



Verwenden Sie lokale Benutzer und Gruppen zur Authentifizierung und Autorisierung

ONTAP 9

NetApp
March 22, 2023

Inhaltsverzeichnis

- Verwenden Sie lokale Benutzer und Gruppen zur Authentifizierung und Autorisierung 1
 - Wie ONTAP lokale Benutzer und Gruppen verwendet 1
 - Welche lokalen Berechtigungen sind 5
 - Richtlinien für die Nutzung von BUILTIN-Gruppen und dem lokalen Administratorkonto 7
 - Anforderungen für lokale Benutzerpasswörter 7
 - Vordefinierte BUILTIN-Gruppen und Standardberechtigungen 8
 - Aktivieren oder Deaktivieren der Funktionen für lokale Benutzer und Gruppen 9
 - Lokale Benutzerkonten verwalten 12
 - Verwaltung lokaler Gruppen 17
 - Lokale Berechtigungen verwalten 24

Verwenden Sie lokale Benutzer und Gruppen zur Authentifizierung und Autorisierung

Wie ONTAP lokale Benutzer und Gruppen verwendet

Lokale Benutzer und Gruppen Konzepte

Sie sollten wissen, was lokale Benutzer und Gruppen sind, und einige grundlegende Informationen über sie, bevor Sie bestimmen, ob lokale Benutzer und Gruppen in Ihrer Umgebung konfigurieren und verwenden.

- **Lokaler Benutzer**

Ein Benutzerkonto mit einer eindeutigen Sicherheitskennung (SID), die nur für die Storage Virtual Machine (SVM) sichtbar ist, auf der sie erstellt wird. Lokale Benutzerkonten haben eine Reihe von Attributen, einschließlich Benutzername und SID. Ein lokales Benutzerkonto authentifiziert sich lokal auf dem CIFS-Server mithilfe der NTLM-Authentifizierung.

Benutzerkonten verfügen über verschiedene Verwendungsmöglichkeiten:

- Wird verwendet, um einem Benutzer „*User Rights Management*“-Berechtigungen zu gewähren.
- Kontrolliert den Zugriff auf Datei- und Ordnerressourcen, die der SVM zur Verfügung stehen.

- **Lokale Gruppe**

Eine Gruppe mit einer eindeutigen SID hat nur Sichtbarkeit auf der SVM, auf der sie erstellt wird. Gruppen enthalten einen Satz Mitglieder. Mitglieder können lokale Benutzer, Domänenbenutzer, Domänengruppen und Domain-Machine-Konten sein. Gruppen können erstellt, geändert oder gelöscht werden.

Gruppen haben verschiedene Verwendungszwecke:

- Wird verwendet, um seinen Mitgliedern „*User Rights Management*“-Berechtigungen zu gewähren.
- Kontrolliert den Zugriff auf Datei- und Ordnerressourcen, die der SVM zur Verfügung stehen.

- **Lokale Domain**

Eine Domäne mit lokalem Umfang, der von der SVM begrenzt wird. Der Name der lokalen Domäne ist der CIFS-Servername. Lokale Benutzer und Gruppen sind in der lokalen Domäne enthalten.

- **Sicherheitskennung (SID)**

Ein SID ist ein numerischer Wert mit variabler Länge, der Sicherheitsgrundel im Windows-Stil identifiziert. Ein typischer SID hat beispielsweise die folgende Form: S-1-5-21-3139654847-1303905135-2517279418-123456.

- * NTLM-Authentifizierung*

Eine Microsoft Windows-Sicherheitsmethode zur Authentifizierung von Benutzern auf einem CIFS-Server.

- **Cluster replizierte Datenbank (RDB)**

Eine replizierte Datenbank mit einer Instanz an jedem Node in einem Cluster. Lokale Benutzer- und

Gruppenobjekte werden in der RDB gespeichert.

Gründe für das Erstellen von lokalen Benutzern und lokalen Gruppen

Es gibt mehrere Gründe, warum Sie lokale Benutzer und lokale Gruppen auf Ihrer Storage Virtual Machine (SVM) erstellen sollten. Sie können beispielsweise über ein lokales Benutzerkonto auf einen SMB-Server zugreifen, wenn die Domänencontroller (DCs) nicht verfügbar sind, Sie lokale Gruppen zum Zuweisen von Berechtigungen verwenden möchten oder sich Ihr SMB-Server in einer Arbeitsgruppe befindet.

Aus folgenden Gründen können Sie ein oder mehrere lokale Benutzerkonten erstellen:

- Ihr SMB-Server befindet sich in einer Arbeitsgruppe, und Domänenbenutzer sind nicht verfügbar.

Lokale Benutzer sind in Arbeitsgruppen-Konfigurationen erforderlich.

- Sie möchten die Möglichkeit haben, sich beim SMB-Server zu authentifizieren und anzumelden, wenn die Domänencontroller nicht verfügbar sind.

Lokale Benutzer können sich beim Ausfall des Domänencontrollers mit dem SMB-Server durch NTLM-Authentifizierung authentifizieren oder wenn Netzwerkprobleme verhindern, dass Ihr SMB-Server den Domänencontroller kontaktiert.

- Sie möchten einem lokalen Benutzer die Berechtigungen „*User Rights Management*“ zuweisen.

User Rights Management bietet einem SMB-Serveradministrator die Möglichkeit, die Rechte der Benutzer und Gruppen auf der SVM zu kontrollieren. Sie können einem Benutzer Berechtigungen zuweisen, indem Sie dem Konto des Benutzers die Berechtigungen zuweisen oder den Benutzer zu einem Mitglied einer lokalen Gruppe mit diesen Berechtigungen machen.

Aus folgenden Gründen können Sie eine oder mehrere lokale Gruppen erstellen:

- Ihr SMB-Server befindet sich in einer Arbeitsgruppe, und Domänengruppen sind nicht verfügbar.

Lokale Gruppen sind in Arbeitsgruppen-Konfigurationen nicht erforderlich, können aber für die Verwaltung von Zugriffsberechtigungen für Benutzer lokaler Arbeitsgruppen nützlich sein.

- Sie möchten den Zugriff auf Datei- und Ordnerressourcen steuern, indem Sie lokale Gruppen zur Freigabe- und Dateizugriffskontrolle verwenden.
- Sie möchten lokale Gruppen mit benutzerdefinierten Berechtigungen *User Rights Management* erstellen.

Einige integrierte Benutzergruppen haben vordefinierte Berechtigungen. Um einen benutzerdefinierten Satz von Berechtigungen zuzuweisen, können Sie eine lokale Gruppe erstellen und dieser Gruppe die erforderlichen Berechtigungen zuweisen. Anschließend können Sie der lokalen Gruppe lokale Benutzer, Domänenbenutzer und Domänengruppen hinzufügen.

Verwandte Informationen

[Funktionsweise der lokalen Benutzerauthentifizierung](#)

[Liste der unterstützten Berechtigungen](#)

Funktionsweise der lokalen Benutzerauthentifizierung

Bevor ein lokaler Benutzer auf Daten auf einem CIFS-Server zugreifen kann, muss er eine authentifizierte Sitzung erstellen.

Da SMB auf Sitzungen basiert ist, kann die Identität des Benutzers nur einmal bestimmt werden, wenn die Sitzung zum ersten Mal eingerichtet wird. Der CIFS-Server verwendet bei der Authentifizierung lokaler Benutzer eine NTLM-basierte Authentifizierung. Sowohl NTLMv1 als auch NTLMv2 werden unterstützt.

