Configure High Availability

SnapCenter Software 4.7

NetApp
October 25, 2022

This PDF was generated from https://docs.netapp.com/us-en/snapcenter/install/concept_configure_snapcenter_servers_for_high_availabiity_using_f5.html on October 25, 2022. Always check docs.netapp.com for the latest.

Table of Contents

Configure High Availability . . . 1
Configure SnapCenter Servers for High Availability using F5 . . . 1
Configure Microsoft Network Load Balancer manually . . . 2
Switch from NLB to F5 for high availability . . . 2
High availability for the SnapCenter MySQL repository . . . 2
Export SnapCenter certificates . . . 3

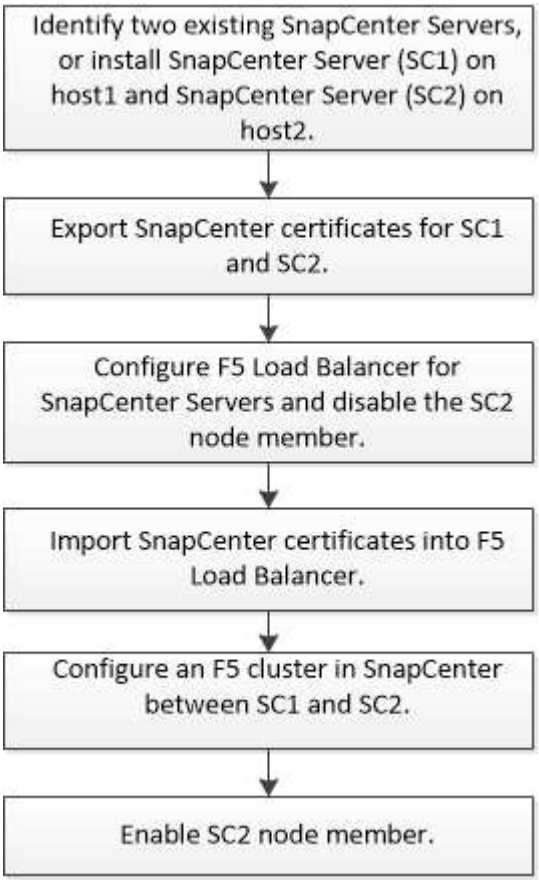
Configure High Availability

Configure SnapCenter Servers for High Availability using F5

To support High Availability (HA) in SnapCenter, you can install the F5 load balancer. F5 enables the SnapCenter Server to support active-passive configurations in up to two hosts that are in the same location. To use F5 Load Balancer in SnapCenter, you should configure the SnapCenter Servers and configure F5 load balancer.

If you have upgraded from SnapCenter 4.2.x and were previously using Network Load Balancing (NLB), you can continue to use that configuration or switch to F5.

The workflow image lists the steps to configure SnapCenter Servers for high availability using F5 load balancer. For detailed instruction, see How to configure SnapCenter Servers for high availability using F5 Load Balancer.



You must be a member of the Local Administrators group on the SnapCenter Servers (in addition to being assigned to the SnapCenterAdmin role) to use the following cmdlets for adding and removing F5 clusters:

- Add-SmServerCluster
- Add-SmServer
- Remove-SmServerCluster

  For more information, see SnapCenter Software Cmdlet Reference Guide.

Additional F5 configuration information

- After you install and configure SnapCenter for high availability, edit the SnapCenter desktop shortcut to point to the F5 cluster IP.
- If a failover occurs between SnapCenter Servers and if there is also an existing SnapCenter session, you must close the browser and log on to SnapCenter again.
- In load balancer setup (NLB or F5), if you add a node that is partially resolved by the NLB or F5 node and if the SnapCenter node is not able to reach out to this node, then the SnapCenter host page switches between hosts down and running state frequently. To resolve this issue, you should ensure that both the SnapCenter nodes are able to resolve the host in NLB or F5 node.
- SnapCenter commands for MFA settings should be executed on all the nodes. Relying party configuration should be done in the Active Directory Federation Services (AD FS) server using F5 cluster details. Node level SnapCenter UI access will be blocked after MFA is enabled.

