



UNIX용 SnapDrive에서 역할 기반 액세스 제어 구성

Snapdrive for Unix

NetApp
June 20, 2025

목차

UNIX용 SnapDrive에서 역할 기반 액세스 제어 구성	1
Operations Manager 콘솔에서 SD-admin 구성	1
명령줄 인터페이스를 사용하여 SD-admin 구성	1
스토리지 시스템에 SD-호스트 이름을 추가하는 중입니다	2
CLI를 사용하여 스토리지 시스템에 SD-호스트 이름을 추가합니다	3
UNIX용 SnapDrive에서 사용자 자격 증명 구성	3
Operations Manager 콘솔을 사용하여 액세스 검사를 수행하기 위한 사용자 이름 형식입니다	4
역할 기반 액세스 제어를 위한 구성 변수	5

UNIX용 SnapDrive에서 역할 기반 액세스 제어 구성

UNIX용 SnapDrive의 역할 기반 액세스 제어(RBAC)를 구성하려면 다양한 작업을 완료해야 합니다. Operations Manager 콘솔 또는 명령줄 인터페이스를 사용하여 작업을 수행할 수 있습니다.

Operations Manager 콘솔에서 SD-admin 구성

Operations Manager 콘솔 관리자는 SD-admin 사용자를 생성할 수 있습니다.

Operations Manager 콘솔 관리자는 글로벌 그룹(글로벌 DFM.Core.AccessCheck)에서 코어 액세스 검사를 수행할 수 있는 기능을 갖춘 SD-ADMIN이라는 사용자를 생성합니다. Operations Manager 콘솔 관리자가 SD-admin 사용자를 구성한 후에는 자격 증명 정보를 SnapDrive for UNIX 관리자에게 수동으로 전송해야 합니다. Operations Manager 콘솔을 사용하여 사용자 및 역할을 구성하는 방법에 대한 자세한 내용은 *Operations Manager* 콘솔 관리 가이드 및 온라인 도움말을 참조하십시오.



SD-admin 대신 모든 이름을 사용할 수 있지만 SD-admin을 사용하는 것이 좋습니다.

Operations Manager 콘솔에서 역할을 만들려면 * Setup * > * Roles * 를 선택합니다. SD-admin 구성 페이지에서 운영 관리자 콘솔 관리자는 글로벌 그룹의 DFM.Database.Write' 기능을 SD-admin 역할에 할당해야 합니다. 그러면 SnapDrive for UNIX가 운영 관리자 콘솔의 스토리지 엔터티를 새로 고칠 수 있습니다.

명령줄 인터페이스를 사용하여 SD-admin 구성

스토리지 시스템 관리자는 명령줄 인터페이스를 사용하여 SD-admin 사용자를 구성할 수 있습니다.

단계

1. SD-admin이라는 사용자를 추가합니다.

```
# useradd sd-admin
```

```
# passwd sd-admin
Changing password for sd-admin.
New password:
Re-enter new password:
Password changed
```

2. 이름이 sd-admin 인 관리자를 추가합니다.

```
# dfm user add sd-admin
Added administrator sd-admin.
```

3. sd-admin-role이라는 역할을 생성합니다.

```
# dfm role create sd-admin-role
Created role sd-admin-role.
```

4. 3단계에서 만든 역할에 기능을 추가합니다.

```
# dfm role add sd-admin-role DFM.Core.AccessCheck Global
Added 1 capability to role sd-admin-role.
```

5. 운영 관리자 관리자는 글로벌 그룹의 DFM.Database.Write 기능을 "<SD-admin>"에 부여하여 SnapDrive for UNIX가 운영 관리자의 스토리지 시스템 엔터티를 새로 고칠 수 있도록 할 수 있습니다.

```
# dfm role add sd-admin-role DFM.Database.Write Global
Added 1 capability to role sd-admin-role.
```

