Comprendere l'accesso al file NAS

ONTAP 9

NetApp
April 24, 2024

Sommario

Comprendere l’accesso al file NAS

Spazi dei nomi e punti di giunzione

Panoramica degli spazi dei nomi e dei punti di giunzione

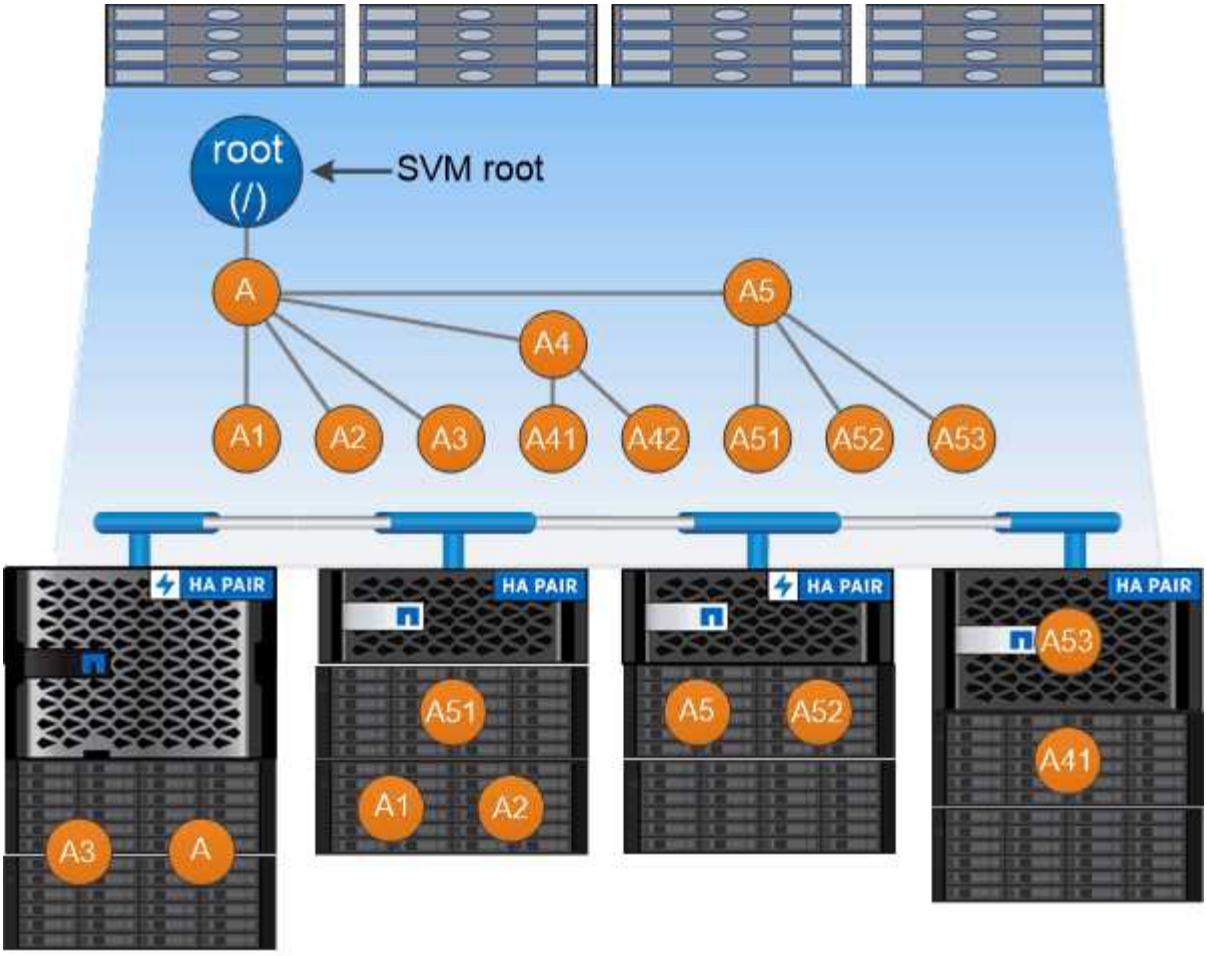
Un *namespace* NAS è un raggruppamento logico di volumi Uniti in *punti di giunzione* per creare una singola gerarchia di file system. Un client con autorizzazioni sufficienti può accedere ai file nello spazio dei nomi senza specificare la posizione dei file nello storage. I volumi Junctioned possono risiedere in qualsiasi punto del cluster.

