ロールベースアクセス制御
ONTAP tools for VMware vSphere 9.11

NetApp
January 18, 2024

目次

ロールベースアクセス制御

ONTAP ツールでのロールベースアクセス制御の概要

vCenter Server の RBAC を使用すると、 vSphere オブジェクトへのアクセスを制御できます。VMware vSphere 用の ONTAP ® ツールでは、 vCenter Server RBAC と ONTAP RBAC により、特定のストレージシステムのオブジェクトに対して特定のユーザが実行できる VSC タスクが決まります。

タスクを完了するには、適切な vCenter Server RBAC アクセス許可が必要です。VSC でのタスクの実行時、まずユーザの vCenter Server アクセス許可が確認され、次にユーザの ONTAP 権限が確認されます。

vCenter Server アクセス許可をルートオブジェクト（ルートフォルダ）に対して設定することができます。その後、アクセス許可が不要な子エンティティのアクセスを禁止することでセキュリティを強化できます。

vCenter Server アクセス許可の要素

vCenter Server で認識されるのはアクセス許可で、権限ではありません。vCenter Server アクセス許可は 3 つの要素で構成されます。

vCenter Server には次のコンポーネントがあります。

- 1 つ以上の権限（ロール）

  ユーザが実行できるタスクを定義します。

- vSphere オブジェクト

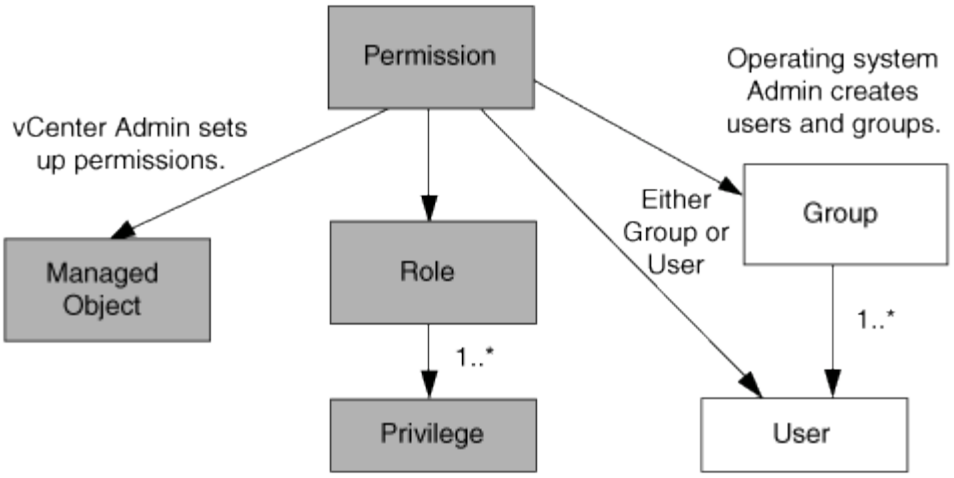
  タスクの対象となるオブジェクトです。

- ユーザまたはグループ

  タスクを実行できるユーザまたはグループを定義します。

次の図に示すように、 3 つの要素がすべて揃っていないとアクセスは許可されません。

グレーのボックスは vCenter Server 側の要素、白のボックスは vCenter Server を実行しているオペレーティングシステム側の要素を表しています。



権限

VMware vSphere 用の ONTAP ツールには、次の 2 種類の権限が関連付けられています。

- vCenter Server 標準の権限

  vCenter Server に付属している権限です。

- VSC 固有の権限

  特定の VSC タスク用に定義された、VSC 固有の権限です。

VSC のタスクを実行するには、 VSC 固有の権限と vCenter Server 標準の権限の両方が必要です。これらの権限は ' ユーザーのロールを構成しますアクセス許可には複数の権限を含めることができます。これらの権限は、 vCenter Server にログインしているユーザを対象としています。

vCenter Server RBAC の使用を簡単にするため、 VSC には、 VSC タスクの実行に必要な VSC 固有の権限と標準の権限をすべて含む標準ロールがいくつか用意されています。

