NumericoMaggioreDi	Confronta una chiave con un valore numerico in base alla corrispondenza "maggiore di".
NumericoMaggioreDiUguale	Confronta una chiave con un valore numerico in base alla corrispondenza "maggiore o uguale a".
NumericoMenoDi	Confronta una chiave con un valore numerico in base alla corrispondenza "minore di".

Operatori di condizione	Descrizione
NumericoMinoreUguale	Confronta una chiave con un valore numerico in base alla corrispondenza "minore o uguale".
Bool	Confronta una chiave con un valore booleano in base alla corrispondenza "vero o falso".
Indirizzo IP	Confronta una chiave con un indirizzo IP o un intervallo di indirizzi IP.
NonIndirizzoIP	Confronta una chiave con un indirizzo IP o un intervallo di indirizzi IP in base alla corrispondenza negata.
Nullo	Controlla se una chiave di condizione è presente nel contesto della richiesta corrente.

Chiavi di condizione supportate

Chiavi di condizione	Azioni	Descrizione
aws:SourceIp	operatori IP	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 amministrativi e sui nodi gateway, questa verrà confrontata con l'indirizzo IP a monte del servizio Load Balancer. **Nota**: se viene utilizzato un bilanciatore del carico di terze parti non trasparente, questo verrà confrontato con l'indirizzo IP di tale bilanciatore del carico. Qualunque `X-Forwarded-For` l'intestazione verrà ignorata perché non è possibile accertarne la validità.
aws:nome utente	Risorsa/Identità	Verrà confrontato con il nome utente del mittente da cui è stata inviata la richiesta. Può essere utilizzato per operazioni su bucket o oggetti.
s3:delimitatore	s3:ListBucket e s3:permessi ListBucketVersions	Verrà confrontato con il parametro delimitatore specificato in una richiesta ListObjects o ListObjectVersions.

Chiavi di condizione	Azioni	Descrizione
s3:ExistingObjectTag/<chiave-tag>	s3:EliminaTaggingOggetto s3:EliminaObjectVersionTagging s3:OttieniOggetto s3:GetObjectAcl 3: Ottieni tag oggetto s3:GetObjectVersion s3:GetObjectVersionAcl s3:GetObjectVersionTagging s3:PutObjectAcl s3:PutObjectTagging s3:PutObjectVersionAcl s3:PutObjectVersionTagging	Richiederà che l'oggetto esistente abbia la chiave e il valore del tag specifici.
s3:max-chiavi	s3:ListBucket e s3:permessi ListBucketVersions	Verrà confrontato con il parametro max-keys specificato in una richiesta ListObjects o ListObjectVersions.
s3:giorni di conservazione rimanenti del blocco dell'oggetto	s3:PutObject	Confronta con la data di conservazione specificata in `x-amz-object-lock-retain-until-date` intestazione della richiesta o calcolata dal periodo di conservazione predefinito del bucket per assicurarsi che questi valori siano compresi nell'intervallo consentito per le seguenti richieste: • MettiOggetto • CopiaOggetto • CreaCaricamentoMultiparte
s3:giorni di conservazione rimanenti del blocco dell'oggetto	s3:PutObjectRetention	Confronta con la retain-until-date specificata nella richiesta PutObjectRetention per garantire che rientri nell'intervallo consentito.

Chiavi di condizione	Azioni	Descrizione
s3:prefisso	s3:ListBucket e s3:permessi ListBucketVersions	Verrà confrontato con il parametro prefisso specificato in una richiesta ListObjects o ListObjectVersions.
s3:RequestObjectTag/<chiave-tag>	s3:PutObject s3:PutObjectTagging s3:PutObjectVersionTagging	Richiederà una chiave e un valore tag specifici quando la richiesta dell'oggetto include il tagging.

Specificare le variabili in una policy

È possibile utilizzare le variabili nelle policy per popolare le informazioni sulle policy quando sono disponibili. È possibile utilizzare le variabili di policy in `Resource` elemento e nei confronti di stringhe in `Condition` elemento.

