Abstract

This document covers multifactor authentication capability for administrative access introduced in NetApp® ONTAP® 9.3 software for NetApp OnCommand® System Manager and OnCommand Unified Manager and Secure Shell (SSH) CLI authentication.
TABLE OF CONTENTS

1 The Requirement for Strong Administrative Credentials ........................................ 3
   1.1 SAML-Based Web Interactive Login ............................................................... 3
   1.2 Secure Shell MFA Access: CLI Login ............................................................. 5

2 Terminology ........................................................................................................... 6

3 Configuration ......................................................................................................... 7
   3.1 ONTAP Secure Shell (SSH) ............................................................................ 7
   3.2 OnCommand System Manager ....................................................................... 8
   OnCommand Unified Manager ............................................................................. 15

4 Best Practices and Caveats ................................................................................... 23
   4.1 Ubiquitous MFA Implementation ................................................................. 23
   4.2 Migration from Single-Factor Authentication to MFA ................................. 24
   4.3 Migration from MFA to Single-Factor Authentication ................................. 25

5 Troubleshooting .................................................................................................... 25
   5.1 Common Problems ......................................................................................... 25
   5.2 Logs ................................................................................................................. 26

6 Disclaimer ............................................................................................................. 28

Where to Find Additional Information ..................................................................... 28
Version History ......................................................................................................... 28
Contact Us ................................................................................................................ 28

Table of Figures

Table 1) MFA methods ................................................................................................. 3
Figure 1) SAML workflow ........................................................................................ 4
Figure 2) SSH public-key authentication followed by password authentication workflow ................................................. 5
Figure 3) Unified Manager remote user definition .................................................... 23
Figure 4) ONTAP SPI log selection ......................................................................... 27
Figure 5) ONTAP SPI shibd.log files ...................................................................... 27
1 The Requirement for Strong Administrative Credentials

According to a 2017 Verizon investigative report on data breaches, 81% of data breaches involved weak or stolen credentials. New requirements from the United States public sector (USPS) and the Payment Card Industry Data Security Standard (PCI DSS) mandate strong administrative credentials for local and network access to privileged accounts and for network access to nonprivileged accounts. Specifically, multifactor authentication (MFA) mechanisms are required. MFA makes it impossible for an attacker to compromise an account using only username and password. MFA requires two or more independent factors to authenticate. An example of two-factor authentication is something a user possesses, such as a private key, and something a user knows, such as a password.

Beginning with NetApp® ONTAP® 9.3, NetApp is addressing this requirement for web authentication in NetApp OnCommand® System Manager and OnCommand Unified Manager, and for Secure Shell (SSH) CLI authentication in ONTAP.

Table 1) MFA methods.

<table>
<thead>
<tr>
<th>Application</th>
<th>MFA Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Shell ONTAP CLI</td>
<td>An ONTAP locally administered administrator account with chained primary and secondary authentication methods of password and publickey, or nsswitch and publickey.</td>
</tr>
<tr>
<td>System Manager ONTAP web user interface or Unified Manager web user interface</td>
<td>SAML 2.0, where ONTAP System Manager or Unified Manager is the service provider (SP) role and either ADFS or Shibboleth is the identity provider (IdP) role. The authentication factors are configured in the IdP.</td>
</tr>
</tbody>
</table>

1.1 SAML-Based Web Interactive Login

Security Assertion Markup Language (SAML) 2.0 is a widely adopted industry standard that allows any third-party SAML-compliant identity provider (IdP) to perform MFA using mechanisms unique to the IdP of the enterprise’s choosing and as a source of single sign-on (SSO).

