Come ONTAP gestisce l'autenticazione del client NFS

ONTAP 9

NetApp
May 09, 2024

Sommario

Come ONTAP gestisce l'autenticazione del client NFS

Panoramica su come ONTAP gestisce l'autenticazione del client NFS

I client NFS devono essere autenticati correttamente prima di poter accedere ai dati sulla SVM. ONTAP autentica i client verificando le credenziali UNIX in base ai servizi di nomi configurati.

Quando un client NFS si connette a SVM, ONTAP ottiene le credenziali UNIX per l'utente controllando i diversi name service, a seconda della configurazione dei name service di SVM. ONTAP può controllare le credenziali per gli account UNIX locali, i domini NIS e i domini LDAP. Almeno uno di questi deve essere configurato in modo che ONTAP possa autenticare correttamente l'utente. È possibile specificare più servizi di nomi e l'ordine in cui ONTAP li cerca.

In un ambiente NFS puro con stili di sicurezza dei volumi UNIX, questa configurazione è sufficiente per autenticare e fornire l'accesso corretto ai file per un utente che si connette da un client NFS.

Se si utilizzano stili di protezione di volumi misti, NTFS o unificati, ONTAP deve ottenere un nome utente SMB per l'utente UNIX per l'autenticazione con un controller di dominio Windows. Ciò può avvenire mappando singoli utenti utilizzando account UNIX locali o domini LDAP oppure utilizzando un utente SMB predefinito. È possibile specificare quali servizi di nomi ONTAP esegue la ricerca in quale ordine o specificare un utente SMB predefinito.

Modalità di utilizzo dei servizi di nome da parte di ONTAP

ONTAP utilizza i name service per ottenere informazioni su utenti e client. ONTAP utilizza queste informazioni per autenticare gli utenti che accedono ai dati sul sistema di storage o ne amministrano l'amministrazione e per mappare le credenziali dell'utente in un ambiente misto.

Quando si configura il sistema di storage, è necessario specificare i servizi dei nomi che si desidera utilizzare per ottenere le credenziali utente per l'autenticazione di ONTAP. ONTAP supporta i seguenti servizi per i nomi:

- Utenti locali (file)
- NIS (External NIS Domain)
- Domini LDAP esterni (LDAP)

Si utilizza `vserver services name-service ns-switch` Famiglia di comandi per configurare le SVM con le origini per la ricerca delle informazioni di rete e l'ordine in cui eseguirne la ricerca. Questi comandi forniscono le funzionalità equivalenti di `/etc/nsswitch.conf` File su sistemi UNIX.

Quando un client NFS si connette a SVM, ONTAP verifica i servizi dei nomi specificati per ottenere le credenziali UNIX per l'utente. Se i name service sono configurati correttamente e ONTAP è in grado di ottenere le credenziali UNIX, ONTAP autentica correttamente l'utente.

In un ambiente con stili di sicurezza misti, ONTAP potrebbe dover mappare le credenziali dell'utente. Per consentire a ONTAP di mappare correttamente le credenziali dell'utente, è necessario configurare i name

service in modo appropriato per l'ambiente in uso.

ONTAP utilizza inoltre i servizi di nome per autenticare gli account amministratore di SVM. È necessario tenere presente questo aspetto durante la configurazione o la modifica dello switch del name service per evitare di disattivare accidentalmente l'autenticazione per gli account amministratore SVM. Per ulteriori informazioni sugli utenti di amministrazione di SVM, vedere "Autenticazione amministratore e RBAC".

In che modo ONTAP garantisce l'accesso ai file SMB dai client NFS

ONTAP utilizza la semantica di protezione del file system di Windows NT per determinare se un utente UNIX, su un client NFS, ha accesso a un file con autorizzazioni NTFS.

A tale scopo, ONTAP converte l'ID utente UNIX dell'utente in una credenziale SMB e utilizza la credenziale SMB per verificare che l'utente disponga dei diritti di accesso al file. Una credenziale SMB è costituita da un identificatore di protezione (SID) primario, di solito il nome utente Windows dell'utente, e da uno o più SID di gruppo che corrispondono ai gruppi Windows di cui l'utente è membro.

Il tempo impiegato da ONTAP per convertire l'UID UNIX in una credenziale SMB può essere compreso tra decine di millisecondi e centinaia di millisecondi, poiché il processo richiede il contatto con un controller di dominio. ONTAP esegue il mapping dell'UID alla credenziale SMB e inserisce il mapping in una cache delle credenziali per ridurre il tempo di verifica causato dalla conversione.

Come funziona la cache delle credenziali NFS

Quando un utente NFS richiede l'accesso alle esportazioni NFS sul sistema di storage, ONTAP deve recuperare le credenziali dell'utente dai name server esterni o dai file locali per autenticare l'utente. ONTAP memorizza quindi queste credenziali in una cache interna per riferimenti futuri. La comprensione del funzionamento delle cache delle credenziali NFS consente di gestire potenziali problemi di performance e accesso.

Senza la cache delle credenziali, ONTAP dovrebbe eseguire query sui servizi dei nomi ogni volta che un utente NFS ha richiesto l'accesso. In un sistema storage occupato a cui molti utenti accedono, questo può causare rapidamente gravi problemi di performance, causando ritardi indesiderati o addirittura negazioni dell'accesso al client NFS.

Con la cache delle credenziali, ONTAP recupera le credenziali dell'utente e le memorizza per un periodo di tempo prestabilito per un accesso rapido e semplice nel caso in cui il client NFS invii un'altra richiesta. Questo metodo offre i seguenti vantaggi:

- Semplifica il carico sul sistema storage gestendo meno richieste ai name server esterni (come NIS o LDAP).
- Semplifica il carico sui server dei nomi esterni inviando loro un numero inferiore di richieste.
- Accelera l'accesso degli utenti eliminando i tempi di attesa per ottenere le credenziali da origini esterne prima che l'utente possa essere autenticato.

ONTAP memorizza le credenziali positive e negative nella cache delle credenziali. Le credenziali positive significano che l'utente è stato autenticato e ha ottenuto l'accesso. Le credenziali negative significano che l'utente non è stato autenticato e l'accesso è stato negato.

Per impostazione predefinita, ONTAP memorizza le credenziali positive per 24 ore, ovvero, dopo

l’autenticazione iniziale di un utente, ONTAP utilizza le credenziali memorizzate nella cache per tutte le richieste di accesso da parte di tale utente per 24 ore. Se l’utente richiede l’accesso dopo 24 ore, il ciclo ha inizio: ONTAP ignora le credenziali memorizzate nella cache e ottiene nuovamente le credenziali dall’origine del name service appropriata. Se le credenziali sono state modificate nel server dei nomi durante le 24 ore precedenti, ONTAP memorizza nella cache le credenziali aggiornate per l’utilizzo nelle 24 ore successive.

Per impostazione predefinita, ONTAP memorizza le credenziali negative per due ore, ovvero, dopo aver inizialmente negato l’accesso a un utente, ONTAP continua a negare qualsiasi richiesta di accesso da parte di tale utente per due ore. Se l’utente richiede l’accesso dopo 2 ore, il ciclo ricomincia: ONTAP ottiene nuovamente le credenziali dall’origine del name service appropriata. Se le credenziali sono state modificate nel server dei nomi nelle due ore precedenti, ONTAP memorizza nella cache le credenziali aggiornate per l’utilizzo nelle due ore successive.