Bei ONTAP wird die lokale Authentifizierung in drei Anwendungsfällen eingesetzt. Jeder Anwendungsfall hängt davon ab, ob der Domain-Teil des Benutzernamens (mit DOMAIN\User Format) mit dem lokalen Domain-Namen des CIFS-Servers (der CIFS-Servername) übereinstimmt:

- Der Domain-Teil stimmt überein

Benutzer, die lokale Benutzeranmeldeinformationen bereitstellen, wenn sie Zugriff auf Daten anfordern, werden lokal auf dem CIFS-Server authentifiziert.

- Der Domain-Teil stimmt nicht überein

ONTAP versucht, NTLM-Authentifizierung mit einem Domain Controller in der Domäne zu verwenden, zu der der CIFS-Server gehört. Wenn die Authentifizierung erfolgreich ist, ist die Anmeldung abgeschlossen. Wenn es nicht gelingt, was als nächstes geschieht, hängt davon ab, warum die Authentifizierung nicht erfolgreich war.

Wenn der Benutzer beispielsweise in Active Directory existiert, das Passwort jedoch ungültig oder abgelaufen ist, versucht ONTAP nicht, das entsprechende lokale Benutzerkonto auf dem CIFS-Server zu verwenden. Stattdessen schlägt die Authentifizierung fehl. In anderen Fällen verwendet ONTAP das entsprechende lokale Konto auf dem CIFS-Server, sofern es existiert, für die Authentifizierung - auch wenn die NetBIOS-Domänennamen nicht übereinstimmen. Wenn beispielsweise ein passendes Domänenkonto existiert, es aber deaktiviert ist, verwendet ONTAP das entsprechende lokale Konto auf dem CIFS-Server zur Authentifizierung.

- Der Domain-Teil wurde nicht angegeben

ONTAP versucht zum ersten Mal, die Authentifizierung als lokaler Benutzer zu aktivieren. Wenn die Authentifizierung als lokaler Benutzer fehlschlägt, dann authentifiziert ONTAP den Benutzer mit einem Domänencontroller in der Domäne, zu der der CIFS-Server gehört.

Nachdem die lokale Benutzerauthentifizierung oder die Domänenbenutzerauthentifizierung erfolgreich abgeschlossen wurde, baut ONTAP ein komplettes Benutzerzugriffstoken auf, das die Mitgliedschaft und Berechtigungen der lokalen Gruppe berücksichtigt.

Weitere Informationen zur NTLM-Authentifizierung für lokale Benutzer finden Sie in der Microsoft Windows-Dokumentation.

Verwandte Informationen

[Aktivieren oder Deaktivieren der lokalen Benutzerauthentifizierung](#)

Wie Benutzer-Access-Token erstellt werden

Wenn ein Benutzer eine Freigabe zuordnet, wird eine authentifizierte SMB-Sitzung eingerichtet und ein Benutzer-Access-Token erstellt, das Informationen über den

Benutzer, die Gruppenmitgliedschaft des Benutzers und die kumulativen Berechtigungen sowie den zugeordneten UNIX-Benutzer enthält.

Sofern die Funktion nicht deaktiviert ist, werden dem Benutzer- und Gruppeninformationen auch lokale Benutzer- und Gruppeninformationen hinzugefügt. Die Art und Weise, wie Access Tokens aufgebaut werden, hängt davon ab, ob sich die Anmeldung für einen lokalen Benutzer oder einen Active Directory-Domänenbenutzer befindet:

- Lokale Benutzeranmeldung

Obwohl lokale Benutzer Mitglieder verschiedener lokaler Gruppen sein können, können lokale Gruppen nicht Mitglieder anderer lokaler Gruppen sein. Das lokale Benutzer-Zugriffstoken besteht aus einer Vereinigung aller Berechtigungen, die Gruppen zugewiesen sind, denen ein bestimmter lokaler Benutzer Mitglied ist.

- Anmeldung für Domänenbenutzer

Wenn sich ein Domänenbenutzer anmeldet, erhält ONTAP ein Benutzerzugriffstoken, das die Benutzer-SID und SIDs für alle Domänengruppen enthält, zu denen der Benutzer Mitglied ist. ONTAP verwendet die Vereinigung des Zugriffstoken für Domänenbenutzer mit dem Zugriffstoken, das von lokalen Mitgliedschaften der Domänengruppen des Benutzers bereitgestellt wird (falls vorhanden), sowie allen direkten Berechtigungen, die dem Domänenbenutzer oder seiner Domänengruppmitgliedschaften zugewiesen sind.

Sowohl bei der lokalen Anmeldung als auch bei der Domain-Anmeldung wird die primäre GRUPPENLOSLUNG auch für das Benutzerzugriffstoken festgelegt. Die Standard-RID ist `Domain Users (513)`. Sie können den Standardwert nicht ändern.

Die Namenszuordnungen von Windows-zu-UNIX und UNIX-zu-Windows befolgen dieselben Regeln für lokale und Domänenkonten.



Es gibt keine implizierte automatische Zuordnung von einem UNIX-Benutzer zu einem lokalen Konto. Ist dies erforderlich, muss mithilfe der vorhandenen Befehle für die Namenszuordnung eine explizite Zuordnungsregel angegeben werden.

Richtlinien zur Verwendung von SnapMirror auf SVMs, die lokale Gruppen enthalten

Beachten Sie die Richtlinien bei der Konfiguration von SnapMirror auf Volumes von SVMs, die lokale Gruppen enthalten.

Sie können keine lokalen Gruppen in Aces verwenden, die auf Dateien, Verzeichnisse oder Freigaben angewendet werden, die von SnapMirror auf eine andere SVM repliziert werden. Wenn Sie mithilfe der SnapMirror Funktion eine DR-Spiegelung für ein Volume auf einer anderen SVM erstellen und das Volume über einen ACE für eine lokale Gruppe verfügt, ist der ACE auf dem Spiegel nicht gültig. Wenn die Daten in eine andere SVM repliziert werden, werden sie effektiv in eine andere lokale Domäne überführt. Die Berechtigungen für lokale Benutzer und Gruppen gelten nur für den Umfang der SVM, auf der sie ursprünglich erstellt wurden.

Was passiert mit lokalen Benutzern und Gruppen beim Löschen von CIFS-Servern

Der Standardsatz lokaler Benutzer und Gruppen wird bei Erstellung eines CIFS-Servers

erstellt und mit der Storage Virtual Machine (SVM) verknüpft, die den CIFS-Server hostet. SVM-Administratoren können jederzeit lokale Benutzer und Gruppen erstellen. Sie müssen sich bewusst sein, was mit lokalen Benutzern und Gruppen passiert, wenn Sie den CIFS Server löschen.

Lokale Benutzer und Gruppen sind SVMs zugeordnet. Daher werden sie nicht gelöscht, wenn CIFS Server aus Sicherheitsgründen gelöscht werden. Lokale Benutzer und Gruppen werden zwar nicht gelöscht, wenn der CIFS-Server gelöscht wird, sind aber ausgeblendet. Sie können lokale Benutzer und Gruppen erst anzeigen oder managen, wenn Sie einen CIFS-Server auf der SVM neu erstellen.



Der Administrationsstatus des CIFS-Servers hat keine Auswirkung auf die Sichtbarkeit lokaler Benutzer oder Gruppen.

Wie Sie Microsoft Management Console mit lokalen Benutzern und Gruppen verwenden können

Sie können Informationen zu lokalen Benutzern und Gruppen in der Microsoft Management Console anzeigen. Mit diesem Release von ONTAP können Sie keine anderen Verwaltungsaufgaben für lokale Benutzer und Gruppen über die Microsoft Verwaltungskonsole ausführen.

Richtlinien zum Zurücksetzen

Wenn Sie das Cluster auf eine ONTAP Version zurücksetzen möchten, die lokale Benutzer und Gruppen nicht unterstützt, und lokale Benutzer und Gruppen für das Management des Dateizugriffs oder von Benutzerrechten verwendet werden, müssen Sie sich über bestimmte Überlegungen im Klaren sein.

