역할 기반 액세스 제어(RBAC) 구성

SnapCenter Software 4.6

NetApp
January 18, 2024

This PDF was generated from https://docs.netapp.com/ko-kr/snapcenter-46/install/task_add_a_user_or_group_and_assign_role_and_assets.html on January 18, 2024. Always check docs.netapp.com for the latest.

목차

역할 기반 액세스 제어(RBAC) 구성 1
사용자 또는 그룹을 추가하고 역할 및 자산을 할당합니다 1
역할을 생성합니다 3
보안 로그인 명령을 사용하여 ONTAP RBAC 역할을 추가합니다 4
최소 권한으로 SVM 역할 생성 6
최소 권한으로 ONTAP 클러스터 역할을 생성합니다 10
Active Directory 읽기 권한을 사용하도록 IIS 응용 프로그램 풀을 구성합니다 15

역할 기반 액세스 제어(RBAC) 구성

사용자 또는 그룹을 추가하고 역할 및 자산을 할당합니다

SnapCenter 사용자에 대한 역할 기반 액세스 제어를 구성하려면 사용자 또는 그룹을 추가하고 역할을 할당할 수 있습니다. 역할에 따라 SnapCenter 사용자가 액세스할 수 있는 옵션이 결정됩니다.

- 필요한 것 *
- "SnapCenterAdmin" 역할로 로그인해야 합니다.
- 운영 체제 또는 데이터베이스의 Active Directory에서 사용자 또는 그룹 계정을 만들어야 합니다. SnapCenter를 사용하여 이러한 계정을 만들 수 없습니다.

> SnapCenter 4.5에서는 공백(), 하이픈(-), 밑줄(_) 및 콜론(:)과 같은 특수 문자만 사용자 이름과 그룹 이름에 포함할 수 있습니다. 이러한 특수 문자로 SnapCenter의 이전 릴리스에서 만든 역할을 사용하려면 SnapCenter WebApp이 설치된 web.config 파일에서 'disableSQLInjectionValidation' 매개 변수의 값을 true 로 변경하여 역할 이름의 유효성 검사를 비활성화할 수 있습니다. 값을 수정한 후에는 서비스를 다시 시작할 필요가 없습니다.

- SnapCenter에는 몇 가지 사전 정의된 역할이 포함되어 있습니다.

  이러한 역할을 사용자에게 할당하거나 새 역할을 만들 수 있습니다.

- SnapCenter RBAC에 추가되는 AD 사용자 및 AD 그룹은 Active Directory의 사용자 컨테이너 및 컴퓨터 컨테이너에 대한 읽기 권한을 가지고 있어야 합니다.
- 적절한 권한이 포함된 사용자 또는 그룹에 역할을 할당한 후에는 호스트 및 스토리지 연결과 같은 SnapCenter 자산에 대한 사용자 액세스를 할당해야 합니다.

  따라서 사용자는 자신에게 할당된 자산에 대한 사용 권한이 있는 작업을 수행할 수 있습니다.

- RBAC 사용 권한 및 효율성을 활용하려면 특정 시점에 사용자나 그룹에 역할을 할당해야 합니다.
- 호스트, 리소스 그룹, 정책, 스토리지 연결, 플러그인, 사용자 또는 그룹을 생성하는 동안 사용자에게 자격 증명을 제공합니다.
- 특정 작업을 수행하기 위해 사용자를 할당해야 하는 최소 자산은 다음과 같습니다.

작동	자산 할당
리소스 보호	호스트, 정책
백업	호스트, 리소스 그룹, 정책
복원	호스트, 리소스 그룹
복제	호스트, 리소스 그룹, 정책

작동	자산 할당
클론 라이프사이클	호스트
리소스 그룹을 만듭니다	호스트

- 새 노드가 Windows 클러스터 또는 DAG(Exchange Server Database Availability Group) 자산에 추가되고 이 새 노드가 사용자에게 할당된 경우 사용자나 그룹에 새 노드를 포함하도록 자산을 재할당해야 합니다.

