Concepts

SANtricity 11.8

NetApp
April 05, 2024

Table of Contents

Concepts

How Access Management works

Use Access Management to establish user authentication in Unified Manager.

Configuration workflow

Access Management configuration works as follows:

1. An administrator logs in to Unified Manager with a user profile that includes Security admin permissions.

   For first-time login, the username `admin` is automatically displayed and cannot be changed. The `admin` user has full access to all functions in the system. The password must be set on first-time login.

2. The administrator navigates to Access Management in the user interface, which includes pre-configured local user roles. These roles are an implementation of RBAC (role-based access control) capabilities.
3. The administrator configures one or more of the following authentication methods:
   - **Local user roles** — Authentication is managed through RBAC capabilities. Local user roles include pre-defined users and roles with specific access permissions. Administrators can use these local user roles as the single method of authentication, or use them in combination with a directory service. No configuration is necessary, other than setting passwords for users.
   - **Directory services** — Authentication is managed through an LDAP (Lightweight Directory Access Protocol) server and directory service, such as Microsoft's Active Directory. An administrator connects to the LDAP server, and then maps the LDAP users to the local user roles.
   - **SAML** — Authentication is managed through an Identity Provider (IdP) using the Security Assertion Markup Language (SAML) 2.0. An administrator establishes communication between the IdP system and the storage array, and then maps IdP users to the local user roles embedded in the storage array.
4. The administrator provides users with login credentials for Unified Manager.
5. Users log in to the system by entering their credentials. During login, the system performs the following background tasks:
   - Authenticates the user name and password against the user account.
   - Determines the user's permissions based on the assigned roles.
   - Provides the user with access to functions in the user interface.
   - Displays the user name in the top banner.

Functions available in Unified Manager

Access to functions depends on a user's assigned roles, which include the following:

- **Storage admin** — Full read/write access to storage objects on the arrays, but no access to the security configuration.
- **Security admin** — Access to the security configuration in Access Management and Certificate Management.
- **Support admin** — Access to all hardware resources on storage arrays, failure data, and MEL events. No

access to storage objects or the security configuration.

- **Monitor** — Read-only access to all storage objects, but no access to the security configuration.

An unavailable function is either grayed out or does not display in the user interface.

Access Management terminology

Learn how the Access Management terms apply to Unified Manager.

Term	Description
Active Directory	Active Directory (AD) is a Microsoft directory service that uses LDAP for Windows domain networks.
Binding	Bind operations are used to authenticate clients to the directory server. Binding usually requires account and password credentials, but some servers allow for anonymous bind operations.
CA	A certificate authority (CA) is a trusted entity that issues electronic documents, called digital certificates, for Internet security. These certificates identify website owners, which allows for secure connections between clients and servers.
Certificate	A certificate identifies the owner of a site for security purposes, which prevents attackers from impersonating the site. The certificate contains information about the site owner and the identity of the trusted entity who certifies (signs) this information.
LDAP	Lightweight Directory Access Protocol (LDAP) is an application protocol for accessing and maintaining distributed directory information services. This protocol allows many different applications and services to connect to the LDAP server for validating users.
RBAC	Role-based access control (RBAC) is a method of regulating access to computer or network resources based on the roles of individual users. Unified Manager includes predefined roles.
SAML	Security Assertion Markup Language (SAML) is an XML-based standard for authentication and authorization between two entities. SAML allows for multi-factor authentication, in which users must provide two or more items for proving their identity (for example, a password and fingerprint). The storage array's embedded SAML feature is SAML2.0 compliant for identity assertion, authentication, and authorization.
SSO	Single sign-on (SSO) is an authentication service that allows for one set of login credentials to access multiple applications.

Term	Description
Web Services Proxy	The Web Services Proxy, which provides access through standard HTTPS mechanisms, allows administrators to configure management services for storage arrays. The proxy can be installed on Windows or Linux hosts. The Unified Manager interface is available with the Web Services Proxy.

Permissions for mapped roles

The RBAC (role-based access control) capabilities include pre-defined users with one or more roles mapped to them. Each role includes permissions for accessing tasks in Unified Manager.

The roles provide user access to tasks, as follows:

- **Storage admin** — Full read/write access to storage objects on the arrays, but no access to the security configuration.
- **Security admin** — Access to the security configuration in Access Management and Certificate Management.
- **Support admin** — Access to all hardware resources on storage arrays, failure data, and MEL events. No access to storage objects or the security configuration.
- **Monitor** — Read-only access to all storage objects, but no access to the security configuration.

