Audit-Richtlinien für Dateien und Ordner konfigurieren

ONTAP 9

NetApp
September 12, 2024

Inhalt

Audit-Richtlinien für Dateien und Ordner konfigurieren

Audit-Richtlinien für Dateien und Ordner konfigurieren

Die Implementierung der Prüfung von Datei- und Ordnerzugriffsereignissen ist ein zweistufiger Prozess. Zunächst müssen Sie eine Audit-Konfiguration auf Storage Virtual Machines (SVMs) erstellen und aktivieren. Zweitens müssen Sie die Audit-Richtlinien für die Dateien und Ordner konfigurieren, die Sie überwachen möchten. Sie können Audit-Richtlinien konfigurieren, um sowohl erfolgreiche als auch fehlgeschlagene Zugriffsversuche zu überwachen.

Sie können sowohl SMB- als auch NFS-Audit-Richtlinien konfigurieren. Audit-Richtlinien für SMB und NFS gelten für unterschiedliche Konfigurationsanforderungen und Audit-Funktionen.

Wenn die entsprechenden Audit-Richtlinien konfiguriert sind, überwacht ONTAP die SMB- und NFS-Zugriffsereignisse wie in den Audit-Richtlinien festgelegt, nur wenn SMB- oder NFS-Server ausgeführt werden.

Konfigurieren Sie die Audit-Richtlinien für Dateien und Verzeichnisse im NTFS-Sicherheitsstil

Bevor Sie Vorgänge in Dateien und Verzeichnissen prüfen können, müssen Sie die Überwachungsrichtlinien für die Dateien und Verzeichnisse konfigurieren, für die Sie Audit-Informationen erfassen möchten. Dies ist zusätzlich zur Einrichtung und Aktivierung der Audit-Konfiguration. Sie können NTFS-Audit-Richtlinien über die Registerkarte Windows-Sicherheit oder über die ONTAP-CLI konfigurieren.

Konfigurieren von NTFS-Audit-Richtlinien über die Registerkarte Windows-Sicherheit

Sie können NTFS-Audit-Richtlinien für Dateien und Verzeichnisse über die Registerkarte **Windows Security** im Fenster Windows-Eigenschaften konfigurieren. Dies ist die gleiche Methode, die bei der Konfiguration von Audit-Richtlinien für Daten auf einem Windows-Client verwendet wird. Auf diese Weise können Sie die gleiche GUI-Schnittstelle verwenden, die Sie gewohnt sind.

Bevor Sie beginnen

Das Auditing muss auf der Storage Virtual Machine (SVM) konfiguriert werden, die die Daten enthält, auf die Sie Systemzugriffssteuerungslisten (SACLs) anwenden.

Über diese Aufgabe

Das Konfigurieren von NTFS-Audit-Richtlinien erfolgt durch Hinzufügen von Einträgen zu NTFS-SACLs, 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. Der Sicherheitsdeskriptor kann Discretionary Access Control Lists (DACLs) zum Anwenden von Datei- und Ordnerzugriffsberechtigungen, SACLs für Datei- und Ordnerprüfung oder SACLs und DACLs enthalten.

Führen Sie die folgenden Schritte auf einem Windows-Host aus, um NTFS-Audit-Richtlinien über die Registerkarte Windows-Sicherheit festzulegen:

Schritte

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

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

   b. Geben Sie im Feld **Ordner** den SMB-Servernamen ein, der die Freigabe enthält und die zu prüfenden Daten sowie den Namen der Freigabe enthält.

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

      Wenn der Name Ihres SMB-Servers „`SMB_SERVER`“ lautet und Ihre Freigabe den Namen „`share1`“ hat, sollten Sie eingeben `\\SMB_SERVER\share1`.

   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 den Audit-Zugriff aktivieren 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**.
6. Klicken Sie Auf **Erweitert**.
7. Wählen Sie die Registerkarte **Revision** aus.
8. Führen Sie die gewünschten Aktionen aus:

Wenn Sie… wollen	Gehen Sie wie folgt vor
Einrichten der Prüfung für einen neuen Benutzer oder eine neue Gruppe	a. Klicken Sie Auf **Hinzufügen**. b. Geben Sie in das Feld Objektnamen eingeben, um auszuwählen, den Namen des Benutzers oder der Gruppe ein, den Sie hinzufügen möchten. c. Klicken Sie auf **OK**.
Audit von einem Benutzer oder einer Gruppe entfernen	a. Wählen Sie im Feld Objektnamen eingeben den Benutzer oder die Gruppe aus, die Sie entfernen möchten. b. Klicken Sie Auf **Entfernen**. c. Klicken Sie auf **OK**. d. Überspringen Sie den Rest dieses Verfahrens.
Ändern Sie die Prüfung für einen Benutzer oder eine Gruppe	a. Wählen Sie im Feld Objektnamen eingeben den Benutzer oder die Gruppe aus, die Sie ändern möchten. b. Klicken Sie Auf **Bearbeiten**. c. Klicken Sie auf **OK**.

Wenn Sie eine Prüfung für einen Benutzer oder eine Gruppe einrichten oder die Prüfung für einen

vorhandenen Benutzer oder eine vorhandene Gruppe ändern, wird das Feld Überwachungseintrag für <Object> geöffnet.

