# Zugriffskontrollrollen verwalten

ONTAP 9

NetApp
September 30, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/authentication/manage-access-control-roles-concept.html on September 30, 2026. Always check docs.netapp.com for the latest.

# Inhalt


Zugriffskontrollrollen verwalten . . . 1
- Informationen zu ONTAP Zugriffskontrollrollen . . . 1
- Die einem ONTAP Administrator zugewiesene Rolle ändern . . . 1
- Benutzerdefinierte Rollen für ONTAP Administratoren definieren . . . 2
- Vordefinierte Rollen für ONTAP Clusteradministratoren . . . 3
- Vordefinierte Rollen für ONTAP SVM Administratoren . . . 5
- ONTAP Administratorzugriff mit System Manager verwalten . . . 7
  - Einem Administrator eine Rolle zuweisen . . . 8
  - Ändern der Administratorrolle . . . 8
- Verwendung der JIT-Berechtigungserweiterung in ONTAP . . . 8
- JIT-Zugangsstufenerhöhung in ONTAP konfigurieren . . . 9
  - Globale JIT Einstellungen anpassen . . . 10
  - JIT-Zugangsstufe für einen Benutzer konfigurieren . . . 11
  - Häufige Anwendungsfälle für JIT . . . 12

# Zugriffskontrollrollen verwalten

## Informationen zu ONTAP Zugriffskontrollrollen

Die einem Administrator zugewiesene Rolle bestimmt, auf welche Befehle der Administrator Zugriff hat. Die Rolle wird zugewiesen, wenn das Konto für den Administrator erstellt wird. Es kann bei Bedarf eine andere Rolle zugewiesen oder benutzerdefinierte Rollen definiert werden.

## Die einem ONTAP Administrator zugewiesene Rolle ändern

Sie können den `security login modify` Befehl verwenden, um die Rolle eines Cluster- oder SVM-Administratorkontos zu ändern. Es kann eine vordefinierte oder eine benutzerdefinierte Rolle zugewiesen werden.

**Bevor Sie beginnen**

Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

**Schritt**

1. Die Rolle eines Cluster- oder SVM-Administrators ändern:

   ```
   security login modify -vserver SVM_name -user-or-group-name user_or_group_name
   -application application -authmethod authentication_method -role role -comment
   comment
   ```

   "Erstellen oder Ändern von Anmeldekonten"

   Der folgende Befehl ändert die Rolle des AD-Cluster-Administratorkontos `DOMAIN1\guest1` zur vordefinierten `readonly` Rolle.

   ```
   cluster1::>security login modify -vserver engCluster -user-or-group-name
   DOMAIN1\guest1 -application ssh -authmethod domain -role readonly
   ```

   Der folgende Befehl ändert die Rolle der SVM-Administratorkonten im Active Directory Gruppe Konto `DOMAIN1\adgroup` zur benutzerdefinierten `vol_role` Rolle.

   ```
   cluster1::>security login modify -vserver engData -user-or-group-name
   DOMAIN1\adgroup -application ssh -authmethod domain -role vol_role
   ```

   Weitere Informationen zu `security login modify` finden sich in der "ONTAP-Befehlsreferenz".

# Benutzerdefinierte Rollen für ONTAP Administratoren definieren

Sie können den `security login role create`Befehl verwenden, um eine benutzerdefinierte Rolle zu definieren. Der Befehl kann beliebig oft ausgeführt werden, um die genaue Kombination von Funktionen zu erreichen, die mit der Rolle verknüpft werden soll.

**Über diese Aufgabe**

- Eine Rolle, ob vordefiniert oder benutzerdefiniert, gewährt oder verweigert den Zugriff auf ONTAP Befehle oder Befehlsverzeichnisse.

  Ein Befehlsverzeichnis (`volume`, beispielsweise, ist eine Gruppe zusammengehöriger Befehle und Befehlsunterverzeichnisse. Sofern in diesem Verfahren nicht anders beschrieben, gewährt oder verweigert die Zugriffsberechtigung für ein Befehlsverzeichnis den Zugriff auf jeden Befehl in diesem Verzeichnis und seinen Unterverzeichnissen.

