VSC 작업에 필요한 권한입니다

VSC, VASA Provider, and SRA 9.7

NetApp
March 21, 2024

목차

VSC 작업에 필요한 권한입니다

VMware vSphere 작업을 위한 다양한 가상 스토리지 콘솔에는 (VSC) 및 기본 vCenter Server 권한에 따라 서로 다른 권한 조합이 필요합니다.

VSC 작업에 필요한 권한에 대한 정보는 NetApp 기술 자료 문서 1032542에서 확인할 수 있습니다.

"가상 스토리지 콘솔에 대한 RBAC 구성 방법"

VMware vSphere용 VSC에 필요한 제품 레벨 권한

VMware vSphere GUI용 가상 스토리지 콘솔에 액세스하려면 올바른 vSphere 개체 레벨에 할당된 제품 수준의 VSC별 View 권한이 있어야 합니다. 이 권한 없이 로그인하는 경우 NetApp 아이콘을 클릭하면 VSC에 오류 메시지가 표시되며 사용자가 VSC에 액세스할 수 없습니다.

다음 정보는 VSC 제품 레벨 뷰 권한에 대해 설명합니다.

권한	설명	배정 수준
보기	VSC GUI에 액세스할 수 있습니다. 이 권한을 통해 VSC 내에서 작업을 수행할 수 없습니다. VSC 작업을 수행하려면 해당 작업에 대한 올바른 VSC 및 기본 vCenter Server 권한이 있어야 합니다.	할당 수준은 UI에서 볼 수 있는 부분을 결정합니다. 루트 개체(폴더)에서 보기 권한을 할당하면 NetApp 아이콘을 클릭하여 VSC를 입력할 수 있습니다. 다른 vSphere 오브젝트 레벨에 보기 권한을 할당할 수 있지만, 이렇게 하면 VSC 메뉴를 표시 및 사용할 수 없습니다. 루트 개체는 보기 권한이 포함된 권한을 할당하는 데 권장되는 장소입니다.

VSC, VASA 공급자, SRA를 위한 가상 어플라이언스에 대한 ONTAP 역할 기반 액세스 제어

ONTAP RBAC(역할 기반 액세스 제어)를 사용하여 특정 스토리지 시스템에 대한 액세스를 제어하고 해당 스토리지 시스템에서 사용자가 수행할 수 있는 작업을 제어할 수 있습니다. VMware vSphere용 가상 스토리지 콘솔에서 ONTAP RBAC는 vCenter Server RBAC와 함께 사용하여 특정 사용자가 특정 스토리지 시스템의 개체에 대해 수행할 수 있는 VSC(가상 스토리지 콘솔) 작업을 결정합니다.

VSC에서는 VSC 내에서 설정한 자격 증명(사용자 이름 및 암호)을 사용하여 각 스토리지 시스템을 인증하고 해당 스토리지 시스템에서 수행할 수 있는 스토리지 작업을 결정합니다. VSC는 스토리지 시스템마다 하나의 자격 증명 세트를 사용합니다. 이러한 자격 증명을 통해 해당 스토리지 시스템에서 수행할 수 있는 VSC 작업을 결정합니다. 즉,

개별 VSC 사용자에 대한 자격 증명이 아니라 VSC에 대한 자격 증명입니다.

ONTAP RBAC는 스토리지 시스템에 액세스하고 가상 시스템 프로비저닝과 같은 스토리지와 관련된 VSC 작업을 수행하는 경우에만 적용됩니다. 특정 스토리지 시스템에 적합한 ONTAP RBAC 권한이 없는 경우 해당 스토리지 시스템에 호스팅된 vSphere 객체에서 작업을 수행할 수 없습니다. ONTAP RBAC와 VSC별 권한을 함께 사용하여 사용자가 수행할 수 있는 VSC 작업을 제어할 수 있습니다.

