# Creare o modificare le dichiarazioni dei criteri di accesso

ONTAP 9

NetApp
April 24, 2024

# Sommario

# Creare o modificare le dichiarazioni dei criteri di accesso

## Informazioni sulle policy dei server bucket e degli archivi di oggetti

L'accesso degli utenti e dei gruppi alle risorse S3 è controllato dalle policy del server bucket e dell'archivio di oggetti. Se si dispone di un numero limitato di utenti o gruppi, probabilmente è sufficiente controllare l'accesso a livello di bucket, ma se si dispone di molti utenti e gruppi, è più semplice controllare l'accesso a livello di server dell'archivio di oggetti.

## Modificare una policy bucket

È possibile aggiungere regole di accesso al criterio bucket predefinito. L'ambito del controllo degli accessi è il bucket contenente, quindi è più appropriato quando è presente un singolo bucket.

**Prima di iniziare**

Una VM di storage abilitata per S3 contenente un server S3 e un bucket deve già esistere.

Prima di concedere le autorizzazioni, è necessario aver già creato utenti o gruppi.

**A proposito di questa attività**

È possibile aggiungere nuove istruzioni per nuovi utenti e gruppi oppure modificare gli attributi delle istruzioni esistenti. Per ulteriori opzioni, vedere `vserver object-store-server bucket policy` pagine man.

Le autorizzazioni per utenti e gruppi possono essere concesse al momento della creazione del bucket o in seguito in base alle necessità. È inoltre possibile modificare la capacità del bucket e l'assegnazione del gruppo di policy QoS.

A partire da ONTAP 9,9.1, se si prevede di supportare la funzionalità di tagging degli oggetti client AWS con il server ONTAP S3, le azioni `GetObjectTagging`, `PutObjectTagging`, e. `DeleteObjectTagging` devono essere consentite utilizzando le policy di gruppo o bucket.

La procedura da seguire dipende dall'interfaccia in uso - System Manager o CLI:

**System Manager**

**Fasi**

1. Modificare il bucket: Fare clic su **Storage > Bucket**, fare clic sul bucket desiderato, quindi su **Edit** (Modifica). Quando si aggiungono o modificano le autorizzazioni, è possibile specificare i seguenti parametri:
   - **Principal**: L'utente o il gruppo a cui viene concesso l'accesso.
   - **Effect**: Consente o nega l'accesso a un utente o a un gruppo.
   - **Azioni**: Azioni consentite nel bucket per un dato utente o gruppo.
   - **Resources**: Percorsi e nomi degli oggetti all'interno del bucket per i quali viene concesso o negato l'accesso.

     I valori predefiniti ***bucketname*** e ***bucketname/**** concedono l'accesso a tutti gli oggetti nel bucket. È inoltre possibile concedere l'accesso a singoli oggetti, ad esempio ***nome_carico di lavoro/*_readme.txt***.

   - **Condizioni** (opzionale): Espressioni che vengono valutate al tentativo di accesso. Ad esempio, è possibile specificare un elenco di indirizzi IP per i quali l'accesso verrà consentito o negato.

> A partire da ONTAP 9.14.1, è possibile specificare le variabili per il criterio bucket nel campo **risorse**. Queste variabili sono segnaposto che vengono sostituiti con valori contestuali quando il criterio viene valutato. Ad esempio, se `${aws:username}` viene specificata come variabile per un criterio, quindi questa variabile viene sostituita con il nome utente del contesto della richiesta e l'azione del criterio può essere eseguita come configurato per quell'utente.

**CLI**

**Fasi**

1. Aggiungere una dichiarazione a una policy bucket:

   ```
   vserver object-store-server bucket policy add-statement -vserver svm_name
   -bucket bucket_name -effect {allow|deny} -action object_store_actions
   -principal user_and_group_names -resource object_store_resources [-sid
   text] [-index integer]
   ```

   I seguenti parametri definiscono le autorizzazioni di accesso:

| | |
|---|---|
| `-effect` | L'istruzione può consentire o negare l'accesso |
| `-action` | È possibile specificare `*` per tutte le azioni o un elenco di una o più delle seguenti azioni: `GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl,GetObjectAcl, ListBucketMultipartUploads,` e. `ListMultipartUploadParts`. |

| | |
|---|---|
| `-principal` | Un elenco di uno o più utenti o gruppi S3.<br>• È possibile specificare un massimo di 10 utenti o gruppi.<br>• Se viene specificato un gruppo S3, deve essere nel modulo `group/group_name`.<br>• `*` può essere specificato per indicare l'accesso pubblico, ovvero l'accesso senza chiave di accesso e chiave segreta.<br>• Se non viene specificato alcun principal, a tutti gli utenti S3 nella VM di storage viene concesso l'accesso. |
| `-resource` | Il bucket e qualsiasi oggetto in esso contenuto. I caratteri jolly `*` e. `?` può essere utilizzato per formare un'espressione regolare per specificare una risorsa. Per una risorsa, è possibile specificare le variabili in un criterio. Si tratta di variabili dei criteri, che vengono sostituite con i valori contestuali al momento della valutazione del criterio. |