- Der Zugriff auf bestimmte Befehle oder Unterverzeichnisse hat Vorrang vor dem Zugriff auf das übergeordnete Verzeichnis.

  Wird eine Rolle mit einem Befehlsverzeichnis definiert und anschließend mit einer anderen Zugangsstufe für einen bestimmten Befehl oder ein Unterverzeichnis des übergeordneten Verzeichnisses neu definiert, so überschreibt die für den Befehl oder das Unterverzeichnis angegebene Zugangsstufe diejenige des übergeordneten Verzeichnisses.

> Einem SVM-Administrator kann keine Rolle zugewiesen werden, die Zugriff auf einen Befehl oder ein Befehlsverzeichnis gewährt, das nur dem `admin`Cluster Administrator zur Verfügung steht, beispielsweise das `security`Befehlsverzeichnis.

**Bevor Sie beginnen**

Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

**Schritt**

1. Eine benutzerdefinierte Rolle festlegen:

   ```
   security login role create -vserver SVM_name -role role -cmddirname
   command_or_directory_name -access access_level -query query
   ```

   Die folgenden Befehle gewähren der `vol_role` Rolle vollen Zugriff auf die Befehle im `volume` Befehlsverzeichnis und Lesezugriff auf die Befehle im `volume snapshot` Unterverzeichnis.

   ```
   cluster1::>security login role create -role vol_role -cmddirname
   "volume" -access all

   cluster1::>security login role create -role vol_role -cmddirname "volume
   snapshot" -access readonly
   ```

   Die folgenden Befehle gewähren der `SVM_storage` Rolle Lesezugriff auf die Befehle im `storage` Befehlsverzeichnis, keinen Zugriff auf die Befehle im `storage encryption` Unterverzeichnis und vollen Zugriff auf den `storage aggregate plex offline` nichtintrinsischen Befehl.

```
cluster1::>security login role create -role SVM_storage -cmddirname
"storage" -access readonly

cluster1::>security login role create -role SVM_storage -cmddirname
"storage encryption" -access none

cluster1::>security login role create -role SVM_storage -cmddirname
"storage aggregate plex offline" -access all
```

Weitere Informationen zu `security login role create` finden sich in der "ONTAP-Befehlsreferenz".

**Verwandte Informationen**

- "security login role create"
- "Storage Aggregate Plex offline"
- "Speicherverschlüsselung"

# Vordefinierte Rollen für ONTAP Clusteradministratoren

Die vordefinierten Rollen für Clusteradministratoren sollten die meisten Ihrer Anforderungen abdecken. Bei Bedarf können benutzerdefinierte Rollen erstellt werden. Standardmäßig wird einem Clusteradministrator die vordefinierte `admin` Rolle zugewiesen.

Die folgende Tabelle enthält die vordefinierten Rollen für Cluster-Administratoren:

| Diese Rolle… | Verfügt über diese Zugriffsebene… | Zu den folgenden Befehlen oder Befehlsverzeichnissen |
|---|---|---|
| Administrator | alle | Alle Befehlsverzeichnisse (`DEFAULT` |
| admin-no-fsa (verfügbar ab ONTAP 9.12.1) | Lesen/Schreiben | • Alle Befehlsverzeichnisse (`DEFAULT`<br>• `security login rest-role`<br>• `security login role` |

| | | |
|---|---|---|
| Nur lesen | • `security login rest-role create`<br>• `security login rest-role delete`<br>• `security login rest-role modify`<br>• `security login rest-role show`<br>• `security login role create`<br>• `security login role create`<br>• `security login role delete`<br>• `security login role modify`<br>• `security login role show`<br>• `volume activity-tracking`<br>• `volume analytics` | Keine |
| `volume file show-disk-usage` | AutoSupport | alle |
| • `set`<br>• `system node autosupport` | keine | Alle anderen Befehlsverzeichnisse (`DEFAULT`) |
| Backup | alle | `vserver services ndmp` |
| schreibgeschützt | `volume` | keine |
| Alle anderen Befehlsverzeichnisse (`DEFAULT`) | schreibgeschützt | alle |
| • `security login password`<br>Nur zur Verwaltung des lokalen Passworts und der Schlüsselinformationen des eigenen Benutzerkontos<br>• `set` | • Ab ONTAP 9.8 ist readonly<br>• Vor ONTAP 9.8 keine | `security` |
| schreibgeschützt | Alle anderen Befehlsverzeichnisse (`DEFAULT`) | SnapLock |