- 스토리지 시스템에 상주하는 스토리지 또는 vCenter Server 객체를 모니터링하고 구성합니다
- 스토리지 시스템에 상주하는 vSphere 객체를 프로비저닝합니다

VSC별 권한과 함께 ONTAP RBAC를 사용하면 스토리지 관리자가 관리할 수 있는 스토리지 중심의 보안 계층을 제공합니다. 따라서 ONTAP RBAC와 단독으로 또는 vCenter Server RBAC가 지원하는 것보다 세분화된 액세스 제어를 사용할 수 있습니다. 예를 들어 vCenter Server RBAC에서는 vCenterUserA가 데이터 저장소를 프로비저닝하지 못하도록 하면서 vCenterUserB가 스토리지에 데이터 저장소를 프로비저닝하도록 할 수 있습니다. 특정 스토리지 시스템의 스토리지 시스템 자격 증명이 스토리지 생성을 지원하지 않는 경우 vCenterUserB와 vCenterUserA는 해당 스토리지 시스템에서 데이터 저장소를 프로비저닝할 수 없습니다.

VSC 작업을 시작할 때 VSC는 먼저 해당 작업에 대한 올바른 vCenter Server 권한이 있는지 확인합니다. vCenter Server의 권한이 부족하여 작업을 수행할 수 없는 경우, 초기 vCenter Server 보안 검사를 통과하지 못했기 때문에 VSC에서 해당 스토리지 시스템에 대한 ONTAP 권한을 확인할 필요가 없습니다. 따라서 스토리지 시스템에 액세스할 수 없습니다.

vCenter Server의 사용 권한이 충분하면 VSC는 스토리지 시스템 자격 증명(사용자 이름 및 암호)과 연결된 ONTAP RBAC 권한(ONTAP 역할)을 확인합니다. 해당 스토리지 시스템에서 VSC 작업에 필요한 스토리지 작업을 수행할 수 있는 충분한 권한이 있는지 확인합니다. 올바른 ONTAP 권한이 있으면 스토리지 시스템에 액세스하여 VSC 작업을 수행할 수 있습니다. ONTAP 역할에 따라 스토리지 시스템에서 수행할 수 있는 VSC 작업이 결정됩니다.

각 스토리지 시스템에는 하나의 ONTAP 권한 세트가 연결되어 있습니다.

ONTAP RBAC와 vCenter Server RBAC를 모두 사용하면 다음과 같은 이점이 있습니다.

- 보안

  관리자는 세분화된 vCenter Server 객체 레벨과 스토리지 시스템 레벨에서 어떤 작업을 수행할 수 있는지 제어할 수 있습니다.

- 감사 정보

  대부분의 경우 VSC는 스토리지 시스템에 대한 감사 추적을 제공하므로 스토리지 수정을 수행한 vCenter Server 사용자에게 이벤트를 다시 추적할 수 있습니다.

- 사용 편의성

  모든 컨트롤러 자격 증명을 한 곳에서 유지 관리할 수 있습니다.

VMware vSphere용 VSC를 사용할 때의 권장 ONTAP 역할

VMware vSphere용 가상 스토리지 콘솔 및 RBAC(역할 기반 액세스 제어)로 작업하기 위해 권장되는 여러 ONTAP 역할을 설정할 수 있습니다. 이러한 역할에는 VSC(VSC) 작업에서 실행되는 필요한 스토리지 작업을 수행하는 데 필요한 ONTAP 권한이 포함됩니다.

새 사용자 역할을 생성하려면 ONTAP를 실행하는 스토리지 시스템에서 관리자로 로그인해야 합니다. 다음 중 하나를 사용하여 ONTAP 역할을 만들 수 있습니다.

- 9.7 이상

  "사용자 역할 및 권한을 구성합니다"

- RBAC ONTAP용 사용자 작성자 도구(ONTAP 9.6 이하를 사용하는 경우)

  "VSC, VASA 공급자 및 VMware vSphere용 스토리지 복제 어댑터 7.0용 RBAC 사용자 작성 툴"

각 ONTAP 역할에는 해당 역할의 자격 증명을 구성하는 연결된 사용자 이름 및 암호 쌍이 있습니다. 이러한 자격 증명을 사용하여 로그인하지 않으면 해당 역할과 연결된 스토리지 작업에 액세스할 수 없습니다.