È possibile specificare una stringa di testo come commento con `-sid` opzione.

**Esempi**

Nell'esempio seguente viene creata un'istruzione del criterio del bucket del server di archiviazione oggetti per la VM di archiviazione svm1.example.com e bucket1 che specifica l'accesso consentito a una cartella Leggimi per l'utente del server di archiviazione oggetti user1.

```
cluster1::> vserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal user1 -resource
bucket1/readme/* -sid "fullAccessToReadmeForUser1"
```

Nell'esempio seguente viene creata un'istruzione dei criteri del bucket server di archivio oggetti per la VM di storage svm1.example.com e bucket1 che specifica l'accesso consentito a tutti gli oggetti per il gruppo di server di archivio oggetti group1.

```
cluster1::> vserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal group/group1
-resource bucket1/* -sid "fullAccessForGroup1"
```

A partire da ONTAP 9.14.1, è possibile specificare le variabili per un criterio bucket. Nell'esempio seguente viene creata un'istruzione del criterio bucket server per la VM di storage `svm1` e. `bucket1`, e specifica `${aws:username}` come variabile per una risorsa di criterio. Quando il criterio viene valutato, la variabile di criterio viene sostituita con il nome utente del contesto della richiesta e l'azione del criterio può essere eseguita come configurato per quell'utente. Ad esempio, quando viene valutata la seguente istruzione di criterio, `${aws:username}` Viene sostituito con l'utente che esegue l'operazione S3. Se un utente `user1` esegue l'operazione, a cui l'utente può accedere `bucket1` come `bucket1/user1/*`.

```
cluster1::> object-store-server bucket policy statement create -vserver
svm1 -bucket bucket1 -effect allow -action * -principal - -resource
bucket1,bucket1/${aws:username}/*##
```

# Creare o modificare un criterio del server di archiviazione oggetti

È possibile creare policy applicabili a uno o più bucket in un archivio di oggetti. È possibile collegare le policy del server dell'archivio di oggetti a gruppi di utenti, semplificando in tal modo la gestione dell'accesso alle risorse in più bucket.

**Prima di iniziare**

Una SVM abilitata per S3 contenente un server S3 e un bucket deve già esistere.

**A proposito di questa attività**

È possibile attivare i criteri di accesso a livello di SVM specificando un criterio predefinito o personalizzato in un gruppo di server di storage a oggetti. I criteri non hanno effetto fino a quando non vengono specificati nella definizione di gruppo.

> Quando si utilizzano i criteri del server di storage a oggetti, si specificano le entità (ovvero utenti e gruppi) nella definizione di gruppo, non nel criterio stesso.

Esistono tre criteri predefiniti di sola lettura per l'accesso alle risorse di ONTAP S3:

- Accesso completo
- NoS3Accesso
- ReadOnlyAccess

È inoltre possibile creare nuovi criteri personalizzati, quindi aggiungere nuove istruzioni per nuovi utenti e gruppi oppure modificare gli attributi delle istruzioni esistenti. Per ulteriori opzioni, vedere `vserver object-store-server policy` "riferimento al comando".

A partire da ONTAP 9,9.1, se si prevede di supportare la funzionalità di tagging degli oggetti client AWS con il server ONTAP S3, le azioni `GetObjectTagging`, `PutObjectTagging`, e. `DeleteObjectTagging` devono essere consentite utilizzando le policy di gruppo o bucket.

La procedura da seguire dipende dall'interfaccia in uso - System Manager o CLI:

**System Manager**

**Utilizzare System Manager per creare o modificare un criterio del server archivio oggetti**

**Fasi**

1. Modificare la VM di storage: Fare clic su **Storage > Storage VM**, fare clic sulla VM di storage, fare clic su **Settings** (Impostazioni), quindi su Sotto S3.
2. Aggiungere un utente: Fare clic su **Policies**, quindi su **Add**.
   a. Inserire un nome di policy e selezionarlo da un elenco di gruppi.
   b. Selezionare un criterio predefinito esistente o aggiungerne uno nuovo.