There are three roles defined in the SAML specification: the principal, the IdP, and the service provider (SP). In the ONTAP implementation, a principal is the cluster administrator gaining access to ONTAP through System Manager or Unified Manager. The IdP is third-party IdP software from an organization such as Microsoft Active Directory Federated Services (ADFS) or the open-source Shibboleth IdP. The SP is the SAML capability built into ONTAP that is used by System Manager or the Unified Manager web application.
1. The administrator connects to a NetApp filer using either the OnCommand System Manager (OCSM) or OnCommand Unified Manager (OCUM) web GUI.
2. System Manager or Unified Manager looks up the configured IdP for the cluster.
3. System Manager or Unified Manager redirects the administrator's browser to the IdP.
4. The IdP prompts the administrator for credentials.
   The IdP is responsible for multiple authentication factors.
5. The IdP verifies the administrator’s credentials in AD.
6. The IdP issues a SAML assertion, and redirects the administrator’s web browser back to System Manager or Unified Manager.
7. System Manager or Unified Manager processes the SAML assertion, and then looks up the authorization role from its internal database.
8. The session is established and System Manager or Unified Manager returns a SAML session token to the administrator’s web browser in the Set-Cookie header.
   From this point on, the administrator is allowed access to System Manager or Unified Manager using a secure SAML token.
1.2 Secure Shell MFA Access: CLI Login

Before ONTAP 9.3, ONTAP supported SSH access through both password-based and public-key-based authentication independent of each other. With ONTAP 9.3, chained authentication is supported: a public-key authentication is followed by password authentication, thus providing two-factor authentication. This capability works only with ONTAP local accounts. The capability is enabled by second-authentication-method in the security login command.

Figure 2) SSH public-key authentication followed by password authentication workflow.

1. An SSH public/private key pair is generated for the administrator.
2. An SSH public key for the administrator is configured in ONTAP as a second authentication method.
3. The administrator invokes an SSH request to ONTAP.
4. Partial authentication is completed with presentation of the administrator public key.
5. ONTAP prompts the administrator for a password, and the administrator provides the password.
6. Full authentication is successful with two factors, and ONTAP presents a command shell.
2 Terminology

Active Directory Federation Service (ADFS). An identity provider developed by Microsoft. It can run on Windows Server operating systems to give users single sign-on access to systems and applications located across organizational boundaries.

Claim rules. Claim rules provide a mechanism for mapping IdP-defined attributes to a relying party. These attributes—such as a user ID or common name—are used by the relying party to map authorizations after IdP authentication.

Kerberos. A computer network authentication protocol that uses “tickets” to allow nodes communicating over a nonsecure network to prove their identity to one another in a secure manner.


Multifactor authentication (MFA). A method of computer access control in which a user is granted access only after successfully presenting several separate pieces of evidence to an authentication mechanism. These pieces of evidence are typically at least two of the following categories: knowledge (something they know—for example, password), possession (something they have—for example, smart card), and inherence (something they are—for example, retinal scan).

National Institute of Standards and Technology (NIST). A measurement standards laboratory and a nonregulatory agency of the U.S. Department of Commerce. Its mission is to promote innovation and industrial competitiveness.

Payment Card Industry Data Security Standard (PCI DSS). A proprietary information security standard for organizations that handle branded credit cards from the major card schemes. The PCI standard is mandated by the card brands and administered by the Payment Card Industry Security Standards Council. As of February 1, 2018, PCI DSS 3.2 started mandating MFA for all nonconsole access into the cardholder data environment (CDE) for personnel with administrative access.

Relying party. A system entity that bases an action on information from another system entity. A SAML relying party depends on receiving assertions from an asserting party (a SAML IdP) about a principal or user.

SAML service provider (SAML SP). Any application (either Unified Manager or System Manager) that wants to support MFA and offloads the authentication to an external entity (the identity provider).

SAML identity provider (SAML IdP). The external entity or service that handles authentication for the SP and redirects back to the SP on successful verification of the credentials (MFA or not). ADFS and Shibboleth IdP are examples of SAML IdPs.

SAML metadata. Determines how configuration information is defined and shared between two communicating entities. For instance, an entity’s support for given SAML bindings, identifier information, and PKI information can be defined.