アクセス許可に含まれる権限が変更された場合、そのアクセス許可が関連付けられたユーザは、更新されたアクセス許可を有効にするためにログアウトしてログインし直す必要があります。

* 権限 *	* 役割 *	* タスク *
NetApp ONTAP Tools Console > View の順にクリックします	• VSC 管理者 • VSC によるプロビジョニング • VSC 読み取り専用	VSC および VASA Provider 固有のタスクにはすべて View 権限が必要です。
NetApp Virtual Storage Console > Policy Based Management > Management または privilege.nvpfVSC.VASAGroup.com.netapp.nvpf.label > Management の順にクリックします	VSC 管理者	ストレージ機能プロファイルおよびしきい値設定に関連する VSC および VASA Provider のタスク。

vSphere オブジェクト

アクセス許可は vSphere オブジェクトに関連付けられます。 vCenter Server 、 ESXi ホスト、仮想マシン、データストア、データセンター、 とフォルダ。任意の vSphere オブジェクトに権限を割り当てることができます。vSphere オブジェクトに割り当てられたアクセス許可に基づいて、そのオブジェクトに対してどのユーザがどのタスクを実行できるかが決まります。VSC 固有のタスクについては、アクセス許可の割り当てと検証はルートフォルダレベル（ vCenter Server ）でのみ行われ、それ以外のエンティティでは行われません。ただし VAAI プラグインの処理は例外で、関連する ESXi に対して権限が検証されます。

ユーザとグループ

ユーザとグループは、 Active Directory （またはローカルの vCenter Server マシン）を使用して設定できます。その後、設定したユーザまたはグループに vCenter Server アクセス許可を付与することで、特定の VSC タスクの実行を許可することができます。

> これらの vCenter Server アクセス許可は、 VSC 管理者以外の VSC vCenter ユーザに適用されます。VSC 管理者には、デフォルトでフルアクセスが許可されるため、アクセス許可を割り当てる必要はありません。

ユーザとグループにはロールは割り当てられません。vCenter Server アクセス許可を割り当てることで、間接的にロールが適用されます。

vCenter Server のアクセス許可の割り当てと変更に関する要点

vCenter Server のアクセス許可を使用する際にはいくつかの点に注意する必要があります。VMware vSphere タスク用の ONTAP ツールを使用できるかどうかは、アクセス許可を割り当てた場所、およびアクセス許可の変更後にユーザが実行した操作によって決まります。

権限を割り当てます

vCenter Server のアクセス許可は、 vSphere のオブジェクトおよびタスクへのアクセスを制限したい場合にのみ設定します。それ以外の場合は、管理者としてログインできます。このログインでは、すべての vSphere オブジェクトに自動的にアクセスできます。

アクセス許可を割り当てる場所によって、ユーザが実行できる VSC タスクが決まります。

タスクによっては、完了を確認するために、ルートオブジェクトなどの上位レベルにアクセス許可を割り当てる必要があります。具体的には、特定の vSphere オブジェクトには適用されない権限（タスクの追跡など）がタスクに必要な場合や、必要な権限環境が vSphere 以外のオブジェクト（ストレージシステムなど）に必要な場合です。

このような場合は、子エンティティに継承されるようにアクセス許可を設定できます。子エンティティには、他の権限も割り当てることができます。子エンティティに割り当てたアクセス許可は、親エンティティから継承されたアクセス許可を上書きします。したがって、子エンティティにアクセス許可を割り当てることで、ルートオブジェクトに割り当てられ、子エンティティに継承されたアクセス許可の対象を制限することができます。

会社のセキュリティポリシーでアクセス許可を厳しく制限することが求められる場合を除き、ルートオブジェクト（ルートフォルダとも呼ばれる）にアクセス許可を割り当てることを推奨します。