| | | |
|---|---|---|
| alle | • `set`<br>• `volume create`<br>• `volume modify`<br>• `volume move`<br>• `volume show` | keine |
| • `volume move governor`<br>• `volume move recommend` | keine | Alle anderen Befehlsverzeichnisse (`DEFAULT`) |
| keine | keine | Alle Befehlsverzeichnisse (`DEFAULT` |

Die `autosupport` Rolle ist dem vordefinierten `autosupport` Konto zugewiesen, das von AutoSupport OnDemand verwendet wird. ONTAP verhindert, dass das `autosupport` Konto geändert oder gelöscht wird. ONTAP verhindert außerdem, dass die `autosupport` Rolle anderen Benutzerkonten zugewiesen wird.

**Verwandte Informationen**

- "Security Login"
- "Set"
- "Volumen"
- "vserver services ndmp"

# Vordefinierte Rollen für ONTAP SVM Administratoren

Die vordefinierten Rollen für SVM-Administratoren sollten die meisten Ihrer Anforderungen abdecken. Bei Bedarf können benutzerdefinierte Rollen erstellt werden. Standardmäßig wird einem SVM-Administrator die vordefinierte `vsadmin` Rolle zugewiesen.

Die folgende Tabelle listet die vordefinierten Rollen für SVM-Administratoren auf:

| Rollenname | Fähigkeiten |
|---|---|

| | |
|---|---|
| vsadmin | • Verwaltung der lokalen Passwort- und Schlüsselinformationen des eigenen Benutzerkontos<br>• Verwaltung von Volumes, ausgenommen Volume-Verschiebungen<br>• Verwaltung von Kontingenten, Qtrees, Snapshots und Dateien<br>• Verwaltung von LUNs<br>• Ausführen von SnapLock-Operationen, außer privilegiertem Löschen<br>• Konfiguration von Protokollen: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC und NVMe/TCP<br>• Konfiguration von Diensten: DNS, LDAP und NIS<br>• Überwachungsaufträge<br>• Überwachung von Netzwerkverbindungen und Netzwerkschnittstellen<br>• Überwachung des Gesundheitszustands der SVM |
| vsadmin-volume | • Verwaltung der lokalen Passwort- und Schlüsselinformationen des eigenen Benutzerkontos<br>• Verwaltung von Volumes, ausgenommen Volume-Verschiebungen<br>• Verwaltung von Kontingenten, Qtrees, Snapshots und Dateien<br>• Verwaltung von LUNs<br>• Konfiguration von Protokollen: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC und NVMe/TCP<br>• Konfiguration von Diensten: DNS, LDAP und NIS<br>• Überwachung der Netzwerkschnittstelle<br>• Überwachung des Gesundheitszustands der SVM |
| vsadmin-protocol | • Verwaltung der lokalen Passwort- und Schlüsselinformationen des eigenen Benutzerkontos<br>• Konfiguration von Protokollen: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC und NVMe/TCP<br>• Konfiguration von Diensten: DNS, LDAP und NIS<br>• Verwaltung von LUNs<br>• Überwachung der Netzwerkschnittstelle<br>• Überwachung des Gesundheitszustands der SVM |

| | |
|---|---|
| vsadmin-backup | • Verwaltung der lokalen Passwort- und Schlüsselinformationen des eigenen Benutzerkontos<br>• Verwaltung von NDMP-Operationen<br>• Ein wiederhergestelltes Volume für lesen/schreiben aktivieren<br>• Verwaltung von SnapMirror-Beziehungen und Snapshots<br>• Anzeige von Volumen und Netzwerkinformationen |
| vsadmin-snaplock | • Verwaltung der lokalen Passwort- und Schlüsselinformationen des eigenen Benutzerkontos<br>• Verwaltung von Volumes, ausgenommen Volume-Verschiebungen<br>• Verwaltung von Kontingenten, Qtrees, Snapshots und Dateien<br>• Durchführen von SnapLock-Operationen, einschließlich privilegiertem Löschen<br>• Konfiguration von Protokollen: NFS und SMB<br>• Konfiguration von Diensten: DNS, LDAP und NIS<br>• Überwachungsaufträge<br>• Überwachung von Netzwerkverbindungen und Netzwerkschnittstellen |
| vsadmin-readonly | • Verwaltung der lokalen Passwort- und Schlüsselinformationen des eigenen Benutzerkontos<br>• Überwachung des Gesundheitszustands der SVM<br>• Überwachung der Netzwerkschnittstelle<br>• Anzeigen von Volumes und LUNs<br>• Anzeigen von Diensten und Protokollen |

