アクセス制御ロールを管理します
ONTAP 9

NetApp
April 24, 2024

目次

アクセス制御ロールを管理します

アクセス制御ロールの概要

管理者がアクセスできるコマンドは、管理者に割り当てられたロールで決まります。ロールは管理者のアカウントを作成するときに割り当てます。必要に応じて、別のロールを割り当てたりカスタムロールを定義したりできます。

管理者に割り当てられているロールを変更します

を使用できます `security login modify` コマンドを使用して、クラスタ管理者アカウントまたはSVM管理者アカウントのロールを変更します。事前定義またはカスタムのロールを割り当てることができます。

作業を開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

ステップ

1. クラスタ管理者または SVM 管理者のロールを変更します。

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

   コマンド構文全体については、を参照してください "ワークシート"。

   "ログインアカウントを作成または変更する"

   次のコマンドは、ADクラスタ管理者アカウントのロールを変更します `DOMAIN1\guest1` に移動します `readonly` ロール。

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

   次のコマンドは、ADグループアカウントのSVM管理者アカウントのロールを変更します `DOMAIN1\adgroup` カスタムに `vol_role` ロール。

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

カスタムロールを定義する

を使用できます `security login role create` カスタムロールを定義するコマン

ド。このコマンドを必要な回数だけ実行して、ロールに関連付ける機能の正確な組み合わせを実現できます。

このタスクについて

- 事前定義かカスタムかにかかわらず、ロールは ONTAP コマンドまたはコマンドディレクトリへのアクセスを許可または拒否します。

  コマンドディレクトリ (`volume`など）は、関連するコマンドとコマンドサブディレクトリのグループです。この手順で説明されている場合を除き、コマンドディレクトリへのアクセスを許可または拒否すると、ディレクトリとそのサブディレクトリに含まれる各コマンドへのアクセスが許可または拒否されます。

- 特定のコマンドまたはサブディレクトリへのアクセスは、親ディレクトリへのアクセスよりも優先されます。

  あるロールにコマンドディレクトリを定義し、そのあとに親ディレクトリの特定のコマンドまたはサブディレクトリに対して異なるアクセスレベルを定義した場合、そのコマンドまたはサブディレクトリに指定したアクセスレベルが親のアクセスレベルよりも優先されます。

> でのみ使用可能なコマンドやコマンドディレクトリへのアクセスを許可するロールをSVM管理者に割り当てることはできません `admin` クラスタ管理者（例：） `security` コマンドディレクトリ。

作業を開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

ステップ

1. カスタムロールを定義します。

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

   コマンド構文全体については、を参照してください "ワークシート"。

   次のコマンドは、を許可します `vol_role` ロールに内のコマンドへのフルアクセス権が付与されます `volume` コマンドディレクトリ、および内のコマンドへの読み取り専用アクセス `volume snapshot` サブディレクトリ。

   ```
   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
   ```

   次のコマンドは、を許可します `SVM_storage` ロール内のコマンドへの読み取り専用アクセス `storage` コマンドディレクトリ。内のコマンドにはアクセスできません `storage encryption` サブディレクトリにアクセスし、へのフルアクセスを許可します `storage aggregate plex offline` 非組み込みコマンド。

```
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
```

クラスタ管理者の事前定義されたロール

ほとんどの場合、クラスタ管理者用に事前定義されたロールで十分です。必要に応じて、カスタムロールを作成することができます。デフォルトでは、クラスタ管理者には事前定義されたが割り当てられます `admin` ロール。

次の表に、クラスタ管理者用の事前定義されたロールを示します。

ロール	アクセスレベル	コマンドまたはコマンドディレクトリに移動します
管理	すべて	すべてのコマンドディレクトリ（`DEFAULT`）
Admin-no-FSA（ONTAP 9.12.1以降で利用可能）	読み取り / 書き込み	• すべてのコマンドディレクトリ（`DEFAULT`） • `security login rest-role` • `security login role`

読み取り専用です	• 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	なし
volume file show-disk-usage	AutoSupport	すべて
• set • system node autosupport	なし	その他すべてのコマンドディレクトリ (DEFAULT)
バックアップ	すべて	vserver services ndmp
• 読み取り専用	volume	なし
その他すべてのコマンドディレクトリ (DEFAULT)	• 読み取り専用	すべて
• security login password 自身のユーザアカウントのローカルパスワードとキー情報のみを管理する場合 • set	なし	security