Invece di montare ogni volume contenente un file di interesse, i client NAS montano un NFS *export* o accedono a una *share.* SMB. L’esportazione o la condivisione rappresenta l’intero namespace o una posizione intermedia all’interno dello spazio dei nomi. Il client accede solo ai volumi montati sotto il proprio access point.

È possibile aggiungere volumi allo spazio dei nomi in base alle esigenze. È possibile creare punti di giunzione direttamente sotto una giunzione di un volume padre o in una directory all’interno di un volume. Il percorso di una giunzione di volume per un volume denominato “vol3” potrebbe essere `/vol1/vol2/vol3`, o. `/vol1/dir2/vol3`, o persino `/dir1/dir2/vol3`. Il percorso è chiamato *percorso di giunzione.*

Ogni SVM dispone di uno spazio dei nomi univoco. Il volume root SVM è il punto di ingresso della gerarchia dello spazio dei nomi.

> Per garantire che i dati rimangano disponibili in caso di interruzione o failover di un nodo, è necessario creare una copia *mirror per la condivisione del carico* per il volume root SVM.



A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.

Esempio

Nell'esempio riportato di seguito viene creato un volume denominato "home4" situato su SVM vs1 con un percorso di giunzione `/eng/home`:

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

Quali sono le tipiche architetture dello spazio dei nomi NAS

Esistono diverse architetture dello spazio dei nomi NAS tipiche che è possibile utilizzare per creare lo spazio dei nomi SVM. È possibile scegliere l'architettura dello spazio dei nomi che soddisfa le esigenze di business e workflow.

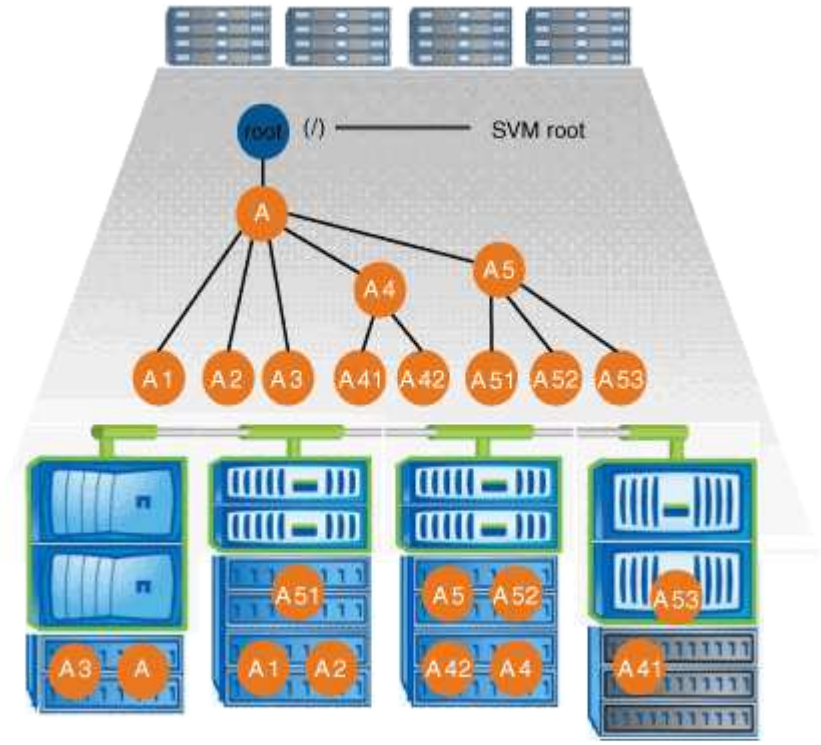
La parte superiore dello spazio dei nomi è sempre il volume root, rappresentato da una barra (/). L'architettura dello spazio dei nomi sotto la radice si suddivide in tre categorie di base:

- Un singolo albero ramificato, con una sola giunzione alla radice dello spazio dei nomi

- Più alberi ramificati, con più punti di giunzione alla radice dello spazio dei nomi
- Più volumi standalone, ciascuno con un punto di giunzione separato per la radice dello spazio dei nomi

Namespace con singolo albero ramificato

Un'architettura con un singolo albero ramificato ha un singolo punto di inserimento alla radice dello spazio dei nomi SVM. Il singolo punto di inserimento può essere un volume giuntato o una directory sotto la root. Tutti gli altri volumi vengono montati nei punti di giunzione sotto il singolo punto di inserimento (che può essere un volume o una directory).

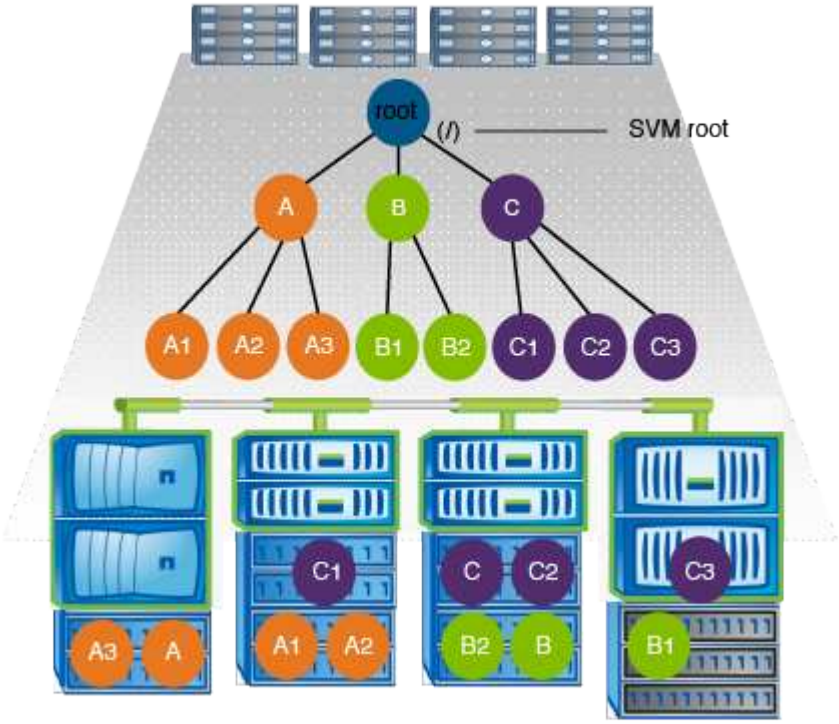


Ad esempio, una configurazione tipica di giunzione di volumi con l'architettura dello spazio dei nomi sopra descritta potrebbe essere simile alla seguente configurazione, in cui tutti i volumi sono congiunti sotto il singolo punto di inserimento, che è una directory denominata "data":

```
                      Junction                          Junction
Vserver Volume        Active   Junction Path            Path Source
------- ------------ -------- -------------------      -----------
vs1     corp1        true     /data/dir1/corp1         RW_volume
vs1     corp2        true     /data/dir1/corp2         RW_volume
vs1     data1        true     /data/data1              RW_volume
vs1     eng1         true     /data/data1/eng1         RW_volume
vs1     eng2         true     /data/data1/eng2         RW_volume
vs1     sales        true     /data/data1/sales        RW_volume
vs1     vol1         true     /data/vol1               RW_volume
vs1     vol2         true     /data/vol2               RW_volume
vs1     vol3         true     /data/vol3               RW_volume
vs1     vs1_root     -        /                        -
```

Namespace con più alberi ramificati

Un'architettura con più alberi ramificati ha più punti di inserimento alla radice dello spazio dei nomi SVM. I punti di inserimento possono essere volumi congiunti o directory sotto la radice. Tutti gli altri volumi vengono montati nei punti di giunzione sotto i punti di inserimento (che possono essere volumi o directory).



