



Controllo degli accessi in SnapDrive per UNIX

Snapdrive for Unix

NetApp
October 04, 2023

This PDF was generated from https://docs.netapp.com/it-it/snapdrive-unix/aix/concept_what_access_control_settings_are.html on October 04, 2023. Always check docs.netapp.com for the latest.

Sommario

- Controllo degli accessi in SnapDrive per UNIX 1
 - Quali sono le impostazioni di controllo degli accessi 1
 - Livelli di controllo degli accessi disponibili 2
 - Impostazione dell'autorizzazione per il controllo degli accessi 2
 - Visualizzazione dell'autorizzazione per il controllo degli accessi 3

Controllo degli accessi in SnapDrive per UNIX

SnapDrive per UNIX consente di controllare il livello di accesso di ciascun host a ciascun sistema storage a cui è connesso l'host.

Il livello di accesso in SnapDrive per UNIX indica le operazioni che l'host può eseguire quando si rivolge a un determinato sistema storage. Ad eccezione delle operazioni di visualizzazione ed elenco, le autorizzazioni per il controllo degli accessi possono influire su tutte le operazioni Snapshot e di storage.

Quali sono le impostazioni di controllo degli accessi

Per determinare l'accesso dell'utente, SnapDrive per UNIX controlla uno dei due file di permessi nel volume root del sistema di storage. Per valutare il controllo dell'accesso, è necessario controllare le regole impostate in tale file.

- `sdhost-name.prbac` il file si trova nella directory `/vol/vol0/sdprbac` (SnapDrive consente il controllo degli accessi basato sui ruoli).

Il nome del file è `sdhost-name.prbac`, dove *host-name* è il nome dell'host a cui si applicano le autorizzazioni. È possibile disporre di un file di autorizzazioni per ciascun host collegato al sistema di storage. È possibile utilizzare `snapdrive config access` per visualizzare informazioni sulle autorizzazioni disponibili per un host su un sistema storage specifico.

Se il `sdhost-name.prbac` non esiste, quindi utilizzare `sdgeneric.prbac` file per controllare le autorizzazioni di accesso.

- `sdgeneric.prbac` il file si trova anche nella directory `/vol/vol0/sdprbac`.

Il nome del file `sdgeneric.prbac` viene utilizzato come impostazioni di accesso predefinite per più host a cui non è possibile accedere `sdhost-name.prbac` sul sistema storage.

Se avete entrambi `sdhost-name.prbac` e `sdgeneric.prbac` file disponibili in `/vol/vol0/sdprbac` quindi utilizzare `sdhost-name.prbac` per controllare le autorizzazioni di accesso, in quanto sovrascrivono i valori forniti per `sdgeneric.prbac` file.

Se non si dispone di entrambe le opzioni `sdhost-name.prbac` e `sdgeneric.prbac` quindi controllare la variabile di configurazione `all-access-if-rbac-unspecified` definito in `snapdrive.conf` file.

L'impostazione del controllo degli accessi da un host a una determinata unità vFiler è un'operazione manuale. L'accesso da un determinato host è controllato da un file che risiede nel volume root dell'unità vFiler interessata. Il file contiene `/vol/<vfiler root volume>/sdprbac/sdhost-name.prbac`, dove il *host-name* è il nome dell'host interessato, come restituito da `gethostname(3)`. Assicurarsi che il file sia leggibile, ma non scrivibile, dall'host che può accedervi.



Per determinare il nome dell'host, eseguire `hostname` comando.

Se il file è vuoto, illeggibile o ha un formato non valido, SnapDrive per UNIX non concede all'host l'accesso a nessuna delle operazioni.

Se il file non è presente, SnapDrive per UNIX controlla la variabile di configurazione `all-access-if-rbac-`

unspecified in `snapdrive.conf` file. Se la variabile è impostata su `on` (valore predefinito), consente agli host di accedere a tutte queste operazioni sul sistema storage. Se la variabile è impostata su `off`, SnapDrive per UNIX nega l'autorizzazione dell'host per eseguire qualsiasi operazione regolata dal controllo dell'accesso su tale sistema di storage.

Livelli di controllo degli accessi disponibili

SnapDrive per UNIX offre agli utenti diversi livelli di controllo degli accessi. Questi livelli di accesso sono correlati alle copie Snapshot e alle operazioni del sistema di storage.

È possibile impostare i seguenti livelli di accesso:

- **NESSUNO** — l'host non ha accesso al sistema di storage.
- **CREAZIONE SNAP**: L'host può creare copie Snapshot.
- **UTILIZZO DI SNAP**: L'host può eliminare e rinominare le copie Snapshot.
- **SNAP ALL (SNAP TUTTO)**: L'host può creare, ripristinare, eliminare e rinominare le copie Snapshot.
- **STORAGE CREATE DELETE (ELIMINA CREAZIONE STORAGE)**: L'host può creare, ridimensionare ed eliminare lo storage.
- **UTILIZZO DELLO STORAGE**: L'host può connettere e disconnettere lo storage ed eseguire anche la stima del clone split e l'avvio del clone split sullo storage.
- **STORAGE ALL (TUTTO STORAGE)**: L'host può creare, eliminare, connettere e disconnettere lo storage ed eseguire anche la stima della divisione dei cloni e l'avvio della divisione dei cloni sullo storage.
- **TUTTI GLI ACCESSI** — l'host ha accesso a tutte le precedenti operazioni SnapDrive per UNIX.

