Client-Autorisierung

ONTAP 9

NetApp
January 17, 2025

Inhalt

Client-Autorisierung

Übersicht und Optionen für die ONTAP-Clientautorisierung

Die ONTAP OAuth 2.0 Implementierung ist flexibel und robust und bietet Ihnen die Funktionen, die Sie zur Sicherung Ihrer ONTAP Umgebung benötigen. Es stehen mehrere Konfigurationsoptionen zur Verfügung, die sich gegenseitig ausschließen. Die Autorisierungsentscheidungen basieren letztlich auf den ONTAP-REST-Rollen, die entweder in den OAuth 2.0-Zugriffstoken enthalten sind oder von diesen abgeleitet wurden.

Sie können nur verwenden"ONTAP REST-Rollen", wenn Sie die Autorisierung für OAuth 2.0 konfigurieren. Die früheren herkömmlichen ONTAP Rollen werden nicht unterstützt.

ONTAP wendet je nach Konfiguration die am besten geeignete Autorisierungsoption an. Weitere Informationen dazu, wie ONTAP Client-Zugriffsentscheidungen trifft, finden Sie unter"Wie ONTAP den Zugriff bestimmt".

OAuth 2.0 eigenständige Oszilloskope

Diese Bereiche enthalten eine oder mehrere benutzerdefinierte REST-Rollen, die jeweils in einer einzigen Zeichenfolge im Zugriffstoken eingekapselt sind. Sie sind unabhängig von den Rollendefinitionen von ONTAP. Sie müssen die Bereichszeichenfolgen auf Ihrem Autorisierungsserver konfigurieren. Weitere Informationen finden Sie unter "Eigenständige Oszilloskope von OAuth 2.0" .

Lokale ONTAP-REST-Rollen

Es kann eine einzelne benannte REST-Rolle verwendet werden, entweder erstellt oder benutzerdefiniert. Die scope Syntax für eine benannte Rolle ist **ontap-role-**<URL-encoded-ONTAP-role-name>. Wenn die Rolle ONTAP beispielsweise der scope string ist `admin`, wird dies der Fall sein `ontap-role-admin`.

Benutzer

Der Benutzername im Zugriffstoken, der mit Zugriff auf die Anwendung "http" definiert ist, kann verwendet werden. Anhand der definierten Authentifizierungsmethode wird ein Benutzer in der folgenden Reihenfolge getestet: Passwort, Domäne (Active Directory), nsswitch (LDAP).

Gruppen

Die Autorisierungsserver können so konfiguriert werden, dass sie ONTAP-Gruppen für die Autorisierung verwenden. Wenn die lokalen ONTAP-Definitionen überprüft werden, aber keine Zugriffsentscheidung getroffen werden kann, werden die Active Directory („Domain“)- oder LDAP („nsswitch“)-Gruppen verwendet. Gruppeninformationen können auf zwei Arten angegeben werden:

- OAuth 2.0-Scope-String

  Unterstützt vertrauliche Anwendungen, die den Ablauf der Clientanmeldeinformationen verwenden, wenn kein Benutzer mit einer Gruppenmitgliedschaft vorhanden ist. Der Umfang sollte benannt werden **ontap-Group-**<URL-encoded-ONTAP-group-name>. Wenn die Gruppe beispielsweise „Entwicklung“ ist, lautet der Scope String „ontap-Group-Development“.

- In der „Gruppe“-Forderung

  Dies ist für Zugriffstoken vorgesehen, die von ADFS unter Verwendung des Ablaufs Resource Owner (Password Grant) ausgegeben werden.

Weitere Informationen finden Sie unter "Arbeiten mit Gruppen" .

Eigenständige Oszilloskope von OAuth 2.0

In sich geschlossene Bereiche sind Strings, die im Zugriffstoken enthalten sind. Jede dieser Rollen ist vollständig definiert und beinhaltet alles, was ONTAP für eine Zugriffsentscheidung benötigt. Der Umfang unterscheidet sich von jeder der REST-Rollen, die in ONTAP selbst definiert sind.