- Aus Sicherheitsgründen werden Informationen zu konfigurierten lokalen Benutzern, Gruppen und Berechtigungen nicht gelöscht, wenn ONTAP auf eine Version zurückgesetzt wird, die keine lokalen Benutzer- und Gruppenfunktionen unterstützt.
- Bei einem Zurücksetzen auf eine vorherige Hauptversion von ONTAP verwendet ONTAP während der Authentifizierung und der Erstellung von Anmeldeinformationen keine lokalen Benutzer und Gruppen.
- Lokale Benutzer und Gruppen werden nicht aus Datei- und Ordner-ACLs entfernt.
- Zugriffsanfragen, die vom Zugriff abhängig sind, die aufgrund von Berechtigungen für lokale Benutzer oder Gruppen gewährt werden, werden verweigert.

Um den Zugriff zu ermöglichen, müssen Sie Dateiberechtigungen neu konfigurieren, um den Zugriff auf der Basis von Domänenobjekten anstelle von lokalen Benutzer- und Gruppenobjekten zu ermöglichen.

Welche lokalen Berechtigungen sind

Liste der unterstützten Berechtigungen

ONTAP verfügt über einen vordefinierten Satz unterstützter Berechtigungen. Bestimmte vordefinierte lokale Gruppen haben einige dieser Berechtigungen standardmäßig hinzugefügt. Sie können außerdem Berechtigungen aus den vordefinierten Gruppen

hinzufügen oder entfernen oder neue lokale Benutzer oder Gruppen erstellen und den von Ihnen erstellten Gruppen oder vorhandenen Domänenbenutzern und -Gruppen Berechtigungen hinzufügen.

In der folgenden Tabelle werden die unterstützten Berechtigungen auf der Storage Virtual Machine (SVM) aufgeführt und eine Liste der BUILTIN-Gruppen mit zugewiesenen Berechtigungen angezeigt:

Berechtigungsname	Standardeinstellung für die Sicherheit	Beschreibung
SeTcbPrivilege	Keine	Als Teil des Betriebssystems agieren
SeBackupPrivilege	BUILTIN\Administrators, BUILTIN\Backup Operators	Sichern Sie Dateien und Verzeichnisse, und überschreiben Sie alle ACLs
SeRestorePrivilege	BUILTIN\Administrators, BUILTIN\Backup Operators	Wiederherstellung von Dateien und Verzeichnissen, Überschreiben aller ACLs setzt alle gültigen Benutzer- oder Gruppen-SID als Eigentümer der Datei
SeTakeOwnershipPrivilege	BUILTIN\Administrators	Übernehmen Sie die Verantwortung für Dateien oder andere Objekte
SeSecurityPrivilege	BUILTIN\Administrators	Verwalten von AuditingDies umfasst das Anzeigen, Dumping und Löschen des Sicherheitsprotokolls.
SeChangeNotifyPrivilege	BUILTIN\Administrators, BUILTIN\Backup Operators, BUILTIN\Power Users, BUILTIN\Users, Everyone	DurchkreuzweigprüfungUser mit dieser Berechtigung sind nicht für Traverse (x)-Berechtigungen erforderlich, um Ordner, Symlinks oder Kreuzungen zu durchlaufen.

Verwandte Informationen

- [Weisen Sie lokale Berechtigungen zu](#)
- [Konfigurieren der Umgehungsüberprüfung](#)

Berechtigungen zuweisen

Sie können lokalen Benutzern oder Domänenbenutzern Berechtigungen direkt zuweisen. Alternativ können Sie lokalen Gruppen Benutzer zuweisen, deren zugewiesene Berechtigungen den Fähigkeiten entsprechen, die diese Benutzer haben sollen.

- Sie können einer von Ihnen erstellten Gruppe einen Satz von Berechtigungen zuweisen.

Anschließend fügen Sie der Gruppe einen Benutzer hinzu, der über die Berechtigungen verfügt, über die dieser Benutzer verfügen soll.

- Sie können auch lokale Benutzer und Domänenbenutzer vordefinierten Gruppen zuweisen, deren Standardberechtigungen mit den Berechtigungen übereinstimmen, die Sie diesen Benutzern gewähren möchten.

Verwandte Informationen

- [Hinzufügen von Berechtigungen zu lokalen oder Domänenbenutzern oder -Gruppen](#)
- [Entfernen von Berechtigungen von lokalen oder Domänenbenutzern oder -Gruppen](#)
- [Zurücksetzen von Berechtigungen für lokale oder Domänenbenutzer und -Gruppen](#)
- [Konfigurieren der Umgehungsüberprüfung](#)

Richtlinien für die Nutzung von BUILTIN-Gruppen und dem lokalen Administratorkonto

Es gibt bestimmte Richtlinien, die Sie beachten sollten, wenn Sie BUILTIN-Gruppen und das lokale Administratorkonto verwenden. Beispielsweise können Sie das lokale Administratorkonto umbenennen, dieses Konto kann jedoch nicht gelöscht werden.

- Das Administratorkonto kann umbenannt, aber nicht gelöscht werden.
- Das Administratorkonto kann nicht aus der BUILTIN\Administrators-Gruppe entfernt werden.
- BUILTIN-Gruppen können umbenannt, aber nicht gelöscht werden.

Nachdem die BUILTIN-Gruppe umbenannt wurde, kann ein anderes lokales Objekt mit dem bekannten Namen erstellt werden; dem Objekt wird jedoch eine neue RID zugewiesen.

- Es gibt kein lokales Gastkonto.

Verwandte Informationen

[Vordefinierte BUILTIN-Gruppen und Standardberechtigungen](#)

Anforderungen für lokale Benutzerpasswörter

Standardmäßig müssen lokale Benutzerpasswörter den Komplexitätsanforderungen entsprechen. Die Anforderungen an die Passwortkomplexität ähneln den in der Microsoft Windows *Local Security Policy* definierten Anforderungen.

Das Passwort muss die folgenden Kriterien erfüllen:

- Muss mindestens sechs Zeichen lang sein
- Darf den Benutzernamen nicht enthalten
- Muss Zeichen aus mindestens drei der folgenden vier Kategorien enthalten:
 - Englische Großbuchstaben (A bis Z)
 - Englische Kleinbuchstaben (A bis z)
 - Basis 10 Ziffern (0 bis 9)

- Sonderzeichen:

~!@#%^&* _ - + = ` \ () [] ; ' < > , . ? /

Verwandte Informationen

[Aktivieren oder Deaktivieren der erforderlichen Passwortkomplexität für lokale SMB-Benutzer](#)

[Anzeigen von Informationen zu den Sicherheitseinstellungen des CIFS-Servers](#)

[Ändern der Passwörter für lokales Benutzerkonto](#)

Vordefinierte BUILTIN-Gruppen und Standardberechtigungen

Sie können einer vordefinierten Gruppe von BUILTIN-Gruppen, die von ONTAP bereitgestellt werden, die Mitgliedschaft eines lokalen Benutzers oder eines Domänenbenutzers zuweisen. Vordefinierte Gruppen verfügen über vordefinierte Berechtigungen.

