



ロールベースアクセス制御（**RBAC**）の設定

SnapCenter Software 4.8

NetApp
January 18, 2024

目次

ロールベースアクセス制御（RBAC）の設定	1
ユーザまたはグループを追加し、ロールとアセットを割り当てます	1
ロールを作成します	4
security login コマンドを使用して、ONTAP RBAC ロールを追加します	5
最小権限を持つ SVM ロールを作成します	7
最小限の権限で ONTAP クラスタロールを作成します	11
Active Directory の読み取り権限を有効にするように IIS アプリケーションプールを設定します	17

ロールベースアクセス制御（RBAC）の設定

ユーザまたはグループを追加し、ロールとアセットを割り当てます

SnapCenter ユーザのロールベースアクセス制御を設定するには、ユーザまたはグループを追加してロールを割り当てます。ロールに基づいて、SnapCenter ユーザがアクセスできるオプションが決まります。

- 必要なもの *
- 「SnapCenterAdmin」ロールでログインする必要があります。
- ユーザまたはグループのアカウントを、オペレーティングシステムまたはデータベースの Active Directory に作成しておく必要があります。SnapCenter を使用してこれらのアカウントを作成することはできません。



SnapCenter 4.5 では、ユーザ名とグループ名に次の特殊文字のみを使用できます。スペース ()、ハイフン (-)、アンダースコア (_)、コロン (:)。これらの特殊文字を使用して以前のリリースの SnapCenter で作成したロールを使用する場合は、SnapCenter WebApp がインストールされている web.config ファイルで「isableSQLInjionValidation」パラメータの値を true に変更することで、ロール名の検証を無効にできます。値を変更した場合、サービスを再起動する必要はありません。

- SnapCenter には、事前定義されたロールが複数あり

これらのロールをユーザに割り当てるか、新しいロールを作成できます。

- SnapCenter RBAC に追加される AD ユーザと AD グループには、Active Directory 内の Users コンテナと Computers コンテナに対する読み取り権限が必要です。
- 適切な権限が割り当てられたユーザまたはグループにロールを割り当てたら、ホストやストレージ接続などの SnapCenter アセットへのユーザアクセスを割り当てる必要があります。

これにより、ユーザは、自身に割り当てられたアセットに対して権限のある処理を実行できます。

- RBAC の権限と効率性を利用するには、いずれかの時点でロールをユーザまたはグループに割り当てる必要があります。
- ホスト、リソースグループ、ポリシー、ストレージ接続、プラグインなどのアセットを割り当てることができます。ユーザまたはグループの作成時にユーザにクレデンシャルを付与する必要があります。
- 特定の処理を実行するためにユーザに割り当てる必要がある最小アセットは次のとおりです。

操作	資産の割り当て
リソースを保護	ホスト、ポリシー
バックアップ	ホスト、リソースグループ、ポリシー

操作	資産の割り当て
リストア	ホスト、リソースグループ
クローン	ホスト、リソースグループ、ポリシー
クローンのライフサイクル	ホスト
リソースグループを作成します	ホスト

- Windows クラスタまたは DAG（Exchange Server データベース可用性グループ）のアセットに新しいノードを追加したときに、その新しいノードをユーザに割り当てた場合は、新しいノードを追加するアセットをユーザまたはグループに再割り当てする必要があります。


RBAC ユーザまたはグループをクラスタまたは DAG に再割り当てして、新しいノードを RBAC ユーザまたはグループに追加する必要があります。たとえば、2 ノードクラスタで RBAC ユーザまたはグループをクラスタに割り当てているとします。クラスタに別のノードを追加した場合は、RBAC のユーザまたはグループをクラスタに再割り当てして、RBAC ユーザまたはグループの新しいノードを追加します。

- Snapshot コピーをレプリケートする場合は、処理を実行するユーザにソースボリュームとデスティネーションボリュームの両方のストレージ接続を割り当てる必要があります。

ユーザにアクセスを割り当てる前にアセットを追加しておく必要があります。



SnapCenter Plug-in for VMware vSphere の機能を使用して VM、VMDK、またはデータストアを保護している場合は、VMware vSphere GUI を使用して、SnapCenter Plug-in for VMware vSphere ロールに vCenter ユーザを追加する必要があります。VMware vSphere のロールについては、を参照してください "[SnapCenter Plug-in for VMware vSphere に組み込みの事前定義のロール](#)"。

- 手順 *
 1. 左側のナビゲーションペインで、* 設定 * をクリックします。
 2. [設定] ページで、[* ユーザーとアクセス >] をクリックします  *
 3. [Add Users/Groups from Active Directory or Workgroup] ページで、次の手順を実行します。

