Konfigurieren Sie Namenszuordnungen

ONTAP 9

NetApp
March 30, 2023

Inhaltsverzeichnis

Konfigurieren Sie Namenszuordnungen

Übersicht über Namenszuordnungen konfigurieren

ONTAP verwendet Namenszuweisung, um CIFS-Identitäten UNIX-Identitäten, Kerberos-Identitäten und UNIX-Identitäten den CIFS-Identitäten zuzuordnen. Es benötigt diese Informationen, um Benutzeranmeldeinformationen zu erhalten und ordnungsgemäßen Dateizugriff bereitzustellen, unabhängig davon, ob sie eine Verbindung von einem NFS-Client oder einem CIFS-Client herstellen.

Es gibt zwei Ausnahmen, in denen Sie keine Namenszuweisung verwenden müssen:

- Sie konfigurieren eine reine UNIX-Umgebung und planen keinen CIFS-Zugriff oder NTFS-Sicherheitsstil auf Volumes.
- Sie konfigurieren stattdessen den Standardbenutzer für die Verwendung.

  In diesem Szenario ist keine Namenszuweisung erforderlich, da anstelle der Zuordnung aller einzelnen Client-Anmeldeinformationen alle Client-Anmeldeinformationen demselben Standardbenutzer zugeordnet werden.

Beachten Sie, dass Sie die Namenszuordnung nur für Benutzer und nicht für Gruppen verwenden können.

Sie können jedoch einem bestimmten Benutzer eine Gruppe von einzelnen Benutzern zuordnen. Sie können beispielsweise alle AD-Benutzer, die mit DEM Wort „VERTRIEB“ beginnen oder enden, einem bestimmten UNIX-Benutzer und der UID des Benutzers zuordnen.

Funktionsweise der Namenszuweisung

Wenn ONTAP Anmeldeinformationen für einen Benutzer zuordnen muss, überprüft er zunächst die Datenbank für die Zuordnung von lokalen Namen und den LDAP-Server auf eine vorhandene Zuordnung. Überprüft wird, ob ein oder beide Einstellungen überprüft werden und in welcher Reihenfolge durch die Name-Service-Konfiguration der SVM bestimmt wird.

- Für die Zuordnung von Windows zu UNIX

  Wenn keine Zuordnung gefunden wird, überprüft ONTAP, ob der kleine Windows-Benutzername ein gültiger Benutzername in der UNIX-Domäne ist. Wenn dies nicht funktioniert, wird der Standard-UNIX-Benutzer verwendet, sofern er konfiguriert ist. Wenn der standardmäßige UNIX-Benutzer nicht konfiguriert ist und ONTAP auf diese Weise keine Zuordnung erhalten kann, schlägt die Zuordnung fehl und es wird ein Fehler zurückgegeben.

- Für die Zuordnung von UNIX zu Windows

  Wenn keine Zuordnung gefunden wird, versucht ONTAP, ein Windows-Konto zu finden, das dem UNIX-Namen in der SMB-Domäne entspricht. Wenn dies nicht funktioniert, wird der SMB-Standardbenutzer verwendet, vorausgesetzt, er ist konfiguriert. Wenn der standardmäßige CIFS-Benutzer nicht konfiguriert ist und ONTAP auch keine Zuordnung auf diese Weise erhalten kann, schlägt die Zuordnung fehl und es wird ein Fehler zurückgegeben.

Computerkonten sind standardmäßig dem angegebenen UNIX-Standardbenutzer zugeordnet. Wenn kein UNIX-Standardbenutzer angegeben ist, schlägt die Zuordnung des Computerkontos fehl.

- Ab ONTAP 9.5 können Sie Computerkonten anderen Benutzern als dem standardmäßigen UNIX-Benutzer zuordnen.
- In ONTAP 9.4 und früher können Sie Computerkonten nicht anderen Benutzern zuordnen.

  Auch wenn Namenszuordnungen für Computerkonten definiert sind, werden die Zuordnungen ignoriert.

Multidomain sucht nach Zuordnungen von UNIX-Benutzern zu Windows-Benutzernamen

ONTAP unterstützt Multidomain-Suchen beim Zuordnen von UNIX-Benutzern zu Windows-Benutzern. Alle erkannten vertrauenswürdigen Domänen werden nach Übereinstimmungen mit dem Ersatzmuster gesucht, bis ein passendes Ergebnis zurückgegeben wird. Alternativ können Sie eine Liste der bevorzugten vertrauenswürdigen Domänen konfigurieren, die anstelle der Liste der erkannten vertrauenswürdigen Domänen verwendet wird und bis zur Rückgabe eines übereinstimmenden Ergebnisses durchsucht wird.

Wie Domain Trusts sich auf UNIX-Benutzer bei der Suche nach der Windows-User Name Mapping auswirken

Um zu verstehen, wie die Zuordnung von Benutzernamen mit mehreren Domänen funktioniert, müssen Sie verstehen, wie Domain Trusts mit ONTAP arbeiten. Active Directory-Vertrauensbeziehungen mit der Home-Domain des CIFS-Servers können ein bidirektionales Vertrauen sein oder eine von zwei Arten von unidirektionalen Trusts sein, entweder ein eingehendes Vertrauen oder ein ausgehendes Vertrauen. Die Home-Domäne ist die Domäne, zu der der CIFS-Server der SVM gehört.