Format der Bereichszeichenfolge

Auf einer Basisebene wird der Umfang als zusammenhängende Zeichenfolge dargestellt und besteht aus sechs durch Doppelpunkte getrennten Werten. Die im Scope String verwendeten Parameter werden im Folgenden beschrieben.

ONTAP-Literal

Der Umfang muss mit dem Literalwert `ontap` in Kleinbuchstaben beginnen. Der ONTAP-spezifische Umfang wird angegeben.

Cluster

Dies definiert, auf welchen ONTAP Cluster sich der Umfang bezieht. Die Werte können Folgendes umfassen:

- Cluster-UUID

  Identifiziert ein einzelnes Cluster.

- Sternchen (*)

  Gibt an, dass der Umfang auf alle Cluster angewendet wird.

Sie können den ONTAP-CLI-Befehl verwenden `cluster identity show`, um die UUID Ihres Clusters anzuzeigen. Falls nicht angegeben, gilt der Umfang für alle Cluster.

Rolle

Der Name der im eigenständigen Bereich enthaltenen REST-Rolle. Dieser Wert wird von ONTAP nicht untersucht oder auf vorhandene REST-Rollen abgestimmt, die für ONTAP definiert sind. Der Name wird für die Protokollierung verwendet.

Zugangsstufe

Dieser Wert gibt die Zugriffsebene an, die auf die Clientanwendung angewendet wird, wenn der API-Endpunkt im Umfang verwendet wird. Es gibt sechs mögliche Werte, wie in der Tabelle unten beschrieben.

Zugangsstufe	Beschreibung
Keine	Verweigert allen Zugriff auf den angegebenen Endpunkt.
readonly	Nur Lesezugriff mit GET ist möglich.

Zugangsstufe	Beschreibung
Read_create	Ermöglicht den Lesezugriff sowie die Erstellung neuer Ressourceninstanzen über POST.
Lesen_ändern	Ermöglicht den Lesezugriff sowie die Möglichkeit, vorhandene Ressourcen mithilfe von PATCHES zu aktualisieren.
Lesen_create_modify	Ermöglicht alle Zugriffe außer Löschen. Zu den zulässigen Operationen gehören GET (read), POST (create) und PATCH (Update).
Alle	Ermöglicht vollständigen Zugriff.

SVM

Der Name der SVM innerhalb des Clusters, für den der Umfang gilt. Verwenden Sie den *-Wert (Sternchen), um alle SVMs anzuzeigen.

> Diese Funktion wird von ONTAP 9.14.1 nicht vollständig unterstützt. Sie können den SVM-Parameter ignorieren und ein Sternchen als Platzhalter verwenden. Überprüfen Sie die "Versionshinweise zu ONTAP", um auf zukünftigen SVM-Support zu prüfen.

REST-API-URI

Der vollständige oder teilweise Pfad zu einer Ressource oder einem Satz zugehöriger Ressourcen. Der String muss mit beginnen `/api`. Wenn Sie keinen Wert angeben, gilt der Umfang für alle API-Endpunkte im ONTAP-Cluster.

Beispiele für den Umfang

Im Folgenden werden einige Beispiele für eigenständige Oszilloskope vorgestellt.

ontap:*:joes-role:read_create_modify:*:/API/Cluster

Bietet dem Benutzer, dem diese Rolle zugewiesen `/cluster` ist, den Zugriff auf den Endpunkt zu lesen, zu erstellen und zu ändern.

CLI-Verwaltungstool

Um die Verwaltung der eigenständigen Bereiche einfacher und weniger fehleranfällig `security oauth2 scope` zu machen, bietet ONTAP den CLI-Befehl, um auf der Grundlage Ihrer Eingabeparameter Scope Strings zu generieren.