Ogni livello è distinto. Se si specifica l'autorizzazione solo per determinate operazioni, SnapDrive per UNIX può eseguire solo tali operazioni. Ad esempio, se si specifica L'UTILIZZO DELLO STORAGE, l'host può utilizzare SnapDrive per UNIX per connettere e disconnettere lo storage, ma non può eseguire altre operazioni governate dalle autorizzazioni di controllo degli accessi.

Impostazione dell'autorizzazione per il controllo degli accessi

È possibile impostare l'autorizzazione per il controllo degli accessi in SnapDrive per UNIX creando una directory e un file speciali nel volume root del sistema di storage.

Assicurarsi di aver effettuato l'accesso come utente root.

Fasi

1. Creare la directory `sdprbac` nel volume root del sistema storage di destinazione.

Un modo per rendere accessibile il volume root è montare il volume utilizzando NFS.

2. Creare il file delle autorizzazioni in `sdprbac` directory. Assicurarsi che le seguenti affermazioni siano vere:
 - Il file deve essere denominato `sdhost-name.prbac` dove `host-name` è il nome dell'host per cui si specificano le autorizzazioni di accesso.
 - Il file deve essere di sola lettura per garantire che SnapDrive per UNIX possa leggerlo, ma che non possa essere modificato.

Per assegnare a un host il permesso di accesso dev-sun1, creare il seguente file sul sistema storage:
`/vol/vol1/sdprbac/sddev-sun1.prbac`

3. Impostare le autorizzazioni nel file per l'host.

Per il file è necessario utilizzare il seguente formato:

- È possibile specificare un solo livello di autorizzazioni. Per fornire all'host l'accesso completo a tutte le operazioni, inserire la stringa ALL ACCESS.
- La stringa di autorizzazione deve essere la prima cosa nel file. Il formato del file non è valido se la stringa di autorizzazione non si trova nella prima riga.
- Le stringhe di permesso non distinguono tra maiuscole e minuscole.
- Nessuno spazio vuoto può precedere la stringa di permesso.
- Non sono consentiti commenti.

Queste stringhe di autorizzazione valide consentono i seguenti livelli di accesso:

- NESSUNO — l'host non ha accesso al sistema di storage.
- CREAZIONE SNAP: L'host può creare copie Snapshot.
- UTILIZZO DI SNAP: L'host può eliminare e rinominare le copie Snapshot.
- SNAP ALL (SNAP TUTTO): L'host può creare, ripristinare, eliminare e rinominare le copie Snapshot.
- STORAGE CREATE DELETE (ELIMINA CREAZIONE STORAGE): L'host può creare, ridimensionare ed eliminare lo storage.
- UTILIZZO DELLO STORAGE: L'host può connettere e disconnettere lo storage ed eseguire anche la stima del clone split e l'avvio del clone split sullo storage.
- STORAGE ALL (TUTTO STORAGE): L'host può creare, eliminare, connettere e disconnettere lo storage ed eseguire anche la stima della divisione dei cloni e l'avvio della divisione dei cloni sullo storage.
- TUTTI GLI ACCESSI — l'host ha accesso a tutte le precedenti operazioni SnapDrive per UNIX. Ciascuna di queste stringhe di autorizzazione è discreta. Se si specifica L'UTILIZZO DELLO SNAP, l'host può eliminare o rinominare le copie Snapshot, ma non può creare copie Snapshot o ripristinare o eseguire operazioni di provisioning dello storage.

Indipendentemente dalle autorizzazioni impostate, l'host può eseguire operazioni di visualizzazione ed elenco.

4. Verificare le autorizzazioni di accesso immettendo il seguente comando:

```
snapdrive config access show filer_name
```

Visualizzazione dell'autorizzazione per il controllo degli accessi

È possibile visualizzare le autorizzazioni per il controllo degli accessi eseguendo `snapdrive config access show` comando.

Fasi

1. Eseguire `snapdrive config access show` comando.

Questo comando ha il seguente formato: `snapdrive config access {show | list} filename`

È possibile utilizzare gli stessi parametri indipendentemente dall'immissione o meno di `show` oppure `list` versione del comando.

Questa riga di comando controlla il tostapane del sistema di storage per determinare le autorizzazioni di cui dispone l'host. In base all'output, le autorizzazioni per l'host su questo sistema di storage sono SNAP-ALL.

```
# snapdrive config access show toaster
This host has the following access permission to filer, toaster:
SNAP ALL
Commands allowed:
snap create
snap restore
snap delete
snap rename
#
```

In questo esempio, il file delle autorizzazioni non si trova sul sistema di storage, quindi SnapDrive per UNIX controlla la variabile `all-access-if-rbac-unspecified` in `snapdrive.conf` file per determinare le autorizzazioni di cui dispone l'host. Questa variabile è impostata su `on`, che equivale alla creazione di un file di permessi con il livello di accesso impostato su TUTTI GLI ACCESSI.

```
# snapdrive config access list toaster
This host has the following access permission to filer, toaster:
ALL ACCESS
Commands allowed:
snap create
snap restore
snap delete
snap rename
storage create
storage resize
snap connect
storage connect
storage delete
snap disconnect
storage disconnect
clone split estimate
clone split start
#
```

Questo esempio mostra il tipo di messaggio ricevuto se non è presente alcun file di permessi sul tostapane

del sistema di storage e la variabile *all-access-if-rbac-unspecified* in `snapdrive.conf` il file è impostato su `off`.

```
# snapdrive config access list toaster
Unable to read the access permission file on filer, toaster. Verify that
the
file is present.
Granting no permissions to filer, toaster.
```

Informazioni sul copyright

Copyright © 2023 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.