      Quando si aggiunge o si modifica un criterio di gruppo, è possibile specificare i seguenti parametri:

      - Group (Gruppo): I gruppi ai quali viene concesso l'accesso.
      - Effetto: Consente o nega l'accesso a uno o più gruppi.
      - Azioni: Azioni consentite in uno o più bucket per un dato gruppo.
      - Resources (risorse): Percorsi e nomi di oggetti all'interno di uno o più bucket per i quali l'accesso viene concesso o negato. Ad esempio:
        - ***** Garantisce l'accesso a tutti i bucket nella VM di storage.
        - **bucketname** e **bucketname/*** concedono l'accesso a tutti gli oggetti in un bucket specifico.
        - **bucketname/readme.txt** concede l'accesso a un oggetto in un bucket specifico.
   c. Se lo si desidera, aggiungere le istruzioni ai criteri esistenti.

**CLI**

**Utilizzare la CLI per creare o modificare un criterio del server archivio oggetti**

**Fasi**

1. Creare un criterio del server di storage a oggetti:

   ```
   vserver object-store-server policy create -vserver svm_name -policy
   policy_name [-comment text]
   ```

2. Creare un'istruzione per la policy:

   ```
   vserver object-store-server policy statement create -vserver svm_name
   -policy policy_name -effect {allow|deny} -action object_store_actions
   -resource object_store_resources [-sid text]
   ```

   I seguenti parametri definiscono le autorizzazioni di accesso:

| | |
|---|---|
| `-effect` | L'istruzione può consentire o negare l'accesso |

| | |
|---|---|
| `-action` | È possibile specificare `*` per tutte le azioni o un elenco di una o più delle seguenti azioni: `GetObject, PutObject, DeleteObject, ListBucket,GetBucketAcl, GetObjectAcl, ListAllMyBuckets, ListBucketMultipartUploads`, e. `ListMultipartUploadParts`. |
| `-resource` | Il bucket e qualsiasi oggetto in esso contenuto. I caratteri jolly `*` e. `?` può essere utilizzato per formare un'espressione regolare per specificare una risorsa. |

È possibile specificare una stringa di testo come commento con `-sid` opzione.

Per impostazione predefinita, le nuove dichiarazioni vengono aggiunte alla fine dell'elenco delle dichiarazioni, che vengono elaborate in ordine. Quando si aggiungono o modificano le dichiarazioni in un secondo momento, è possibile modificarle `-index` impostazione per modificare l'ordine di elaborazione.

# Configurare l'accesso S3 per i servizi di directory esterni

A partire da ONTAP 9.14.1, i servizi per le directory esterne sono stati integrati con lo storage a oggetti ONTAP S3. Questa integrazione semplifica la gestione degli utenti e degli accessi tramite servizi di directory esterni.

È possibile fornire ai gruppi utente appartenenti a un servizio di directory esterno l'accesso all'ambiente di storage a oggetti ONTAP. LDAP (Lightweight Directory Access Protocol) è un'interfaccia per la comunicazione con i servizi di directory, come Active Directory, che forniscono un database e servizi per la gestione delle identità e degli accessi (IAM). Per fornire l'accesso, è necessario configurare i gruppi LDAP nell'ambiente ONTAP S3. Dopo aver configurato l'accesso, i membri del gruppo dispongono delle autorizzazioni per i bucket di ONTAP S3. Per informazioni su LDAP, vedere "Panoramica sull'utilizzo di LDAP".

È inoltre possibile configurare i gruppi di utenti di Active Directory per la modalità di associazione rapida, in modo che le credenziali utente possano essere convalidate e le applicazioni S3 di terze parti e open-source possano essere autenticate tramite connessioni LDAP.

**Prima di iniziare**

Prima di configurare i gruppi LDAP e attivare la modalità di associazione rapida per l'accesso ai gruppi, verificare quanto segue:

1. È stata creata una macchina virtuale di storage abilitata per S3 contenente un server S3. Vedere "Creare una SVM per S3".
2. È stato creato un bucket in quella VM per lo storage. Vedere "Creare un bucket".
3. Il DNS è configurato sulla macchina virtuale di storage. Vedere "Configurare i servizi DNS".
4. Sulla VM di storage viene installato un certificato CA (root Certification Authority) autofirmato del server LDAP. Vedere "Installare il certificato della CA principale autofirmato su SVM".