Der Befehl `security oauth2 scope` hat zwei Anwendungsfälle basierend auf Ihrer Eingabe:

- CLI-Parameter für den Umfang einer Zeichenfolge

  Mit dieser Version des Befehls können Sie auf Grundlage der Eingabeparameter eine Bereichszeichenfolge generieren.

- Scope-String zu CLI-Parametern

  Sie können diese Version des Befehls verwenden, um die Befehlsparameter basierend auf der Zeichenfolge für den Eingabebereich zu generieren.

Beispiel

Im folgenden Beispiel wird eine Scope-String mit der Ausgabe generiert, die nach dem unten stehenden Befehlsbeispiel enthalten ist. Die Definition gilt für alle Cluster.

```
security oauth2 scope cli-to-scope -role joes-role -access readonly -api
/api/cluster
```

```
ontap:*:joes-role:readonly:*:/api/cluster
```

Arbeiten mit Gruppen

ONTAP bietet verschiedene Optionen zum Konfigurieren von Gruppen basierend auf Ihrem Autorisierungsserver. Die Gruppen können dann Rollen zugeordnet werden, die von ONTAP zur Bestimmung des Zugriffs verwendet werden.

Wie Gruppen identifiziert werden

Wenn Sie eine Gruppe auf einem Autorisierungsserver konfigurieren, wird sie identifiziert und in einem OAuth 2.0-Zugriffstoken mit einem Namen oder einer UUID übertragen. Vor der Konfiguration von ONTAP müssen Sie sich darüber im Klaren sein, wie Ihr Autorisierungsserver Gruppen verarbeitet.

Wenn mehrere Gruppen in einem Zugriffstoken enthalten sind, versucht ONTAP, jede Gruppe zu verwenden, bis eine Übereinstimmung vorhanden ist.

Gruppennamen

Viele Autorisierungsserver identifizieren und stellen Gruppen mit einem Namen dar. Hier ist ein Fragment eines JSON-Zugriffstoken, das vom Active Directory Federation Service (ADFS) generiert wird und mehrere Gruppen enthält. Weitere Informationen finden Sie unter Verwalten von Gruppen mit Namen .

```
...
"sub": "User1_TestDev@NICAD5.COM",
"group": [
  "NICAD5\\Domain Users",
  "NICAD5\\Development Group",
  "NICAD5\\Production Group"
],
"apptype": "Confidential",
"appid": "3bff3b2b-8e40-44ba-7c11-d73c3b76e3e8",
...
```

Gruppen-UUIDs

Einige Autorisierungsserver identifizieren und stellen Gruppen mit einer UUID dar. Hier ist ein Fragment eines JSON-Zugriffstoken, das von Microsoft Entra ID mit mehreren Gruppen generiert wird. Weitere Informationen finden Sie unter Verwalten von Gruppen mit UUIDs .

```
...
"appid": "4aff4b4b-8e40-44ba-7c11-d73c3b76e3d7",
"appidacr": "1",
"groups": [
  "8ea4c5b0-bcad-4e66-8f1e-cd395474a448",
  "a8558fc2-a1b2-4cb7-cc41-59bd831840cc"],
"name": "admin007 with group membership",
...
```

Verwalten von Gruppen mit Namen

Wenn Ihr Autorisierungsserver zur Identifizierung von Gruppen Namen verwendet, müssen Sie sicherstellen, dass jede Gruppe für ONTAP definiert ist. Je nach Sicherheitsumgebung ist die Gruppe möglicherweise bereits definiert.

Hier ist ein Beispiel für einen CLI-Befehl, der eine Gruppe zu ONTAP definiert. Beachten Sie, dass es eine benannte Gruppe aus dem Beispiel-Zugriffstoken verwendet. Sie müssen sich auf der ONTAP **admin** Berechtigungsebene befinden, um den Befehl ausgeben zu können.

Beispiel

```
security login create -user-or-group-name "NICAD5\\Domain Users"
-application http -authentication-method domain -role admin
```

Sie können diese Funktion auch mit der ONTAP REST-API konfigurieren. Erfahren Sie mehr in der "Dokumentation zur ONTAP Automatisierung".