# ONTAP Administratorzugriff mit System Manager verwalten

Die einem Administrator zugewiesene Rolle bestimmt, welche Funktionen der Administrator mit System Manager ausführen kann. System Manager stellt vordefinierte Rollen für Cluster-Administratoren und Storage-VM-Administratoren bereit. Die Rolle wird beim Erstellen des Administratorkontos zugewiesen oder kann später geändert werden.

Je nachdem, wie der Kontozugriff aktiviert wurde, kann es erforderlich sein, eine der folgenden Aktionen durchzuführen:

- Ein öffentlicher Schlüssel wird mit einem lokalen Konto verknüpft.
- Ein von einer Zertifizierungsstelle signiertes digitales Serverzertifikat installieren.

- AD-, LDAP- oder NIS-Zugriff konfigurieren.

Diese Aufgaben können vor oder nach der Aktivierung des Kontozugriffs durchgeführt werden.

### Einem Administrator eine Rolle zuweisen

Einem Administrator wird wie folgt eine Rolle zugewiesen:

**Schritte**

1. **Cluster > Einstellungen** auswählen.
2. Wählen Sie → neben **Benutzer und Rollen** aus.
3. Wählen Sie + Add unter **Benutzer** aus.
4. Geben Sie einen Benutzernamen an und wählen Sie im Dropdown-Menü für **Rolle** eine Rolle aus.
5. Eine Anmeldemethode und ein Passwort für den Benutzer angeben.

### Ändern der Administratorrolle

Die Rolle eines Administrators kann wie folgt geändert werden:

**Schritte**

1. **Cluster > Einstellungen** auswählen.
2. Wählen Sie den Namen des Benutzers aus, dessen Rolle Sie ändern möchten, und klicken Sie dann auf das ⋮ Symbol, das neben dem Benutzernamen erscheint.
3. Klicken Sie auf **Bearbeiten**.
4. Im Dropdown-Menü für **Rolle** eine Rolle auswählen.

# Verwendung der JIT-Berechtigungserweiterung in ONTAP

Ab ONTAP 9.17.1 können Cluster-Administratoren "Just-in-Time (JIT) Privileg-Erweiterung konfigurieren" ONTAP Benutzern die Möglichkeit geben, ihre Berechtigungen vorübergehend zu erhöhen, um bestimmte Aufgaben auszuführen. Wenn JIT für einen Benutzer konfiguriert ist, kann dieser seine Berechtigungen vorübergehend auf eine Rolle anheben, die über die erforderlichen Berechtigungen zur Ausführung einer Aufgabe verfügt. Nach Ablauf der Sitzung kehrt der Benutzer zu seiner ursprünglichen Zugangsstufe zurück.

Cluster-Administratoren können die Dauer konfigurieren, für die ein Benutzer Zugriff auf die JIT-Berechtigungserweiterung hat. Beispielsweise kann der Zugriff eines Benutzers auf die JIT-Berechtigungserweiterung mit einem Sitzungslimit von 30 Minuten (dem *Sitzungsgültigkeitszeitraum*) für einen Zeitraum von 30 Tagen (dem *JIT-Gültigkeitszeitraum*) konfiguriert werden. Während des 30-tägigen Zeitraums kann der Benutzer seine Berechtigungen beliebig oft erweitern, jedoch ist jede Sitzung auf 30 Minuten begrenzt.