  RBAC 사용자 또는 그룹을 클러스터 또는 DAG에 재할당하여 RBAC 사용자 또는 그룹에 새 노드를 포함해야 합니다. 예를 들어, 2노드 클러스터가 있고 RBAC 사용자 또는 그룹을 클러스터에 할당했습니다. 클러스터에 다른 노드를 추가하는 경우 RBAC 사용자 또는 그룹을 클러스터에 재할당하여 RBAC 사용자 또는 그룹의 새 노드를 포함해야 합니다.

- 스냅샷 복사본을 복제할 계획인 경우 작업을 수행하는 사용자에게 소스 및 타겟 볼륨 모두에 대한 스토리지 연결을 할당해야 합니다.

  사용자에게 액세스 권한을 할당하기 전에 자산을 추가해야 합니다.

> VMware vSphere용 SnapCenter 플러그인 기능을 사용하여 VM, VMDK 또는 데이터 저장소를 보호하는 경우 VMware vSphere GUI를 사용하여 vCenter 사용자를 VMware vSphere용 SnapCenter 플러그인 역할에 추가해야 합니다. VMware vSphere 역할에 대한 자세한 내용은 를 참조하십시오 "VMware vSphere용 SnapCenter 플러그인과 함께 패키지로 제공되는 사전 정의된 역할".

- 단계 *
  1. 왼쪽 탐색 창에서 * 설정 * 을 클릭합니다.
  2. 설정 페이지에서 * 사용자 및 액세스 * > * 를 클릭합니다 +*.
  3. Active Directory 또는 작업 그룹에서 사용자/그룹 추가 페이지에서 다음을 수행합니다.

이 필드의 내용...	수행할 작업...
액세스 유형	도메인 또는 작업 그룹을 선택합니다 도메인 인증 유형의 경우 사용자를 역할에 추가할 사용자 또는 그룹의 도메인 이름을 지정해야 합니다. 기본적으로 로그인한 도메인 이름으로 미리 채워집니다. 신뢰할 수 없는 도메인은 * 설정 * > * 글로벌 설정 * > * 도메인 설정 * 페이지에서 등록해야 합니다.

이 필드의 내용...	수행할 작업...
유형	사용자 또는 그룹을 선택합니다 SnapCenter는 메일 그룹이 아닌 보안 그룹만 지원합니다.
사용자 이름	a. 부분 사용자 이름을 입력한 다음 * 추가 * 를 클릭합니다. 사용자 이름은 대소문자를 구분합니다. b. 검색 목록에서 사용자 이름을 선택합니다. 다른 도메인 또는 신뢰할 수 없는 도메인의 사용자를 추가할 때는 도메인 간 사용자에 대한 검색 목록이 없으므로 사용자 이름을 완전히 입력해야 합니다. 선택한 역할에 다른 사용자 또는 그룹을 추가하려면 이 단계를 반복합니다.
역할	사용자를 추가할 역할을 선택합니다.

4. Assign * 을 클릭한 다음 Assign Assets 페이지에서 다음을 수행합니다.
   a. 자산 * 드롭다운 목록에서 자산 유형을 선택합니다.
   b. [자산] 테이블에서 자산을 선택합니다.

      사용자가 자산을 SnapCenter에 추가한 경우에만 자산이 나열됩니다.

   c. 필요한 모든 자산에 대해 이 절차를 반복합니다.
   d. 저장 * 을 클릭합니다.
5. 제출 * 을 클릭합니다.

   사용자 또는 그룹을 추가하고 역할을 할당한 후 리소스 목록을 새로 고칩니다.

역할을 생성합니다

기존 SnapCenter 역할을 사용하는 것 외에도 고유한 역할을 만들고 사용 권한을 사용자 지정할 수 있습니다.

"SnapCenterAdmin" 역할로 로그인해야 합니다.

- 단계 *

1. 왼쪽 탐색 창에서 * 설정 * 을 클릭합니다.
2. 설정 페이지에서 * 역할 * 을 클릭합니다.
3. 을 클릭합니다 +.
4. 역할 추가 페이지에서 새 역할의 이름과 설명을 지정합니다.