アクセス許可と非 **vSphere** オブジェクト

作成したアクセス許可は、 vSphere 以外のオブジェクトに適用されます。たとえば、ストレージシステムは vSphere オブジェクトではありません。環境ストレージシステムにアクセス許可を割り当てることができる vSphere オブジェクトがないため、権限がある場合は、その権限を含むアクセス許可を VSC ルートオブジェクトに割り当てる必要があります。

たとえば、「 Add/Modify/Skip storage systems 」といった VSC 権限を含む任意のアクセス許可は、ルートオブジェクトレベルに割り当てる必要があります。

アクセス許可の変更

一度に変更できるアクセス許可は 1 つです。

アクセス許可に含まれる権限が変更された場合、そのアクセス許可が関連付けられたユーザは、更新されたアクセス許可を有効にするためにログアウトしてログインし直す必要があります。

ONTAP ツールに付属の標準ロール

vCenter Server の権限と RBAC を簡単に使用できるように、 Virtual Storage Console （ VSC ）には主要な VSC タスクを実行できる標準の VSC ロールが用意されています。また、タスクの実行を制限し、 VSC 情報の表示のみを許可する読み取り専用ロールもあります。

標準の VSC ロールには、ユーザが VSC タスクを実行するために必要な VSC 固有の権限と vCenter Server 標準の権限の両方が含まれています。また、サポートされるどのバージョンの vCenter Server でも必要な権限が付与されるように設定されています。

管理者は、必要に応じてこれらのロールをユーザに割り当てることができます。

VSC を最新バージョンにアップグレードした場合は、新しいバージョンの VSC で使用できるように自動的にアップグレードされます。

VSC の標準ロールは、 vSphere Client のホームページで * Roles * をクリックすると表示できます。

VSC の組み込みのロールで実行できるタスクを次に示します。

* 役割 *	* 概要 *
VSC 管理者	すべての VSC タスクを実行するために必要な vCenter Server 標準の権限と VSC 固有の権限がすべて含まれています。

VSC 読み取り専用	VSC に対する読み取り専用アクセスが許可されます。アクセスが制御された VSC の処理は実行できません。
VSC によるプロビジョニング	ストレージのプロビジョニングに必要な vCenter Server 標準の権限と VSC 固有の権限がすべて含まれています。次のタスクを実行できます。 • 新しいデータストアを作成する • データストアを削除 • ストレージ機能プロファイルに関する情報を表示する

VSC の標準ロールの使用に関するガイドライン

VMware vSphere の標準的な ONTAP ツールを使用する場合は、一定のガイドラインに従う必要があります。

標準ロールは直接変更しないでください。ロールを直接変更すると、 VSC をアップグレードするたびに変更が上書きされます。VSC をアップグレードするたびに、インストーラによって標準ロールの定義が更新されます。これにより、そのバージョンの VSC およびサポートされるすべてのバージョンの vCenter Server でロールを最新の状態に維持できます。

ただし、標準のロールを使用して環境に合わせたロールを作成することもできます。これを行うには、 VSC の標準ロールをコピーし、コピーしたロールを編集します。新しいロールを作成しても、 VSC Windows サービスを再起動またはアップグレードしてもこのロールを維持できます。

VSC の標準ロールの用途としては、次のようなものがあります。

- すべての VSC タスクに標準の VSC ロールを使用する。

  このシナリオでは、標準ロールは VSC タスクの実行に必要なすべての権限をユーザに提供します。

- 複数のロールを組み合わせてユーザが実行できるタスクを拡張する。

  単独では要件に合う標準の VSC ロールがない場合は、複数のロールを含む上位グループを作成してロールを拡張できます。

  ユーザが vCenter Server 標準の別の権限を必要とする VSC 以外のタスクも実行する必要がある場合は、それらの権限を提供するロールを作成し、グループに追加します。

