RBAC セキュリティ

ONTAP automation

NetApp
January 12, 2026

目次

RBAC セキュリティ

ONTAP REST APIを使用したRBACセキュリティの概要

ONTAP には、堅牢で拡張可能なロールベースアクセス制御（RBAC）機能が搭載されています。各アカウントに異なるロールを割り当てて、REST APIおよびCLIを通じて公開されるリソースへのユーザアクセスを制御することができます。ロールは、ONTAP ユーザごとに異なるレベルの管理アクセスを定義します。

ONTAP RBAC機能は拡張が継続され、ONTAP 9.11.1（およびそれ以降のリリース）で大幅に強化されています。詳細については、およびを参照してください "RBACの機能拡張の概要" "ONTAP REST APIの新機能" 。

ONTAP ロール

ロールとは、ユーザが実行できるアクションをまとめて定義する権限のセットです。各権限は、特定のアクセスパスと関連するアクセスレベルを識別します。ロールはユーザアカウントに割り当てられ、アクセス制御を決定する際にONTAP によって適用されます。

ロールのタイプ

ロールには2つのタイプがあります。ONTAP の進化に合わせてさまざまな環境に導入、カスタマイズされています。

各タイプのロールを使用する場合、メリットとデメリットがあります。を参照してください " ロールタイプの比較" を参照してください。

を入力します	説明
REST	RESTロールはONTAP 9.6で導入されたもので、一般にREST APIを使用してONTAPにアクセスするユーザに適用されます。RESTロールを作成すると、従来の_mapping_roleが自動的に作成されます。
伝統的	これらはONTAP 9.6より前のレガシーロールです。ONTAP CLI環境向けに導入された機能で、引き続きRBACのセキュリティの基盤となります。

適用範囲

すべてのロールには、スコープまたはコンテキストがあり、その中で定義および適用されます。スコープによって、特定のロールがどこでどのように使用されるかが決まります。

ONTAP ユーザアカウントにも、ユーザの定義方法と使用方法を決定する同様のスコープがあります。

適用範囲	説明
クラスタ	クラスタスコープのロールは、ONTAP クラスタレベルで定義されます。クラスタレベルのユーザアカウントに関連付けられます。

適用範囲	説明
SVM	SVMスコープのロールは、特定のデータSVMに対して定義されます。ユーザアカウントは同じSVM内のユーザアカウントに割り当てられます。

ロール定義のソース

ONTAP ロールは2つの方法で定義できます。

役割のソース	説明
カスタム	ONTAP 管理者は、カスタムロールを作成できます。これらのロールは、環境やセキュリティの特定の要件に合わせてカスタマイズできます。
組み込み	カスタムロールはより柔軟な設定が可能ですが、クラスタレベルとSVMレベルの両方で使用できる一連の組み込みロールも用意されています。これらのロールは事前定義されており、一般的な管理タスクに使用できます。

ロールマッピングと**ONTAP** 処理

使用しているONTAP リリースに応じて、すべてまたはほぼすべてのREST API呼び出しが1つ以上のCLIコマンドに対応します。RESTロールを作成すると、従来のロールまたはレガシーロールも作成されます。この* Mapped *トラディショナル・ロールは対応するCLIコマンドに基づいており、操作や変更はできません。

リバースロールマッピングはサポートされません。つまり、従来のロールを作成しても、対応するRESTロールは作成されません。

RBACの機能拡張の概要

ONTAP 9のすべてのリリースに、従来のロールが含まれています。RESTロールはあとから導入されたロールで、以降のセクションで説明します。

ONTAP 9.6

REST APIはONTAP 9.6で導入されました。このリリースには、RESTロールも含まれていました。また、RESTロールを作成すると、対応する従来のロールも作成されます。

ONTAP 9.7～9.10.1

9.7から9.10.1までの各ONTAP リリースには、REST APIの機能拡張が含まれています。たとえば、リリースごとにRESTエンドポイントが追加されているとします。ただし、2つのロールタイプの作成と管理は別々に行われています。また、ONTAP 9.10.1では、リソース修飾エンドポイントである、スナップショットRESTエンドポイント「/api/storage/volumes /{voluu}/snapshots」に対するREST RBACサポートが追加されました。