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

```
"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 condizioni:

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

Variabile	Descrizione
`${aws:SourceIp}`	Utilizza la chiave SourceIp come variabile fornita.
`${aws:username}`	Utilizza la chiave nome utente 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.

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

Creare politiche che richiedono una gestione speciale

Talvolta una policy può concedere autorizzazioni pericolose per la sicurezza o per il proseguimento delle operazioni, ad esempio bloccando l'utente root dell'account. L'implementazione dell'API REST S3 StorageGRID è meno restrittiva durante la convalida delle policy rispetto ad Amazon, ma altrettanto rigorosa durante la valutazione delle policy.

Descrizione della politica	Tipo di polizza	Comportamento di Amazon	Comportamento StorageGRID
Nega a te stesso qualsiasi autorizzazione all'account root	Secchio	Valido e applicato, ma l'account utente root mantiene l'autorizzazione per tutte le operazioni dei criteri del bucket S3	Stesso
Nega a te stesso qualsiasi autorizzazione all'utente/gruppo	Gruppo	Valido e applicato	Stesso
Consentire qualsiasi autorizzazione a un gruppo di account esteri	Secchio	Principale non valido	Valido, ma le autorizzazioni per tutte le operazioni di policy del bucket S3 restituiscono un errore 405 Metodo non consentito quando consentito da una policy
Consentire a un account esterno root o utente qualsiasi autorizzazione	Secchio	Valido, ma le autorizzazioni per tutte le operazioni di policy del bucket S3 restituiscono un errore 405 Metodo non consentito quando consentito da una policy	Stesso

Descrizione della politica	Tipo di polizza	Comportamento di Amazon	Comportamento StorageGRID
Consenti a tutti i permessi per tutte le azioni	Secchio	Valido, ma le autorizzazioni per tutte le operazioni di policy del bucket S3 restituiscono un errore 405 Metodo non consentito per l'account esterno root e gli utenti	Stesso
Nega a tutti i permessi per tutte le azioni	Secchio	Valido e applicato, ma l'account utente root mantiene l'autorizzazione per tutte le operazioni dei criteri del bucket S3	Stesso
Il principale è un utente o un gruppo inesistente	Secchio	Principale non valido	Valido
La risorsa è un bucket S3 inesistente	Gruppo	Valido	Stesso
Principal è un gruppo locale	Secchio	Principale non valido	Valido
La policy concede a un account non proprietario (inclusi gli account anonimi) l'autorizzazione a inserire oggetti.	Secchio	Valido. Gli oggetti sono di proprietà dell'account del creatore e la policy del bucket non si applica. L'account del creatore deve concedere le autorizzazioni di accesso per l'oggetto utilizzando gli ACL degli oggetti.	Valido. Gli oggetti sono di proprietà dell'account proprietario del bucket. Si applica la politica dei 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. È possibile configurare i bucket WORM per consentire la creazione di nuovi oggetti e impedire la sovrascrittura o l'eliminazione di contenuti esistenti. Utilizzare uno degli approcci descritti qui.

Per garantire che le sovrascritture vengano sempre negate, puoi:

- Da Grid Manager, vai su **CONFIGURAZIONE** > **Sicurezza** > **Impostazioni di sicurezza** > **Rete e oggetti** e seleziona la casella di controllo **Impedisci modifiche client**.
- Applicare le seguenti regole e policy S3:
  - Aggiungere un'operazione PutOverwriteObject DENY al criterio S3.
  - Aggiungere un'operazione DeleteObject DENY al criterio S3.
  - Aggiungere un'operazione PutObject ALLOW al criterio S3.

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

Anche quando vengono applicate tutte queste regole e policy, non proteggono dalle scritture simultanee (vedere Situazione A). 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 (protette contro)

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

Informazioni correlate

- "Come le regole StorageGRID ILM gestiscono gli oggetti"
- "Criteri di esempio per i bucket"
- "Criteri di gruppo di esempio"
- "Gestire gli oggetti con ILM"
- "Utilizzare un account tenant"

Criteri di esempio per i bucket

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

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

- "Responsabile degli inquilini" .
- AWS CLI utilizzando questo comando (fare riferimento a"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 l'utente anonimo, è consentito elencare gli oggetti nel bucket ed eseguire operazioni GetObject su tutti gli oggetti nel bucket. Tutte le altre operazioni saranno negate. Si noti che questa

policy potrebbe non essere particolarmente utile perché nessuno, eccetto l'account root, 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: 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 di elencare il bucket ed eseguire operazioni GetObject sugli oggetti nel bucket a partire da `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. A questi oggetti si applica la policy bucket.

```
{
  "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 al gruppo specificato

In questo esempio, a tutti, incluso l'utente 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 è consentito l'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: consentire a tutti l'accesso in lettura e scrittura a un bucket se il client è nell'intervallo IP

In questo esempio, a tutti, compresi gli utenti anonimi, è consentito elencare il bucket ed eseguire qualsiasi operazione sugli oggetti 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 negate e tutte le richieste al di fuori dell'intervallo IP verranno 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: consentire l'accesso completo a un bucket esclusivamente a un utente federato specificato

In questo esempio, all'utente federato Alex è consentito l'accesso completo a `examplebucket` secchio e i suoi oggetti. A tutti gli altri utenti, compreso 'root', viene esplicitamente negata qualsiasi operazione. Si noti tuttavia che a 'root' non vengono mai negati i permessi 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, il `Deny` L'effetto di PutOverwriteObject e DeleteObject garantisce che nessuno possa sovrascrivere o eliminare i dati dell'oggetto, i metadati definiti dall'utente e il tagging dell'oggetto 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 in 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 c'è `Principal` elemento nella politica perché è implicito. I criteri di gruppo vengono configurati tramite Tenant Manager o API.

Esempio: impostare i criteri di gruppo utilizzando 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. 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 venga concesso tramite un criterio bucket. Se si seleziona questa opzione, per impostazione predefinita solo l'utente root avrà accesso alle risorse S3.
- **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 oggetti e leggere dati, metadati e tag degli oggetti. Quando si seleziona questa opzione, nella casella di testo viene visualizzata la stringa JSON per un criterio di gruppo di sola lettura. Non puoi 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 con accesso completo. 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 gli oggetti dai bucket in cui è abilitato il controllo delle versioni degli oggetti.

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

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

Esempio: consentire 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 tenant, a meno che non venga esplicitamente negato dalla policy del bucket.

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

Esempio: consentire al gruppo l'accesso 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 venga esplicitamente negato dai criteri del bucket. Ad esempio, gli utenti di questo gruppo possono elencare oggetti e leggere dati, metadati e 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: consentire ai membri del gruppo l’accesso completo solo alla loro "cartella" in un bucket

In questo esempio, ai membri del gruppo è consentito solo elencare e accedere alla propria cartella specifica (prefisso chiave) nel bucket specificato. Si noti che quando si determina la privacy di queste cartelle, è necessario prendere in considerazione le autorizzazioni di accesso provenienti da altri criteri di gruppo e dai criteri 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