In der folgenden Tabelle werden die vordefinierten Gruppen beschrieben:

Vordefinierte BUILTIN-Gruppe	Standardberechtigungen
<p>BUILTIN\Administrators544 LOSWERDEN</p> <p>Beim ersten Erstellens wird der lokale erstellt Administrator Konto, mit einer RID von 500, wird automatisch ein Mitglied dieser Gruppe. Wenn die Storage Virtual Machine (SVM) zu einer Domäne hinzugefügt wird, wird das angezeigt domain\Domain Admins Die Gruppe wird der Gruppe hinzugefügt. Wenn die SVM die Domäne verlässt, wird der domain\Domain Admins Die Gruppe wird aus der Gruppe entfernt.</p>	<ul style="list-style-type: none"> • SeBackupPrivilege • SeRestorePrivilege • SeSecurityPrivilege • SeTakeOwnershipPrivilege • SeChangeNotifyPrivilege
<p>BUILTIN\Power Users547 LOSWERDEN</p> <p>Bei der ersten Erstellung verfügt diese Gruppe über keine Mitglieder. Mitglieder dieser Gruppe haben folgende Merkmale:</p> <ul style="list-style-type: none"> • Es können lokale Benutzer und Gruppen erstellt und verwaltet werden. • Sie können sich selbst oder ein anderes Objekt dem nicht hinzufügen BUILTIN\Administrators Gruppieren. 	<p>SeChangeNotifyPrivilege</p>

Vordefinierte BUILTIN-Gruppe	Standardberechtigungen
<p>BUILTIN\Backup Operators551 LOSWERDEN</p> <p>Bei der ersten Erstellung verfügt diese Gruppe über keine Mitglieder. Mitglieder dieser Gruppe können Lese- und Schreibberechtigungen für Dateien oder Ordner überschreiben, wenn sie mit Sicherungsziel geöffnet werden.</p>	<ul style="list-style-type: none"> • SeBackupPrivilege • SeRestorePrivilege • SeChangeNotifyPrivilege
<p>BUILTIN\Users545 LOSWERDEN</p> <p>Bei der ersten Erstellung hat diese Gruppe keine Mitglieder (außer dem impliziten Authenticated Users Sondergruppe). Wenn die SVM zu einer Domäne verbunden ist, wird der domain\Domain Users Die Gruppe wird dieser Gruppe hinzugefügt. Wenn die SVM die Domäne verlässt, wird der domain\Domain Users Die Gruppe wurde aus dieser Gruppe entfernt.</p>	SeChangeNotifyPrivilege
<p>EveryoneSID S-1-1-0</p> <p>Diese Gruppe umfasst alle Benutzer, einschließlich Gäste (aber nicht anonyme Benutzer). Hierbei handelt es sich um eine implizite Gruppe mit einer impliziten Mitgliedschaft.</p>	SeChangeNotifyPrivilege

Verwandte Informationen

[Richtlinien für die Nutzung von BUILTIN-Gruppen und dem lokalen Administratorkonto](#)

[Liste der unterstützten Berechtigungen](#)

[Konfigurieren der Umgehungsüberprüfung](#)

Aktivieren oder Deaktivieren der Funktionen für lokale Benutzer und Gruppen

Aktivieren oder Deaktivieren der Funktionsübersicht für lokale Benutzer und Gruppen

Bevor Sie lokale Benutzer und Gruppen für die Zugriffskontrolle von NTFS-Sicherheitsdaten verwenden können, müssen die Funktionen lokaler Benutzer und Gruppen aktiviert sein. Wenn Sie außerdem lokale Benutzer zur SMB-Authentifizierung verwenden möchten, muss die lokale Benutzerauthentifizierungsfunktion aktiviert sein.

Die Funktionen für lokale Benutzer und Gruppen und die lokale Benutzerauthentifizierung sind standardmäßig aktiviert. Wenn sie nicht aktiviert sind, müssen Sie sie aktivieren, bevor Sie lokale Benutzer und Gruppen konfigurieren und verwenden können. Sie können die Funktionen für lokale Benutzer und Gruppen jederzeit deaktivieren.

Zusätzlich zum ausdrücklichen Deaktivieren von Funktionen für lokale Benutzer und Gruppen deaktiviert ONTAP Funktionen für lokale Benutzer und Gruppen, wenn ein Node im Cluster auf eine ONTAP Version zurückgesetzt wird, die die Funktionen nicht unterstützt. Die Funktionen lokaler Benutzer und Gruppen sind erst aktiviert, wenn alle Nodes im Cluster eine Version von ONTAP ausführen, die sie unterstützt.

Verwandte Informationen

[Lokale Benutzerkonten ändern](#)

[Ändern von lokalen Gruppen](#)

[Fügen Sie den lokalen oder Domänenbenutzern oder -Gruppen Berechtigungen hinzu](#)

Aktivieren oder Deaktivieren von lokalen Benutzern und Gruppen

Lokale Benutzer und Gruppen können für den SMB-Zugriff auf Storage Virtual Machines (SVMs) aktiviert oder deaktiviert werden. Die Funktion für lokale Benutzer und Gruppen ist standardmäßig aktiviert.

Über diese Aufgabe

Sie können lokale Benutzer und Gruppen beim Konfigurieren von SMB-Freigaben- und NTFS-Dateiberechtigungen verwenden und können optional lokale Benutzer zur Authentifizierung verwenden, wenn Sie eine SMB-Verbindung erstellen. Um lokale Benutzer für die Authentifizierung zu verwenden, müssen Sie außerdem die Authentifizierungsoption für lokale Benutzer und Gruppen aktivieren.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie möchten, dass lokale Benutzer und Gruppen...	Geben Sie den Befehl ein...
Aktiviert	<pre>vserver cifs options modify -vserver vserver_name -is-local-users-and -groups-enabled true</pre>
Deaktiviert	<pre>vserver cifs options modify -vserver vserver_name -is-local-users-and -groups-enabled false</pre>

3. Zurück zur Administratorberechtigungsebene: `set -privilege admin`

Beispiel

Das folgende Beispiel bietet lokale Benutzer und Gruppen-Funktionen auf SVM vs1:

```

cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-users-and
-groups-enabled true

cluster1::*> set -privilege admin

```

Verwandte Informationen

[Aktivieren oder Deaktivieren der Authentifizierung für lokale Benutzer](#)

[Lokale Benutzerkonten aktivieren oder deaktivieren](#)

Aktivieren oder Deaktivieren der Authentifizierung für lokale Benutzer

Die Authentifizierung von lokalen Benutzern für SMB-Zugriff auf Storage Virtual Machines (SVMs) lässt sich aktivieren oder deaktivieren. Die Standardeinstellung erlaubt die lokale Benutzerauthentifizierung. Dies ist nützlich, wenn die SVM keinen Domänencontroller kontaktieren kann oder Sie keine Zugriffssteuerungen auf Domänenebene verwenden möchten.

Bevor Sie beginnen

Lokale Benutzer und Gruppen müssen auf dem CIFS-Server aktiviert sein.

Über diese Aufgabe

Sie können die lokale Benutzerauthentifizierung jederzeit aktivieren oder deaktivieren. Wenn Sie lokale Benutzer zur Authentifizierung beim Erstellen einer SMB-Verbindung verwenden möchten, müssen Sie auch die Option für lokale Benutzer und Gruppen des CIFS-Servers aktivieren.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Führen Sie eine der folgenden Aktionen aus:

Wenn die lokale Authentifizierung...	Geben Sie den Befehl ein...
Aktiviert	<code>vserver cifs options modify -vserver vserver_name -is-local-auth-enabled true</code>
Deaktiviert	<code>vserver cifs options modify -vserver vserver_name -is-local-auth-enabled false</code>

3. Zurück zur Administratorberechtigungsebene: `set -privilege admin`

Beispiel

Das folgende Beispiel ermöglicht die lokale Benutzerauthentifizierung auf SVM vs1:

```
cluster1::>set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-auth
-enabled true

cluster1::*> set -privilege admin
```

Verwandte Informationen

[Funktionsweise der lokalen Benutzerauthentifizierung](#)

[Aktivieren oder Deaktivieren von lokalen Benutzern und Gruppen](#)

Lokale Benutzerkonten verwalten

Lokale Benutzerkonten ändern

Sie können ein lokales Benutzerkonto ändern, wenn Sie den vollständigen Namen oder die Beschreibung eines vorhandenen Benutzers ändern möchten und wenn Sie das Benutzerkonto aktivieren oder deaktivieren möchten. Sie können auch ein lokales Benutzerkonto umbenennen, wenn der Name des Benutzers kompromittiert ist oder eine Namensänderung für administrative Zwecke erforderlich ist.