Security Assertion Markup Language (SAML). An open standard for exchanging authentication and authorization data between parties—in particular, between an identity provider and a service provider. As its name implies, SAML is an XML-based markup language.

Secure Shell (SSH). A command-line cryptographic network protocol for operating network services securely over an unsecured network. SSH version 2 is used with NetApp ONTAP.

Shibboleth IdP. Shibboleth is an open-source project that provides single sign-on capabilities. It allows sites to make informed authorization decisions for individual access of protected online resources in a privacy-preserving manner.

Single sign-on (SSO). After a SAML IdP authentication, the IdP issues a SAML assertion, and redirects the administrator’s web browser back to System Manager or Unified Manager. System Manager or
Unified Manager processes the SAML assertion, and then looks up the authorization role from its internal database. The session is established, and System Manager or Unified Manager returns a SAML session token to the administrator’s web browser. The IdP is configured with a default lifetime of 2–8 hours for the secure SAML token. The lifetime is overridable by the relying-party-specific setting. The administrator is allowed access to System Manager or Unified Manager for the lifetime of the token.

**United States public sector (USPS).** As of December 2017, USPS government contractors who process, store, or transmit covered defense information (CDI) are required by Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7008 to comply with the 14 control families of the NIST SP 800-171. Under the “identification and authentication” control family, DFARS specifies use of MFA for local and network access to privileged accounts and for network access to nonprivileged accounts. The intention of the directive is to ensure that the safeguards implemented to protect CDI are consistent across nonfederal information systems as they relate to work contracted by the U.S. government.

### 3 Configuration

Configuration of MFA requires NetApp ONTAP 9.3 or later. For CLI access through SSH to ONTAP, local or NIS/LDAP accounts must be defined in ONTAP.

#### 3.1 ONTAP Secure Shell (SSH)

Existing single-factor authentication (1FA) administrator users can be modified to a two-factor authentication (2FA) login method. There are three methods with two combinations available. The three methods are *password, publickey, and nsswitch*. The two combinations are *password and publickey, or nsswitch and publickey*. You can specify either combination for -authentication-method or -second-authentication-method and produce the same result.

As an example, suppose the administrator *sam* is defined to use the *ssh* application with the password authentication method. To add public-key authentication as a second method, you would use the following command:

```
smrcluster-1:~> security login modify -user-or-group-name sam -application ssh -authentication-method password -second-authentication-method publickey
```

Warning: For successful authentication, ensure you create a public key for user "sam" using "security login publickey create" interface.

The warning message says that you must enter a public key for *sam* when adding publickey as the second authentication method. The Linux OpenSSH/OpenSSL command *ssh-keygen* is used to create an RSA public/private key pair for *sam*. In Linux, the key is stored in ~/.ssh/id_rsa.pub for *sam*. If *sam* is using the PuTTY client for SSH, you can use the puttygen utility to generate a public/private key pair for *sam*. For details on using *ssh-keygen* and puttygen, see “Where to Find Additional Information,” later in this document.

To enter *sam’s* public key in ONTAP from the output of *ssh-keygen* from a Linux system, use the following command:

```
smrcluster-1:~> security login publickey create -username sam -index 0 -publickey "ssh-rsa AAAAB3NzaC1yc2EAAAADQABAAAABQD9hsmgjshX4P3OxW8Qd+s1p2jW8K73m8ubYhvb+Alx4ZM9TQsmmYTffPjQO+BDpb6rugjjo88h1lWSVuxUW5xWxWURwYS/rQmHPI/2fudSncwd2cuRxMvNNKSmruF8ee2WRTJ07vU7fakrcFQL9cOhzh3dEHuFR5g0Gcr5nq5v83m2PAyoc7C4/uc91r8UQ4mbct6z6yBFxHtnGRCWgx20DF14pM9Lz93fIQQXCL8xKCrpCziobzH+4Dwug1gBFsrF5a7Kh3JfhtLAVqzhL5e4IHYr8xj3r1TVjysvZlg0/UGpwx5vnuBWE9EczWi6231F05fsUGHqQtCFn smr@cycrh6nbs05.eng.btc.netapp.com" -vserver smrcluster-1
```