> SnapCenter 4.5에서는 공백(), 하이픈(-), 밑줄(_) 및 콜론(:)과 같은 특수 문자만 사용자 이름과 그룹 이름에 포함할 수 있습니다. 이러한 특수 문자로 SnapCenter의 이전 릴리스에서 만든 역할을 사용하려면 SnapCenter WebApp이 설치된 web.config 파일에서 'disableSQLInjectionValidation' 매개 변수의 값을 true 로 변경하여 역할 이름의 유효성 검사를 비활성화할 수 있습니다. 값을 수정한 후에는 서비스를 다시 시작할 필요가 없습니다.

5. 이 역할의 모든 구성원은 다른 구성원의 개체를 볼 수 있습니다 * 를 선택하여 역할의 다른 구성원이 리소스 목록을 새로 고친 후 볼륨 및 호스트와 같은 리소스를 볼 수 있도록 합니다.

   이 역할의 구성원이 다른 구성원이 할당된 개체를 보지 못하도록 하려면 이 옵션을 선택 취소해야 합니다.

> 이 옵션을 사용하면 개체 또는 리소스를 만든 사용자와 동일한 역할에 속한 사용자는 개체 또는 리소스에 대한 사용자 액세스를 할당할 필요가 없습니다.

1. 사용 권한 페이지에서 역할에 할당할 사용 권한을 선택하거나 * 모두 선택 * 을 클릭하여 역할에 모든 사용 권한을 부여합니다.
2. 제출 * 을 클릭합니다.

보안 로그인 명령을 사용하여 **ONTAP RBAC** 역할을 추가합니다

스토리지 시스템에서 clustered ONTAP을 실행 중인 경우 보안 로그인 명령을 사용하여 ONTAP RBAC 역할을 추가할 수 있습니다.

- 필요한 것 *
- Clustered ONTAP을 실행 중인 스토리지 시스템에 대해 ONTAP RBAC 역할을 생성하기 전에 다음을 확인해야 합니다.
  - 수행할 작업(또는 작업)입니다
  - 이러한 작업을 수행하는 데 필요한 권한입니다
- RBAC 역할을 구성하려면 다음 작업을 수행해야 합니다.
  - 명령 및/또는 명령 디렉터리에 권한을 부여합니다.

    명령 /command 디렉토리에는 모두 액세스 및 읽기 전용이라는 두 가지 액세스 레벨이 있습니다.

  항상 먼저 모든 액세스 권한을 할당해야 합니다.

  - 사용자에게 역할을 할당합니다.
  - SnapCenter 플러그인이 전체 클러스터의 클러스터 관리자 IP에 연결되어 있는지, 아니면 클러스터 내의 SVM에 직접 연결되어 있는지 여부에 따라 구성을 다양하게 변경할 수 있습니다.

- 이 작업에 대한 정보 *

스토리지 시스템에서 이러한 역할을 간단히 구성하기 위해 NetApp 커뮤니티 포럼에 게시된 RBAC 사용자 작성자 for Data ONTAP 툴을 사용할 수 있습니다.

이 도구는 자동으로 ONTAP 권한 설정을 올바르게 처리합니다. 예를 들어, RBAC Data ONTAP용 사용자 작성 도구 는 모든 액세스 권한이 먼저 나타나도록 올바른 순서로 권한을 자동으로 추가합니다. 읽기 전용 권한을 먼저 추가한 다음 모든 액세스 권한을 추가하면 ONTAP에서 모든 액세스 권한을 중복으로 표시하고 무시합니다.

> 나중에 SnapCenter 또는 ONTAP를 업그레이드할 경우 RBAC 사용자 생성기 for Data ONTAP 도구를 다시 실행하여 이전에 만든 사용자 역할을 업데이트해야 합니다. 이전 버전의 SnapCenter 또는 ONTAP에 대해 만든 사용자 역할은 업그레이드된 버전에서 제대로 작동하지 않습니다. 이 도구를 다시 실행하면 자동으로 업그레이드를 처리합니다. 역할을 다시 생성할 필요는 없습니다.

ONTAP RBAC 역할 설정에 대한 자세한 내용은 을 참조하십시오 "ONTAP 9 관리자 인증 및 RBAC 전원 가이드".