5. Un client LDAP è configurato con TLS attivato nella SVM. Vedere "Creare una configurazione del client LDAP" e. "Associare la configurazione del client LDAP alle SVM per ottenere informazioni".

## Configurare l'accesso S3 per i servizi di directory esterni

1. Specificare LDAP come *name service database* della SVM per il gruppo e la password per LDAP:

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

   Per ulteriori informazioni su questo comando, vedere "modifica del ns-switch del name service dei servizi vserver" comando.

2. Creare un'istruzione del criterio del bucket dell'archivio oggetti con il `principal` Impostare sul gruppo LDAP a cui si desidera concedere l'accesso:

```
object-store-server bucket policy statement create -bucket <bucket-name>
-effect allow -principal nasgroup/<ldap-group-name> -resource <bucket-
name>, <bucket-name>/*
```

   Esempio: Nell'esempio seguente viene creata un'istruzione criterio bucket per `buck1`. Il criterio consente l'accesso al gruppo LDAP `group1` alla risorsa (bucket e relativi oggetti) `buck1`.

```
vserver object-store-server bucket policy add-statement -bucket buck1
-effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,Li
stBucketMultipartUploads,ListMultipartUploadParts,
ListBucketVersions,GetObjectTagging,PutObjectTagging,DeleteObjectTagging
,GetBucketVersioning,PutBucketVersioning -principal nasgroup/group1
-resource buck1, buck1/*
```

3. Verificare che un utente del gruppo LDAP `group1` È in grado di eseguire operazioni S3 dal client S3.

## Utilizzare la modalità di associazione rapida LDAP per l'autenticazione

1. Specificare LDAP come *name service database* della SVM per il gruppo e la password per LDAP:

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

Per ulteriori informazioni su questo comando, vedere "modifica del ns-switch del name service dei servizi vserver" comando.

2. Assicurarsi che un utente LDAP che accede al bucket S3 disponga delle autorizzazioni definite nei criteri bucket. Per ulteriori informazioni, vedere "Modificare una policy bucket".
3. Verificare che un utente del gruppo LDAP possa eseguire le seguenti operazioni:
   a. Configurare la chiave di accesso sul client S3 in questo formato:
      `"NTAPFASTBIND" + base64-encode(user-name:password)`
      Esempio: `"NTAPFASTBIND"` + base64-encode(ldapuser:password), che risulta in `NTAPFASTBINDbGRhcHVzZXI6cGFzc3dvcmQ=`

      > Il client S3 potrebbe richiedere una chiave segreta. In assenza di una chiave segreta, è possibile immettere qualsiasi password di almeno 16 caratteri.

   b. Eseguire operazioni S3 di base dal client S3 per cui l'utente dispone delle autorizzazioni.

# Consentire agli utenti LDAP o di dominio di generare le proprie chiavi di accesso S3

A partire da ONTAP 9.14.1, in qualità di amministratore ONTAP, è possibile creare ruoli personalizzati e concederli a gruppi locali o di dominio o a gruppi LDAP (Lightweight Directory Access Protocol), in modo che gli utenti appartenenti a tali gruppi possano generare le proprie chiavi di accesso e segrete per l'accesso client S3.

Devi eseguire alcuni passaggi di configurazione sulla macchina virtuale di storage, in modo che sia possibile creare e assegnare il ruolo personalizzato all'utente che richiama l'API per la generazione delle chiavi di accesso.

**Prima di iniziare**

Verificare quanto segue:

1. È stata creata una macchina virtuale di storage abilitata per S3 contenente un server S3. Vedere "Creare una SVM per S3".
2. È stato creato un bucket in quella VM per lo storage. Vedere "Creare un bucket".
3. Il DNS è configurato sulla macchina virtuale di storage. Vedere "Configurare i servizi DNS".
4. Sulla VM di storage viene installato un certificato CA (root Certification Authority) autofirmato del server LDAP. Vedere "Installare il certificato della CA principale autofirmato su SVM".
5. Un client LDAP è configurato con TLS attivato sulla macchina virtuale di storage. Vedere "Creare una configurazione del client LDAP" e .
6. Associare la configurazione del client al Vserver. Vedere "Associare la configurazione del client LDAP alle SVM" e. "creazione ldap del nome del servizio vserver".
7. Se stai utilizzando una macchina virtuale per lo storage dei dati, crea un'interfaccia di rete di gestione (LIF) e una macchina virtuale, oltre a una policy di servizio per la LIF. Vedere "creazione dell'interfaccia di rete" e. "creazione della politica di servizio dell'interfaccia di rete" comandi.

