# SnapCenter の RBAC

SnapCenter Software 4.9

NetApp
March 20, 2024

# 目次

# SnapCenter の RBAC

## RBAC のタイプ

SnapCenter のロールベースアクセス制御（ RBAC ）と ONTAP 権限を使用して、SnapCenter 管理者は SnapCenter リソースの制御を別のユーザまたはユーザのグループに委譲できます。この方法でアクセスを一元管理することで、アプリケーション管理者は委譲された環境で安全に作業することができ

ロールの作成と変更、ユーザへのリソースアクセスの追加はいつでも実行できますが、 SnapCenter を初めて設定するときは、少なくとも Active Directory ユーザまたはグループをロールに追加してから、そのユーザまたはグループにリソースアクセスを追加する必要があります。

SnapCenter を使用してユーザアカウントまたはグループアカウントを作成することはできません。ユーザアカウントまたはグループアカウントは、オペレーティングシステムまたはデータベースの Active Directory に作成する必要があります。

SnapCenter では、次のタイプのロールベースアクセス制御を使用します。

- SnapCenter RBAC
- SnapCenter プラグインの RBAC （一部のプラグイン）
- アプリケーションレベルの RBAC
- ONTAP 権限

### SnapCenter RBAC

ロールと権限

SnapCenter には、権限がすでに割り当てられている事前定義されたロールが付属してこれらのロールにユーザまたはユーザのグループを割り当てることができます。また、新しいロールを作成して権限とユーザを管理することもできます。

- ユーザーまたはグループへのアクセス権の割り当て *

ユーザまたはグループに権限を割り当てて、ホスト、ストレージ接続、リソースグループなどの SnapCenter オブジェクトにアクセスすることができます。SnapCenterAdmin ロールの権限は変更できません。

RBAC の権限は、同じフォレスト内のユーザとグループ、および別のフォレストに属しているユーザに割り当てることができます。フォレストにまたがってネストされたグループに属するユーザには、 RBAC の権限を割り当てることはできません。

カスタムロールを作成する場合は、 SnapCenter Admin ロールのすべての権限を含める必要があります。「 Host add 」や「 Host remove 」など、一部の権限しかコピーしなかった場合、それらの処理を実行することはできません。

認証

ユーザは、グラフィカルユーザインターフェイス（ GUI ）または PowerShell コマンドレットを使用して、ログイン時に認証情報を指定する必要があります。ユーザが複数のロールに属している場合は、ログインクレデンシャルの入力後に、使用するロールを指定するように求められます。また、 API を実行する際にも認証が必要になります。

### アプリケーションレベルの RBAC

SnapCenter では、クレデンシャルを使用して、許可された SnapCenter ユーザにアプリケーションレベルの権限もあるかどうかが検証されます

たとえば、 SQL Server 環境で Snapshot コピーやデータ保護の処理を実行する場合は、 Windows または SQL の適切なクレデンシャルを設定する必要があります。SnapCenter サーバは、どちらの方法で設定されたクレデンシャルも認証します。ONTAP ストレージ上の Windows ファイルシステム環境で Snapshot コピーやデータ保護の処理を実行する場合は、 SnapCenter の admin ロールに Windows ホストに対する管理者権限が必要です。

同様に、 Oracle データベースに対してデータ保護処理を実行する場合、データベースホストでオペレーティングシステム（ OS ）認証が無効なときは、 Oracle データベースまたは Oracle ASM のクレデンシャルを使用してクレデンシャルを設定する必要があります。SnapCenter サーバは、処理に応じて、いずれかの方法で設定されたクレデンシャルを認証します。

### SnapCenter Plug-in for VMware vSphere の RBAC をサポートしています

VM と整合性のあるデータ保護に SnapCenter VMware プラグインを使用している場合、 vCenter Server によってさらに細かく RBAC を実装できます。SnapCenter VMware プラグインは、 vCenter Server RBAC と Data ONTAP RBAC の両方をサポートしています。

詳細については、を参照してください "SnapCenter Plug-in for VMware vSphere の RBAC をサポートしています"

### ONTAP 権限

ストレージシステムにアクセスするには、必要な権限を持つ vsadmin アカウントを作成する必要があります。

アカウントの作成と権限の割り当てについては、を参照してください "最小限の権限で ONTAP クラスタロールを作成します"

# RBAC の権限とロール

SnapCenter のロールベースアクセス制御（ RBAC ）では、ロールを作成して権限を割り当てることができ、そのロールにユーザやそのグループを割り当てることができます。これにより、 SnapCenter 管理者は環境を一元的に管理しながら、アプリケーション管理者はデータ保護ジョブを管理できます。SnapCenter には、事前定義されたロールと権限がいくつか付属してい

## SnapCenter ロール

SnapCenter には、次のロールがあらかじめ定義されています。これらのロールにユーザやグループを割り当てて使用できるほか、新しいロールを作成することもできます。