フィールド	手順
アクセスタイプ	<p>ドメインまたはワークグループのいずれかを選択します</p> <p>ドメイン認証タイプには、ロールにユーザを追加するユーザまたはグループのドメイン名を指定する必要があります。</p> <p>デフォルトでは、ログインしているドメイン名があらかじめ入力されています。</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  信頼されていないドメインは、[* 設定 * > * グローバル設定 * > * ドメイン設定 * (* Settings * > * Global Settings *)] ページで登録する必要があります。 </div>
を入力します	<p>[ユーザー] または [グループ] を選択します</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  SnapCenter でサポートされるのはセキュリティグループのみで、配信グループはサポートされません。 </div>
ユーザ名	<p>a. 部分的なユーザ名を入力し、 * 追加 * をクリックします。</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  ユーザ名では大文字と小文字が区別されます。 </div> <p>b. 検索リストからユーザ名を選択します。</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  別のドメインまたは信頼されていないドメインのユーザを追加する場合は、ユーザ名を完全に入力する必要があります。これは、クロスドメインユーザの検索リストがないためです。 </div> <p>この手順を繰り返して、選択したロールにユーザまたはグループを追加します。</p>
ロール	ユーザを追加するロールを選択します。

4. [Assign] をクリックし、[Assign Assets] ページで次の手順を実行します。

- a. [* アセット *] ドロップダウン・リストからアセットのタイプを選択します。
- b. [アセット] リストで、アセットを選択します。

アセットは、ユーザが SnapCenter にアセットを追加した場合にのみ表示されます。

- c. 必要なすべてのアセットについて、この手順を繰り返します。
 - d. [保存 (Save)] をクリックします。
5. [Submit (送信)] をクリックします。


ユーザまたはグループを追加してロールを割り当てたら、リソースのリストを更新します。

ロールを作成します

既存の SnapCenter ロールに加えて、独自のロールを作成して権限をカスタマイズできます。

「SnapCenterAdmin」ロールでログインする必要があります。

• 手順 *

1. 左側のナビゲーションペインで、* 設定 * をクリックします。
2. 設定ページで、* 役割 * をクリックします。
3. をクリックします .
4. [Add Role] ページで、新しいロールの名前と概要を指定します。



SnapCenter 4.5 では、ユーザ名とグループ名に次の特殊文字のみを使用できます。スペース ()、ハイフン (-)、アンダースコア (_)、コロン (:)。これらの特殊文字を使用して以前のリリースの SnapCenter で作成したロールを使用する場合は、SnapCenter WebApp がインストールされている web.config ファイルで「isableSQLInjionValidation」パラメータの値を true に変更することで、ロール名の検証を無効にできます。値を変更した場合、サービスを再起動する必要はありません。

5. このロールのすべてのメンバーは、他のメンバーのオブジェクトを表示できます * を選択すると、そのロールの他のメンバーは、リソースリストの更新後にボリュームやホストなどのリソースを参照できます。

他のメンバーが割り当てられているオブジェクトをこのロールのメンバーに表示しないようにするには、このオプションを選択解除する必要があります。



このオプションを有効にすると、オブジェクトまたはリソースを作成したユーザと同じロールにユーザが属している場合に、オブジェクトまたはリソースへのアクセスをユーザに割り当てる必要がなくなります。

1. [アクセス許可] ページで、そのロールに割り当てるアクセス許可を選択するか、[すべて選択] をクリックしてそのロールにすべてのアクセス許可を付与します。
2. [Submit (送信)] をクリックします。

security login コマンドを使用して、ONTAP RBAC ロールを追加します

ストレージシステムで clustered ONTAP を実行している場合、security login コマンドを使用して ONTAP RBAC ロールを追加できます。

- 必要なもの *
- clustered ONTAP を実行しているストレージシステム用に ONTAP RBAC ロールを作成する前に、次の項目について確認しておく必要があります。
 - 実行するタスク
 - これらのタスクを実行するために必要な権限
- RBAC ロールを設定するには、次の操作を実行する必要があります。

- コマンドおよびコマンドディレクトリ、またはその両方に権限を付与します。

コマンドおよびコマンドディレクトリのアクセスには、フルアクセスと読み取り専用の 2 つのレベルがあります。

フルアクセス権限は、常に最初に割り当てる必要があります。

- ユーザにロールを割り当てます。
 - SnapCenter プラグインがクラスタ全体のクラスタ管理者 IP に接続されているか、またはクラスタ内の SVM に直接接続されているかに応じて、設定は異なります。
- このタスクについて *