**Über diese Aufgabe**

- Die JIT-Berechtigungserweiterung steht nur Benutzern zur Verfügung, die mit SSH auf ONTAP zugreifen. Erweiterte Berechtigungen stehen nur innerhalb der aktuellen SSH-Sitzung zur Verfügung, können jedoch in beliebig vielen gleichzeitigen SSH-Sitzungen genutzt werden.

- Die JIT-Berechtigungserweiterung wird nur für Benutzer unterstützt, die sich mit Passwort-, nsswitch- oder Domänenauthentifizierung anmelden. Multifaktor-Authentifizierung (MFA) wird für die JIT-Berechtigungserweiterung nicht unterstützt.
- Die JIT-Sitzung eines Benutzers wird beendet, wenn die konfigurierte Sitzungs- oder JIT-Gültigkeitsdauer abläuft oder wenn ein Cluster-Administrator JIT-Zugriff für den Benutzer widerruft.

**Bevor Sie beginnen**

- Um auf die JIT-Berechtigungserweiterung zuzugreifen, muss ein Clusteradministrator den JIT-Zugriff für Ihr Konto konfigurieren. Der Clusteradministrator legt die Rolle fest, auf die Sie Ihre Berechtigungen erweitern können, sowie die Dauer, für die Sie auf erweiterte Berechtigungen zugreifen können.

**Schritte**

1. Vorübergehende Erhöhung der Berechtigungen auf die konfigurierte Rolle:

   ```
   security jit-privilege elevate
   ```

   Nach Eingabe dieses Befehls werden Sie zur Eingabe Ihres Anmeldepassworts aufgefordert. Wenn JIT access für Ihr Konto konfiguriert ist, wird Ihnen für die konfigurierte Sitzungsdauer eine erhöhte Zugangsstufe gewährt. Nach Ablauf der Sitzungsdauer kehren Sie zu Ihrer ursprünglichen Zugangsstufe zurück. Innerhalb des konfigurierten JIT-Gültigkeitszeitraums kann die Erhöhung Ihrer Berechtigungen beliebig oft erfolgen.

2. Die verbleibende Zeit in Ihrer JIT-Sitzung wird angezeigt:

   ```
   security jit-privilege show-remaining-time
   ```

   Wenn Sie sich aktuell in einer JIT-Sitzung befinden, zeigt dieser Befehl die verbleibende Zeit an.

3. Beenden Sie Ihre JIT-Sitzung bei Bedarf vorzeitig:

   ```
   security jit-privilege reset
   ```

   Falls Sie sich aktuell in einer JIT-Sitzung befinden, beendet dieser Befehl die JIT-Sitzung und stellt Ihre ursprüngliche Zugangsstufe wieder her.

# JIT-Zugangsstufenerhöhung in ONTAP konfigurieren

Ab ONTAP 9.17.1 können Cluster-Administratoren die Just-in-Time (JIT) Privilegienerhöhung konfigurieren, damit ONTAP Benutzer ihre Berechtigungen vorübergehend erhöhen können, um bestimmte Aufgaben auszuführen. Wenn JIT für einen Benutzer konfiguriert ist, kann er vorübergehend "ihre Privilegien erhöhen" zu einer Rolle wechseln, die über die erforderlichen Berechtigungen zur Ausführung einer Aufgabe verfügt. Nach Ablauf der Sitzungsdauer kehrt der Benutzer zu seiner ursprünglichen Zugangsstufe zurück.

Cluster-Administratoren können die Dauer konfigurieren, für die ein Benutzer Zugriff auf die JIT-

Berechtigungserweiterung hat. Beispielsweise kann der Benutzerzugriff auf die JIT-Elevation mit einem Sitzungszeitlimit von 30 Minuten (dem *Sitzungsgültigkeitszeitraum*) für einen Zeitraum von 30 Tagen (dem *JIT-Gültigkeitszeitraum*) konfiguriert werden. Während des 30-tägigen Zeitraums kann der Benutzer seine Berechtigungen beliebig oft erweitern, jedoch ist jede Sitzung auf 30 Minuten begrenzt.

