Management von Zugriffssteuerungsrollen

ONTAP 9

NetApp
March 22, 2023

Inhaltsverzeichnis

Management von Zugriffssteuerungsrollen

Übersicht über Zugriffssteuerungsrollen verwalten

Die einem Administrator zugewiesene Rolle legt die Befehle fest, auf die der Administrator zugreifen kann. Sie weisen die Rolle beim Erstellen des Kontos für den Administrator zu. Sie können je nach Bedarf eine andere Rolle zuweisen oder benutzerdefinierte Rollen definieren.

Ändern Sie die einem Administrator zugewiesene Rolle

Sie können das verwenden `security login modify` Befehl zum Ändern der Rolle eines Cluster- oder SVM-Administratorkontos. Sie können eine vordefinierte oder benutzerdefinierte Rolle zuweisen.

Was Sie benötigen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Schritt

1. Ändern Sie die Rolle eines Clusters oder SVM-Administrators:

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

   Eine vollständige Befehlssyntax finden Sie im "Arbeitsblatt".

   "Erstellen oder Ändern von Anmeldekonten"

   Mit dem folgenden Befehl wird die Rolle des AD-Cluster-Administratorkontos geändert `DOMAIN1\guest1` Für den vordefinierten `readonly` Rolle:

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

   Mit dem folgenden Befehl wird die Rolle der SVM-Administratorkonten im AD-Gruppenkonto geändert `DOMAIN1\adgroup` Auf den Benutzer `vol_role` Rolle:

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

Definieren benutzerdefinierter Rollen

Sie können das verwenden `security login role create` Befehl zum Definieren

einer benutzerdefinierten Rolle. Sie können den Befehl so oft wie nötig ausführen, um die genaue Kombination der Funktionen zu erreichen, die Sie mit der Rolle verknüpfen möchten.

Was Sie benötigen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Über diese Aufgabe

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

  Ein Befehlsverzeichnis (`volume`, Zum Beispiel) ist eine Gruppe verwandter Befehle und Unterverzeichnisse. Sofern nicht wie in diesem Verfahren beschrieben, gewährt oder verweigert das Zulassen des Zugriffs auf ein Befehlsverzeichnis jedem Befehl im Verzeichnis und seinen Unterverzeichnissen den Zugriff.

- Bestimmter Befehlszugriff oder Unterverzeichnis-Zugriff überschreibt den Zugriff auf das übergeordnete Verzeichnis.

  Wenn eine Rolle mit einem Befehlsverzeichnis definiert ist und dann erneut mit einer anderen Zugriffsebene für einen bestimmten Befehl oder ein Unterverzeichnis des übergeordneten Verzeichnisses definiert wird, überschreibt die Zugriffsebene, die für den Befehl oder das Unterverzeichnis festgelegt ist, die des übergeordneten Verzeichnisses.

> ⓘ Einem SVM-Administrator kann keine Rolle zugewiesen werden, die einem Befehl oder Befehlsverzeichnis Zugriff gibt, das nur dem zur Verfügung steht `admin` Cluster-Administrator – zum Beispiel der `security` Befehlsverzeichnis.

Schritt

1. Definieren einer benutzerdefinierten Rolle:

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

   Eine vollständige Befehlssyntax finden Sie im "Arbeitsblatt".

