Configuration of role-based access control in SnapDrive for UNIX

Snapdrive for Unix

NetApp
June 20, 2025

This PDF was generated from https://docs.netapp.com/us-en/snapdrive-unix/aix/task_configuring_sd_admin_using_cli.html on June 20, 2025. Always check docs.netapp.com for the latest.

Table of Contents

Configuration of role-based access control in SnapDrive for UNIX . . . 1
- Configuring sd-admin in Operations Manager console . . . 1
  - Configuring sd-admin using command-line interface . . . 1
- Adding sd-hostname to the storage system . . . 2
  - Adding sd- hostname to storage system using CLI . . . 3
- Configuring user credentials on SnapDrive for UNIX . . . 3
- User name formats for performing access checks with Operations Manager console . . . 4
- Configuration variables for role-based access control . . . 5

Configuration of role-based access control in SnapDrive for UNIX

You must complete various tasks to configure Role-Based Access Control (RBAC) for SnapDrive for UNIX. You can use either Operations Manager console or the command-line interface to perform the tasks.

Configuring sd-admin in Operations Manager console

The Operations Manager console administrator can create the sd-admin user.

The Operations Manager console administrator creates a user named, sd-admin, with the capability to perform a core access check on global group (global `DFM.Core.AccessCheck`). After the Operations Manager console administrator configures the sd-admin user, you must manually send the credential information to the SnapDrive for UNIX administrator. For more information about using Operations Manager console to configure users and roles, see the *Operations Manager Console Administration guide* and the Online Help.

You can use any name in place of sd-admin; however, it is best to use sd-admin.

To create a role in Operations Manager console, select **Setup** > **Roles**. In the sd-admin configuration page, the Operations Manager console administrator must assign `DFM.Database.Write` capability on the global group to sd-admin-role, so that SnapDrive for UNIX can refresh storage entities in Operations Manager console.

Configuring sd-admin using command-line interface

The storage system administrator can configure sd-admin user using command-line interface.

Steps

1. Add a user named sd-admin.

```
# useradd sd-admin
```

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

2. Add an administrator named sd-admin.

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

3. Create a role named sd-admin-role.

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

4. Add a capability to the role created in step 3.

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

5. The Operations Manager administrator can also grant `DFM.Database.Write` capability on the global group to `<sd-admin>` to enable SnapDrive for UNIX to refresh storage system entities in Operations Manager.

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

6. Add an sd-admin-role role to the sd-admin user.

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

Adding sd-hostname to the storage system

The Operations Manager console administrator can create the sd-hostname user on the storage system using Operations Manager console. After the steps are completed, the Operations Manager console administrator must manually send the credentials to the SnapDrive for UNIX administrator. You can use any name in place of sd-hostname; however it is best to use sd-hostname.

Steps

1. Obtain the root password of the storage system and store the password.

   To add the password for the storage system, select **Management** > **Storage System**.

2. Create an sd-hostname user for each UNIX system.
3. Assign capabilities `api- and login-` to a role, such as sd-role.
4. Include this role (sd-role) in a new usergroup, such as sd-usergroup.
5. Associate this usergroup (sd-usergroup) with the sd-hostname user on the storage system.

Adding sd- hostname to storage system using CLI

The storage system administrator can create and configure the sd-hostname user using the useradmin command.

Steps

1. Add storage.

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

2. Set the password for the host.

```
# 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. Create a role on the host.

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

4. Create a usergroup.

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

5. Create a local user.

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

Configuring user credentials on SnapDrive for UNIX

The SnapDrive for UNIX administrator receives user credentials from Operations Manager console administrator. These user credentials need to be configured on SnapDrive for UNIX for proper storage operations.

Steps

1. Configure sd-admin on the storage system.

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

2. Configure sd-hostname on the storage system.

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

3. Verify step 1 and step 2, using the `snapdrive config list` command.

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

4. Configure SnapDrive for UNIX to use Operations Manager console Role-based access control (RBAC) by setting the configuration variable `rbac-method="dfm"` in the `snapdrive.conf` file.

> The user credentials are encrypted and saved in the existing `.sdupw` file. The default location of the earlier file is `/opt/NetApp/snapdrive/.sdupw`.

User name formats for performing access checks with Operations Manager console

SnapDrive for UNIX uses the user name formats for performing access checks with Operations Manager console. These formats depends on whether you are a Network Information System (NIS) or a local user.

SnapDrive for UNIX uses the following formats to check whether a user is authorized to perform certain tasks:

- If you are an NIS user running the `snapdrive` command, SnapDrive for UNIX uses the format `<nisdomain>\<username>` (for example, `netapp.com\marc`)
- If you are a local user of a UNIX host such as lnx197-141, SnapDrive for UNIX uses the format `<hostname>\<username>` format (for example, `lnx197-141\john`)
- If you are an administrator (root) of a UNIX host, SnapDrive for UNIX always treats the administrator as a local user and uses the format `lnx197-141\root`.

Configuration variables for role-based access control

You must set the various configuration variables related to role-based access control in the `snapdrive.conf` file.

Variable	Description
contact-http-dfm-port = 8088	Specifies the HTTP port to use for communicating with an Operations Manager console server. The default value is 8088.
contact-ssl-dfm-port = 8488	Specifies the SSL port to use for communicating with an Operations Manager console server. The default value is 8488.
rbac-method=dfm	Specifies the access control methods. The possible values are `native` and `dfm`. If the value is `native`, the access control file stored in `/vol/vol0/sdprbac/sdhost-name.prbac` is used for access checks. If the value is set to `dfm`, Operations Manager console is a prerequisite. In such a case, SnapDrive for UNIX sends access checks to the Operations Manager console.
rbac-cache=on	SnapDrive for UNIX maintains a cache of access check queries and the corresponding results. SnapDrive for UNIX uses this cache only when all the configured Operations Manager console servers are down. You can set this value to either `on` to enable cache, or to `off` to disable it. The default value is off so that you can configure SnapDrive for UNIX to use Operations Manager console and set the `rbac-method` configuration variable to `dfm`.
rbac-cache-timeout	Specifies the rbac cache timeout period and is applicable only when the *rbac-cache* is enabled. The default value is `24` hrs. SnapDrive for UNIX uses this cache only when all the configured Operations Manager console servers are down.
use-https-to-dfm=on	This variable lets you set SnapDrive for UNIX to use SSL encryption (HTTPS) when it communicates with Operations Manager console. The default value is `on`.

Copyright information

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.