Wie ONTAP die NFS-Client-Authentifizierung verarbeitet

ONTAP 9

NetApp
March 21, 2023

Inhaltsverzeichnis

Wie ONTAP die NFS-Client-Authentifizierung verarbeitet

Überblick über die Handhabung der NFS-Client-Authentifizierung durch ONTAP

NFS-Clients müssen ordnungsgemäß authentifiziert werden, bevor sie auf Daten auf der SVM zugreifen können. ONTAP authentifiziert die Clients, indem ihre UNIX-Anmeldeinformationen auf die von Ihnen konfigurierten Namensdienste überprüft werden.

Wenn ein NFS-Client eine Verbindung zur SVM herstellt, erhält ONTAP die UNIX-Anmeldedaten für den Benutzer, indem er abhängig von der Name-Services-Konfiguration der SVM andere Name-Services überprüft. ONTAP kann die Anmeldedaten für lokale UNIX Accounts, NIS-Domänen und LDAP-Domänen prüfen. Mindestens einer von ihnen muss so konfiguriert werden, dass ONTAP den Benutzer erfolgreich authentifizieren kann. Sie können mehrere Namensdienste und die Reihenfolge angeben, in der ONTAP sie durchsucht.

In einer reinen NFS-Umgebung mit UNIX-Volume-Sicherheitsstil genügt diese Konfiguration zur Authentifizierung und Bereitstellung des richtigen Dateizugriffs für einen Benutzer, der sich von einem NFS-Client aus verbinden lässt.

Bei Verwendung von Sicherheitsstilen für gemischte, NTFS- oder einheitliche Volumes muss ONTAP einen SMB-Benutzernamen für den UNIX-Benutzer zur Authentifizierung mit einem Windows Domain Controller erhalten. Dies kann entweder durch die Zuordnung einzelner Benutzer mithilfe lokaler UNIX-Konten oder LDAP-Domänen oder durch die Verwendung eines standardmäßigen SMB-Benutzers erfolgen. Sie können festlegen, nach welchen Namens-Services ONTAP in welcher Reihenfolge gesucht wird, oder einen standardmäßigen SMB-Benutzer angeben.

Verwendung von Name Services durch ONTAP

ONTAP bezieht Informationen zu Benutzern und Clients mithilfe von Name Services. ONTAP verwendet diese Informationen, um Benutzer zu authentifizieren, die auf Daten auf dem Storage-System zugreifen, und um Benutzeranmeldeinformationen in einer heterogenen Umgebung zuzuordnen.

Wenn Sie das Speichersystem konfigurieren, müssen Sie angeben, welche Namensdienste ONTAP zum Abrufen von Benutzeranmeldeinformationen zur Authentifizierung verwenden soll. ONTAP unterstützt folgende Namensdienste:

- Lokale Benutzer (Datei)
- Externe NIS-Domänen (NIS)
- Externe LDAP-Domänen (LDAP)

Sie verwenden das `vserver services name-service ns-switch` Produktfamilie konfiguriert SVMs mit den Quellen für die Suche nach Netzwerkinformationen und der Reihenfolge, in der sie durchsucht werden können. Diese Befehle stellen die gleiche Funktionalität des bereit `/etc/nsswitch.conf` File auf UNIX Systemen.

Wenn ein NFS-Client eine Verbindung zur SVM herstellt, überprüft ONTAP die angegebenen Namensservices,

um die UNIX-Anmeldedaten für den Benutzer abzurufen. Wenn Namensdienste richtig konfiguriert sind und ONTAP die UNIX-Anmeldedaten erhalten kann, authentifiziert ONTAP den Benutzer erfolgreich.

In einer Umgebung mit unterschiedlichen Sicherheitsstilen muss ONTAP möglicherweise Benutzeranmeldeinformationen zuordnen. Sie müssen Name-Services entsprechend für Ihre Umgebung konfigurieren, damit ONTAP die Benutzeranmeldeinformationen ordnungsgemäß zuordnen kann.

ONTAP verwendet außerdem Namensdienste für die Authentifizierung von SVM-Administratorkonten. Dies müssen Sie beachten, wenn Sie den Namespace-Switch konfigurieren oder ändern, um zu vermeiden, dass die Authentifizierung für SVM-Administratorkonten versehentlich deaktiviert wird. Weitere Informationen zu SVM-Verwaltungsbenutzern finden Sie unter "Administratorauthentifizierung und RBAC".

Wie ONTAP über NFS-Clients SMB-Dateizugriff gewährt

ONTAP verwendet die Sicherheitssemantik des Windows NT File System (NTFS), um zu ermitteln, ob ein UNIX-Benutzer auf einem NFS-Client Zugriff auf eine Datei mit NTFS-Berechtigungen hat.