ロールをユーザに割り当てると、 SnapCenter Admin ロールを割り当てていない限り、そのユーザに関連するジョブだけが Jobs ページに表示されます。

- App Backup and Clone Admin の登録を確認します
- Backup and Clone Viewer に表示されます
- インフラ管理者
- SnapCenter Admin

## SnapCenter Plug-in for VMware vSphere のロール

VM 、 VMDK 、およびデータストアの VM 整合性のあるデータ保護を管理するために、 SnapCenter Plug-in for VMware vSphere によって vCenter で次のロールが作成されます。

- SCV 管理者
- SCV ビュー
- SCV バックアップ
- SCV Restore （ SCV リストア）
- SCV ゲストファイルのリストア

詳細については、を参照してください "SnapCenter Plug-in for VMware vSphere ユーザ用の RBAC のタイプ"

| * ベストプラクティス： * SnapCenter Plug-in for VMware vSphere の処理用に ONTAP ロールを 1 つ作成し、必要な権限をすべて割り当てることを推奨します。 |
|---|

## SnapCenter 権限

SnapCenter から提供される権限は次のとおりです。

- リソースグループ
- ポリシー
- バックアップ
- ホスト
- ストレージ接続
- クローン
- Provision （ Microsoft SQL データベースのみ）
- ダッシュボード
- レポート
- リストア

- Full Volume Restore （ Custom Plug-ins のみ）

- リソース

  管理者以外のユーザがリソース検出処理を実行する場合、管理者からプラグインの権限が求められます。

- プラグインのインストールまたはアンインストール

  Plug-in Installation 権限を有効にする場合は、 Host 権限も変更して読み取りと更新を有効にする必要があります。

- データ移行
- mount （ Oracle データベースのみ）
- Unmount （ Oracle データベースのみ）
- Job Monitor サービスの略

  ジョブ監視権限を使用すると、さまざまなロールのメンバーが、割り当てられているすべてのオブジェクトの処理を確認できます。

# 事前定義された SnapCenter ロールと権限

SnapCenter には、事前定義されたロールが用意されており、それぞれ一連の権限がすでに有効になっています。ロールベースアクセス制御（ RBAC ）をセットアップして管理するときは、これらの事前定義されたロールを使用するか、新しいロールを作成できます。

SnapCenter には、次の事前定義されたロールが含まれています。

- SnapCenter 管理者ロール
- App Backup and Clone Admin ロール
- Backup and Clone Viewer ロール
- Infrastructure Admin ロール

ロールにユーザを追加するときは、 Storage Connection 権限を割り当てて Storage Virtual Machine （ SVM ）の通信を有効にするか、 SVM をユーザに割り当ててその SVM を使用する権限を有効にする必要があります。Storage Connection 権限を割り当てられたユーザは SVM 接続を作成できます。

たとえば、 SnapCenter Admin ロールのユーザは、 SVM 接続を作成し、 App Backup and Clone Admin ロールのユーザに割り当てることができます。 App Backup and Clone Admin ロールには、デフォルトでは SVM 接続を作成または編集する権限は付与されていません。SVM 接続がないと、ユーザはバックアップ、クローニング、リストアの処理を実行できません。

## SnapCenter 管理者ロール

SnapCenter Admin ロールでは、すべての権限が有効になっています。このロールの権限は変更できません。ロールにユーザやグループを追加したり削除したりできます。

## App Backup and Clone Admin ロール

App Backup and Clone Admin ロールには、アプリケーションバックアップとクローン関連のタスクに対して管理操作を実行するために必要な権限が付与されています。このロールには、ホストの管理、プロビジョニング、ストレージ接続の管理、リモートインストールを行うための権限はありません。

| 権限 | 有効 | 作成 | 読み取り | 更新 | 削除 |
|---|---|---|---|---|---|
| リソースグループ | 該当なし | はい。 | はい。 | はい。 | はい。 |
| ポリシー | 該当なし | はい。 | はい。 | はい。 | はい。 |
| バックアップ | 該当なし | はい。 | はい。 | はい。 | はい。 |
| ホスト | 該当なし | はい。 | はい。 | はい。 | はい。 |
| ストレージ接続 | 該当なし | いいえ | はい。 | いいえ | いいえ |
| クローン | 該当なし | はい。 | はい。 | はい。 | はい。 |
| プロビジョニング | 該当なし | いいえ | はい。 | いいえ | いいえ |
| ダッシュボード | はい。 | 該当なし | 該当なし | 該当なし | 該当なし |
| レポート | はい。 | 該当なし | 該当なし | 該当なし | 該当なし |
| リストア | はい。 | 該当なし | 該当なし | 該当なし | 該当なし |
| リソース | はい。 | はい。 | はい。 | はい。 | はい。 |
| プラグインのインストールとアンインストール | いいえ | 該当なし | | 該当なし | 該当なし |
| データ移行 | いいえ | 該当なし | 該当なし | 該当なし | 該当なし |
| マウント | はい。 | はい。 | 該当なし | 該当なし | 該当なし |
| アンマウント | はい。 | はい。 | 該当なし | 該当なし | 該当なし |
| フルボリュームリストア | いいえ | いいえ | 該当なし | 該当なし | 該当なし |

| 権限 | 有効 | 作成 | 読み取り | 更新 | 削除 |
| --- | --- | --- | --- | --- | --- |
| Job Monitor サービスの略 | はい。 | 該当なし | 該当なし | 該当なし | 該当なし |