6. SD-ADMIN-ROLE 역할을 SD-ADMIN 사용자에게 추가합니다.

```
# dfm user role set sd-admin sd-admin-role
Set 1 role for administrator sd-admin.
```

스토리지 시스템에 **SD-호스트** 이름을 추가하는 중입니다

Operations Manager 콘솔 관리자는 Operations Manager 콘솔을 사용하여 스토리지 시스템에 SD-호스트 이름 사용자를 생성할 수 있습니다. 단계를 완료한 후 Operations Manager 콘솔 관리자는 SnapDrive for UNIX 관리자에게 자격 증명을 수동으로 전송해야 합니다. SD-호스트 이름 대신 모든 이름을 사용할 수 있지만 SD-호스트 이름을 사용하는 것이 좋습니다.

단계

1. 스토리지 시스템의 루트 암호를 얻고 암호를 저장합니다.

스토리지 시스템의 암호를 추가하려면 * Management * > * Storage System * 을 선택합니다.

2. 각 UNIX 시스템에 대한 SD-호스트 이름 사용자를 생성합니다.
3. SD 역할과 같은 역할에 API- *, login- * 기능을 할당합니다.
4. SD-usergroup과 같은 새 사용자 그룹에 이 역할(SD-ROLE)을 포함합니다.
5. 이 사용자 그룹(SD-usergroup)을 스토리지 시스템의 SD-호스트 이름 사용자와 연결합니다.

CLI를 사용하여 스토리지 시스템에 SD-호스트 이름을 추가합니다

스토리지 시스템 관리자는 `useradmin` 명령을 사용하여 SD-호스트 이름 사용자를 생성하고 구성할 수 있습니다.

단계

1. 스토리지 추가:

```
# dfm host add storage_array1
Added host storage_array1.lab.eng.btc.xyz.in
```

2. 호스트의 암호를 설정합니다.

```
# dfm host password save -u root -p xxxxxxxx storage_array1
Changed login for host storage_array1.lab.eng.btc.xyz.in to root.
Changed Password for host storage_array1.lab.eng.xyz.netapp
.in
```

3. 호스트에 역할을 생성합니다.

```
# dfm host role create -h storage_array1 -c "api-*,login-*" sd-unixhost-
role
Created role sd-unixhost-role on storage_array1
```

4. 사용자 그룹을 생성합니다.

```
# dfm host usergroup create -h storage_array1 -r sd-unixhost-role sd-
unixhost-ug
Created usergroup sd-unixhost-ug(44) on storage_array1
```

5. 로컬 사용자를 생성합니다.

```
# dfm host user create -h storage_array1 -p xxxxxxxx -g sd-unixhost-ug
sd-unixhost
Created local user sd-unixhost on storage_array1
```

UNIX용 SnapDrive에서 사용자 자격 증명 구성

UNIX용 SnapDrive 관리자는 Operations Manager 콘솔 관리자로부터 사용자 자격 증명을 받습니다. 이러한 사용자 자격 증명은 적절한 스토리지 작업을 위해 SnapDrive for UNIX에서

구성해야 합니다.

단계

1. 스토리지 시스템에서 SD-admin을 구성합니다.

```
[root]#snapdrive config set -dfm sd-admin ops_mngr_server
Password for sd-admin:
Retype password:
```

2. 스토리지 시스템에서 SD-호스트 이름을 구성합니다.

```
[root]#snapdrive config set sd-unix_host storage_array1
Password for sd-unix_host:
Retype password:
```

3. 'SnapDrive config list' 명령어를 이용하여 1단계와 2단계를 확인한다.

user name	appliance name	appliance type
sd-admin	ops_mngr_server	DFM
sd-unix_host	storage_array1	StorageSystem

4. UNIX용 SnapDrive를 구성하여 's-drive.conf' 파일에서 'RBAC-method="DFM" 구성 변수를 설정하여 운영 관리자 콘솔 RBAC(역할 기반 액세스 제어)를 사용하십시오.



사용자 자격 증명이 암호화되어 기존 '.sdupw' 파일에 저장됩니다. 이전 파일의 기본 위치는 '/opt/netapp/SnapDrive/.sdupw'입니다.