- より細分化されたロールを作成します。

  標準の VSC ロールよりも少ない権限のロールが必要な場合は、 VSC ロールを使用して新しいロールを作成することができます。

  この場合は、必要な VSC ロールのクローンを作成し、そのクローンを編集してユーザに必要な権限だけを残します。

VSC タスクに必要な権限

VMware vSphere のタスクを実行するために必要な ONTAP ツールの権限の組み合わせは、 Virtual Storage Console （ VSC ）に固有の権限と vCenter Server 標準の権限の組み合わせと異なります。

VSC タスクに必要な権限については、ネットアップの技術情報アーティクル 1032542 を参照してください。

"Virtual Storage Console 用の RBAC の設定方法"

VMware vSphere 用の ONTAP ツールで必要な製品レベルの権限

VMware vSphere GUI の ONTAP ツールにアクセスするには、製品レベルの VSC 固有の View 権限が、適切な vSphere オブジェクトレベルで割り当てられている必要があります。この権限なしでログインすると、 NetApp アイコンをクリックしたときにエラーメッセージが表示され、 VSC にアクセスできません。

次の表に、 VSC の製品レベルの View 権限について説明します。

* 権限 *	* 概要 *	* 割り当てレベル *
表示	VSC の GUI にアクセスできます。VSC でタスクを実行することはできません。VSC のタスクを実行するには、タスクで使用する適切な VSC 固有の権限と vCenter Server の標準権限が必要です。	割り当てレベルによって、表示できる UI の部分が決まります。ルートオブジェクト（フォルダ）に View 権限が割り当てられている場合、 NetApp アイコンをクリックして VSC にアクセスできます。 他の vSphere オブジェクトレベルに View 権限を割り当てることもできますが、その場合は表示および使用できる VSC メニューが制限されます。 View 権限を含むアクセス許可は、ルートオブジェクトに割り当てることを推奨します。

ONTAP ストレージシステムおよび vSphere オブジェクトの権限

ONTAP の RBAC を使用すると、特定のストレージシステムへのアクセスとそれらのストレージシステムで実行できる操作を制御できます。VMware vSphere 用の ONTAP ® ツールでは、 ONTAP RBAC と vCenter Server RBAC により、特定のストレージシステムのオブジェクトに対して特定のユーザが実行できる Virtual Storage Console （ VSC ）タスクが決まります。

VSC では、各ストレージシステムの認証とそのストレージシステムで実行できるストレージ操作の判別に、 VSC で設定したクレデンシャル（ユーザ名とパスワード）が使用されます。ストレージシステムごとに 1 組のクレデンシャルが使用され、そのクレデンシャルに基づいて、ストレージシステムで実行できる VSC タス

クが決まります。つまり、このクレデンシャルは VSC のクレデンシャルであり、個々の VSC ユーザに対するものではありません。

ONTAP RBAC は、ストレージシステムへのアクセス、および仮想マシンのプロビジョニングなど、ストレージに関連する VSC タスクの実行にのみ適用されます。それぞれのストレージシステムに対する適切な ONTAP RBAC 権限がないと、そのストレージシステムでホストされる vSphere オブジェクトに対してタスクを実行することはできません。ONTAP RBAC と VSC 固有の権限を組み合わせることで、ユーザが実行できる VSC タスクを制御することができます。

- ストレージまたはストレージシステムに格納されている vCenter Server オブジェクトの監視と設定
- ストレージシステムに格納されている vSphere オブジェクトのプロビジョニング

ONTAP RBAC と VSC 固有の権限を使用すると、ストレージ主体のセキュリティレイヤをストレージ管理者が管理できるようになります。これにより、 ONTAP RBAC または vCenter Server RBAC のどちらか一方のアクセス制御だけを使用した場合に比べ、よりきめ細かい制御が可能になります。たとえば、 vCenter Server RBAC を使用して、ネットアップストレージでのデータストアのプロビジョニングを vCenterUserB には許可し、 vCenterUserA には許可しないように設定したとします。この場合、特定のストレージシステムのクレデンシャルに対してストレージの作成を禁止すれば、 vCenterUserB と vCenterUserA のどちらもそのストレージシステムでデータストアのプロビジョニングを実行することはできません。