ONTAP 9.11.1

このリリースでは、REST APIを使用して従来のロールを設定および管理できるようになりました。RESTロールの追加のアクセスレベルも追加されました。

ONTAP REST APIでのロールとユーザの操作

基本的なRBAC機能を理解したら、ONTAP のロールとユーザを使用できるようになります。

を参照してください "RBACワークフロー" ONTAP REST APIでロールを作成して使用する方法の例を次に示します。

管理アクセス

ONTAP ロールは、REST APIまたはコマンドラインインターフェイスを使用して作成および管理できます。アクセスの詳細を以下に示します。

REST API

RBACロールとユーザアカウントを使用するときは、いくつかのエンドポイントを使用できます。表の最初の4つは、ロールの作成と管理に使用されます。最後の2つのは、ユーザアカウントの作成と管理に使用します。

ONTAP にはオンラインでアクセスできます "API リファレンス" APIの使用例など、詳細な情報が記載されたドキュメント。

エンドポイント	説明
「/security/roles」を参照してください	このエンドポイントでは、新しいRESTロールを作成できます。また、ONTAP 9.11.1以降では、従来のロールを作成することもできます。この場合、ONTAP は入力パラメータに基づいてロールタイプを決定します。定義済みのロールのリストを取得することもできます。
`/security/roles/{owner.UUID}/{name}`	クラスタまたはSVMを対象とした特定のロールを取得または削除できます。UUIDの値は、ロールが定義されているSVM（クラスタまたはデータSVM）を示します。名前の値はロールの名前です。
`/security/roles/{owner.UUID}/{name}/privileges `	このエンドポイントでは、特定のロールの権限を設定できます。組み込みのロールは取得できますが、更新することはできません。詳細については、お使いのONTAP リリースのAPIリファレンスドキュメントを参照してください。
`/security/roles/{owner.UUID}/{name}/privileges /[path]`	特定の権限のアクセスレベルとオプションのクエリ値を取得、変更、および削除できます。詳細については、お使いのONTAP リリースのAPIリファレンスドキュメントを参照してください。
「/security/accounts」	このエンドポイントを使用すると、クラスタまたはSVMを対象とした新しいユーザアカウントを作成できます。アカウントが使用可能になるには、いくつかの種類の情報が含まれているか、追加されている必要があります。定義済みのユーザアカウントのリストを取得することもできます。
`/security/accounts/{owner.UUID}/{name}`	クラスタまたはSVMを対象とした特定のユーザアカウントを取得、変更、および削除できます。UUIDの値は、ユーザが定義されているSVM（クラスタまたはデータSVM）です。名前の値はアカウントの名前です。

コマンドラインインターフェイス

次に、関連するONTAP CLIコマンドについて説明します。すべてのコマンドには、管理者アカウントを使用してクラスタレベルでアクセスします。

コマンドを実行します	説明
「security login」と入力します	ユーザログインを作成および管理するために必要なコマンドが格納されたディレクトリです。
「security login rest-role」と入力します	ユーザログインに関連付けられたRESTロールの作成と管理に必要なコマンドを格納するディレクトリです。
「security login role」と入力します	ユーザログインに関連付けられた従来のロールを作成および管理するために必要なコマンドが格納されたディレクトリです。

ロールの定義

RESTロールと従来のロールは、一連の属性によって定義されます。

所有者と範囲

ロールは、ONTAP クラスタまたはクラスタ内の特定のデータSVMに所有されます。所有者は、ロールの範囲も暗黙的に決定します。

一意の名前

すべてのロールには、スコープ内で一意の名前を付ける必要があります。クラスタロールの名前はONTAP クラスタレベルで一意である必要があります。一方、SVMロールは特定のSVM内で一意である必要があります。

新しいRESTロールの名前は、RESTロールと従来のロールで一意である必要があります。これは、RESTロールを作成すると同じ名前の新しいtraditional _mapping_roleが作成されるためです。

権限のセット

すべてのロールには、1つ以上の権限のセットが含まれています。各権限では、特定のリソースまたはコマンドと関連するアクセスレベルが識別されます。

権限

ロールには1つ以上の権限を含めることができます。各特権の定義はタプルであり、特定のリソースまたは操作へのアクセスレベルを確立します。

リソースパス

リソースパスは、RESTエンドポイントまたはCLIコマンド/コマンドディレクトリパスのいずれかとして識別されます。

RESTエンドポイント

RESTロールのターゲットリソースはAPIエンドポイントで特定されました。

CLI コマンド

CLIコマンドは、従来のロールのターゲットを特定します。コマンドディレクトリも指定できます。これにより、すべてのダウンストリームコマンドがONTAP CLI階層に含まれます。