## Configurare gli utenti per la generazione delle chiavi di accesso

1. Specificare LDAP come *name service database* della VM di archiviazione per il gruppo e la password per LDAP:

   ```
   ns-switch modify -vserver <vserver-name> -database group -sources
   files,ldap
   ns-switch modify -vserver <vserver-name> -database passwd -sources
   files,ldap
   ```

   Per ulteriori informazioni su questo comando, vedere "modifica del ns-switch del name service dei servizi vserver" comando.

2. Creare un ruolo personalizzato con accesso all'endpoint API REST per S3 utenti:
   `security login rest-role create -vserver <vserver-name> -role <custom-role-name> -api "/api/protocols/s3/services/*/users" -access <access-type>`
   In questo esempio, il `s3-role` Viene generato un ruolo per gli utenti sulla VM di storage `svm-1`, a cui vengono concessi tutti i diritti di accesso, lettura, creazione e aggiornamento.

   ```
   security login rest-role create -vserver svm-1 -role s3role -api
   "/api/protocols/s3/services/*/users" -access all
   ```

   Per ulteriori informazioni su questo comando, vedere "accesso di sicurezza creazione ruolo di pausa" comando.

3. Creare un gruppo di utenti LDAP con il comando di accesso alla sicurezza e aggiungere il nuovo ruolo personalizzato per accedere all'endpoint dell'API REST utente S3. Per ulteriori informazioni su questo comando, vedere "creazione dell'accesso di sicurezza" comando.

   ```
   security login create -user-or-group-name <ldap-group-name> -application
   http -authentication-method nsswitch -role <custom-role-name> -is-ns
   -switch-group yes
   ```

   In questo esempio, il gruppo LDAP `ldap-group-1` viene creato in `svm-1`e il ruolo personalizzato `s3role` Viene aggiunto per accedere all'endpoint API, oltre ad abilitare l'accesso LDAP in modalità di associazione rapida.

   ```
   security login create -user-or-group-name ldap-group-1 -application http
   -authentication-method nsswitch -role s3role -is-ns-switch-group yes
   -second-authentication-method none -vserver svm-1 -is-ldap-fastbind yes
   ```

   Per ulteriori informazioni, vedere "Utilizza il binding rapido LDAP per l'autenticazione nsswitch".

L'aggiunta del ruolo personalizzato al dominio o al gruppo LDAP consente agli utenti di quel gruppo di accedere in modo limitato a ONTAP `/api/protocols/s3/services/{svm.uuid}/users` endpoint.

Richiamando l'API, gli utenti del dominio o del gruppo LDAP possono generare il proprio accesso e le proprie chiavi segrete per accedere al client S3. Possono generare le chiavi solo per se stessi e non per altri utenti.

## Come utente S3 o LDAP, generare le proprie chiavi di accesso

A partire da ONTAP 9.14.1, è possibile generare le proprie chiavi di accesso e segrete per l'accesso ai client S3, se l'amministratore ha concesso il ruolo di generazione delle proprie chiavi. Puoi generare le chiavi solo per te utilizzando il seguente endpoint dell'API REST ONTAP.

#### Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti. Per informazioni sugli altri metodi di questo endpoint, vedere il riferimento "Documentazione API".

| Metodo HTTP | Percorso |
|---|---|
| POST | /api/protocolli/s3/servizi/{svm.uuid}/utenti |

#### Esempio di arricciamento

```
curl
--request POST \
--location "https://$FQDN_IP /api/protocols/s3/services/{svm.uuid}/users "
\
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
--data '{"name":"_name_"}'
```

**Esempio di output JSON**


```
{
  "records": [
    {
      "access_key":
"Pz3SB54G2B_6dsXQPrA5HrTPcf478qoAW6_Xx6qyqZ948AgZ_7YfCf_9nO87YoZmskxx3cq41
U2JAH2M3_fs321B4rkzS3a_oC5_8u7D8j_45N8OsBCBPWGD_1d_ccfq",
      "_links": {
        "next": {
          "href": "/api/resourcelink"
        },
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user-1",
      "secret_key":
"A20_tDhC_cux2C2BmtL45bXB_a_Q65c_96FsAcOdo14Az8V31jBKDTc0uCL62Bh559gPB8s9r
rn0868QrF38_1dsV2u1_9H2tSf3qQ5xp9NT259C6z_GiZQ883Qn63X1"
    }
  ],
  "num_records": "1"
}
```