Operations Manager 콘솔을 사용하여 액세스 검사를 수행하기 위한 사용자 이름 형식입니다

UNIX용 SnapDrive는 사용자 이름 형식을 사용하여 Operations Manager 콘솔을 사용하여 액세스 검사를 수행합니다. 이러한 형식은 사용자가 NIS(Network Information System)인지 로컬 사용자인지에 따라 달라집니다.

UNIX용 SnapDrive는 다음 형식을 사용하여 사용자가 특정 작업을 수행할 수 있는 권한이 있는지 여부를 확인합니다.

- SnapDrive 명령을 실행하는 NIS 사용자인 경우 UNIX용 SnapDrive는 '<nisdomain>\<username>' 형식을 사용합니다(예: 'netapp.com\marc').
- Inx197-141과 같은 UNIX 호스트의 로컬 사용자인 경우 UNIX용 SnapDrive는 '<hostname>\<username>' 형식(예: 'Inx197-141\john')을 사용합니다.
- UNIX 호스트의 관리자(루트)인 경우 UNIX용 SnapDrive는 항상 관리자를 로컬 사용자로 취급하며 "Inx197-

141\root" 형식을 사용합니다.

역할 기반 액세스 제어를 위한 구성 변수

'napdrive.conf' 파일에서 역할 기반 액세스 제어와 관련된 다양한 구성 변수를 설정해야 합니다.

변수	설명
'contact-http-dFM-port=8088'	Operations Manager 콘솔 서버와 통신하는 데 사용할 HTTP 포트를 지정합니다. 기본값은 8088입니다.
'contact-ssl-dFM-port=8488'	Operations Manager 콘솔 서버와 통신하는 데 사용할 SSL 포트를 지정합니다. 기본값은 8488입니다.
'RBAC-method=DFM'	액세스 제어 방법을 지정합니다. 가능한 값은 '네이티브'와 'dfm'입니다. 값이 'native'이면 '/vol/vol0/sdprbac/sdhost-name.prbac'에 저장된 액세스 제어 파일이 액세스 검사에 사용됩니다. 값이 DIFM으로 설정되어 있으면 Operations Manager 콘솔이 필수 구성 요소입니다. 이러한 경우 UNIX용 SnapDrive는 작업 관리자 콘솔에 액세스 검사를 보냅니다.
'RBAC-cache=on'	UNIX용 SnapDrive는 액세스 검사 쿼리의 캐시 및 해당 결과를 유지합니다. UNIX용 SnapDrive는 구성된 모든 Operations Manager 콘솔 서버가 다운된 경우에만 이 캐시를 사용합니다. 이 값은 캐시를 사용하려면 "켜짐"으로 설정하고, 사용하지 않으려면 "꺼짐"으로 설정할 수 있습니다. 기본값은 OFF이며, 이를 통해 SnapDrive for UNIX에서 Operations Manager 콘솔을 사용하도록 구성하고 'RBAC-method' 구성 변수를 'dfm'로 설정할 수 있습니다.
'RBAC-cache-timeout'	RBAC 캐시 시간 초과 기간을 지정하며 'RBAC-cache'가 활성화된 경우에만 적용됩니다. 기본값은 24시간입니다. UNIX용 SnapDrive는 구성된 모든 Operations Manager 콘솔 서버가 다운된 경우에만 이 캐시를 사용합니다.
'use-https-to-DFM = on'	이 변수를 사용하면 UNIX용 SnapDrive가 Operations Manager 콘솔과 통신할 때 SSL 암호화(HTTPS)를 사용하도록 설정할 수 있습니다. 기본값은 'on'입니다.

저작권 정보

Copyright © 2025 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 라이선스와 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 라이선스도 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 라이선스를 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 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

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