If a user does not have permissions for a certain function, that function is either unavailable for selection or does not display in the user interface.

Access Management with local user roles

Administrators can use RBAC (role-based access control) capabilities enforced in Unified Manager. These capabilities are referred to as "local user roles."

Configuration workflow

Local user roles are pre-configured in the system. To use local user roles for authentication, administrators can do the following:

1. An administrator logs in to Unified Manager with a user profile that includes Security admin permissions.

   The `admin` user has full access to all functions in the system.

2. An administrator reviews the user profiles, which are predefined and cannot be modified.
3. Optionally, the administrator assigns new passwords for each user profile.
4. Users log in to the system with their assigned credentials.

Management

When using only local user roles for authentication, administrators can perform the following management tasks:

- Change passwords.
- Set a minimum length for passwords.
- Allow users to log in without passwords.

Access Management with directory services

Administrators can use an LDAP (Lightweight Directory Access Protocol) server and a directory service, such as Microsoft's Active Directory.

Configuration workflow

If an LDAP server and directory service are used in the network, configuration works as follows:

1. An administrator logs in to Unified Manager with a user profile that includes Security admin permissions.

   The `admin` user has full access to all functions in the system.

2. The administrator enters the configuration settings for the LDAP server. Settings include the domain name, URL, and Bind account information.
3. If the LDAP server uses a secure protocol (LDAPS), the administrator uploads a certificate authority (CA) certificate chain for authentication between the LDAP server and the host system where the Web Services Proxy is installed.
4. After the server connection is established, the administrator maps the user groups to the local user roles. These roles are predefined and cannot be modified.
5. The administrator tests the connection between the LDAP server and the Web Services Proxy.
6. Users log in to the system with their assigned LDAP/Directory Services credentials.

Management

When using directory services for authentication, administrators can perform the following management tasks:

- Add a directory server.
- Edit directory server settings.
- Map LDAP users to local user roles.
- Remove a directory server.
- Change passwords.
- Set a minimum length for passwords.
- Allow users to log in without passwords.

Access Management with SAML

For Access Management, administrators can use the Security Assertion Markup Language (SAML) 2.0 capabilities embedded in the array.

Configuration workflow

SAML configuration works as follows:

1. An administrator logs in to Unified Manager with a user profile that includes Security Admin permissions.

   The `admin` user has full access to all functions in System Manager.

2. The administrator goes to the **SAML** tab under Access Management.
3. An administrator configures communications with the Identity Provider (IdP). An IdP is an external system used to request credentials from a user and determine if the user is successfully authenticated. To configure communications with the storage array, the administrator downloads the IdP metadata file from the IdP system, and then uses Unified Manager to upload the file to the storage array.
4. An administrator establishes a trust relationship between the Service Provider and the IdP. A Service Provider controls user authorization; in this case, the controller in the storage array acts as the Service Provider. To configure communications, the administrator uses Unified Manager to export a Service Provider metadata file for the controller. From the IdP system, the administrator then imports the metadata file to the IdP.

   Administrators should also make sure that the IdP supports the ability to return a Name ID on authentication.

5. The administrator maps the storage array's roles to user attributes defined in the IdP. To do this, the administrator uses Unified Manager to create the mappings.
6. The administrator tests the SSO login to the IdP URL. This test ensures the storage array and IdP can communicate.

   Once SAML is enabled, you *cannot* disable it through the user interface, nor can you edit the IdP settings. If you need to disable or edit the SAML configuration, contact Technical Support for assistance.

7. From Unified Manager, the administrator enables SAML for the storage array.
8. Users log in to the system with their SSO credentials.

Management

When using SAML for authentication, administrators can perform the following management tasks:

- Modify or create new role mappings
- Export Service Provider files

Access restrictions

When SAML is enabled, users cannot discover or manage storage for that array from the legacy Storage Manager interface.

In addition, the following clients cannot access storage array services and resources:

- Enterprise Management Window (EMW)
- Command-line interface (CLI)

- Software Developer Kits (SDK) clients
- In-band clients
- HTTP Basic Authentication REST API clients
- Login using standard REST API endpoint

Copyright information

Trademark information