VSC タスクに必要な権限

VSC, VASA Provider, and SRA 9.7

NetApp
March 21, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/vsc-vasa-provider-sra-97/deploy/reference-product-level-privilege-required-by-vsc-for-vmware-vsphere.html on March 21, 2024. Always check docs.netapp.com for the latest.

目次

VSC タスクに必要な権限

Virtual Storage Console for VMware vSphereのタスクを実行するために必要な権限の組み合わせは、（VSC）とvCenter Server標準の権限のそれぞれに異なります。

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"

VSC for VMware vSphereで必要な製品レベルの権限

Virtual Storage Console for VMware vSphereのGUI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	説明	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。

VSC、VASA Provider、SRA仮想アプライアンスに対するONTAP のロールベースアクセス制御

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。Virtual Storage Console for VMware vSphere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、vCenterUserBにデータストアのプロビジョニングを許可し、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。

VSC for VMware vSphere使用時に推奨されるONTAP ロール

推奨されるONTAP ロールを設定して、Virtual Storage Console for VMware vSphereおよびRole-Based Access Control（RBAC；ロールベースアクセス制御）を使用できます。これらのロールには、（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。

- 9.7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。

VSC for VMware vSphere用のONTAP RBACの設定方法

Virtual Storage Console for VMware vSphere（VSC）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。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ユーザーには特定のタスクを実行するために必要なすべての役割と機能が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、クラスタまたはをVSC、VASA Provider、SRA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 System Manager 9.7 以降が必要です

  "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。

> ONTAP コマンドを使用してロールと権限を手動で設定する場合は、ナレッジベースの記事を参照してください。

- "VSC 、 VASA 、 SRA 7.0 の ONTAP RBAC 設定"
- "SVM レベルで VSC と SRA に対するすべてのコマンドを集計します"

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。

ユーザロールと権限を設定

VSC、VASA Provider、SRA仮想アプライアンスに付属のJSONファイルとONTAP System Managerを使用して、ストレージシステムの管理に使用する新しいユーザロールを設定できます。

作業を開始する前に

- VSC、VASA Provider、SRA仮想アプライアンスから、「+ https://{virtual_appliance_IP}:9083/vsc/config/VSC_ONTAP_User_Privileges.zip+`」を使用してONTAP Privilegesファイルをダウンロードしておく必要があります。
- ONTAP 9.7 System Managerを設定しておく必要があります。
- ストレージシステムの管理者権限でログインしている必要があります。

手順

1. ダウンロードした「+ https://{virtual_appliance_IP}:9083/vsc/config/VSC_ONTAP_User_Privileges.zip+`」

ファイルを解凍します。

2. ONTAP システムマネージャにアクセスします。
3. メニューをクリックします。cluster [設定]、[ユーザとロール]の順に選択します。
4. [ユーザーの追加] をクリックします。
5. [ユーザーの追加*]ダイアログボックスで、[仮想化製品*]を選択します。
6. [* Browse] をクリックして、 ONTAP 権限 JSON ファイルを選択し、アップロードします。

   プロダクトフィールドには、自動的に値が入力されます。

7. 必要な機能を*Product Capability (製品機能)ドロップダウンメニューから選択します。

   [* 役割 * （ * role * ）] フィールドは、選択したプロダクト機能に基づいて自動的に入力されます。

8. 必要なユーザ名とパスワードを入力します。
9. ユーザに必要な権限（ Discovery 、 Create Storage 、 Modify Storage 、 Destroy Storage ）を選択し、 * Add * をクリックします。

結果

新しいロールとユーザが追加され、設定したロールの詳細な権限が表示されます。

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権を有し、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権については、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。