Die JIT-Berechtigungserweiterung unterstützt das Prinzip der minimalen Berechtigungen und ermöglicht Benutzern die Ausführung von Aufgaben, die erhöhte Berechtigungen erfordern, ohne ihnen diese Berechtigungen dauerhaft zu erteilen. Dies trägt dazu bei, das Risiko unberechtigten Zugriffs oder versehentlicher Änderungen am System zu verringern. Die folgenden Beispiele beschreiben einige gängige Anwendungsfälle für die JIT-Berechtigungserweiterung:

- Temporärer Zugriff auf die `security login create`- und `security login delete`-Befehle ermöglicht das Onboarding und Offboarding von Benutzern.
- Temporärer Zugriff auf `system node image update` und `system node upgrade-revert` kann während eines Aktualisierungsfensters gewährt werden. Nach Abschluss der Aktualisierung wird der Befehlszugriff widerrufen.
- Vorübergehender Zugriff auf `cluster add-node`, `cluster remove-node` und `cluster modify` ermöglicht die Clustererweiterung oder Neukonfiguration. Nach Abschluss der Clusteränderungen wird der Befehlszugriff entzogen.
- Temporärer Zugriff auf `volume snapshot restore` wird gewährt, um Wiederherstellungsvorgänge und die Verwaltung von Sicherungszielen zu ermöglichen. Nach Abschluss der Wiederherstellung oder Konfiguration wird der Befehlszugriff entzogen.
- Temporärer Zugriff auf `security audit log show` kann gewährt werden, um die Überprüfung und den Export des Revisionsprotokolls während einer Compliance-Prüfung zu ermöglichen.

Eine ausführlichere Liste gängiger JIT-Anwendungsfälle ist unter Häufige Anwendungsfälle für JIT zu finden.

Cluster-Administratoren können den JIT Zugang für ONTAP Benutzer einrichten und die standardmäßigen JIT Gültigkeitszeiträume entweder global für den gesamten Cluster oder für bestimmte SVMs konfigurieren.

**Über diese Aufgabe**

- Die JIT-Berechtigungserweiterung steht nur Benutzern zur Verfügung, die mit SSH auf ONTAP zugreifen. Erweiterte Berechtigungen sind nur innerhalb der aktuellen SSH-Sitzung des Benutzers verfügbar, können jedoch in beliebig vielen gleichzeitigen SSH-Sitzungen genutzt werden.
- Die JIT-Berechtigungserweiterung wird nur für Benutzer unterstützt, die sich mit Passwort-, nsswitch- oder Domänenauthentifizierung anmelden. Multifaktor-Authentifizierung (MFA) wird für die JIT-Berechtigungserweiterung nicht unterstützt.

**Bevor Sie beginnen**

- Sie müssen ONTAP Cluster-Administrator auf der `admin`Zugangsstufe sein, um die folgenden Aufgaben auszuführen.

## Globale JIT Einstellungen anpassen

Sie können die Standard-JIT-Einstellungen global für den gesamten ONTAP Cluster oder für eine bestimmte SVM ändern. Diese Einstellungen legen die Standardgültigkeitsdauer der Sitzung und die maximale JIT-Gültigkeitsdauer für Benutzer fest, die für den JIT-Zugang konfiguriert sind.

**Über diese Aufgabe**

- Der Standard `default-session-validity-period`wert beträgt eine Stunde. Diese Einstellung legt fest, wie lange ein Benutzer in einer JIT-Sitzung auf erhöhte Berechtigungen zugreifen kann, bevor eine erneute

Erhöhung erforderlich ist.

- Der Standard `max-jit-validity-period`wert beträgt 90 Tage. Diese Einstellung legt den maximalen Zeitraum fest, in dem ein Benutzer nach dem konfigurierten Startdatum auf die JIT-Elevation zugreifen kann. Die JIT-Gültigkeitsdauer kann für einzelne Benutzer konfiguriert werden, sie darf jedoch die maximale JIT-Gültigkeitsdauer nicht überschreiten.

**Schritte**

1. Aktuelle JIT-Einstellungen prüfen:

```
security jit-privilege show -vserver <svm_name>
```

`-vserver` ist optional. Wenn keine SVM angegeben wird, zeigt der Befehl die globalen JIT-Einstellungen.