Now *sam* can log in from his Linux system as an ONTAP administrator using chained 2FA. First, public-key authentication is performed (partial success). Then ONTAP prompts *sam* for a password, and the authentication is complete:
Note: This example shows a passphrase prompt for access to sam's private key. Linux SSH produces this prompt if a passphrase was applied during ssh-keygen. Although it is not necessary to enter a passphrase during ssh-keygen, it is a best practice, because it protects access to the private key.

The ONTAP command `security login modify -user-or-group-name sam -application ssh -authentication-method password -second-authentication-method publickey` specifies that `password` is the primary authentication method and `publickey` is the secondary authentication method. These methods can be reversed in the configuration. However, in a 2FA login, the order of authentication is always public key, then password, by means of either local password files or NIS/LDAP passwords.

For more details on SSH MFA authentication, see “Enabling SSH Multifactor Authentication” in the [Administrator Authentication and RBAC Power Guide](#).

### 3.2 OnCommand System Manager

**About System Manager**

If an ONTAP administrator prefers to use a graphical interface instead of the CLI for accessing and managing a cluster, use NetApp OnCommand System Manager, which is included with ONTAP as a web service, enabled by default, and accessible by using a browser. Point the browser to the host name if using DNS or the IPv4 or IPv6 address through `https://cluster-management-LIF`.

If the cluster uses a self-signed digital certificate, the browser might display a warning indicating that the certificate is not trusted. You can either acknowledge the risk to continue the access or install a certificate authority (CA) signed digital certificate on the cluster for server authentication.

Starting with ONTAP 9.3, SAML authentication is an option for System Manager.

**Enabling SAML Authentication for System Manager**

Unlike the SSH MFA configuration process, once activated, System Manager requires all existing administrators to authenticate through the SAML IdP. No changes are required to the cluster user accounts. When SAML authentication is enabled, a new authentication method of `saml` is added to existing users with administrator roles for `http` and `ontapi` applications.

After SAML authentication is enabled, additional new accounts requiring SAML IdP access should be defined in ONTAP with the administrator role, and the `saml` authentication method for `http` and `ontapi` applications. If SAML authentication is disabled at some point, these new accounts will require the password authentication method to be defined with the administrator role for `http` and `ontapi` applications and addition of the `console` application for local ONTAP authentication to System Manager.

After the SAML IdP is enabled, the IdP performs authentication for System Manager access by using methods available to the IdP, such as Lightweight Directory Access Protocol (LDAP), Active Directory (AD), Kerberos, password, and so on. The methods available are unique to the IdP. It is important that the accounts configured in ONTAP have user IDs that map to the IdP authentication methods.

IdPs that have been validated by NetApp are Microsoft ADFS and open-source Shibboleth IdP.
Before Getting Started

If your IdP is misconfigured after you enable SAML authentication in System Manager, you might not be able to log in to the System Manager web interface. To disable SAML authentication while remediating the IdP, you must access the Remote LAN Module (RLM) console. For details, see “Failure When Attempting to Enable SAML Authentication for System Manager” later in this document, in the “Troubleshooting” section.

Steps to Enable SAML Authentication for System Manager

1. Open System Manager using the cluster management interface (DNS name or IP address).
   https://cluster-mgmt-LIF

2. Authenticate using administrator credentials.
Click Configuration > Authentication.

3. Select the Enable SAML Authentication checkbox.
4. Configure System Manager to use IdP authentication:
   a. Enter the URI of the IdP.
   b. Enter the DNS name or IP address of the host system.
   c. Optional: If required, change the host system certificate to a CA-signed certificate.
5. Click Retrieve Host Metadata to retrieve the host URI and host metadata information.
6. Copy the host URI or host metadata details.
7. Click Save.
8. Click Save and Confirm. Ensure that you have copied the host URI or metadata to the IdP and done the trust configuration on the IdP server. (Refer to your IdP documentation.)

