In che modo gli stili di sicurezza influiscono sull'accesso ai dati

ONTAP 9

NetApp
April 24, 2024

Sommario

In che modo gli stili di sicurezza influiscono sull'accesso ai dati

Quali sono gli stili di sicurezza e i loro effetti

Esistono quattro diversi stili di sicurezza: UNIX, NTFS, misto e unificato. Ogni stile di sicurezza ha un effetto diverso sul modo in cui vengono gestite le autorizzazioni per i dati. È necessario comprendere i diversi effetti per assicurarsi di selezionare lo stile di sicurezza appropriato per i propri scopi.

È importante comprendere che gli stili di sicurezza non determinano quali tipi di client possono o non possono accedere ai dati. Gli stili di sicurezza determinano solo il tipo di autorizzazioni utilizzate da ONTAP per controllare l'accesso ai dati e il tipo di client in grado di modificare tali autorizzazioni.

Ad esempio, se un volume utilizza lo stile di sicurezza UNIX, i client SMB possono comunque accedere ai dati (purché autenticino e autorizzino correttamente) a causa della natura multiprotocollo di ONTAP. Tuttavia, ONTAP utilizza autorizzazioni UNIX che solo i client UNIX possono modificare utilizzando strumenti nativi.

Stile di sicurezza	Client in grado di modificare le autorizzazioni	Autorizzazioni che i client possono utilizzare	Risultato di uno stile di sicurezza efficace	Client che possono accedere ai file
UNIX	NFS	Bit di modalità NFSv3	UNIX	NFS e SMB
		ACL NFSv4.x		
NTFS	PMI	ACL NTFS	NTFS	
Misto	NFS o SMB	Bit di modalità NFSv3	UNIX	
		NFSv4.ACL		
		ACL NTFS	NTFS	
Unificato (solo per volumi infiniti, in ONTAP 9.4 e versioni precedenti).	NFS o SMB	Bit di modalità NFSv3	UNIX	
		ACL NFSv4.1		
		ACL NTFS	NTFS	

I volumi FlexVol supportano UNIX, NTFS e stili di sicurezza misti. Quando lo stile di sicurezza è misto o unificato, le autorizzazioni effettive dipendono dal tipo di client che ha modificato le autorizzazioni per ultima, perché gli utenti impostano lo stile di sicurezza su base individuale. Se l'ultimo client che ha modificato le autorizzazioni era un client NFSv3, le autorizzazioni sono bit di modalità UNIX NFSv3. Se l'ultimo client era un client NFSv4, le autorizzazioni sono ACL NFSv4. Se l'ultimo client era un client SMB, le autorizzazioni sono ACL NTFS di Windows.

Lo stile di sicurezza unificato è disponibile solo con volumi infiniti, che non sono più supportati in ONTAP 9.5 e versioni successive. Per ulteriori informazioni, vedere Panoramica sulla gestione dei volumi FlexGroup.

A partire da ONTAP 9.2, la `show-effective-permissions` al `vserver security file-directory` Il comando consente di visualizzare le autorizzazioni effettive concesse a un utente Windows o UNIX sul

percorso di file o cartella specificato. Inoltre, il parametro opzionale `-share-name` consente di visualizzare l'autorizzazione di condivisione effettiva.

> ONTAP imposta inizialmente alcune autorizzazioni predefinite per i file. Per impostazione predefinita, lo stile di sicurezza effettivo su tutti i dati nei volumi UNIX, misti e di sicurezza unificata è UNIX e il tipo di permessi effettivo è UNIX mode bits (0755 se non diversamente specificato) fino a quando non viene configurato da un client come consentito dallo stile di sicurezza predefinito. Per impostazione predefinita, lo stile di sicurezza effettivo su tutti i dati nei volumi di sicurezza NTFS è NTFS e dispone di un ACL che consente il controllo completo di tutti.

Dove e quando impostare gli stili di sicurezza

Gli stili di sicurezza possono essere impostati su volumi FlexVol (sia root che volumi di dati) e qtree. Gli stili di sicurezza possono essere impostati manualmente al momento della creazione, ereditati automaticamente o modificati in un secondo momento.

Decidere quale stile di sicurezza utilizzare sulle SVM

Per aiutarti a decidere quale stile di sicurezza utilizzare su un volume, devi considerare due fattori. Il fattore principale è il tipo di amministratore che gestisce il file system. Il fattore secondario è il tipo di utente o servizio che accede ai dati sul volume.

