Sicherer Dateizugriff durch Verwenden von Dateiberechtigungen

ONTAP 9

NetApp
March 30, 2023

Inhaltsverzeichnis

Sicherer Dateizugriff durch Verwenden von Dateiberechtigungen

Konfigurieren Sie die erweiterten NTFS-Dateiberechtigungen mithilfe der Registerkarte Windows-Sicherheit

Sie können Standard-NTFS-Dateiberechtigungen für Dateien und Ordner konfigurieren, indem Sie im Fenster Windows-Eigenschaften die Registerkarte **Windows-Sicherheit** verwenden.

Bevor Sie beginnen

Der Administrator, der diese Aufgabe ausführt, muss über ausreichende NTFS-Berechtigungen verfügen, um Berechtigungen für die ausgewählten Objekte zu ändern.

Über diese Aufgabe

Die Konfiguration von NTFS-Dateiberechtigungen erfolgt auf einem Windows-Host durch Hinzufügen von Einträgen zu NTFS-Ermessensary Access Control Lists (DACLs), die mit einem NTFS-Sicherheitsdeskriptor verknüpft sind. Der Sicherheitsdeskriptor wird dann auf NTFS-Dateien und -Verzeichnisse angewendet. Diese Aufgaben werden automatisch von der Windows GUI übernommen.

Schritte

1. Wählen Sie im Menü **Tools** im Windows Explorer die Option **Netzwerklaufwerk zuordnen** aus.
2. Füllen Sie das Dialogfeld **Map Network Drive** aus:

   a. Wählen Sie einen **Drive**-Buchstaben aus.

   b. Geben Sie im Feld **Ordner** den CIFS-Servernamen ein, der den Share enthält, der die Daten enthält, auf die Sie Berechtigungen anwenden möchten, und den Namen der Freigabe.

      Wenn der Name Ihres CIFS-Servers „`CIFS_SERVER`“ lautet und Ihre Freigabe „`share1`“ heißt, sollten Sie eingeben `\\CIFS_SERVER\share1`.

      Sie können die IP-Adresse der Datenschnittstelle für den CIFS-Server anstelle des CIFS-Servernamens angeben.

   c. Klicken Sie Auf **Fertig Stellen**.

   Das ausgewählte Laufwerk ist mit dem Windows Explorer-Fenster verbunden und bereit, in dem die Dateien und Ordner in der Freigabe angezeigt werden.

3. Wählen Sie die Datei oder das Verzeichnis aus, für die Sie NTFS-Dateiberechtigungen festlegen möchten.
4. Klicken Sie mit der rechten Maustaste auf die Datei oder das Verzeichnis, und wählen Sie dann **Eigenschaften** aus.
5. Wählen Sie die Registerkarte **Sicherheit**.

   Auf der Registerkarte **Sicherheit** wird die Liste der Benutzer und Gruppen angezeigt, für die NTFS-Berechtigungen festgelegt sind. Im Feld **Berechtigungen für** wird eine Liste mit Berechtigungen für jeden ausgewählten Benutzer oder jede ausgewählte Gruppe angezeigt.

6. Klicken Sie Auf **Erweitert**.

   Im Fenster Windows-Eigenschaften werden Informationen über vorhandene Dateiberechtigungen angezeigt, die Benutzern und Gruppen zugewiesen sind.

7. Klicken Sie Auf **Berechtigungen Ändern**.

   Das Fenster Berechtigungen wird geöffnet.

8. Führen Sie die gewünschten Aktionen aus:

Ihr Ziel ist	Gehen Sie wie folgt vor…
Einrichten erweiterter NTFS-Berechtigungen für einen neuen Benutzer oder eine neue Gruppe	a. Klicken Sie Auf **Hinzufügen**. b. Geben Sie in das Feld *Geben Sie den Objektnamen ein, den Sie auswählen möchten. Geben Sie den Namen des Benutzers oder der Gruppe ein, den Sie hinzufügen möchten. c. Klicken Sie auf **OK**.
Ändern Sie erweiterte NTFS-Berechtigungen von einem Benutzer oder einer Gruppe	a. Wählen Sie im Feld **Berechtigungen Einträge:** den Benutzer oder die Gruppe aus, deren erweiterte Berechtigungen Sie ändern möchten. b. Klicken Sie Auf **Bearbeiten**.
Entfernen Sie erweiterte NTFS-Berechtigungen für einen Benutzer oder eine Gruppe	a. Wählen Sie im Feld **Berechtigungen Einträge:** den Benutzer oder die Gruppe aus, die Sie entfernen möchten. b. Klicken Sie Auf **Entfernen**. c. Weiter mit Schritt 13.