The IdP login window is displayed.
9. Log in to System Manager by using the IdP login window. (You might see a prompt from the IdP stating that you are about to share specific attributes with the ONTAP cluster. For successful login, you must allow sharing.)

After the SAML IdP authentication succeeds, the session has a lifetime configured in the IdP. For other service providers (SPs) that use the same IdP, this configuration allows the authentication to exist within the session lifetime period. If Unified Manager is one of the SPs service providers that uses the same IdP, access to Unified Manager is allowed without an additional authentication. Thus, SSO is enabled.
Steps to Disable SAML Authentication for System Manager
Open System Manager using the cluster management interface (DNS name or IP address) [https://cluster-mgmt-LIF](https://cluster-mgmt-LIF), authenticate through the IdP, and deselect the Enable SAML Authentication checkbox.
1. Click Save and respond Yes to the warning.

2. System Manager displays the login prompt.
**OnCommand Unified Manager**

**About Unified Manager**
Starting with NetApp ONTAP 9.3, SAML authentication is an option for Unified Manager 7.3.

**Enabling SAML Authentication for Unified Manager**

Unlike the SSH MFA configuration process (but like the System Manager configuration process), once activated, Unified Manager requires all existing remote users to authenticate through the SAML IdP. No changes are required to the Unified Manager remote user accounts. Local and maintenance users lose access when SAML authentication is activated. The Unified Manager maintenance console remains accessible. New accounts requiring SAML IdP access should be defined in Unified Manager as remote accounts. If the SAML IdP is disabled in Unified Manager, these new accounts require the credentials on the remote authentication system whether it is AD or LDAP.

After enabling the SAML IdP, the IdP performs authentication for Unified Manager access by using methods available to the IdP, such as LDAP, AD, Kerberos, password, and so on. The methods available are unique to the IdP deployed.

**Before Getting Started**

If your IdP is misconfigured after you enable SAML authentication in Unified Manager, you might not be able to log in to the Unified Manager web interface. To disable SAML authentication while remediating the IdP, you must access the Unified Manager maintenance console by using SSH. For details, refer to the “Failure When Attempting to Enable SAML Authentication for Unified Manager” section later in this document, in the “Troubleshooting” section.

**Steps to Enable SAML Authentication for Unified Manager**

1. Ensure that you have network connectivity between Unified Manager, the IdP, and Unified Manager web clients.
2. Launch the Unified Manager web GUI.
3. Authenticate using maintenance user credentials.
4. In the upper-right toolbar, click the gear icon and select Authentication in the left Setup menu.
5. If you haven’t enabled remote authentication, you must do so for SAML IdP users to have access to Unified Manager:
   a. Select the Enable Remote Authentication checkbox.
   b. Set the authentication service to Active Directory or OpenLDAP (Microsoft Lightweight Directory Services is not supported).
   c. Enter the administrator name and password. For AD, specify Base Distinguished Name; for LDAP, specify Bind Distinguished Name, Bind Password, and Base Distinguished Name.
   d. In the Authentication Servers section, enter the authentication server’s DNS name or IP address.
   e. Use Test Authentication to ensure that Remote Authentication Settings are operational.
f. Navigate to the Settings > Management > Users Page and add users of type remote user or remote group with the OnCommand administrator role.

7. Click View Host Metadata, copy the metadata into a file, and save it. This file will be used to configure Unified Manager in the IdP.

8. Select the Enable SAML Authentication checkbox, enter the IdP URL, and click Fetch IdP Metadata to populate Unified Manager with the IdP data.
9. Click Save and Yes in the warning dialog box.