RBAC User Creator for Data ONTAP ツールを使用して、これらのロールのストレージシステムへの設定を簡素化することができます。このツールは、ネットアップコミュニティフォーラムに掲載されています。

このツールは、ONTAP 権限の適切な設定を自動的に処理します。たとえば、Data ONTAP フルアクセス権限が最初に表示されるように、権限が自動的に正しい順序で追加されます。読み取り専用権限を最初に追加し、次にフルアクセス権限を追加すると、ONTAP はフルアクセス権限を重複するものとしてマーキングし、無視します。



SnapCenter または ONTAP をあとからアップグレードする場合は、RBAC User Creator for Data ONTAP ツールを再度実行して、以前に作成したユーザロールを更新する必要があります。以前のバージョンの SnapCenter または ONTAP 用に作成したユーザロールは、アップグレード後のバージョンでは正常に機能しません。ツールを再実行すると、アップグレードが自動的に処理されます。ロールを再作成する必要はありません。

ONTAP RBAC ロールの設定の詳細については、を参照してください ["ONTAP 9 管理者認証と RBAC パワーガイド"](#)。



SnapCenter のドキュメントではロールに割り当てる要素を「権限」と呼びますが、OnCommand システムマネージャ GUI では、_privilege ではなく、TERM_attribute__ が使用されます。ONTAP RBAC ロールを設定する場合は、この 2 つの用語は同じ意味です。

- 手順 *

1. ストレージシステムで次のコマンドを入力して、新しいロールを作成します。

```
security login role create <role_name\> -cmddirname "command" -access all  
-vserver <svm_name\>
```

- `svm_name` は、SVM ユーザの名前です。空白のままにすると、デフォルトでクラスタ管理者が指定されます。
- `role_name` は、ロールに指定する名前です。
- `command` は、ONTAP の機能です。



このコマンドは権限ごとに実行する必要があります。フルアクセスコマンドは、読み取り専用コマンドの前にリストする必要があります。

権限のリストについては、を参照してください "[ロールの作成および権限の割り当てに使用する ONTAP CLI コマンド](#)"。

2. 次のコマンドを入力して、ユーザ名を作成します。

```
security login create -username <user_name\> -application ontapi -authmethod  
<password\> -role <name_of_role_in_step_1\> -vserver <svm_name\> -comment  
"user_description"
```

- `user_name` は、作成するユーザの名前です。
- `<password>` は、パスワードです。パスワードを指定しないと、パスワードの入力を求めるプロンプトが表示されます。
- `svm_name` は、SVM ユーザの名前です。

3. 次のコマンドを入力して、ユーザにロールを割り当てます。

```
security login modify username <user_name\> -vserver <svm_name\> -role  
<role_name\> -application ontapi -application console -authmethod  
<password\>
```

- `<user_name>` は、手順 2 で作成したユーザの名前です。このコマンドでは、ロールに関連付けるユーザを変更できます。
- `<svm_name>` は SVM の名前です。
- `<role_name>` は、手順 1 で作成したロールの名前です。
- `<password>` は、パスワードです。パスワードを指定しないと、パスワードの入力を求めるプロンプトが表示されます。

4. 次のコマンドを入力して、ユーザが正しく作成されたことを確認します。

```
security login show -vserver <svm_name\> -user-or-group-name <user_name\>
```

`user_name` は、手順 3 で作成したユーザの名前です。

最小権限を持つ SVM ロールを作成します

ONTAP で新しい SVM ユーザのロールを作成する場合、実行する必要がある ONTAP CLI コマンドがいくつかあります。ONTAP 内の SVM を SnapCenter で使用するよう設定し、vsadmin ロールを使用したくない場合、このロールが必要です。

• 手順 *

1. ストレージシステムで、ロールを作成し、そのロールにすべての権限を割り当てます。

```
security login role create -vserver <svm_name\>- role <SVM_Role_Name\>  
-cmddirname <permission\>
```



このコマンドは権限ごとに実行する必要があります。

1. ユーザを作成し、そのユーザにロールを割り当てます。

```
security login create -user <user_name\> -vserver <svm_name\> -application  
ontapi -authmethod password -role <SVM_Role_Name\>
```

2. ユーザのロックを解除します。

```
security login unlock -user <user_name\> -vserver <svm_name\>
```

