Modalità di utilizzo di utenti e gruppi locali da parte di ONTAP

ONTAP 9

NetApp
April 24, 2024

Sommario

Modalità di utilizzo di utenti e gruppi locali da parte di ONTAP

Concetti relativi a utenti e gruppi locali

Prima di stabilire se configurare e utilizzare utenti e gruppi locali nel proprio ambiente, è necessario conoscere gli utenti e i gruppi locali e alcune informazioni di base.

- **Utente locale**

  Un account utente con un identificatore di protezione univoco (SID) che ha visibilità solo sulla macchina virtuale di storage (SVM) su cui è creato. Gli account utente locali dispongono di una serie di attributi, tra cui nome utente e SID. Un account utente locale esegue l'autenticazione locale sul server CIFS utilizzando l'autenticazione NTLM.

  Gli account utente possono essere utilizzati in diversi modi:

  - Utilizzato per concedere privilegi di *User Rights Management* a un utente.
  - Utilizzato per controllare l'accesso a livello di condivisione e di file alle risorse di file e cartelle di proprietà della SVM.

- **Gruppo locale**

  Un gruppo con un SID univoco ha visibilità solo sulla SVM su cui è creato. I gruppi contengono un insieme di membri. I membri possono essere utenti locali, utenti di dominio, gruppi di dominio e account di computer di dominio. I gruppi possono essere creati, modificati o cancellati.

  I gruppi hanno diversi utilizzi:

  - Utilizzato per concedere privilegi a *User Rights Management* ai propri membri.
  - Utilizzato per controllare l'accesso a livello di condivisione e di file alle risorse di file e cartelle di proprietà della SVM.

- **Dominio locale**

  Dominio con ambito locale, delimitato dalla SVM. Il nome del dominio locale è il nome del server CIFS. Gli utenti e i gruppi locali sono contenuti all'interno del dominio locale.

- **Identificatore di sicurezza (SID)**

  Un SID è un valore numerico di lunghezza variabile che identifica le entità di protezione di tipo Windows. Ad esempio, un SID tipico assume la seguente forma: S-1-5-21-3139654847-1303905135-2517279418-123456.

- **Autenticazione NTLM**

  Metodo di protezione Microsoft Windows utilizzato per autenticare gli utenti su un server CIFS.

- **Cluster Replicated Database (RDB)**

  Database replicato con un'istanza su ciascun nodo di un cluster. Gli oggetti utente e gruppo locali vengono memorizzati nell'RDB.

Motivi per la creazione di utenti locali e gruppi locali

Esistono diversi motivi per creare utenti locali e gruppi locali sulla macchina virtuale di storage (SVM). Ad esempio, è possibile accedere a un server SMB utilizzando un account utente locale se i controller di dominio (DC) non sono disponibili, se si desidera utilizzare gruppi locali per assegnare privilegi o se il server SMB si trova in un gruppo di lavoro.

È possibile creare uno o più account utente locali per i seguenti motivi:

- Il server SMB si trova in un gruppo di lavoro e gli utenti di dominio non sono disponibili.

  Nelle configurazioni dei gruppi di lavoro sono richiesti utenti locali.

- Se i controller di dominio non sono disponibili, si desidera eseguire l'autenticazione e l'accesso al server SMB.

  Gli utenti locali possono autenticarsi con il server SMB utilizzando l'autenticazione NTLM quando il controller di dominio non è attivo o quando i problemi di rete impediscono al server SMB di contattare il controller di dominio.

- Si desidera assegnare i privilegi di *User Rights Management* a un utente locale.

  User Rights Management è la capacità di un amministratore del server SMB di controllare i diritti degli utenti e dei gruppi sulla SVM. È possibile assegnare i privilegi a un utente assegnando i privilegi all'account dell'utente o facendo in modo che l'utente sia membro di un gruppo locale che dispone di tali privilegi.

È possibile creare uno o più gruppi locali per i seguenti motivi:

- Il server SMB si trova in un gruppo di lavoro e i gruppi di dominio non sono disponibili.

  I gruppi locali non sono richiesti nelle configurazioni dei gruppi di lavoro, ma possono essere utili per la gestione dei privilegi di accesso per gli utenti dei gruppi di lavoro locali.