Verwalten von Gruppen mit UUIDs

Wenn Ihr Autorisierungsserver Gruppen mit UUID-Werten darstellt, müssen Sie vor der Verwendung einer Gruppe eine Konfiguration in zwei Schritten durchführen. Ab ONTAP 9.16.1 sind zwei Mapping-Funktionen verfügbar und wurden mit Microsoft Entra ID getestet. Sie müssen sich auf der ONTAP **admin** Berechtigungsebene befinden, um die CLI Befehle ausgeben zu können.

Sie können diese Funktionen auch mit der ONTAP-REST-API konfigurieren. Erfahren Sie mehr in der "Dokumentation zur ONTAP Automatisierung".

Verwandte Informationen

- "ONTAP-CLI-Befehle"

Ordnen Sie eine Gruppen-UUID einem Gruppennamen zu

Wenn Sie einen Autorisierungsserver verwenden, der Gruppen darstellt, die UUID-Werte verwenden, müssen Sie die Gruppen-UUIDs Gruppennamen zuordnen. Die primären ONTAP CLI-Vorgänge werden im Folgenden beschrieben.

Erstellen

Mit dem Befehl können Sie eine neue Gruppenzuordnungskonfiguration definieren `security login group create`. Die Gruppen-UUID und der Name müssen mit der Konfiguration auf dem Autorisierungsserver übereinstimmen.

Parameter

Die Parameter, die zum Erstellen einer Gruppenzuordnung verwendet werden, werden im Folgenden beschrieben.

Parameter	Beschreibung
`vserver`	Gibt optional den Namen der SVM (vServer) an, mit der die Gruppe verknüpft ist. Wenn sie nicht angegeben ist, ist die Gruppe dem ONTAP-Cluster zugeordnet.
`name`	Der eindeutige Name der Gruppe, die ONTAP verwendet.
`type`	Dieser Wert gibt den Identitätsanbieter an, von dem die Gruppe stammt.
`uuid`	Gibt die universell eindeutige Kennung der Gruppe an, die vom Autorisierungsserver bereitgestellt wird.

Hier ist ein Beispiel für einen CLI-Befehl, der eine Gruppe zu ONTAP definiert. Beachten Sie, dass es eine UUID-Gruppe aus dem Beispiel-Zugriffstoken verwendet.

Beispiel

```
security login group create -vserver ontap-cls-1 -name IAM_Dev -type entra
-uuid 8ea4c5b0-bcad-4e66-8f1e-cd395474a448
```

Nach dem Erstellen der Gruppe wird eine eindeutige schreibgeschützte Ganzzahl-ID für die Gruppe generiert.

Zusätzliche CLI-Vorgänge

Der Befehl unterstützt mehrere zusätzliche Vorgänge, darunter:

- Anzeigen
- Ändern
- Löschen

Sie können die Option verwenden `show`, um die eindeutige Gruppen-ID abzurufen, die für eine Gruppe generiert wurde. Weitere Informationen finden Sie in der Referenzdokumentation zu ONTAP-Befehlen.

Ordnen Sie eine Gruppen-UUID einer Rolle zu

Wenn Sie einen Autorisierungsserver verwenden, der Gruppen darstellt, die UUID-Werte verwenden, können Sie die Gruppe einer Rolle zuordnen. Die primären ONTAP CLI-Vorgänge werden im Folgenden beschrieben. Außerdem müssen Sie sich auf der ONTAP **admin** Berechtigungsebene befinden, um die Befehle ausgeben zu können.

Sie müssen zuerst Ordnen Sie eine Gruppen-UUID einem Gruppennamen zudie eindeutige Integer-ID abrufen, die für die Gruppe generiert wurde. Sie benötigen die ID, um die Gruppe einer Rolle zuzuordnen.