SVM ロールの作成および権限の割り当てに使用する ONTAP CLI コマンド

SVM ロールを作成して権限を割り当てるには、いくつかの ONTAP CLI コマンドを実行する必要があります。

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror list-destinations" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "event generate-autosupport-log" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job history show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job stop" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup add" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "network interface" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname

```

"snapmirror policy show" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"snapmirror restore" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"snapmirror show" -access all
• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
"snapmirror show-history" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"snapmirror update" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"snapmirror update-ls-set" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"version" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"volume clone create" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"volume clone show" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"volume clone split start" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"volume clone split stop" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"volume create" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"volume destroy" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"volume file clone create" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"volume file show-disk-usage" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"volume modify" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"volume offline" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"volume online" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"volume qtree create" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"volume qtree delete" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"volume qtree modify" -access all

```

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname

```
"vserver iscsi connection show" -access all
```

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver iscsi" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume clone split status" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume managed-feature" -access all

最小限の権限で **ONTAP** クラスタロールを作成します

最小限の権限で ONTAP クラスタロールを作成して、SnapCenter の admin ロールを使用して ONTAP で処理を実行する必要があるようにする必要があります。ONTAP のいくつかの CLI コマンドを実行して、ONTAP クラスタロールを作成し、最小限の権限を割り当てることができます。

• 手順 *

1. ストレージシステムで、ロールを作成し、そのロールにすべての権限を割り当てます。

```
security login role create -vserver <cluster_name>- role <role_name>  
-cmddirname <permission>
```



このコマンドは権限ごとに実行する必要があります。

1. ユーザを作成し、そのユーザにロールを割り当てます。

```
security login create -user <user_name> -vserver <cluster_name>  
-application ontapi -authmethod password -role <role_name>
```

2. ユーザのロックを解除します。

```
security login unlock -user <user_name> -vserver <cluster_name>
```

クラスタロールの作成および権限の割り当てに使用する **ONTAP CLI** コマンド

クラスタロールを作成して権限を割り当てるには、いくつかの ONTAP CLI コマンドを実行する必要があります。

- security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "metrocluster show" -access readonly
- security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "cluster identity modify" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster identity show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster peer show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "event generate-autosupport-log" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job history show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

```

"lun mapping show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun move-in-volume" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun offline" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun online" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun persistent-reservation clear" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun resize" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun serial" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "network interface create" -access readonly
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "network interface delete" -access readonly
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "network interface modify" -access readonly
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "network interface show" -access readonly
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "security login" -access readonly
• security login role create -role Role_Name -cmddirname "snapmirror create"
  -vserver Cluster_name -access all
• security login role create -role Role_Name -cmddirname "snapmirror list-
  destinations" -vserver Cluster_name -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "snapmirror policy add-rule" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "snapmirror policy create" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "snapmirror policy delete" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "snapmirror policy modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "snapmirror policy modify-rule" -access all

```

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license clean-up" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "version" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname


```

"volume create" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
"volume destroy" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
"volume file clone create" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
"volume file show-disk-usage" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
"volume modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
"volume offline" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
"volume online" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
"volume qtree create" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
"volume qtree delete" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
"volume qtree modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
"volume qtree show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
"volume restrict" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
"volume show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
"volume snapshot create" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
"volume snapshot delete" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
"volume snapshot modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
"volume snapshot promote" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
"volume snapshot rename" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
"volume snapshot restore" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
"volume snapshot restore-file" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
"volume snapshot show" -access all

```

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver iscsi connection show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

```
"vserver modify" -access all
```

- security login role create -vserver Cluster_name -role Role_Name -cmddirname
"vserver show" -access all

Active Directory の読み取り権限を有効にするように IIS アプリケーションプールを設定します

SnapCenter の Active Directory 読み取り権限を有効にする必要がある場合は、Windows Server でインターネットインフォメーションサービス (IIS) を構成して、カスタムのアプリケーションプールアカウントを作成できます。

• 手順 *

1. SnapCenter がインストールされている Windows サーバーで IIS マネージャーを開きます。
2. 左側のナビゲーションペインで、* アプリケーションプール * をクリックします。
3. [アプリケーションプール] リストで [SnapCenter] を選択し、[アクション] ペインで [* 詳細設定 *] をクリックします。
4. [ID] を選択し、[*...] をクリックして SnapCenter アプリケーションプール ID を編集します。
5. [カスタムアカウント] フィールドに、Active Directory の読み取り権限を持つドメインユーザーまたはドメイン管理者アカウント名を入力します。
6. [OK] をクリックします。

カスタムアカウントは、SnapCenter アプリケーションプールに組み込まれている ApplicationPoolIdentity アカウントに代わるものです。

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。