Maximize security

ONTAP 9

NetApp
May 08, 2021

This PDF was generated from https://docs.netapp.com/us-en/ontap/task_security_mfa_setup.html on May 08, 2021. Always check docs.netapp.com for the latest.

Table of Contents

Maximize security . . . 1
- Security overview for System Manager . . . 1
- Set up multifactor authentication . . . 2
- Control administrator access . . . 3
- Encrypt stored data using software-based encryption . . . 4
- Encrypt stored data using self-encrypting drives . . . 4
- Diagnose and correct file access issues . . . 5

Maximize security

The topics in this section show you how to manage cluster security with ONTAP System Manager in ONTAP 9.7 and later releases.

If you are using the ONTAP CLI to manage cluster security, see this content:

- Administrator Authentication and RBAC Power Guide
- Antivirus Configuration Guide
- NetApp Encryption Power Guide

If you are using legacy OnCommand System Manager for ONTAP 9.7 and earlier releases to manage cluster security, see the content for your ONTAP release:

- Cluster management using System Manager 9.6 and 9.7
- Cluster management using System Manager 9.5
- Cluster management using System Manager 9.3 and 9.4
- Cluster management using System Manager 9.2 and earlier

Security overview for System Manager

With System Manager, you use ONTAP standard methods to secure client and administrator access to storage and to protect against viruses. Advanced technologies are available for encryption of data at rest and for WORM storage.

Client authentication and authorization

ONTAP authenticates a client machine and user by verifying their identities with a trusted source. ONTAP authorizes a user to access a file or directory by comparing the user's credentials with the permissions configured on the file or directory.

Administrator authentication and RBAC

Administrators use local or remote login accounts to authenticate themselves to the cluster and storage VM. Role-Based Access Control (RBAC) determines the commands to which an administrator has access.

Virus scanning

You can use integrated antivirus functionality on the storage system to protect data from being compromised by viruses or other malicious code. ONTAP virus scanning, called *Vscan*, combines best-in-class third-party antivirus software with ONTAP features that give you the flexibility you need to control which files get scanned and when.

Encryption

ONTAP offers both software- and hardware-based encryption technologies for ensuring that data at rest cannot be read if the storage medium is repurposed, returned, misplaced, or stolen.

WORM storage

SnapLock is a high-performance compliance solution for organizations that use *write once*, *read many (WORM)* storage to retain critical files in unmodified form for regulatory and governance purposes.

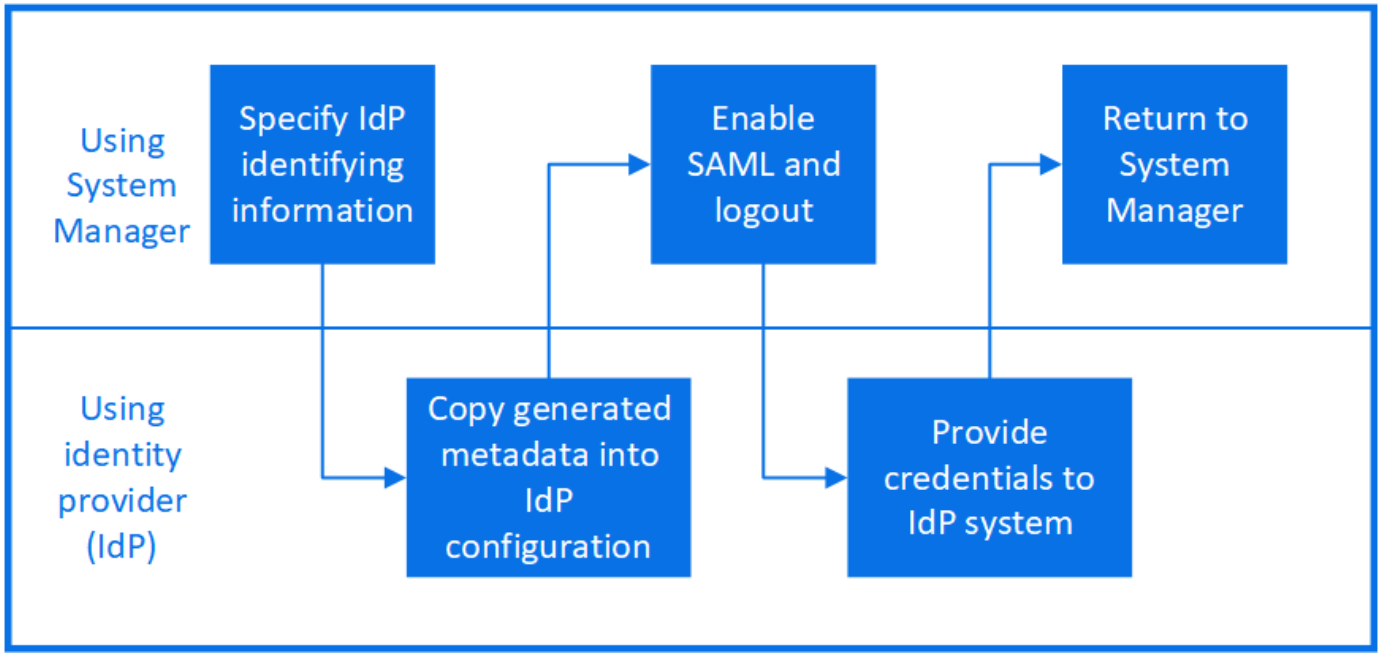
Set up multifactor authentication

Security Assertion Markup Language (SAML) authentication allows users to log in to an application by using a secure identity provider (IdP).

