アクセス制御ロールを管理します。
ONTAP 9

NetApp
December 20, 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管理の概要

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たロールを変更する

コマンドを使用すると、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できます `security login modify`。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。

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の作成または変更"

   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事前定義された `readonly`ロールに変更し `DOMAIN1\guest1`ます。

   ```
   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内のSVM管理者アカウントのロールをカスタムロールに `vol_role`変更します `DOMAIN1\adgroup`。

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

カスタムロールの定義

カスタムロールを定義するには、コマンドを使用し `security login role create`ます。こ

のコマンドは、必要な回数だけ実行して、ロールに関連付ける機能を正確に組み合わせることができます。

タスクの内容

- ONTAPコマンドまたはコマンドディレクトリへのアクセスは、ロール（事前定義またはカスタム）によって許可または拒否されます。

  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、ディレクトリおよびそのサブディレクトリ内の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。

  コマンドディレクトリを使用してロールを定義したあとに、特定のコマンドまたは親ディレクトリのサブディレクトリに対して別のアクセスレベルで再度定義した場合、コマンドまたはサブディレクトリに指定されたアクセスレベルは親のアクセスレベルよりも優先されます。

> クラスタ管理者のみが使用できるコマンドやコマンドディレクトリ（コマンドディレクトリなど） `security`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`

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、ロールに対し、コマンドディレクトリ内のコマンドへのフルアクセス `volume`と、サブディレクトリ内のコマンドへの読み取り専用アクセスを `volume snapshot`許可し `vol_role`ます。

   ```
   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、ロールに対し、コマンドディレクトリ内のコマンドへの読み取り専用アクセス `storage`、サブディレクトリ内のコマンドへのアクセスなし、 `storage encryption`および非組み込みコマンドへのフルアクセスを `storage aggregate plex offline`許可し `SVM_storage`ます。

```
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ロールが割り当てられ `admin`ます。

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
管理者	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以降で使用可能）	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 自分のユーザアカウントのローカルパスワードとキーの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)	SnapLock
すべて	• set • volume create • volume modify • volume move • volume show	なし
• volume move governor • volume move recommend	なし	その他すべてのコマンドディレクトリ(DEFAULT)
なし	なし	すべてのコマンドディレクトリ(DEFAULT)

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

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できます。デフォルトでは、SVM管理者には事前定義されたロールが割り当てられ`vsadmin`ます。

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、ローカル パスワード、キー情報の管理 • ボリュームの管理（ボリュームの移動を除く） • クォータ、qtree、Snapshotコピー、およびファイルの管理 • LUNの管理 • SnapLock処理の実行（privileged deleteを除く） • 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 • ネットワーク接続とネットワーク インターフェイスの監視 • SVMの健全性の監視
vsadmin-volume	• 自身のユーザ アカウント、ローカル パスワード、キー情報の管理 • ボリュームの管理（ボリュームの移動を含む） • 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の健全性の監視
vsadmin-protocol	• 自身のユーザ アカウント、ローカル パスワード、キー情報の管理 • 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 • LUNの管理 • ネットワークインターフェイスの監視 • SVMの健全性の監視

vsadmin-backup	• 自身のユーザ アカウント、ローカル パスワード、キー情報の管理 • NDMP処理の管理 • リストアしたボリュームの読み取り/書き込み許可 • 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、ローカル パスワード、キー情報の管理 • ボリュームの管理（ボリュームの移動を除く） • クォータ、qtree、Snapshotコピー、およびファイルの管理 • SnapLock処理の実行（privileged deleteを含む） • 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 • ネットワーク接続とネットワーク インターフェイスの監視
vsadmin -読み取り専用	• 自身のユーザ アカウント、ローカル パスワード、キー情報の管理 • SVMの健全性の監視 • ネットワークインターフェイスの監視 • ボリュームとLUNの表示 • サービスとプロトコルの表示

管理者アクセスの制御

管理者がSystem Managerで実行できる機能は、管理者に割り当てられたロールによって決まります。System Managerには、クラスタ管理者とStorage VM管理者用の事前定義されたロールが用意されています。ロールは管理者アカウントの作成時に割り当てるか、あと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、次のいずれかの操作が必要になる場合があります。

- 公開鍵をローカルアカウントに関連付けます。
- 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。

管理者へのロールの割り当て

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. [Users and Roles]*の横にあるを選択します → 。
3. [ユーザ]*でを選択します + Add 。
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とパスワードを指定します。

管理者のロールの変更

管理者のロールを次のように変更します。

手順

1. [クラスタ]>[設定]*をクリックします。
2. ロールを変更するユーザの名前を選択し、ユーザ名の横に表示されるをクリックします ⋮ 。
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。

著作権に関する情報

商標に関する情報