Wie ONTAP lokale Benutzer und Gruppen verwendet

ONTAP 9

NetApp
February 12, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/smb-admin/local-users-groups-concepts-concept.html on February 12, 2026. Always check docs.netapp.com for the latest.

Inhalt

Wie ONTAP lokale Benutzer und Gruppen verwendet . . . 1
- Erfahren Sie mehr über lokale ONTAP SMB-Benutzer und -Gruppen . . . 1
- Gründe für die Erstellung lokaler ONTAP SMB-Benutzer und lokaler Gruppen . . . 2
- Erfahren Sie mehr über die lokale ONTAP SMB-Benutzerauthentifizierung . . . 3
- Erfahren Sie mehr über ONTAP SMB-Benutzerzugriffstoken . . . 4
- Erfahren Sie mehr über die Verwendung von SnapMirror auf ONTAP SMB SVMs, die lokale Gruppen enthalten . . . 4
- Erfahren Sie, welche Auswirkungen das Löschen von ONTAP SMB-Servern auf Benutzer und Gruppen hat . . . 5
- Erfahren Sie, wie Sie die Microsoft Management Console mit lokalen ONTAP SMB-Benutzern und -Gruppen verwenden . . . 5
- Erfahren Sie mehr über das Zurücksetzen von ONTAP SMB-Clustern . . . 5

Wie ONTAP lokale Benutzer und Gruppen verwendet

Erfahren Sie mehr über lokale ONTAP SMB-Benutzer und -Gruppen

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 die Erstellung lokaler ONTAP SMB-Benutzer und lokaler 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

- Erfahren Sie mehr über die lokale Benutzerauthentifizierung
- Liste der unterstützten Berechtigungen

Erfahren Sie mehr über die lokale ONTAP SMB-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. NTLMv1 und 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 auf Servern

Erfahren Sie mehr über ONTAP SMB-Benutzerzugriffstoken

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 GRUPPENLOSUNG auch für das Benutzerzugriffstoken festgelegt. Der Standard RID ist `Domain Users` (RID 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.

Erfahren Sie mehr über die Verwendung von SnapMirror auf ONTAP SMB 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.

Erfahren Sie, welche Auswirkungen das Löschen von ONTAP SMB-Servern auf Benutzer und Gruppen hat

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.

Erfahren Sie, wie Sie die Microsoft Management Console mit lokalen ONTAP SMB-Benutzern und -Gruppen verwenden

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.

Erfahren Sie mehr über das Zurücksetzen von ONTAP SMB-Clustern

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.

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers 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, BEISPIELHAFTE 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 IRGENDEINER 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.