ONTAP konvertiert dazu die UNIX-Benutzer-ID (UID) des Benutzers in eine SMB-Berechtigung und überprüft anschließend mit den SMB-Anmeldeinformationen, ob der Benutzer über Zugriffsrechte auf die Datei verfügt. Eine SMB-Berechtigung besteht aus einer primären Sicherheits-ID (SID), in der Regel dem Windows-Benutzernamen des Benutzers und einer oder mehreren Gruppen-SIDs, die den Windows-Gruppen entsprechen, deren Mitglied der Benutzer ist.

Die Zeit, die ONTAP aus der Konvertierung der UNIX UID in eine SMB-Zugangsdaten zieht, kann von Millisekunden in hunderte von Millisekunden betragen, da der Prozess die Kontaktaufnahme mit einem Domain Controller erfordert. ONTAP ordnet die UID den SMB-Anmeldedaten zu und gibt die Zuordnung in einen Anmeldeinformationscache ein, um die durch die Konvertierung verursachte Verifizierungszeit zu reduzieren.

Funktionsweise des NFS-Caches für Zugangsdaten

Wenn ein NFS-Benutzer Zugriff auf NFS-Exporte im Storage-System anfordert, muss ONTAP zur Authentifizierung des Benutzers seine Zugangsdaten entweder von externen Name Servern oder aus lokalen Dateien abrufen. ONTAP speichert diese Zugangsdaten dann in einem internen Cache für Zugangsdaten, um sie später verwenden zu können. Wenn die Funktionsweise der NFS-Caches für Zugangsdaten klar ist, können auch potenzielle Performance- und Zugriffsprobleme vermieden werden.

Ohne den Cache für Zugangsdaten müsste ONTAP jedes Mal, wenn ein NFS-Benutzer Zugriff angefordert hätte, Nameservices abfragen. Auf einem überlasteten Storage-System, auf das viele Benutzer zugreifen, kann dies schnell zu ernsthaften Performance-Problemen führen, was zu unerwünschten Verzögerungen oder gar zum NFS-Client-Zugriff führt.

Im Cache für Zugangsdaten ruft ONTAP die Zugangsdaten ab und speichert sie anschließend für einen vorab festgelegten Zeitraum für den schnellen und einfachen Zugriff, sollte der NFS-Client eine weitere Anforderung senden. Diese Methode bietet die folgenden Vorteile:

- Sie vereinfacht die Belastung des Storage-Systems durch die Verarbeitung von weniger Anfragen an externe Name Server (z. B. NIS oder LDAP).
- Dies vereinfacht die Belastung von externen Name Servern, indem weniger Anfragen an sie gesendet

werden.

- Es beschleunigt den Benutzerzugriff, da die Wartezeit für den Erhalt von Anmeldeinformationen von externen Quellen entfällt, bevor der Benutzer authentifiziert werden kann.

ONTAP speichert sowohl positive als auch negative Anmeldedaten im Cache für Zugangsdaten. Positive Anmeldeinformationen bedeuten, dass der Benutzer authentifiziert wurde und Zugriff gewährt wurde. Negative Anmeldeinformationen bedeuten, dass der Benutzer nicht authentifiziert wurde und der Zugriff verweigert wurde.

Standardmäßig speichert ONTAP 24 Stunden lang positive Anmeldeinformationen. Das heißt, nach der erstmaligen Authentifizierung eines Benutzers verwendet ONTAP die im Cache gespeicherten Zugangsdaten für alle Zugriffsanfragen dieses Benutzers für 24 Stunden. Wenn der Benutzer nach 24 Stunden Zugriff anfordert, beginnt der Zyklus: ONTAP entnimmt die zwischengespeicherten Anmeldeinformationen und erhält die Anmeldeinformationen erneut aus der entsprechenden Namensdienstquelle. Wenn sich die Anmeldeinformationen auf dem Namensserver während der letzten 24 Stunden geändert haben, speichert ONTAP die aktualisierten Anmeldeinformationen für die nächsten 24 Stunden im Cache.

Standardmäßig speichert ONTAP negative Zugangsdaten für zwei Stunden. Das heißt, nachdem ONTAP den Zugriff zunächst einem Benutzer verweigert hat, werden alle Zugriffsanfragen des Benutzers für zwei Stunden lang verweigert. Wenn der Benutzer nach 2 Stunden Zugriff anfordert, beginnt der Zyklus: ONTAP erhält die Anmeldeinformationen erneut aus der entsprechenden Namensdienstquelle. Wenn sich die Anmeldeinformationen auf dem Namensserver in den letzten zwei Stunden geändert haben, speichert ONTAP die aktualisierten Anmeldeinformationen für die nächsten zwei Stunden im Cache.