2. Die JIT-Einstellungen können global oder für eine SVM angepasst werden:

```
security jit-privilege modify -vserver <svm_name> -default-session
-validity-period <period> -max-jit-validity-period <period>
```

Wird keine SVM angegeben, ändert der Befehl die globalen JIT-Einstellungen. Das folgende Beispiel legt die Standard-JIT-Sitzungsdauer auf 45 Minuten und die maximale JIT-Dauer auf 30 Tage für SVM fest `svm1`:
`security jit-privilege modify -vserver svm1 -default-session-validity-period 45m -max-jit-validity-period 30d`

In diesem Beispiel können Benutzer jeweils 45 Minuten lang auf die JIT-Berechtigungserweiterung zugreifen und JIT-Sitzungen für maximal 30 Tage nach dem konfigurierten Startdatum initiieren.

## JIT-Zugangsstufe für einen Benutzer konfigurieren

Sie können ONTAP Benutzern die Zugangsstufe für JIT-Berechtigungserweiterung zuweisen.

**Schritte**

1. Aktueller JIT Zugriff für einen Benutzer:

```
security jit-privilege user show -username <username>
```

`-username` ist optional. Wenn kein Benutzername angegeben wird, zeigt der Befehl den JIT-Zugang für alle Benutzer an.

2. Neuen JIT Zugang für einen Benutzer zuweisen:

```
security jit-privilege create -username <username> -vserver <svm_name>
-role <rbac_role> -session-validity-period <period> -jit-validity-period
<period> -start-time <date>
```

- Wenn `-vserver`nicht angegeben ist, wird der JIT Zugriff auf Cluster Ebene zugewiesen.
- `-role` ist die RBAC Rolle, zu der der Benutzer erhöht wird. Falls nicht angegeben, `-role` ist der Standardwert `admin`.
- `-session-validity-period` ist die Dauer, für die der Benutzer auf die erhöhte Rolle zugreifen kann, bevor eine neue JIT-Sitzung gestartet werden muss. Falls nicht angegeben, wird der globale oder SVM `default-session-validity-period` verwendet.
- `-jit-validity-period` ist die maximale Dauer, für die ein Benutzer JIT-Sitzungen nach dem konfigurierten Startdatum initiieren kann. Falls nicht angegeben, wird der `session-validity-period` verwendet. Dieser Parameter darf den globalen oder SVM- `max-jit-validity-period` nicht überschreiten.
- `-start-time` ist das Datum und die Uhrzeit, ab der der Benutzer JIT-Sitzungen initiieren kann. Falls nicht angegeben, werden das aktuelle Datum und die aktuelle Uhrzeit verwendet.

  Das folgende Beispiel ermöglicht `ontap_user` den Zugriff auf die `admin` Rolle für 1 Stunde, bevor eine neue JIT-Sitzung gestartet werden muss. `ontap_user` kann JIT-Sitzungen für einen Zeitraum von 60 Tagen ab dem 1. Juli 2025 um 13:00 Uhr initiieren:
  `security jit-privilege user create -username ontap_user -role admin -session -validity-period 1h -jit-validity-period 60d -start-time "7/1/25 13:00:00"`

3. Bei Bedarf den JIT-Zugang eines Benutzers widerrufen:

```
security jit-privilege user delete -username <username> -vserver
<svm_name>
```

Dieser Befehl widerruft die JIT-Zugangsstufe eines Benutzers, selbst wenn diese noch nicht abgelaufen ist. Wenn `-vserver` nicht angegeben ist, wird die JIT-Zugangsstufe auf Clusterebene widerrufen. Befindet sich der Benutzer in einer aktiven JIT-Sitzung, wird die Sitzung beendet.