Quando si configura lo stile di protezione su un volume, è necessario considerare le esigenze dell'ambiente per assicurarsi di selezionare lo stile di protezione migliore ed evitare problemi con la gestione delle autorizzazioni. Le seguenti considerazioni possono aiutarti a decidere:

Stile di sicurezza	Scegliere se…
UNIX	• Il file system è gestito da un amministratore UNIX. • La maggior parte degli utenti sono client NFS. • Un'applicazione che accede ai dati utilizza un utente UNIX come account del servizio.
NTFS	• Il file system è gestito da un amministratore di Windows. • La maggior parte degli utenti è costituita da client SMB. • Un'applicazione che accede ai dati utilizza un utente Windows come account del servizio.
Misto	• Il file system è gestito dagli amministratori UNIX e Windows e gli utenti sono costituiti da client NFS e SMB.

Come funziona l'ereditarietà dello stile di sicurezza

Se non si specifica lo stile di protezione durante la creazione di un nuovo volume FlexVol o di un qtree, questo eredita il proprio stile di protezione in modi diversi.

Gli stili di sicurezza vengono ereditati nel modo seguente:

- Un volume FlexVol eredita lo stile di sicurezza del volume root del volume SVM contenente.
- Un qtree eredita lo stile di protezione del volume FlexVol contenente.
- Un file o una directory eredita lo stile di protezione del volume o qtree FlexVol contenente.

In che modo ONTAP conserva le autorizzazioni UNIX

Quando i file in un volume FlexVol che dispongono attualmente di autorizzazioni UNIX vengono modificati e salvati dalle applicazioni Windows, ONTAP può conservare le autorizzazioni UNIX.

Quando le applicazioni sui client Windows modificano e salvano i file, leggono le proprietà di protezione del file, creano un nuovo file temporaneo, applicano tali proprietà al file temporaneo e assegnano al file temporaneo il nome del file originale.

Quando i client Windows eseguono una query per le proprietà di protezione, ricevono un ACL costruito che rappresenta esattamente le autorizzazioni UNIX. L'unico scopo di questo ACL costruito è quello di preservare le autorizzazioni UNIX del file, poiché i file vengono aggiornati dalle applicazioni Windows per garantire che i file risultanti abbiano le stesse autorizzazioni UNIX. ONTAP non imposta alcun ACL NTFS utilizzando l'ACL costruito.

Gestire le autorizzazioni UNIX utilizzando la scheda protezione di Windows

Se si desidera modificare le autorizzazioni UNIX di file o cartelle in volumi misti di sicurezza o qtree su SVM, è possibile utilizzare la scheda Security (protezione) sui client Windows. In alternativa, è possibile utilizzare applicazioni in grado di eseguire query e impostare gli ACL di Windows.

- Modifica delle autorizzazioni UNIX

  È possibile utilizzare la scheda protezione di Windows per visualizzare e modificare le autorizzazioni UNIX per un volume misto di sicurezza o qtree. Se si utilizza la scheda principale di Windows Security per modificare le autorizzazioni UNIX, è necessario rimuovere prima l'ACE esistente che si desidera modificare (in questo modo i bit di modalità vengono impostati su 0) prima di apportare le modifiche. In alternativa, è possibile utilizzare l'editor avanzato per modificare le autorizzazioni.

  Se vengono utilizzate le autorizzazioni di modalità, è possibile modificare direttamente le autorizzazioni di modalità per UID, GID e altri (tutti gli altri utenti con un account sul computer). Ad esempio, se l'UID visualizzato dispone delle autorizzazioni r-x, è possibile modificare le autorizzazioni UID in rwx.

- Modifica delle autorizzazioni UNIX in autorizzazioni NTFS

  È possibile utilizzare la scheda protezione di Windows per sostituire gli oggetti di protezione UNIX con oggetti di protezione di Windows su un volume misto di tipo sicurezza o qtree in cui i file e le cartelle hanno uno stile di protezione efficace UNIX.

  Prima di poter sostituire le voci di autorizzazione UNIX con gli oggetti utente e gruppo di Windows desiderati, è necessario rimuovere tutte le voci di autorizzazione UNIX elencate. È quindi possibile configurare gli ACL basati su NTFS sugli oggetti utente e Gruppo di Windows. Rimuovendo tutti gli oggetti

di protezione UNIX e aggiungendo solo utenti e gruppi Windows a un file o a una cartella in un volume o qtree misto di sicurezza, è possibile modificare lo stile di protezione effettivo del file o della cartella da UNIX a NTFS.

Quando si modificano le autorizzazioni di una cartella, il comportamento predefinito di Windows consiste nel propagare queste modifiche a tutte le sottocartelle e a tutti i file. Pertanto, se non si desidera propagare una modifica dello stile di protezione a tutte le cartelle figlio, le sottocartelle e i file, è necessario modificare l'impostazione di propagazione desiderata.