> 일관성을 위해 SnapCenter 문서는 사용 권한을 사용하는 역할을 나타냅니다. OnCommand 시스템 관리자 GUI는 ""권한" 대신 ""속성""을 사용합니다. ONTAP RBAC 역할을 설정할 때 이 두 용어는 모두 동일합니다.

- 단계 *

1. 스토리지 시스템에서 다음 명령을 입력하여 새 역할을 생성합니다.

   'Security login role create <role_name\> - cmddirname "command" - access all – vserver <svm_name\>'

   - SVM_NAME은 SVM의 이름입니다. 이 필드를 비워 두면 기본적으로 클러스터 관리자가 됩니다.
   - role_name 은 역할에 대해 지정하는 이름입니다.
   - 명령은 ONTAP 기능입니다.

     > 각 권한에 대해 이 명령을 반복해야 합니다. 모든 액세스 명령은 읽기 전용 명령 앞에 나열되어야 합니다.

   사용 권한 목록에 대한 자세한 내용은 을 참조하십시오 "역할을 생성하고 권한을 할당하는 ONTAP CLI 명령입니다".

2. 다음 명령을 입력하여 사용자 이름을 생성합니다.

   '보안 로그인 생성 - 사용자 이름 <user_name\> - 응용 프로그램 ontapi - AuthMethod <password\> - 역할 <name_of_role_in_step_1\> - vserver <svm_name\> - 설명 "user_description"

   - user_name은 만들고 있는 사용자의 이름입니다.
   - password>는 사용자의 암호입니다. 암호를 지정하지 않으면 시스템에 암호를 입력하라는 메시지가 표시됩니다.
   - SVM_NAME은 SVM의 이름입니다.

3. 다음 명령을 입력하여 사용자에게 역할을 할당합니다.

   '보안 로그인 수정 사용자 이름 <user_name\> – vserver <svm_name\> - role <role_name\> - application

ontapi-application console - AuthMethod <password\>'

- user_name>은 2단계에서 만든 사용자의 이름입니다. 이 명령을 사용하면 사용자를 수정하여 역할에 연결할 수 있습니다.
- svm_name>은 SVM의 이름입니다.
- role_name>은 1단계에서 만든 역할의 이름입니다.
- password>는 사용자의 암호입니다. 암호를 지정하지 않으면 시스템에 암호를 입력하라는 메시지가 표시됩니다.

4. 다음 명령을 입력하여 사용자가 올바르게 생성되었는지 확인합니다.

   'Security login show –vserver <svm_name\>-user-or-group-name <user_name\>'

user_name 은 3단계에서 만든 사용자의 이름입니다.

최소 권한으로 **SVM** 역할 생성

ONTAP에서 새 SVM 사용자의 역할을 생성할 때 실행해야 하는 ONTAP CLI 명령은 여러 가지가 있습니다. ONTAP에서 SnapCenter와 함께 사용하도록 SVM을 구성하고 vsadmin 역할을 사용하지 않으려는 경우 이 역할이 필요합니다.

- 단계 *

1. 스토리지 시스템에서 역할을 생성하고 역할에 모든 권한을 할당합니다.

   '보안 로그인 역할 생성 – vserver <svm_name\> - role <SVM_Role_Name\> - cmddirname <permission\>'

   각 권한에 대해 이 명령을 반복해야 합니다.

1. 사용자를 생성하고 해당 사용자에게 역할을 할당합니다.

   '보안 로그인 생성 - 사용자 <user_name\> - vserver <svm_name\> - application ontapi - AuthMethod password - role <SVM_Role_Name\>'

2. 사용자 잠금을 해제합니다.

   '보안 로그인 잠금 해제 - 사용자 <user_name\> - vserver <svm_name\>'

SVM 역할 생성 및 권한 할당을 위한 **ONTAP CLI** 명령

SVM 역할을 생성하고 권한을 할당하려면 몇 가지 ONTAP CLI 명령을 실행해야 합니다.