   Wenn Sie erweiterte NTFS-Berechtigungen für einen neuen Benutzer oder eine neue Gruppe hinzufügen oder die erweiterten NTFS-Berechtigungen für einen vorhandenen Benutzer oder eine vorhandene Gruppe ändern, wird das Feld Berechtigung für <Objekt> geöffnet.

9. Wählen Sie im Feld **Apply to** aus, wie Sie diesen NTFS-Dateiberechtigungseintrag anwenden möchten.

   Wenn Sie NTFS-Dateiberechtigungen für eine einzelne Datei einrichten, ist das Feld **Apply to** nicht aktiv. Die Einstellung **Apply to** ist standardmäßig auf **nur dieses Objekt** eingestellt.

10. Wählen Sie im Feld **Berechtigungen** die Felder **erlauben** oder **verweigern** für die erweiterten Berechtigungen, die Sie für dieses Objekt festlegen möchten.

    - Um den angegebenen Zugriff zuzulassen, wählen Sie das Feld **Zulassen** aus.
    - Um den angegebenen Zugriff nicht zuzulassen, wählen Sie das Feld **Deny** aus. Sie können Berechtigungen für die folgenden erweiterten Rechte festlegen:
    - **Volle Kontrolle**

      Wenn Sie dieses erweiterte Recht wählen, werden alle anderen erweiterten Rechte automatisch ausgewählt (entweder Rechte zulassen oder verweigern).

- **Traverse Ordner / Datei ausführen**
- **Ordner auflisten / Daten lesen**
- **Attribute lesen**
- **Erweiterte Attribute lesen**
- **Dateien erstellen / Daten schreiben**
- **Ordner erstellen / Daten anhängen**
- **Attribute schreiben**
- **Erweiterte Attribute schreiben**
- **Löschen von Unterordnern und Dateien**
- **Löschen**
- **Berechtigungen lesen**
- **Berechtigungen ändern**
- **Besitzrechte übernehmen**

> Wenn eines der Felder mit erweiterten Berechtigungen nicht ausgewählt werden kann, liegt dies daran, dass die Berechtigungen vom übergeordneten Objekt übernommen werden.

11. Wenn Sie möchten, dass Unterordner und Dateien dieses Objekts diese Berechtigungen erben, wählen Sie das Feld **Diese Berechtigungen auf Objekte und/oder Container innerhalb dieses Containers only** anwenden.
12. Klicken Sie auf **OK**.
13. Geben Sie nach dem Hinzufügen, Entfernen oder Bearbeiten von NTFS-Berechtigungen die Vererbung für dieses Objekt an:

    - Wählen Sie aus dem Feld **include inheritable Berechtigungen aus dem übergeordneten** dieses Objekts aus.

      Dies ist die Standardeinstellung.

    - Wählen Sie aus diesem Objekt* das Feld *Alle Berechtigungen für untergeordnete Objekte mit vererbbaren Berechtigungen ersetzen aus.

      Diese Einstellung ist nicht im Feld Berechtigungen vorhanden, wenn Sie NTFS-Dateiberechtigungen für eine einzelne Datei festlegen.

      > Gehen Sie bei der Auswahl dieser Einstellung vorsichtig vor. Mit dieser Einstellung werden alle bestehenden Berechtigungen für alle untergeordneten Objekte entfernt und durch die Berechtigungseinstellungen dieses Objekts ersetzt. Sie können versehentlich Berechtigungen entfernen, die Sie nicht entfernen möchten. Es ist besonders wichtig, wenn Berechtigungen in einem gemischten Volume oder qtree im Sicherheitsstil festgelegt werden. Wenn untergeordnete Objekte einen effektiven UNIX-Sicherheitsstil haben, führt die Weitergabe von NTFS-Berechtigungen an diese untergeordneten Objekte dazu, dass ONTAP diese Objekte vom UNIX-Sicherheitsstil auf den NTFS-Sicherheitsstil ändert. Alle UNIX-Berechtigungen für diese untergeordneten Objekte werden durch NTFS-Berechtigungen ersetzt.