Erstellen

Mit dem Befehl können Sie eine neue Rollenzuordnung definieren `security login group role-mapping create`.

Parameter

Im Folgenden werden die Parameter beschrieben, mit denen eine Gruppe einer Rolle zugeordnet werden kann.

Parameter	Beschreibung
`group-id`	Gibt die eindeutige ID an, die mit dem Befehl für die Gruppe generiert `security login group create` wurde.
`role`	Der Name der ONTAP-Rolle, der die Gruppe zugeordnet ist.

Beispiel

```
security login group role-mapping create -group-id 1 -role admin
```

Zusätzliche CLI-Vorgänge

Der Befehl unterstützt mehrere zusätzliche Vorgänge, darunter:

- Anzeigen
- Ändern
- Löschen

Weitere Informationen finden Sie in der Referenzdokumentation zu ONTAP-Befehlen.

Externe Rollenzuordnung

Eine externe Rolle wird bei einem Identifizieren-Anbieter definiert, der für die Verwendung durch ONTAP konfiguriert ist. Sie können Zuordnungsbeziehungen zwischen diesen externen Rollen und den ONTAP Rollen mit der ONTAP CLI erstellen und verwalten.

Sie können auch die externe Rollenzuordnungsfunktion mit der ONTAP REST-API konfigurieren. Erfahren Sie mehr in der "Dokumentation zur ONTAP Automatisierung".

Verwandte Informationen

- "ONTAP-CLI-Befehle".

Externe Rollen in einem Zugriffstoken

Hier ist ein Fragment eines JSON-Zugriffstoken, der zwei externe Rollen enthält.

```
...
"appidacr": "1",
"family_name": "User",
"name": "Test User 1",
"oid": "4c2215c7-6d52-40a7-ce71-096fa41379ba",
"roles": [
  "Global Administrator",
  "Application Administrator"
],
"ver": "1.0",
...
```

Konfiguration

Sie können die externe Rollenzuordnungsfunktion über die ONTAP-Befehlszeilenschnittstelle verwalten.

Erstellen

Mit dem Befehl können Sie eine Rollenzuordnungskonfiguration definieren `security login external-role-mapping create`. Sie müssen auf der ONTAP **admin** Berechtigungsebene sein, um diesen Befehl sowie die damit verbundenen Optionen ausgeben zu können.

Parameter

Die Parameter, die zum Erstellen einer Gruppenzuordnung verwendet werden, werden im Folgenden beschrieben.

Parameter	Beschreibung
`external-role`	Der Name der Rolle, die beim externen Identitätsanbieter definiert wurde.
`provider`	Der Name des Identitätsanbieters. Dies sollte die Kennung für das System sein.
`ontap-role`	Gibt die vorhandene ONTAP-Rolle an, der die externe Rolle zugeordnet ist.

Beispiel

```
security login external-role-mapping create -external-role "Global
Administrator" -provider entra -ontap-role admin
```

Zusätzliche CLI-Vorgänge

Der Befehl unterstützt mehrere zusätzliche Vorgänge, darunter:

- Anzeigen
- Ändern
- Löschen

Weitere Informationen finden Sie in der Referenzdokumentation zu ONTAP-Befehlen oder in den ONTAP CLI-

man-Pages.

Wie ONTAP den Client-Zugriff bestimmt

Um OAuth 2.0 richtig zu entwickeln und zu implementieren, müssen Sie verstehen, wie Ihre Autorisierungskonfiguration von ONTAP verwendet wird, um Zugriffsentscheidungen für die Clients zu treffen. Die wichtigsten Schritte zur Bestimmung des Zugriffs sind unten auf der Grundlage der ONTAP Version dargestellt.

Es gab keine signifikanten Updates für OAuth 2.0 mit ONTAP 9.15.1. Wenn Sie Version 9.15.1 verwenden, lesen Sie die Beschreibung für ONTAP 9.14.1.