- 'Security login role create - role SVM_Role_Name - cmddirname "SnapMirror list-destinations" - vserver SVM_Name - access all'
- 'Security login role create - role SVM_Role_Name - cmddirname' event generate-autosupport-log" - vserver SVM_Name - access all'
- 'Security login role create - vserver SVM_Name - role SVM_Role_Name - cmddirname "job history show" -

access all'

- 'Security login role create - vserver SVM_Name - role SVM_Role_Name - cmddirname "job stop" - access all'
- 'Security login role create - vserver SVM_Name - role SVM_Role_Name - cmddirname "lun" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "lun create" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "lun delete" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "lun igroup add" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "lun igroup create" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "lun igroup delete" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "lun igroup rename" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "lun igroup show" - access all'을 선택합니다
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "lun mapping add-reporting-nodes" - access all'
- 'Security login role create - vserver SVM_Name - role SVM_Role_Name - cmddirname "lun mapping create" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "lun mapping delete" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "lun mapping remove-reporting-nodes" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "lun mapping show" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "lun modify" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "lun move-in-volume" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "lun offline" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "lun online" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "lun resize" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "lun serial" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "lun show" - access all'
- 'Security login role create - vserver SVM_Name - role SVM_Role_Name - cmddirname "network interface" - access readonly'

- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "SnapMirror policy add-rule" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "snapmirror policy modify -rule" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "SnapMirror policy remove-rule" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "SnapMirror policy show" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "SnapMirror restore" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "snapmirror show" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "SnapMirror update" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "snapmirror update-ls-set" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "version" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "volume clone create" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "volume clone show" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "volume clone split start" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "volume clone split stop" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "volume create" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "volume destroy" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "volume file clone create" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "volume file show -disk-usage" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "volume modify" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "volume offline" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "volume online" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "volume qtree create" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "volume qtree delete" - access all'

- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "volume qtree modify" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "volume qtree show" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "volume restrict" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "volume show" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "volume snapshot create" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "volume snapshot delete" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "volume snapshot modify" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "volume snapshot rename" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "volume snapshot restore" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "volume snapshot restore-file" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "volume snapshot show" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "volume unmount" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "vserver cifs share create" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "vserver cifs share delete" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "vserver cifs share show" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "vserver cifs show" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "vserver export-policy create" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "vserver export-policy delete" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "vserver export-policy rule create" - access all'
- '보안 로그인 역할 생성 - vserver SVM_name - role SVM_Role_Name - cmddirname "vserver export-policy rule show" - access all'을 선택합니다
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "vserver export-policy show" - access all'
- 'Security login role create - vserver SVM_Name - role SVM_Role_Name - cmddirname "vserver iscsi connection show" - access all'

- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "vserver" - access readonly'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "vserver export-policy" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "vserver iscsi" - access all'
- 'Security login role create - vserver SVM_Name - role SVM_Role_Name - cmddirname "volume clone split status" - access all'

최소 권한으로 **ONTAP** 클러스터 역할을 생성합니다

SnapCenter에서 작업을 수행하기 위해 ONTAP 관리자 역할을 사용할 필요가 없도록 최소 권한으로 ONTAP 클러스터 역할을 생성해야 합니다. 여러 ONTAP CLI 명령을 실행하여 ONTAP 클러스터 역할을 생성하고 최소 권한을 할당할 수 있습니다.

- 단계 *

  1. 스토리지 시스템에서 역할을 생성하고 역할에 모든 권한을 할당합니다.

     'Security login role create – vserver <cluster_name\> - role <role_name\> - cmddirname <permission\>'

     각 권한에 대해 이 명령을 반복해야 합니다.

  1. 사용자를 생성하고 해당 사용자에게 역할을 할당합니다.

     '보안 로그인 생성 - 사용자 <user_name\> - vserver <cluster_name\> - application ontapi - AuthMethod password - role <role_name\>'

  2. 사용자 잠금을 해제합니다.

     '보안 로그인 잠금 해제 - 사용자 <user_name\> - vserver <cluster_name\>'

클러스터 역할을 생성하고 권한을 할당하는 **ONTAP CLI** 명령입니다

클러스터 역할을 생성하고 권한을 할당하려면 몇 가지 ONTAP CLI 명령을 실행해야 합니다.

- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "metrocluster show" -access readonly`
- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "cluster identity modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster identity show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster peer show" -access all`

- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "event generate-autosupport-log" -access all`
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "job history show" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "job stop" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "lun" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "lun create" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "lun delete" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "lun igroup add" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "lun igroup create" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "lun igroup delete" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "lun igroup modify" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "lun igroup rename" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "lun igroup show" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "lun mapping add-reporting-nodes" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "lun mapping create" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "lun mapping delete" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "lun mapping remove-reporting-nodes" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "lun mapping show" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "lun modify" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "lun move-in-volume" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "lun offline" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "lun online" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "lun persistent-reservation clear" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "lun resize" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "lun serial" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "lun show" - access all'

- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "network interface create" - access readonly
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "network interface delete" - access readonly'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "network interface modify" - access readonly
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname' network interface show "-access readonly
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "security login" - access readonly'
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror list-destinations" -access all`
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "SnapMirror policy add-rule" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "SnapMirror policy create" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "SnapMirror policy delete" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "SnapMirror policy modify" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "snapmirror policy modify -rule" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "SnapMirror policy remove-rule" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "SnapMirror policy show" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "SnapMirror restore" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "snapmirror show" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "snapmirror show-history" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "SnapMirror update" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "SnapMirror update-ls-set" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "system license add" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "system license clean-up" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "system license delete" - access all'

- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname' system license show "-access all'을 참조하십시오
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "system license status show" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "system node modify" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname' system node show "-access all'을 선택합니다
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "system status show" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "version" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "volume clone create" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "volume clone show" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "volume clone split start" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "volume clone split stop" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "volume create" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "volume destroy" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "volume file clone create" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "volume file show -disk -usage" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "volume modify" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "volume offline" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "volume online" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "volume qtree create" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "volume qtree delete" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "volume qtree modify" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "volume qtree show" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "volume restrict" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "volume show" - access

all'

- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "volume snapshot create" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "volume snapshot delete" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "volume snapshot modify" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "volume snapshot promote" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "volume snapshot rename" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "volume snapshot restore" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "volume snapshot restore-file" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "volume snapshot show" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "volume unmount" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "vserver" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "vserver cifs create" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "vserver cifs delete" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "vserver cifs modify" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "vserver cifs share modify" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "vserver cifs share create" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "vserver cifs share delete" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "vserver cifs share modify" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "vserver cifs share show" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "vserver cifs show" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "vserver create" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "vserver export-policy create" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "vserver export - policy delete" - access all'

- '보안 로그인 역할 생성 - vserver Cluster_name - role Role_Name - cmddirname "vserver export-policy rule create" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "vserver export-policy rule delete" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "vserver export-policy rule modify" - access all'
- '보안 로그인 역할 생성 - vserver Cluster_name - role Role_Name - cmddirname "vserver export-policy rule show" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "vserver export-policy show" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "vserver iscsi connection show" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "vserver modify" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "vserver show" - access all'

Active Directory 읽기 권한을 사용하도록 IIS 응용 프로그램 풀을 구성합니다

SnapCenter에 대해 Active Directory 읽기 권한을 설정해야 할 때 사용자 지정 응용 프로그램 풀 계정을 만들도록 Windows Server에서 IIS(인터넷 정보 서비스)를 구성할 수 있습니다.

- 단계 *
  1. SnapCenter가 설치된 Windows 서버에서 IIS 관리자를 엽니다.
  2. 왼쪽 탐색 창에서 * 응용 프로그램 풀 * 을 클릭합니다.
  3. 응용 프로그램 풀 목록에서 SnapCenter를 선택한 다음 작업 창에서 * 고급 설정 * 을 클릭합니다.
  4. ID를 선택한 다음 *… * 를 클릭하여 SnapCenter 응용 프로그램 풀 ID를 편집합니다.
  5. 사용자 지정 계정 필드에 Active Directory 읽기 권한이 있는 도메인 사용자 또는 도메인 관리자 계정 이름을 입력합니다.
  6. 확인 을 클릭합니다.

     사용자 지정 계정은 SnapCenter 응용 프로그램 풀의 기본 제공 ApplicationPoolIdentity 계정을 대체합니다.

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이센스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이센스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 http://www.netapp.com/TM에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.