    - Wählen Sie beide Felder aus.

    - Wählen Sie keine der Kontrollkästchen aus.
14. Klicken Sie auf **OK**, um das Feld **Berechtigungen** zu schließen.
15. Klicken Sie auf **OK**, um das Feld **Erweiterte Sicherheitseinstellungen für <Objekt>** zu schließen.

    Weitere Informationen zum Festlegen erweiterter NTFS-Berechtigungen finden Sie in der Windows-Dokumentation.

Verwandte Informationen

Konfigurieren und Anwenden der Dateisicherheit auf NTFS-Dateien und Ordnern mithilfe der CLI

Anzeigen von Informationen zur Dateisicherheit auf NTFS-SicherheitsVolumes

Anzeigen von Informationen zur Dateisicherheit auf Volumes mit gemischter Sicherheitsart

Anzeigen von Informationen zur Dateisicherheit auf UNIX-Volumes im Sicherheitsstil

Konfigurieren Sie die NTFS-Dateiberechtigungen mit der ONTAP-CLI

Sie können NTFS-Dateiberechtigungen für Dateien und Verzeichnisse mithilfe der ONTAP-CLI konfigurieren. Auf diese Weise können Sie NTFS-Dateiberechtigungen konfigurieren, ohne eine Verbindung mit den Daten über eine SMB-Freigabe auf einem Windows-Client herstellen zu müssen.

Sie können NTFS-Dateiberechtigungen konfigurieren, indem Sie Einträge zu den NTFS-Ermessensary-Zugriffssteuerungslisten (DACLs) hinzufügen, die mit einem NTFS-Sicherheitsdeskriptor verknüpft sind. Der Sicherheitsdeskriptor wird dann auf NTFS-Dateien und -Verzeichnisse angewendet.

Sie können NTFS-Dateiberechtigungen nur über die Befehlszeile konfigurieren. NFSv4-ACLs können nicht über die CLI konfiguriert werden.

Wie UNIX-Dateiberechtigungen beim Zugriff auf Dateien über SMB Zugriffskontrolle bieten

Ein FlexVol Volume kann einen von drei Arten von Sicherheitstyp haben: NTFS, UNIX oder gemischt. Sie können unabhängig vom Sicherheitsstil auf Daten über SMB zugreifen. Für den Zugriff auf Daten mit UNIX-Sicherheit sind jedoch entsprechende UNIX-Dateiberechtigungen erforderlich.

Wenn über SMB auf Daten zugegriffen wird, gibt es mehrere Zugriffskontrollen, die bei der Entscheidung, ob ein Benutzer zur Durchführung einer angeforderten Aktion berechtigt ist, verwendet werden:

- Exportberechtigungen

  Die Konfiguration von Exportberechtigungen für SMB-Zugriff ist optional.

- Freigabeberechtigungen
- Dateiberechtigungen

Die folgenden Arten von Dateiberechtigungen können auf die Daten angewendet werden, auf die der Benutzer eine Aktion ausführen möchte:

- NTFS
- UNIX NFSv4-ACLs
- Bits im UNIX-Modus

Für Daten mit festgelegten NFSv4-ACLs oder UNIX-Modus-Bits werden Berechtigungen im UNIX-Stil verwendet, um die Zugriffsrechte für die Daten auf den Dateizugriff zu ermitteln. Der SVM-Administrator muss die entsprechende Dateiberechtigung festlegen, um sicherzustellen, dass Benutzer über die Rechte zur Durchführung der gewünschten Aktion verfügen.

Bei Daten in einem Volume mit gemischtem Sicherheitsstil sind möglicherweise NTFS oder UNIX Sicherheitstyp aktiviert. Wenn die Daten über einen effektiven UNIX-Sicherheitsstil verfügen, werden NFSv4-Berechtigungen oder UNIX-Modus-Bits verwendet, wenn die Zugriffsrechte auf die Daten bestimmt werden.