## Häufige Anwendungsfälle für JIT

Die folgende Tabelle enthält gängige Anwendungsfälle für die JIT-Berechtigungserweiterung. Für jeden Anwendungsfall muss eine RBAC-Rolle konfiguriert werden, um Zugriff auf die relevanten Befehle zu ermöglichen. Jeder Befehl ist mit der ONTAP Command Reference verlinkt, die weitere Informationen zum Befehl und seinen Parametern enthält.

| Anwendungsfall | Befehle | Details |
|---|---|---|
| Benutzer- und Rollenverwaltung | • `security login create`<br>• `security login delete` | Temporäre Rechteerweiterung zum Hinzufügen oder Entfernen von Benutzern oder zum Ändern von Rollen während des Onboardings oder Offboardings. |
| Zertifikatsverwaltung | • `security certificate create`<br>• `security certificate install` | Kurzfristiger Zugriff für die Installation oder Verlängerung des Zertifikats wird gewährt. |

| Anwendungsfall | Befehle | Details |
| --- | --- | --- |
| SSH/CLI Zugriffskontrolle | • `security login create -application ssh` | Vorübergehender SSH-Zugriff für die Fehlerbehebung oder den Support durch den Hersteller. |
| Lizenzverwaltung | • `system license add`<br>• `system license delete` | Berechtigungen zum Hinzufügen oder Entfernen von Lizenzen während der Aktivierung oder Deaktivierung von Funktionen gewähren. |
| Systemaktualisierungen und Patches | • `system node image update`<br>• `system node upgrade-revert` | Für das Upgrade-Fenster erhöhen, dann widerrufen. |
| Netzwerksicherheitseinstellungen | • `security login role create`<br>• `security login role modify` | Temporäre Änderungen an netzwerkbezogenen Sicherheitsrollen ermöglichen. |
| Clusterverwaltung | • `cluster add-node`<br>• `cluster remove-node`<br>• `cluster modify` | Für Clustererweiterung oder -rekonfiguration Elevate verwenden. |
| SVM Management | • `vserver create`<br>• `vserver delete`<br>• `vserver modify` | Einem SVM vorübergehend Administratorrechte für die Bereitstellung oder Außerbetriebnahme zuweisen. |
| Volumenmanagement | • `volume create`<br>• `volume delete`<br>• `volume modify` | Elevate für Volume-Bereitstellung, -Größenänderung oder -Entfernung. |
| Snapshot Verwaltung | • `volume snapshot create`<br>• `volume snapshot delete`<br>• `volume snapshot restore` | Für das Löschen oder Wiederherstellen von Snapshots während der Wiederherstellung sind erhöhte Berechtigungen erforderlich. |
| Netzwerkkonfiguration | • `network interface create`<br>• `network port vlan create` | Rechte für Netzwerkänderungen während Wartungsfenstern gewähren. |
| Festplatten-/Aggregatverwaltung | • `storage disk assign`<br>• `storage aggregate create`<br>• `storage aggregate add-disks` | Elevate dient zum Hinzufügen oder zur Entfernung von Datenträgern oder zum Verwalten von Aggregaten. |

| Anwendungsfall | Befehle | Details |
| --- | --- | --- |
| Datenschutz | • `snapmirror create`<br>• `snapmirror modify`<br>• `snapmirror restore` | Temporär erhöhen, um SnapMirror-Beziehungen zu konfigurieren oder wiederherzustellen. |
| Leistungsoptimierung | • `qos policy-group create`<br>• `qos policy-group modify` | Elevate zur Fehlerbehebung bei der Performance oder zum Tuning. |
| Zugriff auf das Revisionsprotokoll | • `security audit log show` | Temporär für die Überprüfung oder den Export des Revisionsprotokolls während Compliance-Prüfungen erhöhen. |
| Ereignis- und Alarmmanagement | • `event notification create`<br>• `event notification modify` | Elevate dient zum Konfigurieren oder Testen von Ereignisbenachrichtigungen oder SNMP Traps. |
| Compliance-gesteuerter Datenzugriff | • `volume show`<br>• `security audit log show` | Vorübergehender Lesezugriff für Prüfer, um sensible Daten oder Protokolle zu überprüfen. |
| Überprüfungen des privilegierten Zugriffs | • `security login show`<br>• `security login role show` | Vorübergehende Erhöhung zur Überprüfung und Berichterstattung über privilegierten Zugriff. Schreibgeschützter, erhöhter Zugriff für eine begrenzte Zeit. |

**Verwandte Informationen**

- "Cluster"
- "Ereignisbenachrichtigung"
- "Netzwerk"
- "QoS Richtliniengruppe"
- "Sicherheit"
- "SnapMirror"
- "Storage"
- "System"
- "Volumen"
- "vserver"

**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.