- *Bidirektionales Vertrauen*

  Bei bidirektionalen Trusts vertrauen sich beide Domänen gegenseitig. Wenn die Home-Domain des CIFS-Servers bidirektional mit einer anderen Domäne vertraut ist, kann die Home-Domäne einen Benutzer authentifizieren und autorisieren, der der vertrauenswürdigen Domäne angehört, und umgekehrt.

  Die Suche nach der Zuordnung von UNIX-Benutzern zu Windows-Benutzernamen kann nur auf Domänen mit bidirektionalen Vertrauensstellungen zwischen der Home-Domain und der anderen Domain ausgeführt werden.

- *Outbound Trust*

  Mit einem ausgehenden Vertrauen vertraut die Home Domain der anderen Domain. In diesem Fall kann die Home-Domain einen Benutzer authentifizieren und autorisieren, der der vertrauenswürdigen Outbound-Domäne angehört.

  Eine Domäne mit einem abgehenden Vertrauen in die Home-Domäne wird beim Durchführen der Suche nach UNIX-Benutzern zu Windows-Benutzernamenzuordnung *not* durchsucht.

- *Inbound Trust*

  Mit einem eingehenden Vertrauen vertraut die andere Domäne auf die Home Domain des CIFS-Servers. In

diesem Fall kann die Home-Domäne einen Benutzer der eingehenden vertrauenswürdigen Domäne nicht authentifizieren oder autorisieren.

Eine Domäne mit einem eingehenden Vertrauen in die Home-Domäne wird beim Durchführen der Suche nach UNIX-Benutzern bei der Zuordnung von Windows-Benutzernamen *Not* durchsucht.

Wie Platzhalter (*) zum Konfigurieren von Mehrfachdomain-Suchen für das Namenszuordnungen verwendet werden

Suchvorgänge für die Zuordnung von Mehrfachdomänen werden durch die Verwendung von Wildcards im Domain-Bereich des Windows-Benutzernamens erleichtert. In der folgenden Tabelle wird veranschaulicht, wie Wildcards im Domain-Teil eines Namenszuordnungseintrags verwendet werden, um Mehrfachdomain-Suchen zu ermöglichen:

Muster	Austausch	Ergebnis
Stamm	*\\Administrator	Der UNIX-Benutzer „`root`“ ist dem Benutzer „`Administrator`“ zugeordnet. Alle vertrauenswürdigen Domains werden so lange durchsucht, bis der erste übereinstimmende Benutzer namens „`Administrator`“ gefunden wurde.
*	**	Gültige UNIX-Benutzer werden den entsprechenden Windows-Benutzern zugeordnet. Alle vertrauenswürdigen Domänen werden so lange durchsucht, bis der erste übereinstimmende Benutzer mit diesem Namen gefunden wurde. Das Muster ** gilt nur für die Namenszuweisung von UNIX zu Windows, nicht umgekehrt.

Durchführen von Suchvorgängen mit mehreren Domänen

Sie können eine von zwei Methoden wählen, um die Liste der vertrauenswürdigen Domänen zu bestimmen, die für die Suche nach Namen mehrerer Domänen verwendet werden:

- Verwenden Sie die automatisch erkannte bidirektionale Vertrauensliste, die von ONTAP erstellt wurde
- Verwenden Sie die Liste der bevorzugten vertrauenswürdigen Domänen, die Sie kompilieren

Wenn ein UNIX-Benutzer einem Windows-Benutzer mit einem Platzhalter zugeordnet ist, der für den Domain-

Abschnitt des Benutzernamens verwendet wird, wird der Windows-Benutzer in allen vertrauenswürdigen Domänen wie folgt angezeigt:

- Wenn eine bevorzugte Liste der vertrauenswürdigen Domäne konfiguriert ist, wird der zugeordnete Windows-Benutzer nur in dieser Suchliste in der entsprechenden Reihenfolge angezeigt.
- Wenn eine bevorzugte Liste der vertrauenswürdigen Domänen nicht konfiguriert ist, wird der Windows-Benutzer in allen bidirektionalen vertrauenswürdigen Domänen der Home-Domäne gesucht.
- Wenn es keine bidirektional vertrauenswürdigen Domänen für die Home-Domain gibt, wird der Benutzer in der Home-Domain angezeigt.

Wenn ein UNIX-Benutzer einem Windows-Benutzer ohne Domain-Abschnitt im Benutzernamen zugeordnet ist, wird der Windows-Benutzer in der Home-Domain angezeigt.

Konvertierungsregeln für Namenszuordnungen

Ein ONTAP System behält eine Reihe von Konversionsregeln für jede SVM bei. Jede Regel besteht aus zwei Teilen: Einem *pattern* und einem *Replacement*. Konvertierungen beginnen am Anfang der entsprechenden Liste und führen eine Substitution basierend auf der ersten übereinstimmenden Regel durch. Das Muster ist ein normaler Ausdruck im UNIX-Stil. Der Ersatz ist eine Zeichenkette, die Escape-Sequenzen enthält, die Unterausdrücke aus dem Muster darstellen, wie im UNIX `sed` Programm.