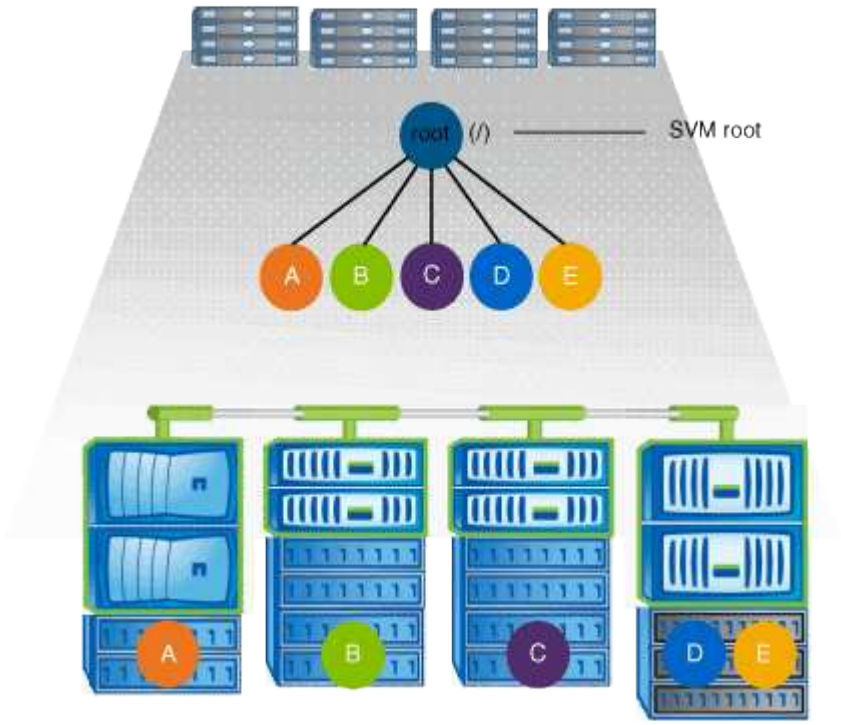
Ad esempio, una configurazione tipica di giunzione del volume con l'architettura dello spazio dei nomi di cui sopra potrebbe essere simile alla seguente configurazione, in cui sono presenti tre punti di inserimento nel volume root della SVM. Due punti di inserimento sono directory denominate "data" e "projects". Un punto di inserimento è un volume giuntato denominato "audit":

```
                      Junction                          Junction
Vserver Volume        Active   Junction Path            Path Source
------- ------------ -------- -------------------      -----------
vs1     audit        true     /audit                   RW_volume
vs1     audit_logs1  true     /audit/logs1             RW_volume
vs1     audit_logs2  true     /audit/logs2             RW_volume
vs1     audit_logs3  true     /audit/logs3             RW_volume
vs1     eng          true     /data/eng                RW_volume
vs1     mktg1        true     /data/mktg1              RW_volume
vs1     mktg2        true     /data/mktg2              RW_volume
vs1     project1     true     /projects/project1       RW_volume
vs1     project2     true     /projects/project2       RW_volume
vs1     vs1_root     -        /                        -
```

Namespace con più volumi standalone

In un'architettura con volumi standalone, ogni volume ha un punto di inserimento nella directory principale

dello spazio dei nomi SVM; tuttavia, il volume non è giuntato sotto un altro volume. Ogni volume ha un percorso univoco ed è posto direttamente sotto la root oppure è posto sotto una directory sotto la root.



