



# 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 .....	1
アクセス制御ロールの概要 .....	1
管理者に割り当てられているロールを変更します .....	1
カスタムロールを定義する .....	1
クラスタ管理者の事前定義されたロール .....	3
SVM 管理者の事前定義されたロール .....	5
管理者アクセスの制御 .....	7

# 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

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

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	<ul style="list-style-type: none"> <li>すべてのコマンドディレクトリ (DEFAULT)</li> <li><code>security login rest-role</code></li> <li><code>security login role</code></li> </ul>

読み取り専用です	<ul style="list-style-type: none"> <li>• security login rest-role create</li> <li>• security login rest-role delete</li> <li>• security login rest-role modify</li> <li>• security login rest-role show</li> <li>• security login role create</li> <li>• security login role create</li> <li>• security login role delete</li> <li>• security login role modify</li> <li>• security login role show</li> <li>• volume activity-tracking</li> <li>• volume analytics</li> </ul>	なし
volume file show-disk-usage	AutoSupport	すべて
<ul style="list-style-type: none"> <li>• set</li> <li>• system node autosupport</li> </ul>	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
<ul style="list-style-type: none"> <li>• 読み取り専用</li> </ul>	volume	なし
その他すべてのコマンドディレクトリ (DEFAULT)	<ul style="list-style-type: none"> <li>• 読み取り専用</li> </ul>	すべて
<ul style="list-style-type: none"> <li>• security login password</li> </ul> <p>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</p> <ul style="list-style-type: none"> <li>• set</li> </ul>	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	<ul style="list-style-type: none"> <li>• 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</li> <li>• ボリューム移動を除くボリュームの管理</li> <li>• クォータ、qtree、Snapshot コピー、およびファイルの管理</li> <li>• LUN の管理</li> <li>• privileged delete を除く SnapLock 処理の実行</li> <li>• プロトコルの設定：NFS、SMB、iSCSI、FC、FCoE、NVMe/FCとNVMe/TCP</li> <li>• サービスの設定：DNS、LDAP、NIS</li> <li>• ジョブの監視</li> <li>• 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</li> <li>• SVM の健全性を監視</li> </ul>

vsadmin-volume	<ul style="list-style-type: none"> <li>• 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</li> <li>• ボリュームの移動を含む、ボリュームの管理</li> <li>• クォータ、qtree、Snapshot コピー、およびファイルの管理</li> <li>• LUN の管理</li> <li>• プロトコルの設定：NFS、SMB、iSCSI、FC、FCoE、NVMe/FCとNVMe/TCP</li> <li>• サービスの設定：DNS、LDAP、NIS</li> <li>• ネットワークインターフェースの監視</li> <li>• SVM の健全性を監視</li> </ul>
vsadmin-protocol のいずれかです	<ul style="list-style-type: none"> <li>• 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</li> <li>• プロトコルの設定：NFS、SMB、iSCSI、FC、FCoE、NVMe/FCとNVMe/TCP</li> <li>• サービスの設定：DNS、LDAP、NIS</li> <li>• LUN の管理</li> <li>• ネットワークインターフェースの監視</li> <li>• SVM の健全性を監視</li> </ul>
vsadmin-backup のストレージシステムで	<ul style="list-style-type: none"> <li>• 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</li> <li>• NDMP 処理の管理</li> <li>• 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</li> <li>• SnapMirror 関係と Snapshot コピーの管理</li> <li>• ボリュームとネットワーク情報の表示</li> </ul>



vsadmin-snaplock	<ul style="list-style-type: none"> <li>• 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</li> <li>• ボリューム移動を除くボリュームの管理</li> <li>• クォータ、qtree、Snapshot コピー、およびファイルの管理</li> <li>• privileged delete などの SnapLock 処理の実行</li> <li>• プロトコルの設定：NFSとSMB</li> <li>• サービスの設定：DNS、LDAP、NIS</li> <li>• ジョブの監視</li> <li>• 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</li> </ul>
vsadmin-readonly（読み取り専用）	<ul style="list-style-type: none"> <li>• 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</li> <li>• SVM の健全性を監視</li> <li>• ネットワークインターフェイスの監視</li> <li>• ボリュームと LUN を表示します</li> <li>• サービスとプロトコルの表示</li> </ul>

## 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。

## 著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

## 商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。