VSC タスクを開始すると、最初にそのタスクに対する正しい vCenter Server アクセス許可がユーザにあるかどうかが検証されます。タスクを実行するための十分な vCenter Server アクセス許可がなければ、最初の vCenter Server のセキュリティチェックをパスできないため、そのストレージシステムの ONTAP 権限は確認されません。そのため、ストレージシステムにアクセスできません。

十分な vCenter Server アクセス許可がある場合は、次にストレージシステムのクレデンシャル（ユーザ名とパスワード）に関連付けられた ONTAP RBAC 権限（ ONTAP ロール）が確認されます。 その VSC タスクで必要なストレージ処理をストレージシステムで実行するための十分な権限があるかどうかを確認すること。適切な ONTAP 権限があれば、ストレージシステムにアクセスして VSC タスクを実行できます。ストレージシステムで実行できる VSC タスクは ONTAP ロールで決まります。

各ストレージシステムには、一連の ONTAP 権限が関連付けられます。

ONTAP RBAC と vCenter Server RBAC の両方を使用すると、次のような利点があります。

- セキュリティ

  どのユーザがどのタスクを実行できるかを、 vCenter Server オブジェクトレベルおよびストレージシステムレベルで制御できます。

- 監査情報

  多くの場合、 VSC はストレージシステムについての監査証跡を提供します。これにより、ストレージに対して変更を行った vCenter Server ユーザまでさかのぼってイベントを追跡できます。

- 使いやすさ

  コントローラのクレデンシャルをすべて集約して一元管理できます。

VMware vSphere 用の ONTAP ツールを使用する際に推奨される ONTAP ロール

VMware vSphere および Role-Based Access Control （ RBAC ；ロールベースアクセス制御）用の ONTAP ®

ツールを使用する際に推奨される ONTAP ロールをいくつか設定できます。これらのロールには、 Virtual Storage Console （ VSC ）タスクで実行するストレージ処理に必要な ONTAP 権限が含まれています。

新しいユーザロールを作成するには、 ONTAP を実行しているストレージシステムに管理者としてログインする必要があります。次のいずれかを使用して ONTAP ロールを作成できます。

- ONTAP システムマネージャ 9.8P1 以降

  "ユーザロールと権限を設定"

- RBAC User Creator for ONTAP ツール（ ONTAP 9.6 以前を使用している場合）

  "VSC 、 VASA Provider 、 Storage Replication Adapter 7.0 for VMware vSphere 用の RBAC User Creator ツール"

各 ONTAP ロールには、ロールのクレデンシャルを構成するユーザ名とパスワードのペアが関連付けられています。このクレデンシャルを使用してログインしないと、ロールに関連付けられたストレージ処理にアクセスできません。

セキュリティ対策として、 VSC 固有の ONTAP ロールは階層構造になっています。最初のロールは最も制限のあるロールで、 VSC の最も基本的なストレージ処理に関連する権限だけを含みます。次のロールには、そのロール独自の権限と、前のロールに関連付けられているすべての権限が含まれます。以降、上位のロールほど制限が少なく、より多くのストレージ処理をサポートします。

VSC を使用する際に推奨される ONTAP RBAC ロールのいくつかを次に示します。ロールを作成したら、仮想マシンのプロビジョニングなど、ストレージに関するタスクを実行する必要があるユーザにそのロールを割り当てることができます。

1. 検出

   ストレージシステムを追加できます。

2. ストレージを作成します

   ストレージを作成できます。また、 Discovery ロールに関連付けられているすべての権限が含まれます。

3. ストレージを変更します

   ストレージを変更できます。また、 Discovery ロールと Create Storage ロールに関連付けられているすべての権限が含まれます。

4. ストレージを破棄します

   ストレージを破棄できます。また、 Discovery ロール、 Create Storage ロール、 Modify Storage ロールに関連付けられているすべての権限が含まれます。

