SnapCenterのロールベースアクセス制御（RBAC）

SnapCenter Software 6.0

NetApp
September 23, 2024

目次

SnapCenterのロールベースアクセス制御（RBAC）

RBACノシユルイ

SnapCenterのロールベースアクセス制御（RBAC）とONTAP権限を使用すると、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グループに委譲できます。この一元管理されたアクセスにより、アプリケーション管理者は委任された環境で安全に作業を行うことができます。

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。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ケンケン

SnapCenter RBAC

ロールと権限

SnapCenterには、権限が割り当てられた事前定義されたロールが付属していますこれらのロールには、ユーザまたはユーザ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ロールの権限を変更することはできません。

RBACの権限は、同じフォレスト内のユーザとグループ、および異なるフォレストに属するユーザに割り当てることができます。フォレスト間でネストされたグループに属するユーザにRBAC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が含まれている必要があります。Host addやHost removeなど、一部の権限のみをコピーした場合は、それらの処理を実行できません。

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、ログイン時に認証を指定する必要があります。ユーザが複数のロールのメンバーである場合は、ログインクレデンシャルを入力すると、使用するロールを指定するように求められます。また、APIを実行するための認証も必要です。

アプリケーションレベルの**RBAC**

SnapCenterは、クレデンシャルを使用して、許可されたSnapCenterユーザがアプリケーションレベルの権限も持っていることを確認します。

たとえば、SQL Server環境でSnapshot処理やデータ保護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、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。Windowsファイルシステム環境でONTAPストレージ上でSnapshot処理とデータ保護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admin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に、データベースホストでオペレーティングシステム（OS）認証が無効になっている場合は、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、操作に応じて、次のいずれかの方法を使用して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は、vCenter ServerでRBACをさらに強化できます。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。

詳しくは、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ケンケン

ストレージシステムへのアクセスに必要な権限を持つ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Role-Based Access Control（RBAC；ロールベースアクセス制御）を使用すると、ロールを作成して権限を割り当て、そのロールにユーザまたはユーザ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。

- アプリケーションのバックアップとクローンの管理
- バックアップ/クローンビューア
- インフラ管理者
- SnapCenterAdmin

SnapCenter Plug-in for VMware vSphere のロール

VM、VMDK、およびデータストアのVMと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では次のロールがvCenterで作成されます。

- 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ユーザ向けの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。

- 移行
- Mount（Oracleデータベースのみ）
- unmount（Oracleデータベースのみ）
- ジョブモニタ

  Job Monitor権限を使用すると、さまざまなロールのメンバーは、割り当てられているすべてのオブジェクトに対する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）を設定および管理する場合は、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、アプリケーションの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あります。このロールには、ホスト管理、プロビジョニング、ストレージ接続管理、またはリモートインストールに関する権限はありません。

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/アンインストール	いいえ	該当なし		該当なし	該当なし
移行	いいえ	該当なし	該当なし	該当なし	該当なし
マウントする	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
ジョブモニタ	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、すべての権限が読み取り専用で表示されます。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/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
移行	いいえ	該当なし	該当なし	該当なし	該当なし
マウントする	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
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
ジョブモニタ	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、ホスト管理、ストレージ管理、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レポート、 をクリックし、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/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
移行	いいえ	該当なし	該当なし	該当なし	該当なし
マウントする	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
ジョブモニタ	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