10. Wait 5 minutes for the Unified Manager services to restart.

11. Configure the IdP (refer to your IdP documentation).
   a. Populate the IdP with the Unified Manager metadata from step 7.
   b. Add Unified Manager as a Relying Party.
c. Add claim rules. Set Name to `urn:oid:0.9.2342.19200300.100.1.1` and Unqualified Name to `urn:oid:1.3.6.1.4.1.5923.1.5.1.1`.

12. Launch the Unified Manager web GUI.

13. Authenticate using a remote user defined in step 5f.

As in the System Manager section, after the SAML IdP authentication succeeds, the session has a lifetime configured in the IdP. For other SPs that use the same IdP, this allows the authentication to exist within the session lifetime period. If System Manager is one of the SPs that uses the same IdP, access to System Manager is allowed without an additional authentication after a successful Unified Manager authentication.

**Steps to Disable SAML Authentication for Unified Manager**

1. Launch the Unified Manager web GUI, authenticate through the IdP, and deselect the Enable SAML Authentication checkbox. Click the gear icon and select Authentication.
2. Click Save and respond Yes to the warning.

3. Wait 5 minutes for the Unified Manager services to restart.

4. Launch the Unified Manager web GUI.
4 Best Practices and Caveats

4.1 Ubiquitous MFA Implementation

NetApp ONTAP 9.3 SSH MFA allows user-by-user incremental implementation. Although this is useful for a gradual incremental deployment, the end goal of an MFA deployment must be for all administrative users to use login credentials with strong multifactor authentication.

In addition to having MFA login credentials for all users, each administrator’s mode of access should use MFA. For ONTAP, this implies SSH CLI and SAML for System Manager HTTP access. For a user sam, the following login configuration would need to be in place:

```
ontap9-tme-8040::* security login show sam
Vserver: ontp9-tme-8040
```

<table>
<thead>
<tr>
<th>User/Group Name</th>
<th>Application</th>
<th>Authentication Method</th>
<th>Role Name</th>
<th>Locked Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>sam</td>
<td>console</td>
<td>password</td>
<td>admin</td>
<td>no</td>
</tr>
<tr>
<td>sam</td>
<td>http</td>
<td>password</td>
<td>admin</td>
<td>no</td>
</tr>
<tr>
<td>sam</td>
<td>http</td>
<td>saml</td>
<td>admin</td>
<td>none</td>
</tr>
<tr>
<td>sam</td>
<td>ontp</td>
<td>password</td>
<td>admin</td>
<td>none</td>
</tr>
<tr>
<td>sam</td>
<td>ontp</td>
<td>saml</td>
<td>admin</td>
<td>none</td>
</tr>
<tr>
<td>sam</td>
<td>ssh</td>
<td>password</td>
<td>admin</td>
<td>publickey</td>
</tr>
</tbody>
</table>

6 entries were displayed.

**Note:** After SAML authentication is configured for the http and ontp applications, the password authentication method does not need to be configured. They remain configured for administrator accounts to enable external supportability tools to continue administrator access with single-factor user ID/password authentication. If no such tools require user ID/password access, delete all password authentication methods for all administrator accounts for http and ontp applications to provide the most secure administrative access environment.

For Unified Manager SAML authentication, sam would need to be defined as a remote user with a role of OnCommand administrator.

Figure 3) Unified Manager remote user definition.

**Note:** Before Unified Manager SAML authentication configuration, sam would have been authenticated by either AD or OpenLDAP. After SAML authentication is enabled, sam is authenticated only by the SAML IdP.
4.2 Migration from Single-Factor Authentication to MFA

SSH CLI
If there is only one ONTAP administrator account, create at least a second local single-factor authentication account in case something goes wrong with the migration of your primary account. If the starting state of ONTAP login accounts uses local SSH password or public-key authentication methods, migrate from single-factor to two-factor authentication by using the command `security login modify -user-or-group-name [username] -application ssh -second-authentication-method [password or publickey]. If the new second factor is publickey, associate a public key with the user by using the command `security login publickey create -vserver [SVM_name] -username [username] -index [index_number] -publickey "[public_key_data]".