VASA Provider for ONTAP を使用する場合は、 Policy-Based Management （ PBM ；ポリシーベース管理）ロールも設定します。ストレージポリシーを使用してストレージを管理できます。このロールを使用するには、「検出」ロールも設定する必要があります。

VMware vSphere 用の ONTAP ツール用に ONTAP の RBAC を設定する方法

VMware vSphere 用の ONTAP ツールでロールベースアクセス制御を使用する場合は、ストレージシステムで ONTAP RBAC を設定する必要があります。ONTAP RBAC 機能を使用すると、アクセス権限を制限したカスタムユーザアカウントを 1 つ以上作成できます。

VSC と SRA は、クラスタレベルまたは Storage Virtual Machine （ SVM ）レベルでストレージシステムにアクセスできます。クラスタレベルでストレージシステムを追加する場合、必要なすべての機能を使用するには、管理者ユーザのクレデンシャルを指定する必要があります。SVM の詳細を直接追加してストレージシステムを追加する場合は、「 vsadmin 」ユーザには特定のタスクを実行するために必要なすべてのロールと機能が付与されるわけではないことに注意してください。

VASA Provider は、クラスタレベルでのみストレージシステムにアクセスできます。特定のストレージコントローラで VASA Provider が必要な場合は、 VSC または SRA を使用している場合でも、クラスタレベルでストレージシステムを VSC に追加する必要があります。

新しいユーザを作成し、クラスタまたは SVM を ONTAP ツールに接続するには、次の作業を行う必要があります。

- クラスタ管理者または SVM 管理者ロールを作成する

  これらのロールは、次のいずれかを使用して作成できます。

  - ONTAP システムマネージャ 9.8P1 以降

    "ユーザロールと権限を設定"

  - RBAC User Creator for ONTAP ツール（ ONTAP 9.6 以前を使用している場合）

    "VSC 、 VASA Provider 、 Storage Replication Adapter 7.0 for VMware vSphere 用の RBAC User Creator ツール"

- ONTAP を使用して、ロールが割り当てられ、適切なアプリケーションが設定されたユーザを作成します

  作成したストレージシステムクレデンシャルは、 VSC 用にストレージシステムを構成する際に必要になります。VSC 用のストレージシステムを構成するには、 VSC でクレデンシャルを入力する必要があります。これらのクレデンシャルを使用してストレージシステムにログインすると、クレデンシャルの作成時に ONTAP で設定した VSC 機能に対する権限が付与されます。

- VSC にストレージシステムを追加し、作成したユーザのクレデンシャルを指定します

VSC ロール

VSC では、 ONTAP の権限を以下に示す VSC ロールに分類します。

- 検出

  接続されているすべてのストレージコントローラを検出できます

- ストレージを作成します

  ボリュームおよび論理ユニット番号（ LUN ）を作成できます

- ストレージを変更します

  ストレージシステムのサイズ変更と重複排除を実行できます

- ストレージを破棄します

  ボリュームおよび LUN を破棄できます

VASA Provider ロール

クラスタレベルで作成できるのは Policy Based Management のみです。ストレージ機能プロファイルを使用してポリシーベースでストレージを管理できます。

SRA ロール

SRA では、 ONTAP 権限をクラスタレベルまたは SVM レベルで SAN または NAS ロールに分類します。これにより、ユーザは SRM 処理を実行できるようになります。

VSC にクラスタを追加する場合は、 ONTAP RBAC ロールの権限の初期検証が実行されます。直接接続の SVM のストレージ IP を追加した場合、初期検証は実行されません。タスクワークフローの段階で権限が確認されて適用されます。

著作権に関する情報

商標に関する情報