   Die folgenden Befehle erteilen das `vol_role` Rollen vollständigen Zugriff auf die Befehle im `volume` Befehlsverzeichnis und schreibgeschützter Zugriff 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 erteilen das `SVM_storage` Rolle nur-Lese-Zugriff auf die Befehle in der `storage` Befehlsverzeichnis, kein Zugriff auf die Befehle im `storage encryption` Unterverzeichnis und vollständigen Zugriff auf das `storage aggregate plex offline` Nicht-intrinsischer 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
```

Vordefinierte Rollen für Cluster-Administratoren

Die vordefinierten Rollen für Cluster-Administratoren sollten die meisten Ihrer Anforderungen erfüllen. Sie können bei Bedarf benutzerdefinierte Rollen erstellen. Standardmäßig wird einem Cluster-Administrator das vordefinierte zugewiesen `admin` Rolle:

In der folgenden Tabelle werden die vordefinierten Rollen für Cluster-Administratoren aufgeführt:

Diese Rolle…	Verfügt über diese Zugriffsebene…	Zu den folgenden Befehlen oder Befehlsverzeichnissen
Admin	Alle	Alle Befehlsverzeichnisse (`DEFAULT`)
Admin-no-fsa (ab ONTAP 9.12.1 verfügbar)	Lese-/Schreibzugriff	• Alle Befehlsverzeichnisse (`DEFAULT`) • `security login rest-role` • `security login role`

Schreibgeschützt	• `security login rest-role create` • `security login rest-role delete` • `security login rest-role modify` • `security login rest-role show` • `security login role create` • `security login role create` • `security login role delete` • `security login role modify` • `security login role show` • `volume activity-tracking` • `volume analytics`	Keine
`volume file show-disk-usage`	AutoSupport	Alle
• `set` • `system node autosupport`	Keine	Alle anderen Befehlsverzeichnisse (`DEFAULT`)
Backup	Alle	`vserver services ndmp`
readonly	`volume`	Keine
Alle anderen Befehlsverzeichnisse (`DEFAULT`)	readonly	Alle

• `security login password` Nur zur Verwaltung des eigenen Benutzerkontos mit lokalem Passwort und Schlüsselinformationen • `set`	Keine	`security`
readonly	Alle anderen Befehlsverzeichnisse (`DEFAULT`)	Keine

Der `autosupport` Rolle ist dem vordefinierten zugewiesen `autosupport` Konto, das von AutoSupport OnDemand verwendet wird. ONTAP verhindert, dass Sie den ändern oder löschen können `autosupport` Konto. ONTAP verhindert darüber hinaus, dass Sie das zuweisen `autosupport` Rolle für andere Benutzerkonten.

Vordefinierte Rollen für SVM-Administratoren

Die vordefinierten Rollen für SVM-Administratoren sollten die meisten Ihrer Anforderungen erfüllen. Sie können bei Bedarf benutzerdefinierte Rollen erstellen. Standardmäßig wird einem SVM-Administrator das vordefinierte zugewiesen `vsadmin` Rolle:

In der folgenden Tabelle sind die vordefinierten Rollen für SVM-Administratoren aufgeführt:

Rollenname	Sorgen
Vsadmin	• Verwaltung des eigenen Benutzerkontos mit lokalem Passwort und Schlüsselinformationen • Verwalten von Volumes, außer Verschieben von Volumes • Verwalten von Quotas, qtrees, Snapshot Kopien und Dateien • Verwalten von LUNs • Durchführung von SnapLock-Vorgängen mit Ausnahme von privilegierten Löschen • Konfiguration der Protokolle NFS, SMB, iSCSI und FC Einschließlich FCoE • Dienste konfigurieren: DNS, LDAP und NIS • Überwachen von Jobs • Monitoring von Netzwerkverbindungen und Netzwerkschnittstelle • Monitoring des Systemzustands der SVM

Vsadmin-Volume	• Verwaltung des eigenen Benutzerkontos mit lokalem Passwort und Schlüsselinformationen • Managen von Volumes, einschließlich Volume-Verschiebungen • Verwalten von Quotas, qtrees, Snapshot Kopien und Dateien • Verwalten von LUNs • Konfiguration von Protokollen NFS, SMB, iSCSI und FC, einschließlich FCoE • Dienste konfigurieren: DNS, LDAP und NIS • Monitoring der Netzwerkschnittstelle • Monitoring des Systemzustands der SVM
Vsadmin-Protokoll	• Verwaltung des eigenen Benutzerkontos mit lokalem Passwort und Schlüsselinformationen • Konfiguration von Protokollen NFS, SMB, iSCSI und FC, einschließlich FCoE • Dienste konfigurieren: DNS, LDAP und NIS • Verwalten von LUNs • Monitoring der Netzwerkschnittstelle • Monitoring des Systemzustands der SVM
Vsadmin-Backup	• Verwaltung des eigenen Benutzerkontos mit lokalem Passwort und Schlüsselinformationen • Verwalten des NDMP-Betriebs • Erstellung eines wiederhergestellten Lese-/Schreibvorgangs eines Volumes • Verwalten von SnapMirror Beziehungen und Snapshot Kopien • Anzeigen von Volumes und Netzwerkinformationen

Vsadmin-snaplock	• Verwaltung des eigenen Benutzerkontos mit lokalem Passwort und Schlüsselinformationen • Verwalten von Volumes, außer Verschieben von Volumes • Verwalten von Quotas, qtrees, Snapshot Kopien und Dateien • Durchführung von SnapLock-Vorgängen einschließlich privilegierter Löschung • Konfiguration von Protokollen: NFS und SMB • Dienste konfigurieren: DNS, LDAP und NIS • Überwachen von Jobs • Monitoring von Netzwerkverbindungen und Netzwerkschnittstelle
Vsadmin-Readonly	• Verwaltung des eigenen Benutzerkontos mit lokalem Passwort und Schlüsselinformationen • Monitoring des Systemzustands der SVM • Monitoring der Netzwerkschnittstelle • Anzeigen von Volumes und LUNs • Anzeigen von Services und Protokollen