Configure Microsoft Network Load Balancer manually

You can configure Microsoft Network Load Balancing (NLB) to set up SnapCenter High Availability. From SnapCenter 4.2, you should manually configure NLB outside of SnapCenter installation for high availability.

For information about how to configure Network Load Balancing (NLB) with SnapCenter see How to configure NLB with SnapCenter.

SnapCenter 4.1.1 or earlier supported configuration of Network Load Balancing (NLB) while installing SnapCenter.

Switch from NLB to F5 for high availability

You can change your SnapCenter HA configuration from Network Load Balancing (NLB) to use F5 Load Balancer.

Steps

1. Configure SnapCenter Servers for high availability using F5. Learn more.
2. On the SnapCenter Server host, launch PowerShell.
3. Start a session by using the Open-SmConnection cmdlet, and then enter your credentials.
4. Update the SnapCenter Server to point to the F5 cluster IP address using the Update-SmServerCluster cmdlet.

   The information regarding the parameters that can be used with the cmdlet and their descriptions can be obtained by running *Get-Help command_name*. Alternatively, you can also refer to the SnapCenter Software Cmdlet Reference Guide.

High availability for the SnapCenter MySQL repository

MySQL replication is a feature of MySQL Server that enables you to replicate data from one MySQL database server (master) to another MySQL database server (slave).

SnapCenter supports MySQL replication for high availability only on two Network Load Balancing-enabled (NLB-enabled) nodes.

SnapCenter performs read or write operations on the master repository and routes its connection to the slave repository when there is a failure on the master repository. The slave repository then becomes the master repository. SnapCenter also supports reverse replication, which is enabled only during failover.

If you want to use the MySQL high availability (HA) feature, you must configure Network Load Balancer (NLB) on the first node. The MySQL repository is installed on this node as part of the installation. While installing SnapCenter on the second node, you must join to the F5 of the first node and create a copy of the MySQL repository on the second node.

SnapCenter provides the *Get-SmRepositoryConfig* and *Set-SmRepositoryConfig* PowerShell cmdlets to manage MySQL replication.

The information regarding the parameters that can be used with the cmdlet and their descriptions can be obtained by running *Get-Help command_name*. Alternatively, you can also refer to the SnapCenter Software Cmdlet Reference Guide.

You must be aware of the limitations related to the MySQL HA feature:

- NLB and MySQL HA are not supported beyond two nodes.
- Switching from a SnapCenter standalone installation to an NLB installation or vice versa and switching from a MySQL standalone setup to MySQL HA are not supported.
- Automatic failover is not supported if the slave repository data is not synchronized with the master repository data.

  You can initiate a forced failover by using the *Set-SmRepositoryConfig* cmdlet.

- When failover is initiated, jobs that are running might fail.

  If failover happens because MySQL Server or SnapCenter Server is down, then any jobs that are running might fail. After failing over to the second node, all subsequent jobs run successfully.

For information about configuring high availability, see How to configure NLB and ARR with SnapCenter.

Export SnapCenter certificates

Steps

1. Go to the Microsoft management console (MMC), and then click **File** > **Add/Remove Snap-in**.
2. In the Add or Remove Snap-ins window, select **Certificates** and then click **Add**.
3. In the Certificates snap-in window, select the **My user account** option, and then click **Finish**.
4. Click **Console Root** > **Certificates - Current User** > **Trusted Root Certification Authorities** > **Certificates**.
5. Right-click the certificate that has the SnapCenter Friendly Name, and then select **All Tasks** > **Export** to start the export wizard.
6. Complete the wizard, as follows:

In this wizard window…	Do the following…
Export Private Key	Select the option **Yes, export the private key**, and then click **Next**.
Export File Format	Make no changes; click **Next**.
Security	Specify the new password to be used for the exported certificate, and then click **Next**.
File to Export	Specify a file name for the exported certificate (you must use .pfx), and then click **Next**.
Completing the Certificate Export Wizard	Review the summary, and then click **Finish** to start the export.

Results

Certificates are exported in .pfx format.

Copyright Information

Copyright © 2022 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.