If the starting state of ONTAP login accounts uses the remote NIS/LDAP `nsswitch` SSH authentication method, migrate from single-factor to two-factor authentication by using the command `security login modify -user-or-group-name [username] -application ssh -authentication-method nsswitch -second-authentication-method publickey`. Then associate a public key with the user by using the command `security login publickey create -vserver [SVM_name] -username [username] -index [index_number] -publickey "[public_key_data]".

Note: Two-factor authentication for `nsswitch` group users (security login create ... -is-nsswitch-group=yes) is not supported.

If the starting states of ONTAP administrator login accounts are domain (AD), the accounts must be deleted and re-added to local SSH account `publickey` and `password`, or `publickey` and `nsswitch` authentication methods. If you don’t delete remote `domain` accounts and create a local two-factor authentication account, logins can fail because of password conflicts if they are different from the local and remote login definitions.

Note: In a future release of ONTAP, enablement of local and remote login accounts will be mutually exclusive.

System Manager and Unified Manager SAML Authentication
Although SAML authentication in System Manager and Unified Manager is similar, the activation and implementation of the SAML IdP is different.

Enabling SAML authentication on System Manager automatically adds a new authentication method of `saml` for existing users with administrator roles for `http` and `ontapi` applications. At that point, the authentication methods deployed by the IdP for System Manager are in effect. The local password, domain, or `nsswitch` (AD or LDAP/NIS) is longer in effect.

Enabling SAML authentication on Unified Manager automatically enables all remote users defined in Unified Manager to authenticate by using methods deployed in the IdP. Remote authentication methods of AD or LDAP will no longer be in effect.

It is possible that AD or LDAP is one of the factors in the IdP implementation. If other factors are deployed, they should be implemented for each administrator user. There can be a broad range of factors. The most commonly used factors are username/password, public key, and a variety of attributes that can be verified, such as group, role, IP address, and email address.

For more details, refer to the ADFS and Shibboleth IdP links in “Where to Find Additional Information,” later in this document.

IdP Availability Considerations
As with remote authentication mechanisms such as AD or LDAP, after enabling SAML authentication, continuation of connectivity to the IdP and continuous uptime of the IdP function become critical.
Configuration of redundant, highly available IdP configurations is necessary to ensure availability to administrative access for System Manager and Unified Manager.

Since ADFS and Shibboleth are architecturally unique, the approaches to creating high-availability configurations are also unique. ADFS can create a federation server farm by using SQL Server to replicate data between servers in diverse locations. Shibboleth’s recommended approach for high availability is to create a cluster that replicates stateful data between Shibboleth nodes by using either software or hardware load-balancing mechanisms.

For more details, refer to the ADFS and Shibboleth IdP links in “Where to Find Additional Information,” later in this document.

4.3 Migration from MFA to Single-Factor Authentication

SSH CLI

To revert to single-factor authentication for ONTAP SSH local accounts, use the command `security login modify -user-or-group-name [username] -application ssh -second-authentication-method none` to remove the second factor for each administrator user. If the second factor was publickey, the public key associated with that administrator user is deleted.

System Manager or Unified Manager SAML Authentication

To disable MFA for System Manager or Unified Manager, deselect Enable SAML Authentication on the respective SAML Authentication webpage. For details on disabling SAML authentication for System Manager or Unified Manager, refer to the “Configuration” section, earlier in this document.

After disabling SAML authentication on System Manager, the function is disabled in ONTAP. However, SAML authentication methods remain in `security login administrator` configurations for http and ontapi applications.

Disabling SAML authentication on Unified Manager reverts remote users back to either LDAP or AD authentication as configured in the Unified Manager remote authentication.

