Wie ONTAP den Zugriff auf Dateien steuert

ONTAP 9

NetApp
March 24, 2023

Inhaltsverzeichnis

Wie ONTAP den Zugriff auf Dateien steuert . . . 1
Wie ONTAP den Zugriff auf Dateien steuert, Übersicht . . . 1
Authentifizierungsbasierte Einschränkungen . . . 1
Dateibasierte Einschränkungen . . . 1

Wie ONTAP den Zugriff auf Dateien steuert

Wie ONTAP den Zugriff auf Dateien steuert, Übersicht

ONTAP steuert den Zugriff auf Dateien gemäß den von Ihnen angegebenen Authentifizierungs- und dateibasierten Einschränkungen.

Wenn ein Client eine Verbindung zum Storage-System herstellt, um auf Dateien zuzugreifen, muss ONTAP zwei Aufgaben erledigen:

- Authentifizierung

  ONTAP muss den Client authentifizieren, indem die Identität mit einer vertrauenswürdigen Quelle überprüft wird. Darüber hinaus ist der Authentifizierungstyp des Clients eine Methode, mit der bestimmt werden kann, ob ein Client beim Konfigurieren von Exportrichtlinien auf Daten zugreifen kann (optional für CIFS).

- Autorisierung

  ONTAP muss den Benutzer autorisieren, indem er die Anmeldeinformationen des Benutzers mit den in der Datei oder dem Verzeichnis konfigurierten Berechtigungen vergleicht und bestimmt, welche Art von Zugriff, falls vorhanden, zur Verfügung stellt.

Um die Kontrolle über den Dateizugriff ordnungsgemäß zu managen, muss ONTAP mit externen Services wie NIS, LDAP und Active Directory Servern kommunizieren. Um ein Storage-System für Dateizugriff über CIFS oder NFS zu konfigurieren, müssen Sie die entsprechenden Services je nach Ihrer Umgebung in ONTAP einrichten.

Authentifizierungsbasierte Einschränkungen

Bei authentifizierungsbasierten Einschränkungen kann festgelegt werden, welche Client-Machines und welche Benutzer eine Verbindung zur Storage Virtual Machine (SVM) herstellen können.

ONTAP unterstützt Kerberos-Authentisierung von UNIX und Windows Servern.

Dateibasierte Einschränkungen

ONTAP bewertet drei Sicherheitsstufen, um zu ermitteln, ob eine Einheit autorisiert ist, eine angeforderte Aktion für Dateien und Verzeichnisse, die sich auf einer SVM befinden, durchzuführen. Der Zugriff wird durch die effektiven Berechtigungen nach Auswertung der drei Sicherheitsstufen bestimmt.

Jedes Storage-Objekt kann bis zu drei Typen von Sicherheitsebenen enthalten:

- Exportsicherheit (NFS) und Freigabe (SMB)

  Die Export- und Share-Sicherheit gilt für den Client-Zugriff auf einen bestimmten NFS-Export oder eine bestimmte SMB-Freigabe. Benutzer mit Administratorrechten können die Sicherheit von Export- und Share-Ebene über SMB- und NFS-Clients managen.

- Sicherheit von Datei- und Verzeichnisdateien auf Storage-Ebene

  Die Sicherheit der Storage-Level Access Guard-Lösung gilt für den Zugriff von SMB- und NFS-Clients auf SVM Volumes. Es werden nur NTFS-Zugriffsberechtigungen unterstützt. Damit ONTAP auf UNIX-Benutzern Sicherheitsüberprüfungen für den Zugriff auf Daten auf Volumes durchführen kann, für die der Storage-Level Access Guard angewendet wurde, muss der UNIX-Benutzer einem Windows-Benutzer auf der SVM, der auch Eigentümer des Volumes ist, zuordnen.

  > Wenn Sie die Sicherheitseinstellungen einer Datei oder eines Verzeichnisses von einem NFS- oder SMB-Client aus anzeigen, wird die Sicherheit des Access Guard auf Storage-Ebene nicht angezeigt. Die Sicherheit des Access Guard auf Storage-Ebene kann nicht von einem Client entzogen werden, selbst wenn ein System-Administrator (Windows oder UNIX) dies durchführt.

- Native Sicherheit auf Dateiebene durch NTFS, UNIX und NFSv4

  Die Datei oder das Verzeichnis, die das Storage-Objekt repräsentieren, enthält native Sicherheit auf Dateiebene. Sie können die Sicherheit auf Dateiebene von einem Client aus festlegen. Die Dateiberechtigungen haben unabhängig davon, ob SMB oder NFS für den Zugriff auf die Daten verwendet wird.