Ihr Ziel ist	Geben Sie den Befehl ein...
Ändern Sie den vollständigen Namen des lokalen Benutzers	<code>vserver cifs users-and-groups local-user modify -vserver <i>vserver_name</i> -user -name <i>user_name</i> -full-name <i>text</i></code> Wenn der vollständige Name ein Leerzeichen enthält, muss er in doppelte Anführungszeichen eingeschlossen werden.
Ändern Sie die Beschreibung des lokalen Benutzers	<code>vserver cifs users-and-groups local-user modify -vserver <i>vserver_name</i> -user -name <i>user_name</i> -description <i>text</i></code> Wenn die Beschreibung ein Leerzeichen enthält, muss sie in doppelte Anführungszeichen eingeschlossen werden.
Aktivieren oder deaktivieren Sie das lokale Benutzerkonto	<code>`vserver cifs users-and-groups local-user modify -vserver <i>vserver_name</i> -user-name <i>user_name</i> -is -account-disabled {true</code>

Ihr Ziel ist	Geben Sie den Befehl ein...
false}`	Benennen Sie das lokale Benutzerkonto um

Beispiel

Im folgenden Beispiel wird der lokale Benutzer „CIFS_SERVER\sue“ als „CIFS_SERVER\sue_New“ auf der Storage Virtual Machine (SVM, früher Vserver genannt) vs1 umbenannt:

```
cluster1::> vserver cifs users-and-groups local-user rename -user-name
CIFS_SERVER\sue -new-user-name CIFS_SERVER\sue_new -vserver vs1
```

Lokale Benutzerkonten aktivieren oder deaktivieren

Sie aktivieren ein lokales Benutzerkonto, wenn der Benutzer über eine SMB-Verbindung auf Daten in der Storage Virtual Machine (SVM) zugreifen soll. Sie können auch ein lokales Benutzerkonto deaktivieren, wenn dieser Benutzer nicht über SMB auf SVM-Daten zugreifen soll.

Über diese Aufgabe

Sie aktivieren einen lokalen Benutzer, indem Sie das Benutzerkonto ändern.

Schritt

1. Führen Sie die entsprechende Aktion aus:

Ihr Ziel ist	Geben Sie den Befehl ein...
Aktivieren Sie das Benutzerkonto	<pre>vserver cifs users-and-groups local- user modify -vserver vserver_name -user-name user_name -is-account -disabled false</pre>
Deaktivieren des Benutzerkontos	<pre>vserver cifs users-and-groups local- user modify -vserver vserver_name -user-name user_name -is-account -disabled true</pre>

Ändern Sie die Passwörter für das lokale Benutzerkonto

Sie können das Kontokennwort eines lokalen Benutzers ändern. Dies kann nützlich sein, wenn das Kennwort des Benutzers kompromittiert wird oder wenn der Benutzer das Passwort vergessen hat.

Schritt

1. Ändern Sie das Passwort, indem Sie die entsprechende Aktion ausführen: `vserver cifs users-and-groups local-user set-password -vserver vserver_name -user-name user_name`

Beispiel

Im folgenden Beispiel wird das Passwort für den lokalen Benutzer „CIFS_SERVER\sue“ festgelegt, der mit der Storage Virtual Machine (SVM, früher unter dem Namen „Vserver“ bekannt) vs1 verknüpft ist:

```
cluster1::> vserver cifs users-and-groups local-user set-password -user  
-name CIFS_SERVER\sue -vserver vs1
```

Enter the new password:

Confirm the new password:

Verwandte Informationen

[Aktivieren oder Deaktivieren der erforderlichen Passwortkomplexität für lokale SMB-Benutzer](#)

[Anzeigen von Informationen zu den Sicherheitseinstellungen des CIFS-Servers](#)

Informationen zu lokalen Benutzern anzeigen

Sie können eine Liste aller lokalen Benutzer in einem Übersichtsformular anzeigen. Wenn Sie festlegen möchten, welche Kontoeinstellungen für einen bestimmten Benutzer konfiguriert sind, können Sie detaillierte Kontoinformationen für diesen Benutzer sowie die Kontoinformationen für mehrere Benutzer anzeigen. Mithilfe dieser Informationen können Sie feststellen, ob Sie die Einstellungen eines Benutzers ändern müssen, und auch Probleme mit der Authentifizierung oder dem Dateizugriff beheben.

Über diese Aufgabe

Es werden nie Informationen zum Passwort eines Benutzers angezeigt.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den Befehl ein...
Informationen über alle Benutzer auf der Storage Virtual Machine (SVM) anzeigen	<code>vserver cifs users-and-groups local-user show -vserver <i>vserver_name</i></code>
Anzeigen detaillierter Kontoinformationen für einen Benutzer	<code>vserver cifs users-and-groups local-user show -instance -vserver <i>vserver_name</i> -user-name <i>user_name</i></code>

Es gibt weitere optionale Parameter, die Sie wählen können, wenn Sie den Befehl ausführen. Weitere Informationen finden Sie auf der man-Seite.

Beispiel

Das folgende Beispiel zeigt Informationen über alle lokalen Benutzer auf SVM vs1:


```

cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                               Full Name      Description
-----  -
vs1      CIFS_SERVER\Administrator                 James Smith    Built-in administrator
account
vs1      CIFS_SERVER\sue                           Sue    Jones

```

Informationen zu Gruppenmitgliedschaften für lokale Benutzer anzeigen

Sie können Informationen darüber anzeigen, zu welchen lokalen Gruppen ein lokaler Benutzer gehört. Anhand dieser Informationen können Sie bestimmen, auf welchen Zugriff der Benutzer auf Dateien und Ordner zugreifen soll. Diese Informationen können nützlich sein, um zu bestimmen, welche Zugriffsrechte der Benutzer für Dateien und Ordner haben sollte, oder wenn Sie Probleme mit dem Dateizugriff beheben.

Über diese Aufgabe

Sie können den Befehl so anpassen, dass nur die Informationen angezeigt werden, die angezeigt werden sollen.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den Befehl ein...
Zeigt Informationen zur lokalen Benutzermitgliedschaft für einen bestimmten lokalen Benutzer an	<code>vserver cifs users-and-groups local-user show-membership -user-name <i>user_name</i></code>
Zeigen Sie lokale Benutzermitgliedschaftsinformationen für die lokale Gruppe an, von der dieser lokale Benutzer Mitglied ist	<code>vserver cifs users-and-groups local-user show-membership -membership <i>group_name</i></code>
Anzeigen von Informationen zur Benutzermitgliedschaft für lokale Benutzer, die einer bestimmten SVM (Storage Virtual Machine) zugeordnet sind	<code>vserver cifs users-and-groups local-user show-membership -vserver <i>vserver_name</i></code>
Anzeige detaillierter Informationen für alle lokalen Benutzer auf einer angegebenen SVM	<code>vserver cifs users-and-groups local-user show-membership -instance -vserver <i>vserver_name</i></code>

Beispiel

Im folgenden Beispiel werden die Mitgliedsinformationen für alle lokalen Benutzer auf SVM vs1 angezeigt; Benutzer „CIFS_SERVER\Administrator“ ist Mitglied der Gruppe „BUILTIN\Administrators“ und „CIFS_SERVER\sue“ ist Mitglied der Gruppe „CIFS_SERVER\g1“:

```

cluster1::> vserver cifs users-and-groups local-user show-membership
-vserver vs1
Vserver      User Name                Membership
-----
vs1          CIFS_SERVER\Administrator BUILTIN\Administrators
            CIFS_SERVER\sue         CIFS_SERVER\g1

```

Lokale Benutzerkonten löschen

Sie können lokale Benutzerkonten von Ihrer Storage Virtual Machine (SVM) löschen, wenn diese nicht mehr für die lokale SMB-Authentifizierung am CIFS-Server oder zur Bestimmung der Zugriffsrechte auf den Daten auf Ihrer SVM benötigt werden.