보안 조치로서 VSC별 ONTAP 역할은 계층적으로 정렬됩니다. 즉, 첫 번째 역할이 가장 제한적인 역할이며 가장 기본적인 VSC 스토리지 운영 세트와 연관된 권한만 가집니다. 다음 역할에는 자신의 권한과 이전 역할과 연결된 모든 권한이 모두 포함됩니다. 각각의 추가 역할은 지원되는 스토리지 작업과 관련하여 덜 제한적입니다.

다음은 VSC를 사용할 때 권장되는 ONTAP RBAC 역할 중 일부입니다. 이러한 역할을 생성한 후에는 가상 시스템 프로비저닝과 같은 스토리지 관련 작업을 수행해야 하는 사용자에게 역할을 할당할 수 있습니다.

1. 탐색

   이 역할을 통해 스토리지 시스템을 추가할 수 있습니다.

2. 스토리지 생성

   이 역할을 사용하여 스토리지를 생성할 수 있습니다. 이 역할에는 검색 역할과 연결된 모든 권한도 포함됩니다.

3. 스토리지 수정

   이 역할을 사용하여 스토리지를 수정할 수 있습니다. 이 역할에는 검색 역할 및 스토리지 생성 역할과 연결된 모든 권한도 포함됩니다.

4. 스토리지 폐기

   이 역할을 사용하면 스토리지를 제거할 수 있습니다. 이 역할에는 검색 역할, 스토리지 생성 역할 및 스토리지 수정 역할과 연결된 모든 권한도 포함됩니다.

VASA Provider for ONTAP를 사용하는 경우 PBM(정책 기반 관리) 역할도 설정해야 합니다. 이 역할을 통해 스토리지 정책을 사용하여 스토리지를 관리할 수 있습니다. 이 역할을 수행하려면 "Discovery" 역할도 설정해야 합니다.

VMware vSphere용 VSC에 대한 ONTAP 역할 기반 액세스 제어를 구성하는 방법

VSC(VMware vSphere)용 가상 스토리지 콘솔에서 역할 기반 액세스 제어를 사용하려면 스토리지 시스템에서 RBAC(ONTAP 역할 기반 액세스 제어)를 구성해야 합니다. ONTAP RBAC 기능을 사용하여 액세스 권한이 제한된 사용자 지정 사용자 계정을 하나 이상 생성할 수 있습니다.

VSC 및 SRA는 클러스터 수준 또는 수준에서 스토리지 시스템에 액세스할 수 있습니다. 클러스터 레벨에서 스토리지 시스템을 추가하는 경우 필요한 모든 기능을 제공하려면 admin 사용자의 자격 증명을 제공해야 합니다. 세부 정보를 직접 추가하여 스토리지 시스템을 추가하는 경우 ""vsadmin" 사용자에게 특정 작업을 수행하는 데 필요한 역할 및 기능이 모두 포함되어 있지 않습니다.

VASA Provider는 클러스터 레벨에서만 스토리지 시스템에 액세스할 수 있습니다. 특정 스토리지 컨트롤러에 VASA Provider가 필요한 경우 VSC 또는 SRA를 사용하는 경우에도 클러스터 레벨에서 VSC에 스토리지 시스템을 추가해야 합니다.

새 사용자를 생성하고 클러스터 또는 을 VSC, VASA 공급자 및 SRA에 연결하려면 다음을 수행해야 합니다.

- 클러스터 관리자 또는 관리자 역할을 생성합니다

  다음 중 하나를 사용하여 이러한 역할을 만들 수 있습니다.

  - ONTAP 시스템 관리자 9.7 이상

  "사용자 역할 및 권한을 구성합니다"

  - RBAC ONTAP용 사용자 작성자 도구(ONTAP 9.6 이하를 사용하는 경우)

  "VSC, VASA 공급자 및 VMware vSphere용 스토리지 복제 어댑터 7.0용 RBAC 사용자 작성 툴"

- 할당된 역할과 ONTAP를 사용하여 적절한 애플리케이션 세트를 가진 사용자를 생성합니다

  VSC용 스토리지 시스템을 구성하려면 이러한 스토리지 시스템 자격 증명이 필요합니다. VSC에 자격 증명을 입력하여 VSC용 스토리지 시스템을 구성할 수 있습니다. 이러한 자격 증명을 사용하여 스토리지 시스템에 로그인할 때마다 자격 증명을 생성하는 동안 ONTAP에서 설정한 VSC 기능에 대한 권한이 부여됩니다.