9. Wählen Sie im Feld **Apply to** aus, wie Sie diesen Prüfungseintrag anwenden möchten.

   Sie können eine der folgenden Optionen auswählen:

   - **Dieser Ordner, Unterordner und Dateien**
   - **Dieser Ordner und Unterordner**
   - **Nur dieser Ordner**
   - **Dieser Ordner und die Dateien**
   - **Nur Unterordner und Dateien**
   - **Nur Unterordner**
   - **Nur Dateien** Wenn Sie eine Prüfung auf eine einzelne Datei einrichten, ist die Box **Apply to** nicht aktiv. Die Einstellung **auf** anwenden ist standardmäßig auf **nur dieses Objekt** eingestellt.

   > Da durch das Auditing SVM-Ressourcen belegt werden, wählen Sie nur die minimale Stufe aus, die die Auditing-Ereignisse erfüllt, die Ihre Sicherheitsanforderungen erfüllen.

10. Wählen Sie im Feld **Zugriff** aus, was geprüft werden soll und ob erfolgreiche Ereignisse, Fehlereignisse oder beides geprüft werden sollen.
    - Wenn erfolgreiche Ereignisse geprüft werden sollen, wählen Sie das Feld Erfolg aus.
    - Um Fehlerereignisse zu überwachen, wählen Sie das Feld Fehler aus.

      Wählen Sie nur die Aktionen aus, die Sie überwachen müssen, um Ihre Sicherheitsanforderungen zu erfüllen. Weitere Informationen zu diesen prüffähigen Ereignissen finden Sie in Ihrer Windows-Dokumentation. Sie können die folgenden Ereignisse prüfen:

    - **Volle Kontrolle**
    - **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**
11. Wenn Sie nicht möchten, dass sich die Überwachungseinstellung auf nachfolgende Dateien und Ordner des ursprünglichen Containers verbreitet, wählen Sie die Option **Diese Überwachungseinträge auf Objekte und/oder Container innerhalb dieses Containers only** anwenden aus.

12. Klicken Sie Auf **Anwenden**.
13. Klicken Sie nach dem Hinzufügen, Entfernen oder Bearbeiten von Prüfungseinträgen auf **OK**.

    Das Feld Überwachungseintrag für <Object> wird geschlossen.

14. Wählen Sie im Feld **Revision** die Vererbungseinstellungen für diesen Ordner aus.

    Wählen Sie nur die minimale Stufe aus, die die Überwachungsereignisse enthält, die Ihren Sicherheitsanforderungen entsprechen. Sie können eine der folgenden Optionen auswählen:

    - Wählen Sie aus dem übergeordneten Feld dieses Objekts die Option vererbbare Überwachungseinträge einschließen aus.
    - Wählen Sie das Kontrollkästchen Alle bestehenden vererbbaren Überwachungseinträge für alle abhängigen Elemente durch vererbbare Prüfeinträge aus diesem Objekt ersetzen aus.
    - Wählen Sie beide Felder aus.
    - Wählen Sie keine der Kontrollkästchen aus. Wenn Sie SACLs auf eine einzelne Datei setzen, ist das Ersetzen aller vorhandenen vererbbaren Überwachungseinträge auf allen Nachkommen durch vererbbare Prüfeinträge aus diesem Objektfeld nicht im Feld Auditing vorhanden.
15. Klicken Sie auf **OK**.

    Das Feld Auditing wird geschlossen.

Konfigurieren Sie die NTFS-Audit-Richtlinien mithilfe der ONTAP-CLI

Über die ONTAP-Befehlszeilenschnittstelle können Sie die Audit-Richtlinien für Dateien und Ordner konfigurieren. So können Sie NTFS-Audit-Richtlinien konfigurieren, ohne dass eine Verbindung zu den Daten über eine SMB-Freigabe auf einem Windows-Client hergestellt werden muss.

Sie können NTFS-Audit-Richtlinien mit konfigurieren `vserver security file-directory` Befehlsfamilie.

Sie können NTFS SACLs nur mit der CLI konfigurieren. Das Konfigurieren von NFSv4 SACLs wird von dieser ONTAP-Befehlfamilie nicht unterstützt. Weitere Informationen über die Verwendung dieser Befehle zum Konfigurieren und Hinzufügen von NTFS-SACLs zu Dateien und Ordnern finden Sie auf den man-Pages.

Konfigurieren Sie Auditing für Dateien und Verzeichnisse im UNIX-Sicherheitsstil

Sie konfigurieren Audit für Dateien und Verzeichnisse im UNIX-Sicherheitsstil durch Hinzufügen von Audit ACLs zu NFSv4.x ACLs. So können Sie bestimmte NFS-Datei- und Verzeichniszugriffe zu Sicherheitszwecken überwachen.

Über diese Aufgabe

Für NFSv4.x sind Ermessenswert- und SystemAsse in derselben ACL gespeichert. Sie werden nicht in separaten DACLs und SACLs gespeichert. Daher müssen Sie beim Hinzufügen von Audit Aces zu einer vorhandenen ACL Vorsicht walten lassen, um zu vermeiden, dass eine vorhandene ACL überschrieben und verloren geht. Die Reihenfolge, in der Sie die Audit Aces zu einer bestehenden ACL hinzufügen, ist nicht von Bedeutung.

Schritte

1. Rufen Sie die vorhandene ACL für die Datei oder das Verzeichnis mithilfe von ab `nfs4_getfacl` Oder gleichwertiger Befehl.

   Weitere Informationen zum Bearbeiten von ACLs finden Sie in den man-Pages des NFS-Clients.

2. Fügen Sie die gewünschten Audit Aces hinzu.
3. Wenden Sie die aktualisierte ACL mithilfe des auf die Datei oder das Verzeichnis an `nfs4_setfacl` Oder gleichwertiger Befehl.