Über diese Aufgabe

Beachten Sie beim Löschen lokaler Benutzer Folgendes:

- Das Dateisystem wird nicht verändert.

Windows-Sicherheitsdeskriptoren für Dateien und Verzeichnisse, die auf diesen Benutzer verweisen, werden nicht angepasst.

- Alle Verweise auf lokale Benutzer werden aus den Mitgliedschafts- und Berechtigungsdatenbanken entfernt.
- Bekannte Standardbenutzer wie Administrator können nicht gelöscht werden.

Schritte

1. Legen Sie den Namen des lokalen Benutzerkontos fest, das Sie löschen möchten: `vserver cifs users-and-groups local-user show -vserver vserver_name`
2. Lokalen Benutzer löschen: `vserver cifs users-and-groups local-user delete -vserver vserver_name -user-name username_name`
3. Vergewissern Sie sich, dass das Benutzerkonto gelöscht wurde: `vserver cifs users-and-groups local-user show -vserver vserver_name`

Beispiel

Im folgenden Beispiel wird der lokale Benutzer „CIFS_SERVER\sue“ gelöscht, der mit SVM vs1 verknüpft ist:

```

cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                               Full Name           Description
-----  -
vs1      CIFS_SERVER\Administrator                 James Smith         Built-in administrator
account
vs1      CIFS_SERVER\sue                           Sue    Jones

cluster1::> vserver cifs users-and-groups local-user delete -vserver vs1
-user-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver      User Name                               Full Name           Description
-----  -
vs1          CIFS_SERVER\Administrator                 James Smith         Built-in administrator
account

```

Verwaltung lokaler Gruppen

Ändern von lokalen Gruppen

Sie können vorhandene lokale Gruppen ändern, indem Sie die Beschreibung für eine vorhandene lokale Gruppe ändern oder die Gruppe umbenennen.

Ihr Ziel ist	Verwenden Sie den Befehl...
Ändern Sie die Beschreibung der lokalen Gruppe	<code>vserver cifs users-and-groups local-group modify -vserver <i>vserver_name</i> -group-name <i>group_name</i> -description <i>text</i></code> Wenn die Beschreibung ein Leerzeichen enthält, muss sie in doppelte Anführungszeichen eingeschlossen werden.
Benennen Sie die lokale Gruppe um	<code>vserver cifs users-and-groups local-group rename -vserver <i>vserver_name</i> -group-name <i>group_name</i> -new-group-name <i>new_group_name</i></code>

Beispiele

Im folgenden Beispiel wird die lokale Gruppe „CIFS_SERVER\Engineering“ in „CIFS_SERVER\Engineering_New“ umbenannt:

```
cluster1::> vserver cifs users-and-groups local-group rename -vserver vs1
-group-name CIFS_SERVER\engineering -new-group-name
CIFS_SERVER\engineering_new
```

Im folgenden Beispiel wird die Beschreibung der lokalen Gruppe „CIFS_SERVER\Engineering“ geändert:

```
cluster1::> vserver cifs users-and-groups local-group modify -vserver vs1
-group-name CIFS_SERVER\engineering -description "New Description"
```

Zeigt Informationen zu lokalen Gruppen an

Sie können eine Liste aller auf dem Cluster konfigurierten lokalen Gruppen oder auf einer angegebenen SVM (Storage Virtual Machine) anzeigen. Diese Informationen können nützlich sein, wenn Sie Probleme beim Dateizugriff bei den Daten in der SVM oder Problemen mit den Benutzerrechten (Berechtigungen) auf der SVM beheben.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Informationen über...	Geben Sie den Befehl ein...
Alle lokalen Gruppen im Cluster	<code>vserver cifs users-and-groups local-group show</code>
Alle lokalen Gruppen auf der SVM	<code>vserver cifs users-and-groups local-group show -vserver vserver_name</code>

Es gibt weitere optionale Parameter, die Sie bei der Ausführung dieses Befehls auswählen können. Weitere Informationen finden Sie auf der man-Seite.

Beispiel

Das folgende Beispiel zeigt Informationen zu allen lokalen Gruppen auf SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver  Group Name                Description
-----  -
vs1      BUILTIN\Administrators    Built-in Administrators group
vs1      BUILTIN\Backup Operators  Backup Operators group
vs1      BUILTIN\Power Users       Restricted administrative privileges
vs1      BUILTIN\Users             All users
vs1      CIFS_SERVER\engineering
vs1      CIFS_SERVER\sales
```

Verwaltung der lokalen Gruppenmitgliedschaft

Sie können die lokale Gruppenmitgliedschaft verwalten, indem Sie lokale Benutzer oder Domänenbenutzer hinzufügen und entfernen oder Domänengruppen hinzufügen und entfernen. Dies ist nützlich, wenn Sie den Zugriff auf Daten anhand von Zugriffskontrollen, die in der Gruppe platziert sind, steuern möchten oder wenn Benutzer über Berechtigungen verfügen möchten, die dieser Gruppe zugeordnet sind.

Über diese Aufgabe

Richtlinien zum Hinzufügen von Mitgliedern zu einer lokalen Gruppe:

- Sie können keine Benutzer zur speziellen *everyone*-Gruppe hinzufügen.
- Die lokale Gruppe muss vorhanden sein, bevor Sie einen Benutzer hinzufügen können.
- Der Benutzer muss vorhanden sein, bevor Sie den Benutzer einer lokalen Gruppe hinzufügen können.
- Sie können einer anderen lokalen Gruppe keine lokale Gruppe hinzufügen.
- Um einen Domänenbenutzer oder eine Gruppe zu einer lokalen Gruppe hinzuzufügen, muss Data ONTAP in der Lage sein, den Namen zu einem SID aufzulösen.

Richtlinien zum Entfernen von Mitgliedern aus einer lokalen Gruppe:

- Sie können keine Mitglieder aus der speziellen *everyone*-Gruppe entfernen.
- Die Gruppe, aus der Sie ein Mitglied entfernen möchten, muss vorhanden sein.
- ONTAP muss in der Lage sein, die Namen der Mitglieder zu lösen, die Sie aus der Gruppe zu einem entsprechenden SID entfernen möchten.

Schritt

1. Fügen Sie ein Mitglied einer Gruppe hinzu oder entfernen Sie es.

Ihr Ziel ist	Verwenden Sie dann den Befehl...
Ein Mitglied zu einer Gruppe hinzufügen	<pre>vserver cifs users-and-groups local- group add-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]</pre> Sie können eine kommagetrennte Liste von lokalen Benutzern, Domänenbenutzern oder Domänengruppen angeben, die der angegebenen lokalen Gruppe hinzugefügt werden sollen.
Entfernen Sie ein Mitglied aus einer Gruppe	<pre>vserver cifs users-and-groups local- group remove-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]</pre> Sie können eine durch Komma getrennte Liste der lokalen Benutzer, Domänenbenutzer oder Domänengruppen angeben, die aus der angegebenen lokalen Gruppe entfernt werden sollen.

Im folgenden Beispiel wird der lokalen Gruppe „SMB_SERVER\sue“ und der lokalen Gruppe „AD_DOM\dom_eng“ auf SVM vs1 ein lokaler Benutzer „SMB_SERVER\Engineering“ hinzugefügt:

```
cluster1::> vserver cifs users-and-groups local-group add-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,AD_DOMAIN\dom_eng
```

Im folgenden Beispiel werden die lokalen Benutzer „SMB_SERVER\sue“ und „SMB_SERVER\james“ aus der lokalen Gruppe „SMB_SERVER\Engineering“ auf SVM vs1 entfernt:

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

Verwandte Informationen

[Anzeigen von Informationen zu Mitgliedern von lokalen Gruppen](#)

Zeigt Informationen zu Mitgliedern lokaler Gruppen an

Sie können eine Liste aller Mitglieder der lokalen Gruppen anzeigen, die auf dem Cluster oder auf einer angegebenen Storage Virtual Machine (SVM) konfiguriert sind. Diese Informationen können hilfreich sein, wenn Probleme mit dem Zugriff auf Dateien oder Probleme mit Benutzerrechten (Berechtigungen) behoben werden.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Informationen über... anzeigen möchten	Geben Sie den Befehl ein...
Mitglieder aller lokalen Gruppen auf dem Cluster	<code>vserver cifs users-and-groups local-group show-members</code>
Mitglieder aller lokalen Gruppen auf der SVM	<code>vserver cifs users-and-groups local-group show-members -vserver <i>vserver_name</i></code>

Beispiel

Im folgenden Beispiel werden Informationen über Mitglieder aller lokalen Gruppen auf SVM vs1 angezeigt:

```

cluster1::> vserver cifs users-and-groups local-group show-members
-vserver vs1
Vserver      Group Name                               Members
-----
vs1          BUILTIN\Administrators                  CIFS_SERVER\Administrator
                                                AD_DOMAIN\Domain Admins
                                                AD_DOMAIN\dom_grp1
          BUILTIN\Users                       AD_DOMAIN\Domain Users
                                                AD_DOMAIN\dom_usr1
          CIFS_SERVER\engineering             CIFS_SERVER\james

```

Lokale Gruppe löschen

Sie können eine lokale Gruppe von der Storage Virtual Machine (SVM) löschen, wenn sie nicht mehr zum Ermitteln der Zugriffsrechte für Daten benötigt wird, die dieser SVM zugeordnet sind, oder wenn sie nicht mehr zum Zuweisen von SVM-Benutzerrechten (Berechtigungen) zu Gruppenmitgliedern benötigt wird.

Über diese Aufgabe

Beachten Sie beim Löschen von lokalen Gruppen Folgendes:

- Das Dateisystem wird nicht verändert.
Windows-Sicherheitsdeskriptoren für Dateien und Verzeichnisse, die sich auf diese Gruppe beziehen, werden nicht angepasst.
- Wenn die Gruppe nicht vorhanden ist, wird ein Fehler zurückgegeben.
- Die spezielle *Everyone*-Gruppe kann nicht gelöscht werden.
- Integrierte Gruppen wie *BUILTIN\Administrators* *BUILTIN\Users* können nicht gelöscht werden.

Schritte

1. Geben Sie den Namen der lokalen Gruppe an, die Sie löschen möchten, indem Sie die Liste der lokalen Gruppen auf der SVM anzeigen: `vserver cifs users-and-groups local-group show -vserver vserver_name`
2. Lokale Gruppe löschen: `vserver cifs users-and-groups local-group delete -vserver vserver_name -group-name group_name`
3. Vergewissern Sie sich, dass die Gruppe gelöscht wurde: `vserver cifs users-and-groups local-user show -vserver vserver_name`

Beispiel

Im folgenden Beispiel wird die lokale Gruppe „CIFS_SERVER\Sales“ gelöscht, die mit SVM vs1 verknüpft ist:

```

cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver      Group Name          Description
-----
vs1          BUILTIN\Administrators  Built-in Administrators group
vs1          BUILTIN\Backup Operators Backup Operators group
vs1          BUILTIN\Power Users    Restricted administrative
privileges
vs1          BUILTIN\Users          All users
vs1          CIFS_SERVER\engineering
vs1          CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group delete -vserver vs1
-group-name CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver      Group Name          Description
-----
vs1          BUILTIN\Administrators  Built-in Administrators group
vs1          BUILTIN\Backup Operators Backup Operators group
vs1          BUILTIN\Power Users    Restricted administrative
privileges
vs1          BUILTIN\Users          All users
vs1          CIFS_SERVER\engineering

```

Domänenbenutzer- und Gruppennamen in lokalen Datenbanken aktualisieren

Sie können den lokalen Gruppen eines CIFS-Servers Domänenbenutzer und -Gruppen hinzufügen. Diese Domänenobjekte sind in lokalen Datenbanken auf dem Cluster registriert. Wenn ein Domänenobjekt umbenannt wird, müssen die lokalen Datenbanken manuell aktualisiert werden.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) angeben, auf der Sie Domänennamen aktualisieren möchten.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Führen Sie die entsprechende Aktion aus:

Wenn Sie Domänenbenutzer und -Gruppen aktualisieren möchten und...	Befehl
Domänenbenutzer und -Gruppen anzeigen, die erfolgreich aktualisiert wurden und die nicht aktualisiert werden konnten	<code>vserver cifs users-and-groups update-names -vserver vserver_name</code>

Wenn Sie Domänenbenutzer und -Gruppen aktualisieren möchten und...	Befehl
Zeigen Sie Domänenbenutzer und -Gruppen an, die erfolgreich aktualisiert wurden	<code>vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only false</code>
Nur die Domänenbenutzer und -Gruppen anzeigen, die nicht aktualisiert werden können	<code>vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only true</code>
Alle Statusinformationen zu Aktualisierungen unterdrücken	<code>vserver cifs users-and-groups update-names -vserver vserver_name -suppress -all-output true</code>

3. Zurück zur Administratorberechtigungsebene: `set -privilege admin`

Beispiel

Im folgenden Beispiel werden die Namen der Domänenbenutzer und Gruppen aktualisiert, die mit der Storage Virtual Machine (SVM, ehemals Vserver genannt) vs1 verknüpft sind. Für das letzte Update gibt es eine abhängige Kette von Namen, die aktualisiert werden müssen:

```

cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs users-and-groups update-names -vserver vs1

Vserver:          vs1
SID:              S-1-5-21-123456789-234565432-987654321-12345
Domain:           EXAMPLE1
Out-of-date Name: dom_user1
Updated Name:     dom_user2
Status:           Successfully updated

Vserver:          vs1
SID:              S-1-5-21-123456789-234565432-987654322-23456
Domain:           EXAMPLE2
Out-of-date Name: dom_user1
Updated Name:     dom_user2
Status:           Successfully updated

Vserver:          vs1
SID:              S-1-5-21-123456789-234565432-987654321-123456
Domain:           EXAMPLE1
Out-of-date Name: dom_user3
Updated Name:     dom_user4
Status:           Successfully updated; also updated SID "S-1-5-21-
123456789-234565432-987654321-123457"
                  to name "dom_user5"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123458"
                  to name "dom_user6"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123459"
                  to name "dom_user7"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123460"
                  to name "dom_user8"

The command completed successfully. 7 Active Directory objects have been
updated.