Verwandte Informationen

- "In ONTAP unterstützte Funktionen von OAuth 2.0"

ONTAP 9.16.1

ONTAP 9.16.1 erweitert die Standard-OAuth 2.0-Unterstützung um Microsoft-Entra-ID-spezifische Erweiterungen für native Entra-ID-Gruppen sowie externe Rollenzuordnung.

Bestimmen Sie den Client-Zugriff für ONTAP 9.16.1

Schritt 1: Eigenständige Bereiche

Wenn das Zugriffstoken eigenständige Bereiche enthält, untersucht ONTAP diese Bereiche zuerst. Wenn keine eigenständigen Bereiche vorhanden sind, mit Schritt 2 fortfahren.

Wenn ein oder mehrere eigenständige Bereiche vorhanden sind, wendet ONTAP jeden Bereich an, bis eine explizite **ALLOW**- oder **DENY**-Entscheidung getroffen werden kann. Wenn eine explizite Entscheidung getroffen wird, endet die Verarbeitung.

Wenn ONTAP keine explizite Zugriffsentscheidung treffen kann, fahren Sie mit Schritt 2 fort.

Schritt 2: Überprüfen Sie die lokale Rollenmarkierung

ONTAP überprüft den booleschen Parameter `use-local-roles-if-present`. Der Wert dieses Flags wird für jeden Autorisierungsserver, der für ONTAP definiert ist, separat festgelegt.

- Wenn der Wert lautet, `true` fahren Sie mit Schritt 3 fort.
- Wenn der Wert `false` verarbeitet wird, endet und der Zugriff verweigert wird.

Schritt 3: Benannte ONTAP REST-Rolle

Wenn das Zugriffstoken eine benannte REST-Rolle im Feld oder oder `scp` als Antrag enthält `scope`, verwendet ONTAP diese Rolle, um die Zugriffsentscheidung zu treffen. Dies führt immer zu einer **ALLOW** oder **DENY** Entscheidung und Verarbeitungsende.

Wenn keine benannte REST-Rolle vorhanden ist oder die Rolle nicht gefunden wurde, fahren Sie mit Schritt 4 fort.

Schritt 4: Benutzer

Extrahieren Sie den Benutzernamen aus dem Zugriffstoken und versuchen Sie, ihn mit Benutzern zu vergleichen, die Zugriff auf die Anwendung „http“ haben. Die Benutzer werden anhand der Authentifizierungsmethode in der folgenden Reihenfolge untersucht:

- Passwort
- Domäne (Active Directory)
- Nsswitch (LDAP)

Wenn ein übereinstimmender Benutzer gefunden wird, verwendet ONTAP die für den Benutzer definierte Rolle, um eine Zugriffsentscheidung zu treffen. Dies führt immer zu einer **ALLOW** oder **DENY** Entscheidung und Verarbeitungsende.

Wenn ein Benutzer nicht stimmt oder kein Benutzername im Zugriffstoken vorhanden ist, fahren Sie mit Schritt 5 fort.

Schritt 5: Gruppen

Wenn eine oder mehrere Gruppen eingeschlossen sind, wird das Format geprüft. Wenn die Gruppen als UUIDs dargestellt werden, wird eine interne Gruppenzuordnungstabelle durchsucht. Wenn ein Gruppenabgleich und eine zugehörige Rolle vorhanden sind, verwendet ONTAP die für die Gruppe definierte Rolle, um eine Zugriffsentscheidung zu treffen. Dies führt immer zu einer **ALLOW** oder **DENY** Entscheidung und Verarbeitungsende. Weitere Informationen finden Sie unter "Arbeiten mit Gruppen".

Wenn Gruppen als Namen dargestellt und mit Domain- oder nsswitch-Autorisierung konfiguriert werden, versucht ONTAP, sie einer Active Directory- bzw. LDAP-Gruppe zuzuordnen. Wenn eine

Gruppenübereinstimme vorhanden ist, verwendet ONTAP die für die Gruppe definierte Rolle, um eine Zugriffsentscheidung zu treffen. Dies führt immer zu einer **ALLOW** oder **DENY** Entscheidung und Verarbeitungsende.