- Si desidera controllare l'accesso alle risorse di file e cartelle utilizzando gruppi locali per il controllo della condivisione e dell'accesso ai file.
- Si desidera creare gruppi locali con privilegi personalizzati di *User Rights Management*.

  Alcuni gruppi di utenti integrati dispongono di privilegi predefiniti. Per assegnare un set personalizzato di privilegi, è possibile creare un gruppo locale e assegnare i privilegi necessari a tale gruppo. È quindi possibile aggiungere utenti locali, utenti di dominio e gruppi di dominio al gruppo locale.

Informazioni correlate

Come funziona l'autenticazione utente locale

Elenco dei privilegi supportati

Come funziona l'autenticazione utente locale

Prima che un utente locale possa accedere ai dati su un server CIFS, l'utente deve

creare una sessione autenticata.

Poiché SMB è basato sulla sessione, l'identità dell'utente può essere determinata una sola volta, quando la sessione viene configurata per la prima volta. Il server CIFS utilizza l'autenticazione basata su NTLM per l'autenticazione degli utenti locali. Sono supportati sia NTLMv1 che NTLMv2.

ONTAP utilizza l'autenticazione locale in tre casi di utilizzo. Ogni caso di utilizzo dipende dal fatto che la parte di dominio del nome utente (con il formato DOMINIO/utente) corrisponda al nome di dominio locale del server CIFS (il nome del server CIFS):

- La parte di dominio corrisponde

  Gli utenti che forniscono credenziali utente locali quando richiedono l'accesso ai dati vengono autenticati localmente sul server CIFS.

- La porzione di dominio non corrisponde

  ONTAP tenta di utilizzare l'autenticazione NTLM con un controller di dominio nel dominio a cui appartiene il server CIFS. Se l'autenticazione ha esito positivo, l'accesso è completo. In caso contrario, ciò che accade in seguito dipende dal motivo per cui l'autenticazione non ha avuto esito positivo.

  Ad esempio, se l'utente esiste in Active Directory ma la password non è valida o è scaduta, ONTAP non tenta di utilizzare l'account utente locale corrispondente sul server CIFS. Al contrario, l'autenticazione non riesce. In altri casi, ONTAP utilizza l'account locale corrispondente sul server CIFS, se esistente, per l'autenticazione, anche se i nomi di dominio NetBIOS non corrispondono. Ad esempio, se esiste un account di dominio corrispondente ma è disattivato, ONTAP utilizza l'account locale corrispondente sul server CIFS per l'autenticazione.

- La porzione di dominio non è specificata

  ONTAP tenta innanzitutto l'autenticazione come utente locale. Se l'autenticazione come utente locale non riesce, ONTAP autentica l'utente con un controller di dominio nel dominio a cui appartiene il server CIFS.

Una volta completata correttamente l'autenticazione dell'utente locale o di dominio, ONTAP crea un token di accesso utente completo, che tiene conto dell'appartenenza al gruppo locale e dei privilegi.

Per ulteriori informazioni sull'autenticazione NTLM per gli utenti locali, consultare la documentazione di Microsoft Windows.

Informazioni correlate

Attivazione o disattivazione dell'autenticazione utente locale

Come vengono costruiti i token di accesso degli utenti

Quando un utente mappa una condivisione, viene stabilita una sessione SMB autenticata e viene creato un token di accesso utente che contiene informazioni sull'utente, l'appartenenza al gruppo dell'utente e i privilegi cumulativi e l'utente UNIX mappato.

A meno che la funzionalità non sia disattivata, al token di accesso dell'utente vengono aggiunte anche le informazioni relative all'utente locale e al gruppo. La modalità di creazione dei token di accesso dipende dal fatto che l'accesso sia destinato a un utente locale o a un utente di dominio Active Directory:

- Accesso utente locale

Sebbene gli utenti locali possano essere membri di diversi gruppi locali, i gruppi locali non possono essere membri di altri gruppi locali. Il token di accesso dell'utente locale è composto da un'Unione di tutti i privilegi assegnati ai gruppi a cui è membro un particolare utente locale.