Ad esempio, una configurazione tipica di giunzione del volume con l'architettura dello spazio dei nomi di cui sopra potrebbe essere simile alla seguente configurazione, in cui sono presenti cinque punti di inserimento nel volume root della SVM, con ciascun punto di inserimento che rappresenta un percorso per un volume.

```
                      Junction                        Junction
Vserver Volume        Active   Junction Path          Path Source
------- ------------ -------- -------------------    -----------
vs1     eng           true     /eng                   RW_volume
vs1     mktg          true     /vol/mktg              RW_volume
vs1     project1      true     /project1              RW_volume
vs1     project2      true     /project2              RW_volume
vs1     sales         true     /sales                 RW_volume
vs1     vs1_root      -        /                      -
```

Come ONTAP controlla l'accesso ai file

Panoramica delle modalità di controllo dell'accesso ai file da parte di ONTAP

ONTAP controlla l'accesso ai file in base alle restrizioni basate sull'autenticazione e sui file specificate dall'utente.

Quando un client si connette al sistema di storage per accedere ai file, ONTAP deve eseguire due operazioni:

- Autenticazione

ONTAP deve autenticare il client verificando l'identità con un'origine attendibile. Inoltre, il tipo di autenticazione del client è un metodo che può essere utilizzato per determinare se un client può accedere ai dati durante la configurazione dei criteri di esportazione (facoltativo per CIFS).

- Autorizzazione

  ONTAP deve autorizzare l'utente confrontando le credenziali dell'utente con le autorizzazioni configurate nel file o nella directory e determinando il tipo di accesso, se presente, da fornire.

Per gestire correttamente il controllo dell'accesso ai file, ONTAP deve comunicare con servizi esterni come server NIS, LDAP e Active Directory. La configurazione di un sistema storage per l'accesso ai file mediante CIFS o NFS richiede la configurazione dei servizi appropriati in base all'ambiente in uso in ONTAP.

Restrizioni basate sull'autenticazione

Con le restrizioni basate sull'autenticazione, è possibile specificare quali macchine client e quali utenti possono connettersi alla SVM (Storage Virtual Machine).

ONTAP supporta l'autenticazione Kerberos da server UNIX e Windows.

Restrizioni basate su file

ONTAP valuta tre livelli di sicurezza per determinare se un'entità è autorizzata a eseguire un'azione richiesta su file e directory che risiedono su una SVM. L'accesso è determinato dalle autorizzazioni effettive dopo la valutazione dei tre livelli di protezione.

Qualsiasi oggetto di storage può contenere fino a tre tipi di livelli di sicurezza:

- Sicurezza di esportazione (NFS) e condivisione (SMB)

  La sicurezza di esportazione e condivisione si applica all'accesso client a una data esportazione NFS o condivisione SMB. Gli utenti con privilegi amministrativi possono gestire la sicurezza a livello di esportazione e condivisione dai client SMB e NFS.

- Protezione di file e directory di Access Guard a livello di storage

  La sicurezza di Access Guard a livello di storage si applica all'accesso dei client SMB e NFS ai volumi SVM. Sono supportate solo le autorizzazioni di accesso NTFS. Affinché ONTAP esegua controlli di sicurezza sugli utenti UNIX per l'accesso ai dati sui volumi per i quali è stato applicato Storage-Level Access Guard, l'utente UNIX deve eseguire il mapping a un utente Windows sulla SVM proprietaria del volume.

  > Se si visualizzano le impostazioni di sicurezza su un file o una directory da un client NFS o SMB, la protezione Storage-Level Access Guard non viene visualizzata. La protezione di Storage-Level Access Guard non può essere revocata da un client, nemmeno da un amministratore di sistema (Windows o UNIX).

- Sicurezza nativa a livello di file in NTFS, UNIX e NFSv4

  La protezione nativa a livello di file esiste nel file o nella directory che rappresenta l'oggetto di storage. È possibile impostare la sicurezza a livello di file da un client. Le autorizzazioni dei file sono efficaci indipendentemente dal fatto che SMB o NFS vengano utilizzati per accedere ai dati.

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.