Wenn keine Gruppenübereinstimme vorhanden ist oder keine Gruppe im Zugriffstoken vorhanden ist, wird der Zugriff verweigert und die Verarbeitung wird beendet.

ONTAP 9.14.1

Die Unterstützung von OAuth 2.0 wird mit ONTAP 9.14.1 auf Basis der Standard-OAuth 2.0-Funktionen eingeführt.

Bestimmen Sie den Client-Zugriff für ONTAP 9.14.1

Schritt 1: Eigenständige Bereiche

Wenn das Zugriffstoken eigenständige Bereiche enthält, untersucht ONTAP diese Bereiche zuerst. Wenn keine eigenständigen Bereiche vorhanden sind, mit Schritt 2 fortfahren.

Wenn ein oder mehrere eigenständige Bereiche vorhanden sind, wendet ONTAP jeden Bereich an, bis eine explizite **ALLOW**- oder **DENY**-Entscheidung getroffen werden kann. Wenn eine explizite Entscheidung getroffen wird, endet die Verarbeitung.

Wenn ONTAP keine explizite Zugriffsentscheidung treffen kann, fahren Sie mit Schritt 2 fort.

Schritt 2: Überprüfen Sie die lokale Rollenmarkierung

ONTAP überprüft den booleschen Parameter `use-local-roles-if-present`. Der Wert dieses Flags wird für jeden Autorisierungsserver, der für ONTAP definiert ist, separat festgelegt.

- Wenn der Wert lautet, `true` fahren Sie mit Schritt 3 fort.
- Wenn der Wert `false` verarbeitet wird, endet und der Zugriff verweigert wird.

Schritt 3: Benannte ONTAP REST-Rolle

Wenn das Zugriffstoken eine benannte REST-Rolle im Feld oder `scp` enthält `scope`, verwendet ONTAP die Rolle, um die Zugriffsentscheidung zu treffen. Dies führt immer zu einer **ALLOW** oder **DENY** Entscheidung und Verarbeitungsende.

Wenn keine benannte REST-Rolle vorhanden ist oder die Rolle nicht gefunden wurde, fahren Sie mit Schritt 4 fort.

Schritt 4: Benutzer

Extrahieren Sie den Benutzernamen aus dem Zugriffstoken und versuchen Sie, ihn mit Benutzern zu vergleichen, die Zugriff auf die Anwendung „http“ haben. Die Benutzer werden anhand der Authentifizierungsmethode in der folgenden Reihenfolge untersucht:

- Passwort
- Domäne (Active Directory)
- Nsswitch (LDAP)

Wenn ein übereinstimmender Benutzer gefunden wird, verwendet ONTAP die für den Benutzer definierte Rolle, um eine Zugriffsentscheidung zu treffen. Dies führt immer zu einer **ALLOW** oder **DENY** Entscheidung und Verarbeitungsende.

Wenn ein Benutzer nicht stimmt oder kein Benutzername im Zugriffstoken vorhanden ist, fahren Sie mit Schritt 5 fort.

Schritt 5: Gruppen

Wenn eine oder mehrere Gruppen eingeschlossen und mit einer Domain- oder nsswitch-Autorisierung konfiguriert sind, versucht ONTAP, sie einer Active Directory- bzw. LDAP-Gruppe zuzuordnen.

Wenn eine Gruppenübereinstimme vorhanden ist, verwendet ONTAP die für die Gruppe definierte Rolle, um eine Zugriffsentscheidung zu treffen. Dies führt immer zu einer **ALLOW** oder **DENY** Entscheidung und Verarbeitungsende.

Wenn keine Gruppenübereinstimme vorhanden ist oder keine Gruppe im Zugriffstoken vorhanden ist,

wird der Zugriff verweigert und die Verarbeitung wird beendet.

Copyright-Informationen

Markeninformationen