アクセスレベル

アクセスレベルは、特定のリソースパスまたはコマンドに対するロールのアクセスタイプを定義します。アクセスレベルは、事前に定義された一連のキーワードによって識別されます。ONTAP 9.6では3つのアクセスレベルが導入されました。従来のロールとRESTロールの両方に使用できます。また、ONTAP 9.11.1で3つの新しいアクセスレベルが追加されました。これらの新しいアクセスレベルは、RESTロールでのみ使用できます。

アクセスレベルはCRUDモデルに従います。RESTでは、主なHTTPメソッド（POST、GET、PATCH、DELETE）に基づいています。対応するCLI処理は、一般にREST処理（create、show、modify、delete）と対応します。

アクセスレベル	**REST**プリミティブ	を追加しました	**REST**ロールのみ
なし	該当なし	9.6	いいえ
- 読み取り専用	取得	9.6	いいえ
すべて	GET、POST、PATCH、DELETE	9.6	いいえ
READ_CREATE	GET、POST	9.11.1	はい。
READ_MODIFY	取得、パッチ	9.11.1	はい。
READ_CREATE _MODIFY	GET、POST、PATCH	9.11.1	はい。

オプションのクエリ

従来のロールを作成する場合、コマンドまたはコマンドディレクトリに適用可能なオブジェクトのサブセットを特定する* query *値をオプションで指定できます。

組み込みのロールの概要

ONTAP には、クラスタレベルまたはSVMレベルで使用できる事前定義されたロールがいくつか用意されています。

クラスタを対象としたロール

クラスタ内には、複数の組み込みのロールを使用できます。

を参照してください "クラスタ管理者の事前定義されたロール" を参照してください。

ロール	説明
管理	このロールの管理者には制限のない権限があり、ONTAP システムであらゆる操作を実行できます。クラスタレベルおよびSVMレベルのすべてのリソースを設定できます。
AutoSupport	これは、AutoSupport アカウント専用のロールです。
バックアップ	この特殊な役割は、システムのバックアップが必要なバックアップソフトウェアに適用されます。
SnapLock	これは、SnapLock アカウント専用のロールです。

ロール	説明
- 読み取り専用	このロールの管理者は、すべてのデータをクラスタレベルで表示できますが、変更はできません。
なし	管理機能は提供されません。

SVMを対象としたロール

SVMには、SVMスコープで使用できる組み込みのロールがいくつかあります。* vsadmin *は、最も一般的で強力な機能へのアクセスを提供します。特定の管理タスクに応じて、次のような追加のロールが用意されています。

- vsadmin-volume
- vsadmin-protocol のいずれかです
- vsadmin-backup のストレージシステムで
- vsadmin-snaplock
- vsadmin-readonly （読み取り専用

を参照してください "SVM 管理者の事前定義されたロール" を参照してください。

ロールタイプの比較

REST *ロールまたは*従来の*ロールを選択する前に、これらの違いを理解しておく必要があります。この2つのロールタイプの比較方法の一部を次に示します。

RBACのユースケースが複雑で高度な場合は、通常は従来のロールを使用します。

ユーザが**ONTAP** にアクセスする方法

ロールを作成する前に、ユーザがONTAP システムにどのようにアクセスするかを理解しておくことが重要です。このロールに基づいて、ロールのタイプを決定できます。

にアクセスします	推奨されるタイプ
REST APIのみ	RESTロールは、REST APIで使用するように設計されています。
REST APIおよびCLI	対応する従来のロールも作成するRESTロールを定義できます。
CLIのみ	従来のロールを作成できます。

アクセスパスの精度

RESTロールに対して定義されるアクセスパスは、RESTエンドポイントに基づいています。従来のロールのアクセスパスは、CLIコマンドまたはコマンドディレクトリに基づきます。また、オプションのクエリパラメータを従来のロールと一緒に指定することで、コマンドパラメータの値に基づいてアクセスをさらに制限することもできます。

著作権に関する情報

商標に関する情報