5 Troubleshooting

5.1 Common Problems

Failure When Attempting to Enable SAML Authentication for System Manager

If you enable SAML authentication and the IdP is misconfigured, administrative users will not be able to log in to System Manager. You will not be able to disable SAML from the cluster management LIF; you must disable SAML from the RLM console.

```
tonap9-tme-8040::> security saml-sp show
    Identity Provider URI: https://centos7.ntap2016.local:8443/idp/shibboleth
    Service Provider Host: ontap9-tme-8040.NTAP2016.LOCAL
    Certificate Authority: ontap9-tme-8040
    Certificate Serial: 054D9DDD623882
    Common Name: ontap9-tme-8040
    Is SAML Enabled: true
ntonap9-tme-8040::> security saml-sp modify -is-enabled false
Error: command failed: SAML authentication can only be disabled from the "console" application or from a SAML authenticated application.
```
You can then log in to System Manager, remediate IdP issues, and reenable SAML authentication.

### Failure When Attempting to Enable SAML Authentication for Unified Manager

If you enable SAML authentication and the IdP is misconfigured, you will not be able to log in to Unified Manager as a local or remote user. You must use SSH to access the Unified Manager maintenance console with the maintenance user’s credentials and select the menu item to disable SAML authentication.

<table>
<thead>
<tr>
<th>Main Menu</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 ) Upgrade (Disabled. Must be run on virtual machine console.)</td>
</tr>
<tr>
<td>2 ) Network Configuration</td>
</tr>
<tr>
<td>3 ) System Configuration</td>
</tr>
<tr>
<td>4 ) Support/Diagnostics</td>
</tr>
<tr>
<td>5 ) Reset Server Certificate</td>
</tr>
<tr>
<td>6 ) External Data Provider</td>
</tr>
<tr>
<td>7 ) Performance Polling Interval Configuration</td>
</tr>
<tr>
<td>8 ) Migrate Data from OnCommand Performance Manager 7.1</td>
</tr>
<tr>
<td>9 ) Disable SAML authentication</td>
</tr>
<tr>
<td>x ) Exit</td>
</tr>
</tbody>
</table>

You can then log in to Unified Manager, remediate IdP issues, and reenable SAML authentication.

### 5.2 Logs

The `shibd.log` file provides valuable information for debugging IdP implementation issues. In NetApp ONTAP, `shibd.log` is accessible through the service processor interface (SPI) node management logs.
Figure 4) ONTAP SPI log selection.

Figure 5) ONTAP SPI shibd.log files.

Note: In the Shibboleth IdP, there is an analogous log: /opt/shibboleth-idp/logs/idp-process.log.
6 Disclaimer

NetApp provides no representations or warranties regarding the accuracy, reliability, or serviceability of any information or recommendations provided in this publication, or with respect to any results that may be obtained by the use of the information or observance of any recommendations provided herein. The information in this document is distributed AS IS, and the use of this information or the implementation of any recommendations or techniques herein is a customer’s responsibility and depends on the customer’s ability to evaluate and integrate them into the customer’s operational environment. This document and the information contained herein may be used solely in connection with the NetApp products discussed in this document.

Where to Find Additional Information

The following references were used in this technical report:

- NIST Special Publication 800-171: Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations
- PCI DSS 3.2 Resource Guide
- Administrator Authentication and RBAC Power Guide
- ssh-keygen
- Generate RSA Keys with SSH by Using PuTTYgen
- Active Directory Federation Services (ADFS)
- Shibboleth IdP wiki
- Verizon 2017 data breach investigations report

Version History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Document Version History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 1.0</td>
<td>November 2017</td>
<td>Initial Release: Dan Tulledge</td>
</tr>
<tr>
<td>Version 1.1</td>
<td>March 2018</td>
<td>Dan Tulledge: 9.4 update</td>
</tr>
</tbody>
</table>

Contact Us

Let us know how we can improve this technical report. Contact us at docfeedback@netapp.com. Include TECHNICAL REPORT TR-4647 in the subject line.
Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

Copyright Information

Copyright © 1994–2017 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.