## Backup and Clone Viewer ロール

Backup and Clone Viewer ロールには、すべての権限の読み取り専用権限が付与されています。また、検出、レポート、およびダッシュボードへのアクセスに必要な権限も有効になっています。

| 権限 | 有効 | 作成 | 読み取り | 更新 | 削除 |
| --- | --- | --- | --- | --- | --- |
| リソースグループ | 該当なし | いいえ | はい。 | いいえ | いいえ |
| ポリシー | 該当なし | いいえ | はい。 | いいえ | いいえ |
| バックアップ | 該当なし | いいえ | はい。 | いいえ | いいえ |
| ホスト | 該当なし | いいえ | はい。 | いいえ | いいえ |
| ストレージ接続 | 該当なし | いいえ | はい。 | いいえ | いいえ |
| クローン | 該当なし | いいえ | はい。 | いいえ | いいえ |
| プロビジョニング | 該当なし | いいえ | はい。 | いいえ | いいえ |
| ダッシュボード | はい。 | 該当なし | 該当なし | 該当なし | 該当なし |
| レポート | はい。 | 該当なし | 該当なし | 該当なし | 該当なし |
| リストア | いいえ | いいえ | 該当なし | 該当なし | 該当なし |
| リソース | いいえ | いいえ | はい。 | はい。 | いいえ |
| プラグインのインストールとアンインストール | いいえ | 該当なし | 該当なし | 該当なし | 該当なし |
| データ移行 | いいえ | 該当なし | 該当なし | 該当なし | 該当なし |
| マウント | はい。 | 該当なし | 該当なし | 該当なし | 該当なし |
| アンマウント | はい。 | 該当なし | 該当なし | 該当なし | 該当なし |

| 権限 | 有効 | 作成 | 読み取り | 更新 | 削除 |
| --- | --- | --- | --- | --- | --- |
| フルボリュームリストア | いいえ | 該当なし | 該当なし | 該当なし | 該当なし |
| Job Monitor サービスの略 | はい。 | 該当なし | 該当なし | 該当なし | 該当なし |

## Infrastructure Admin ロール

Infrastructure Admin ロールでは、ホストの管理、ストレージの管理、プロビジョニング、リソースグループ、リモートインストールのレポートに対して権限が有効になっています。 ダッシュボードにアクセスします。

| 権限 | 有効 | 作成 | 読み取り | 更新 | 削除 |
| --- | --- | --- | --- | --- | --- |
| リソースグループ | 該当なし | はい。 | はい。 | はい。 | はい。 |
| ポリシー | 該当なし | いいえ | はい。 | はい。 | はい。 |
| バックアップ | 該当なし | はい。 | はい。 | はい。 | はい。 |
| ホスト | 該当なし | はい。 | はい。 | はい。 | はい。 |
| ストレージ接続 | 該当なし | はい。 | はい。 | はい。 | はい。 |
| クローン | 該当なし | いいえ | はい。 | いいえ | いいえ |
| プロビジョニング | 該当なし | はい。 | はい。 | はい。 | はい。 |
| ダッシュボード | はい。 | 該当なし | 該当なし | 該当なし | 該当なし |
| レポート | はい。 | 該当なし | 該当なし | 該当なし | 該当なし |
| リストア | はい。 | 該当なし | 該当なし | 該当なし | 該当なし |
| リソース | はい。 | はい。 | はい。 | はい。 | はい。 |
| プラグインのインストールとアンインストール | はい。 | 該当なし | 該当なし | 該当なし | 該当なし |
| データ移行 | いいえ | 該当なし | 該当なし | 該当なし | 該当なし |

| 権限 | 有効 | 作成 | 読み取り | 更新 | 削除 |
| --- | --- | --- | --- | --- | --- |
| マウント | いいえ | 該当なし | 該当なし | 該当なし | 該当なし |
| アンマウント | いいえ | 該当なし | 該当なし | 該当なし | 該当なし |
| フルボリューム リストア | いいえ | いいえ | 該当なし | 該当なし | 該当なし |
| Job Monitor サービスの略 | はい。 | 該当なし | 該当なし | 該当なし | 該当なし |

## 著作権に関する情報



## 商標に関する情報