• 読み取り専用	その他すべてのコマンドディレクトリ (DEFAULT)	なし

。 autosupport ロールは事前定義されたに割り当てられます autosupport AutoSupport OnDemandで使用されるアカウント。ONTAP では、を変更または削除することはできません autosupport アカウント：また、ONTAP ではを割り当てることもできません autosupport 他のユーザアカウントへのロール。

SVM 管理者の事前定義されたロール

SVM 管理者用に、ほとんどのニーズに合わせて事前定義されたロールが用意されています。必要に応じて、カスタムロールを作成することができます。デフォルトでは、SVM 管理者には事前定義されたが割り当てられます vsadmin ロール。

次の表に、 SVM 管理者用の事前定義されたロールを示します。

ロール名	機能
vsadmin	• 自身のユーザアカウントのローカルパスワードとキー情報を管理します • ボリューム移動を除くボリュームの管理 • クォータ、 qtree 、 Snapshot コピー、およびファイルの管理 • LUN の管理 • privileged delete を除く SnapLock 処理の実行 • プロトコルの設定：NFS、SMB、iSCSI、FC 、FCoE、 NVMe/FCとNVMe/TCP • サービスの設定： DNS 、 LDAP 、 NIS • ジョブの監視 • ネットワーク接続およびネットワークインターフェイスの監視 • SVM の健常性を監視

vsadmin-volume	• 自身のユーザアカウントのローカルパスワードとキー情報を管理します • ボリュームの移動を含む、ボリュームの管理 • クォータ、 qtree 、 Snapshot コピー、およびファイルの管理 • LUN の管理 • プロトコルの設定：NFS、SMB、iSCSI、FC 、FCoE、 NVMe/FCとNVMe/TCP • サービスの設定： DNS 、 LDAP 、 NIS • ネットワークインターフェイスの監視 • SVM の健常性を監視
vsadmin-protocol のいずれかです	• 自身のユーザアカウントのローカルパスワードとキー情報を管理します • プロトコルの設定：NFS、SMB、iSCSI、FC 、FCoE、 NVMe/FCとNVMe/TCP • サービスの設定： DNS 、 LDAP 、 NIS • LUN の管理 • ネットワークインターフェイスの監視 • SVM の健常性を監視
vsadmin-backup のストレージシステムで	• 自身のユーザアカウントのローカルパスワードとキー情報を管理します • NDMP 処理の管理 • リストアしたボリュームを読み取り / 書き込み可能にします • SnapMirror 関係と Snapshot コピーの管理 • ボリュームとネットワーク情報の表示

vsadmin-snaplock	• 自身のユーザアカウントのローカルパスワードとキー情報を管理します • ボリューム移動を除くボリュームの管理 • クォータ、 qtree 、 Snapshot コピー、およびファイルの管理 • privileged delete などの SnapLock 処理の実行 • プロトコルの設定：NFSとSMB • サービスの設定： DNS 、 LDAP 、 NIS • ジョブの監視 • ネットワーク接続およびネットワークインターフェイスの監視
vsadmin-readonly （読み取り専用	• 自身のユーザアカウントのローカルパスワードとキー情報を管理します • SVM の健常性を監視 • ネットワークインターフェイスの監視 • ボリュームと LUN を表示します • サービスとプロトコルの表示

管理者アクセスの制御

管理者に割り当てるロールによって、 System Manager で実行できる機能が決まります。クラスタ管理者と Storage VM 管理者の事前定義されたロールは System Manager から提供されます。 ロールは、管理者のアカウントを作成するときに割り当てるか、後で別のロールを割り当てることができます。

アカウントアクセスを有効にした方法によっては、次のいずれかを実行する必要があります。

- ローカルアカウントに公開鍵を関連付けます。
- CA 署名済みサーバデジタル証明書をインストールする。
- AD 、 LDAP 、または NIS アクセスを設定

これらのタスクは、アカウントアクセスを有効にする前後どちらでも実行できます。

管理者にロールを割り当てます

次のように、管理者にロールを割り当てます。

手順

1. [* Cluster]>[Settings]（設定）*を選択します。
2. 選択するオプション → をクリックします。

3. 選択するオプション + Add [* ユーザー *] の下。
4. ユーザー名を指定し、 * 役割 * のドロップダウンメニューで役割を選択します。
5. ユーザのログイン方法およびパスワードを指定します。

管理者のロールを変更する

管理者のロールを次のように変更します。

手順

1. [**Cluster] > [Settings**] の順にクリックします。
2. ロールを変更するユーザの名前を選択し、をクリックします ⋮ ユーザ名の横に表示されます。
3. [編集（ Edit ）] をクリックします。
4. [*Role] のドロップダウンメニューで、ロールを選択します。