cluster1::*> set -privilege admin

```

Lokale Berechtigungen verwalten

Fügen Sie den lokalen oder Domänenbenutzern oder -Gruppen Berechtigungen hinzu

Sie können Benutzerrechte für lokale oder Domänenbenutzer oder -Gruppen verwalten, indem Sie Berechtigungen hinzufügen. Die hinzugefügten Berechtigungen überschreiben die Standardberechtigungen, die einem dieser Objekte zugewiesen sind. Dadurch erhalten Sie verbesserte Sicherheit, indem Sie die Berechtigungen eines Benutzers oder einer Gruppe anpassen können.

Bevor Sie beginnen

Der lokale Benutzer oder die Domänengruppe, zu der Berechtigungen hinzugefügt werden sollen, muss bereits vorhanden sein.

Über diese Aufgabe

Beim Hinzufügen einer Berechtigung zu einem Objekt werden die Standardberechtigungen für diesen Benutzer oder diese Gruppe überschrieben. Beim Hinzufügen einer Berechtigung werden zuvor hinzugefügte Berechtigungen nicht entfernt.

Beim Hinzufügen von Berechtigungen zu lokalen oder Domänenbenutzern oder -Gruppen müssen Sie Folgendes beachten:

- Sie können eine oder mehrere Berechtigungen hinzufügen.
- Beim Hinzufügen von Berechtigungen zu einem Domänenbenutzer oder einer Gruppe kann ONTAP den Domänenbenutzer oder die Gruppe validieren, indem er sich an den Domänencontroller wenden kann.

Der Befehl schlägt möglicherweise fehl, wenn ONTAP den Domain-Controller nicht kontaktieren kann.

Schritte

1. Fügen Sie einem lokalen Benutzer oder einer Domänengruppe eine oder mehrere Berechtigungen hinzu:
`vserver cifs users-and-groups privilege add-privilege -vserver _vserver_name_
-user-or-group-name name -privileges _privilege_[,...]`
2. Vergewissern Sie sich, dass die gewünschten Berechtigungen auf das Objekt angewendet werden:
`vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-
group-name name`

Beispiel

Im folgenden Beispiel werden die Berechtigungen „SeTcbPrivilege“ und „SeTakeownershipPrivilege“ für den Benutzer „CIFS_SERVER\sue“ auf Storage Virtual Machine (SVM, ehemals Vserver) vs1 hinzugefügt:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege
```

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          CIFS_SERVER\sue        SeTcbPrivilege
                                     SeTakeOwnershipPrivilege
```

Entfernen Sie Berechtigungen von lokalen oder Domänenbenutzern oder -Gruppen

Sie können Benutzerrechte für lokale oder Domänenbenutzer oder -Gruppen verwalten, indem Sie Berechtigungen entfernen. Dadurch erhalten Sie verbesserte Sicherheit, indem Sie die maximalen Berechtigungen von Benutzern und Gruppen anpassen können.

Bevor Sie beginnen

Der lokale Benutzer oder die Domänengruppe, aus der Berechtigungen entfernt werden sollen, muss bereits vorhanden sein.

Über diese Aufgabe

Beim Entfernen von Berechtigungen von lokalen oder Domänenbenutzern oder -Gruppen müssen Sie Folgendes beachten:

- Sie können eine oder mehrere Berechtigungen entfernen.
- Wenn Sie Berechtigungen von einem Domänenbenutzer oder einer Gruppe entfernen, kann ONTAP den Domänenbenutzer oder die Gruppe validieren, indem Sie sich an den Domänencontroller wenden.

Der Befehl schlägt möglicherweise fehl, wenn ONTAP den Domain-Controller nicht kontaktieren kann.

Schritte

1. Entfernen Sie mindestens eine Berechtigung von einem lokalen Benutzer oder einer Domänengruppe:
`vserver cifs users-and-groups privilege remove-privilege -vserver
_vserver_name_ -user-or-group-name _name_ -privileges _privilege_[,...]`
2. Überprüfen Sie, ob die gewünschten Berechtigungen aus dem Objekt entfernt wurden: `vserver cifs
users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

Beispiel

Im folgenden Beispiel werden die Berechtigungen „SeTcbPrivilege“ und „SeTakeownershipPrivilege“ des Benutzers „CIFS_SERVER\sue“ auf Storage Virtual Machine (SVM, ehemals Vserver) vs1 entfernt:

```

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name      Privileges
-----
vs1        CIFS_SERVER\sue        SeTcbPrivilege
                                SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name      Privileges
-----
vs1        CIFS_SERVER\sue        -

```

Berechtigungen für lokale oder Domänenbenutzer und -Gruppen zurücksetzen

Sie können Berechtigungen für lokale Benutzer oder Domänenbenutzer und -Gruppen zurücksetzen. Dies kann nützlich sein, wenn Sie Änderungen an Berechtigungen für einen lokalen Benutzer oder eine Domänengruppe vorgenommen haben und diese Änderungen nicht mehr gewünscht oder erforderlich sind.

Über diese Aufgabe

Beim Zurücksetzen der Berechtigungen für einen lokalen oder Domänenbenutzer oder eine Gruppe werden alle Berechtigungseinträge für dieses Objekt entfernt.

Schritte

1. Zurücksetzen der Berechtigungen für einen lokalen Benutzer oder eine Domänenbenutzer oder -Gruppe:
`vserver cifs users-and-groups privilege reset-privilege -vserver vserver_name -user-or-group-name name`
2. Vergewissern Sie sich, dass die Berechtigungen auf dem Objekt zurückgesetzt wurden:
`vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

Beispiele

Im folgenden Beispiel werden die Berechtigungen des Benutzers „CIFS_SERVER\sue“ auf der Storage Virtual Machine (SVM, früher als Vserver bezeichnet) vs1 zurückgesetzt. Standardmäßig verfügen normale Benutzer über keine Berechtigungen, die mit ihren Konten verknüpft sind:

```

cluster1::> vserver cifs users-and-groups privilege show
Vserver    User or Group Name      Privileges
-----
vs1        CIFS_SERVER\sue        SeTcbPrivilege
                               SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.

```

Das folgende Beispiel setzt die Berechtigungen für die Gruppe „BUILTIN\Administrators“ zurück und entfernt damit effektiv den Eintrag für Berechtigungen:

```

cluster1::> vserver cifs users-and-groups privilege show
Vserver    User or Group Name      Privileges
-----
vs1        BUILTIN\Administrators  SeRestorePrivilege
                               SeSecurityPrivilege
                               SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name BUILTIN\Administrators

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.

```

Zeigt Informationen zu Berechtigungsüberschreibungen an

Sie können Informationen über benutzerdefinierte Berechtigungen anzeigen, die Domänenkonten oder lokalen Benutzerkonten oder Gruppen zugewiesen sind. Anhand dieser Informationen können Sie feststellen, ob die gewünschten Benutzerrechte angewendet werden.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Informationen über... anzeigen möchten	Diesen Befehl eingeben...
Benutzerdefinierte Berechtigungen für alle Domänen- und lokalen Benutzer und Gruppen auf der Storage Virtual Machine (SVM)	<code>vserver cifs users-and-groups privilege show -vserver <i>vserver_name</i></code>

Wenn Sie Informationen über... anzeigen möchten	Diesen Befehl eingeben...
Benutzerdefinierte Berechtigungen für eine bestimmte Domäne oder einen lokalen Benutzer und eine bestimmte Gruppe auf der SVM	<code>vserver cifs users-and-groups privilege show -vserver <i>vserver_name</i> -user-or-group-name <i>name</i></code>

Es gibt weitere optionale Parameter, die Sie bei der Ausführung dieses Befehls auswählen können. Weitere Informationen finden Sie auf der man-Seite.

Beispiel

Mit dem folgenden Befehl werden alle Berechtigungen angezeigt, die explizit lokalen oder Domänenbenutzern und Gruppen für SVM vs1 zugeordnet sind:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          BUILTIN\Administrators  SeTakeOwnershipPrivilege
                                     SeRestorePrivilege
vs1          CIFS_SERVER\sue         SeTcbPrivilege
                                     SeTakeOwnershipPrivilege
```

Copyright-Informationen

Copyright © 2023 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.