- Login utente di dominio

  Quando un utente di dominio effettua l'accesso, ONTAP ottiene un token di accesso utente che contiene il SID e i SID dell'utente per tutti i gruppi di dominio a cui l'utente è membro. ONTAP utilizza l'Unione del token di accesso dell'utente di dominio con il token di accesso fornito dalle appartenenze locali dei gruppi di dominio dell'utente (se presenti), nonché qualsiasi privilegio diretto assegnato all'utente di dominio o a una qualsiasi delle sue appartenenze ai gruppi di dominio.

Per l'accesso dell'utente locale e di dominio, viene impostato anche l'RID del gruppo primario per il token di accesso dell'utente. L'RID predefinito è `Domain Users` (RID 513). Non è possibile modificare l'impostazione predefinita.

Il processo di mappatura dei nomi da Windows a UNIX e da UNIX a Windows segue le stesse regole per gli account locali e di dominio.

> Non esiste alcuna mappatura automatica implicita da un utente UNIX a un account locale. Se necessario, è necessario specificare una regola di mappatura esplicita utilizzando i comandi di mappatura dei nomi esistenti.

Linee guida per l'utilizzo di SnapMirror su SVM che contengono gruppi locali

È necessario conoscere le linee guida per la configurazione di SnapMirror su volumi di proprietà di SVM che contengono gruppi locali.

Non è possibile utilizzare gruppi locali nelle ACE applicate a file, directory o condivisioni replicate da SnapMirror su un'altra SVM. Se si utilizza la funzione SnapMirror per creare un mirror DR su un volume su un altro SVM e il volume dispone di un ACE per un gruppo locale, l'ACE non è valido sul mirror. Se i dati vengono replicati su una SVM diversa, i dati vengono effettivamente trasferiti in un dominio locale diverso. Le autorizzazioni concesse agli utenti e ai gruppi locali sono valide solo nell'ambito della SVM in cui sono stati creati originariamente.

Cosa accade agli utenti e ai gruppi locali quando si eliminano i server CIFS

Il set predefinito di utenti e gruppi locali viene creato quando viene creato un server CIFS e sono associati alla macchina virtuale di storage (SVM) che ospita il server CIFS. Gli amministratori di SVM possono creare utenti e gruppi locali in qualsiasi momento. È necessario essere consapevoli di ciò che accade agli utenti e ai gruppi locali quando si elimina il server CIFS.

Gli utenti e i gruppi locali sono associati alle SVM; pertanto, non vengono cancellati quando i server CIFS vengono cancellati a causa di considerazioni di sicurezza. Anche se gli utenti e i gruppi locali non vengono cancellati quando il server CIFS viene cancellato, essi sono nascosti. Non è possibile visualizzare o gestire utenti e gruppi locali fino a quando non viene ricreato un server CIFS su SVM.

Lo stato amministrativo del server CIFS non influisce sulla visibilità degli utenti o dei gruppi locali.

Come utilizzare Microsoft Management Console con utenti e gruppi locali

È possibile visualizzare informazioni su utenti e gruppi locali dalla console di gestione Microsoft. Con questa versione di ONTAP, non è possibile eseguire altre attività di gestione per utenti e gruppi locali dalla console di gestione Microsoft.

Linee guida per il ripristino

Se si prevede di ripristinare il cluster a una release di ONTAP che non supporta utenti e gruppi locali e utenti e gruppi locali vengono utilizzati per gestire l'accesso ai file o i diritti utente, è necessario tenere presente alcune considerazioni.

- A causa di motivi di sicurezza, le informazioni relative a utenti, gruppi e privilegi locali configurati non vengono eliminate quando ONTAP viene reimpostato su una versione che non supporta la funzionalità di utenti e gruppi locali.
- In caso di ripristino di una versione principale precedente di ONTAP, ONTAP non utilizza utenti e gruppi locali durante l'autenticazione e la creazione delle credenziali.
- Gli utenti e i gruppi locali non vengono rimossi dagli ACL di file e cartelle.
- Le richieste di accesso ai file che dipendono dall'accesso concesso a causa delle autorizzazioni concesse agli utenti o ai gruppi locali vengono negate.

  Per consentire l'accesso, è necessario riconfigurare le autorizzazioni dei file in modo da consentire l'accesso in base agli oggetti di dominio anziché agli oggetti utente e gruppo locali.