Erstellen einer Namenszuweisung

Sie können das verwenden `vserver name-mapping create` Befehl zum Erstellen einer Namenszuweisung. Sie verwenden Namenszuordnungen, um Windows-Benutzern den Zugriff auf UNIX-Sicherheitsstil-Volumes zu ermöglichen und umgekehrt.

Über diese Aufgabe

Für jede SVM unterstützt ONTAP bis zu 12,500 Namenszuordnungen für jede Richtung.

Schritt

1. Erstellen einer Namenszuweisung: `vserver name-mapping create -vserver` *`vserver_name`* `-direction {krb-unix|win-unix|unix-win} -position` *`integer`* `-pattern text -replacement` *`text`*

   

   Der `-pattern` Und `-replacement` Aussagen können als reguläre Ausdrücke formuliert werden. Sie können auch die verwenden `-replacement` Anweisung, eine Zuordnung zum Benutzer durch Verwendung der leeren Ersatzzeichenfolge explizit zu verweigern `" "` (Das Leerzeichen). Siehe `vserver name-mapping create` Man-Page für Details.

   Beim Erstellen von Windows-zu-UNIX-Zuordnungen müssen sich alle SMB-Clients, die zum Zeitpunkt der Erstellung der neuen Zuordnungen offene Verbindungen zum ONTAP System haben, abmelden und zurück anmelden, um die neuen Zuordnungen zu sehen.

Beispiele

Mit dem folgenden Befehl wird eine Namenszuweisung auf der SVM mit dem Namen vs1 erstellt. Die Zuordnung ist eine Zuordnung von UNIX zu Windows an Position 1 in der Prioritätenliste. Das Mapping ordnet

den UNIX-Benutzer johnd dem Windows-Benutzer eng\JohnDoe zu.

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

Mit dem folgenden Befehl wird eine weitere Namenszuweisung auf der SVM mit dem Namen vs1 erstellt. Die Zuordnung ist eine Zuordnung von Windows zu UNIX an Position 1 in der Prioritätenliste. Hier sind Muster und Ersatz enthalten reguläre Ausdrücke. Das Mapping ordnet jedem CIFS-Benutzer in der Domäne eng Benutzern in der mit der SVM verknüpften LDAP-Domäne zu.

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\1"
```

Mit dem folgenden Befehl wird eine weitere Namenszuweisung auf der SVM mit dem Namen vs1 erstellt. Hier enthält das Muster „` €`“ als Element im Windows-Benutzernamen, das entkommen sein muss. Das Mapping ordnet den Windows-Benutzer eng\ john€3ps dem UNIX-Benutzer john_OPS zu.

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

Konfigurieren Sie den Standardbenutzer

Sie können einen Standardbenutzer so konfigurieren, dass er verwendet wird, wenn alle anderen Zuordnungsversuche für einen Benutzer fehlschlagen oder wenn Sie nicht einzelne Benutzer zwischen UNIX und Windows zuordnen möchten. Wenn die Authentifizierung von nicht zugeordneten Benutzern fehlschlägt, sollten Sie keinen Standardbenutzer konfigurieren.

Über diese Aufgabe

Wenn Sie bei der CIFS-Authentifizierung nicht jeden Windows-Benutzer einem einzelnen UNIX-Benutzer zuordnen möchten, können Sie stattdessen einen standardmäßigen UNIX-Benutzer festlegen.

Wenn Sie bei der NFS-Authentifizierung nicht jeden UNIX-Benutzer einem einzelnen Windows-Benutzer zuordnen möchten, können Sie stattdessen einen standardmäßigen Windows-Benutzer festlegen.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den folgenden Befehl ein…
Konfigurieren Sie den UNIX-Standardbenutzer	`vserver cifs options modify -default -unix-user` *`user_name`*

Ihr Ziel ist	Geben Sie den folgenden Befehl ein…
Konfigurieren Sie den Windows-Standardbenutzer	`vserver nfs modify -default-win-user` *`user_name`*

Befehle zum Verwalten von Name-Zuordnungen

Zum Verwalten von Name-Zuordnungen gibt es bestimmte ONTAP-Befehle.

Ihr Ziel ist	Befehl
Erstellen einer Namenszuweisung	`vserver name-mapping create`
Eine Namenszuordnung an einer bestimmten Position einfügen	`vserver name-mapping insert`
Namenszuordnungen anzeigen	`vserver name-mapping show`
Tauschen Sie die Position von zwei Namenszuordnungen aus Ein Austausch ist nicht zulässig, wenn die Namenszuordnung mit einem ip-Qualifier-Eintrag konfiguriert ist.	`vserver name-mapping swap`
Ändern einer Namenszuweisung	`vserver name-mapping modify`
Löschen einer Namenszuweisung	`vserver name-mapping delete`
Überprüfen Sie die richtige Namenszuweisung	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

Weitere Informationen finden Sie auf der man-Page für jeden Befehl.