In System Manager, in addition to standard ONTAP authentication, SAML-based authentication is provided as an option for multifactor authentication.

Security Assertion Markup Language (SAML) is an XML-based framework for authentication and authorization between two entities: a service provider and an identity provider.

Enable SAML authentication



To enable SAML authentication, perform the following steps:

Steps

1. Click **Cluster > Settings**.
2. Next to **SAML Authentication**, click ⚙.
3. Ensure there is a check in the **Enable SAML Authentication** checkbox.
4. Enter the URL of the IdP URI (including "https://").
5. Modify the host system address, if needed.
6. Ensure the correct certificate is being used:
   - If your system was mapped with only one certificate with type "server", then that certificate is considered the default and it isn't displayed.

    - If your system was mapped with multiple certificates as type "server", then one of the certificates is displayed. To select a different certificate, click **Change**.
7. Click **Save**. A confirmation window displays the metadata information, which has been automatically copied to your clipboard.
8. Go to the IdP system you specified and copy the metadata from your clipboard to update the system metadata.
9. Return to the confirmation window (in System Manager) and check the checkbox **I have configured the IdP with the host URI or metadata**.
10. Click **Logout** to enable SAML-based authentication. The IdP system will display an authentication screen.
11. In the IdP system, enter your SAML-based credentials. After your credentials are verified, you will be directed to the System Manager home page.

Disable SAML authentication

To disable SAML authentication, perform the following steps:

Steps

1. Click **Cluster > Settings**.
2. Under **SAML Authentication**, click the **Enabled** toggle button.
3. *Optional*: You can also click ⚙ next to **SAML Authentication**, and then uncheck the **Enable SAML Authentication** checkbox.

Control administrator access

The role assigned to an administrator determines which functions the administrator can perform with System Manager. Predefined roles for cluster administrators and storage VM administrators are provided by System Manager. You assign the role when you create the administrator's account, or you can assign a different role later.

Depending on how you have enabled account access, you might need to perform any of the following:

- Associate a public key with a local account.
- Install a CA-signed server digital certificate.
- Configure AD, LDAP, or NIS access.

You can perform these tasks before or after enabling account access.

Assigning a role to an administrator

Assign a role to an administrator, as follows:

Steps

1. Click **Cluster > Settings**.
2. Click → next to **Users and Roles**.
3. Click + Add under **Users**.
4. Specify a user name, and select a role in the drop-down menu for **Role**.

5. Specify a login method and password for the user.

Changing an administrator's role

Change the role for an administrator, as follows:

Steps

1. Click **Cluster > Settings**.
2. Select the name of user whose role you want to change, then click the ⋮ that appears next to the user name.
3. Click **Edit**.
4. Select a role in the drop-down menu for **Role**.

Encrypt stored data using software-based encryption

Use volume encryption to ensure that volume data cannot be read if the underlying device is repurposed, returned, misplaced, or stolen. Volume encryption does not require special disks; it works with all HDDs and SSDs.

Volume encryption requires a key manager. You can configure the Onboard Key Manager using ONTAP System Manager. You can also use an external key manager, but you need to first set it up using the ONTAP CLI.

After the key manager is configured, new volumes are encrypted by default.

Steps

1. Click **Cluster > Settings**.
2. Under **Encryption**, click ⚙ to configure the Onboard Key Manager for the first time.
3. To encrypt existing volumes, click **Storage > Volumes**.
4. On the desired volume, click ⋮ and then click **Edit**.
5. Select **Enable encryption**.

Encrypt stored data using self-encrypting drives

Use disk encryption to ensure that all data in a local tier cannot be read if the underlying device is repurposed, returned, misplaced, or stolen. Disk encryption requires special self-encrypting HDDs or SSDs.

Disk encryption requires a key manager. You can configure the onboard key manager using ONTAP System Manager. You can also use an external key manager, but you need to first set it up using the ONTAP CLI.

If ONTAP detects self-encrypting disks, it prompts you to configure the onboard key manager when you create the local tier.

Steps

1. Under **Encryption**, click ⚙ to configure the onboard key manager.
2. If you see a message that disks need to be rekeyed, click ⋮, and then click **Rekey Disks**.

Diagnose and correct file access issues

Starting with ONTAP 9.8, you can trace file access permissions with System Manager to diagnose why clients cannot access files.

Steps

1. In ONTAP System Manager, select **Storage > Storage VMs**.
2. Select the storage VM on which you want to perform a trace.
3. Click **More**.
4. Click **Trace File Access**.
5. Provide the user name and client IP address, then click **Start Tracing**.

   The trace results are displayed in a table. The **Reasons** column provides the reason why a file could not be accessed.

6. Click in the left column of the results table to view the file access permissions.

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.