



Using the SnapDrive configuration wizard

Snapdrive for Unix

Ivana Devine
January 25, 2021

Table of Contents

- Using the SnapDrive configuration wizard 1
 - Steps to configure in NFS environment 1
 - Steps to configure in SAN environment 1
 - Steps to configure in Mixed SAN and NFS environment 2

Using the SnapDrive configuration wizard


The configuration wizard allows you to configure in NFS, SAN or Mixed environment.

Steps to configure in NFS environment

The following are the steps to configure in NFS environment.

Steps

1. Select the **NFS** profile.
2. Enable the Protection Manager Integration.
 - Select **Yes** to enable the access permission checks by using the DataFabric Manager.
 - Enter the DataFabric Manager server name or IP address followed by user name and password.
 - Enter the `http/https` port to communicate with the DataFabric Manager. The default value is 8088.
 - Enter the SSL server port to access the DataFabric Manager. The default value is 8488.
 - Enable the HTTPs enabled to communicate with the DataFabric Manager.
 - Select **No** to enable the access permission checks by using the rbac.
3. Specify the role-based access control methods. The possible values are `native` and `dfm`.
 - Select `native` to check the access permission for the host using the control file stored in `/vol/vol0/sdprbac/sdhost-name.prbac` or `/vol/vol0/sdprbac/sdgenericname.prbac`.
 - Select `dfm` to check the access permission using the Operations Manager console.



If you select `dfm` as `rbac-method` without configuring DataFabric Manager, a warning message specifying that the RBAC method is selected as `dfm` without enabling Protection Manager Integration is displayed.
4. Specify `https` or `http` to communicate with the storage system.
5. The final step is to save the configuration changes in the `snapdrive.conf` file, and restart the daemon.
 - If you select **Yes**, the SnapDrive daemon is restarted and the configuration changes are reflected.
 - If you select **No**, the variable values are changed in `snapdrive.conf` file, but the changes are not reflected.

Steps to configure in SAN environment

The following are the steps to configure in SAN environment.

Steps

1. Select the SAN profile.
2. Select the required transport protocol.
 - Select `fc` to set the default-transport.
 - Select `iscsi` to set the default-transport.

3. Select the SAN Storage Stack (combination of MPIO Solution, volume manager, and file system). The options are `native`, `veritas`, and `none`.

SnapDrive does not support `veritas` for iSCSI transport protocol.

4. Enable the Protection Manager Integration.

- Select `Yes` to enable the access permission checks by using the DataFabric Manager.
 - Enter the DataFabric Manager server name or IP address followed by user name and password.
 - Enter the `http/https` port to communicate with the DataFabric Manager. The default value is `8088`.
 - Enter the SSL server port to access the DataFabric Manager. The default value is `8488`.
 - Enable the HTTPs enabled to communicate with the DataFabric Manager
- Select `No` to enable the access permission checks by using the `rbac`.

5. Specify the role-based access control methods. The possible values are `native` and `dfm`.

- Select `native` to check the access permission for the host using the control file stored in `/vol/vol0/sdprbac/sdhost-name.prbac` or `/vol/vol0/sdprbac/sdgenericname.prbac`.
- Select `dfm` to check the access permission using the Operations Manager.



If you select `dfm` as `rbac-method` without configuring DataFabric Manager, a warning message specifying that the RBAC method is selected as `dfm` without enabling Protection Manager Integration is displayed.

6. Specify `https` or `http` to communicate with the storage system.
7. The final step is to save the configuration changes in the `snapdrive.conf` file, and restart the daemon.
 - If you select `Yes`, the SnapDrive daemon is restarted and the configuration changes are reflected.
 - If you select `No`, the variable values are changed in `snapdrive.conf` file, but the changes are not reflected.

Steps to configure in Mixed SAN and NFS environment

The following are the steps to configure in Mixed SAN and NFS environment.

Steps

1. Select the Mixed profile.
2. Select the required transport protocol.
 - Select `fcp` to set the default-transport.
 - Select `iscsi` to set the default-transport.
3. Select the SAN Storage Stack (combination of MPIO Solution, volume manager, file system). The options are `native`, `veritas`, and `none`.

SnapDrive does not support `veritas` for iSCSI transport protocol.

4. Enable the Protection Manager Integration.

- Select `Yes` to enable the access permission checks by using the DataFabric Manager
 - Enter the DataFabric Manager server name or IP address followed by user name and password.
 - Enter the `http/https` port to communicate with the DataFabric Manager. The default value is 8088.
 - Enter the SSL server port to access the DataFabric Manager. The default value is 8488.
 - Enable the HTTPs enabled to communicate with the DataFabric Manager.
- Select `No` to enable the access permission checks by using the `rbac`.

5. Specify the role-based access control methods. The possible values are `native` and `dfm`.

- Select `native` to check the access permission for the host using the control file stored in `/vol/vol0/sdprbac/sdhost-name.prbac` or `/vol/vol0/sdprbac/sdgenericname.prbac`
- Select `dfm` to check the access permission using the Operations Manager console.



If you select `dfm` as `rbac-method` without configuring DataFabric Manager, a warning message specifying that the RBAC method is selected as `dfm` without enabling Protection Manager Integration is displayed.

6. Specify `https` or `http` to communicate with the storage system.

7. The final step is to save the configuration changes in the `snapdrive.conf` file, and restart the daemon.

- If you select `Yes`, the SnapDrive daemon is restarted and the configuration changes are reflected.
- If you select `No`, the variable values are changed in `snapdrive.conf` file, but the changes are not reflected.

SnapDrive modifies the following variables in the `snapdrive.conf` file.

- `contact-http-dfm-port`
- `contact-ssl-dfm-port`
- `use-https-to-dfm`
- `default-transport`
- `use-https-to-filer`
- `fstype`
- `multipathing-type`
- `vmtype`
- `rbac-method`
- `rbac-cache`

Copyright Information

Copyright © 2021 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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

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.