- 스토리지 시스템을 VSC에 추가하고 방금 생성한 사용자의 자격 증명을 제공합니다

VSC 역할

VSC는 ONTAP 권한을 다음 VSC 역할 세트로 분류합니다.

- 탐색

  연결된 모든 스토리지 컨트롤러를 검색할 수 있습니다

- 스토리지 생성

  볼륨 및 LUN(Logical Unit Number) 생성 지원

- 스토리지 수정

  스토리지 시스템의 크기 조정 및 중복 제거를 설정합니다

- 스토리지 폐기

  볼륨 및 LUN을 소멸하도록 설정합니다

VASA 공급자 역할

클러스터 수준에서는 정책 기반 관리만 생성할 수 있습니다. 스토리지 용량 프로필을 사용하여 정책을 기반으로 스토리지를 관리할 수 있습니다.

SRA 역할

SRA에서는 ONTAP 권한을 클러스터 수준 또는 수준에서 SAN 또는 NAS 역할로 분류합니다. 이를 통해 사용자는 SRM 작업을 실행할 수 있습니다.

> ONTAP 명령을 사용하여 역할과 권한을 수동으로 구성하려면 기술 자료 문서를 참조해야 합니다.

- "VSC, VASA 및 SRA 7.0 ONTAP RBAC 구성"
- "SVM 레벨에서 VSC 및 SRA를 위한 모든 명령 롤업"

VSC는 클러스터를 VSC에 추가할 때 ONTAP RBAC 역할의 초기 권한 검증을 수행합니다. 직접 스토리지 IP를 추가한 경우 VSC에서 초기 검증을 수행하지 않습니다. VSC는 나중에 작업 워크플로에서 권한을 확인하고 적용합니다.

사용자 역할 및 권한을 구성합니다

VSC, VASA Provider, SRA 및 ONTAP System Manager용 가상 어플라이언스와 함께 제공된 JSON 파일을 사용하여 스토리지 시스템 관리를 위한 새 사용자 역할을 구성할 수 있습니다.

시작하기 전에

- VSC, VASA Provider 및 SRA를 위해 가상 어플라이언스에서 'https://{virtual_appliance_IP}:9083/vsc/config/VSC_ONTAP_User_Privileges.zip` 사용하여 ONTAP 권한 파일을 다운로드해야 합니다.
- ONTAP 9.7 System Manager를 구성해야 합니다.
- 스토리지 시스템에 대한 관리자 권한으로 로그인해야 합니다.

단계

1. 다운로드한 'https://{virtual_appliance_IP}:9083/vsc/config/VSC_ONTAP_User_Privileges.zip` 파일의 압축을 풉니다.
2. ONTAP 시스템 관리자에 액세스합니다.
3. MENU: cluster [Settings > Users and Roles] 를 클릭합니다.
4. 사용자 추가 * 를 클릭합니다.
5. 사용자 추가 * 대화 상자에서 * 가상화 제품 * 을 선택합니다.
6. 찾아보기 * 를 클릭하여 ONTAP 권한 JSON 파일을 선택하여 업로드합니다.

   제품 필드가 자동으로 채워집니다.

7. PRODUCT Capability * 드롭다운 메뉴에서 필요한 기능을 선택합니다.

   역할 * 필드는 선택한 제품 기능에 따라 자동으로 채워집니다.

8. 필요한 사용자 이름과 암호를 입력합니다.
9. 사용자에게 필요한 권한(검색, 스토리지 생성, 스토리지 수정, 스토리지 폐기)을 선택한 다음 * 추가 * 를 클릭합니다.

결과

새 역할 및 사용자가 추가되고 구성한 역할 아래에서 자세한 권한을 볼 수 있습니다.