概念
SANtricity 11.8

NetApp
December 16, 2024

目錄

概念

存取管理的運作方式

使用Access Management在Unified Manager中建立使用者驗證。

組態工作流程

存取管理組態的運作方式如下：

1. 系統管理員使用包含安全管理員權限的使用者設定檔登入Unified Manager。

   首次登入時，系統會自動顯示使用者名稱 `admin`，且無法變更。 `admin`使用者可完全存取系統中的所有功能。首次登入時必須設定密碼。

2. 系統管理員會在使用者介面中導覽至「存取管理」、其中包含預先設定的本機使用者角色。這些角色是RBAC（角色型存取控制）功能的實作。
3. 系統管理員可設定下列一或多種驗證方法：
   - 本機使用者角色-驗證是透過RBAC功能來管理。本機使用者角色包括具有特定存取權限的預先定義使用者和角色。系統管理員可以使用這些本機使用者角色做為單一驗證方法、或搭配目錄服務使用。除了為使用者設定密碼之外、不需要進行任何組態。
   - 目錄服務-驗證是透過LDAP（輕量型目錄存取傳輸協定）伺服器和目錄服務（例如Microsoft的Active Directory）來管理。系統管理員會連線至LDAP伺服器、然後將LDAP使用者對應至本機使用者角色。
   - * SAML *-驗證是透過身分識別供應商（IDP）、使用安全聲明標記語言（SAML）2.0來管理。系統管理員會在IDP系統與儲存陣列之間建立通訊、然後將IDP使用者對應至儲存陣列內嵌的本機使用者角色。
4. 系統管理員可為使用者提供Unified Manager的登入認證。
5. 使用者輸入認證資料以登入系統。登入期間、系統會執行下列背景工作：
   - 根據使用者帳戶驗證使用者名稱和密碼。
   - 根據指派的角色來決定使用者的權限。
   - 讓使用者能夠存取使用者介面中的功能。
   - 在上方橫幅中顯示使用者名稱。

Unified Manager提供的功能

存取功能取決於使用者指派的角色、包括下列項目：

- 儲存設備管理-完整讀寫陣列上的儲存物件存取權、但無法存取安全性組態。
- 安全管理：存取存取管理與憑證管理中的安全性組態。
- 支援**admin**：存取儲存陣列、故障資料及MEL事件上的所有硬體資源。無法存取儲存物件或安全性組態。
- 監控-對所有儲存物件的唯讀存取、但無法存取安全性組態。

無法使用的功能會呈現灰色、或不會顯示在使用者介面中。

存取管理術語

瞭解存取管理條款如何適用於Unified Manager。

期限	說明
Active Directory	Active Directory（AD）是一項Microsoft目錄服務、用於Windows網域網路的LDAP。
連結	連結作業用於驗證目錄伺服器的用戶端。綁定通常需要帳戶和密碼認證、但有些伺服器允許匿名連結作業。
CA	憑證授權單位（CA）是信任的實體、可發行稱為數位憑證的電子文件、以確保網際網路安全。這些憑證可識別網站擁有者、以便在用戶端與伺服器之間進行安全連線。
憑證	憑證可識別站台的擁有者、以確保安全性、防止攻擊者模擬站台。憑證包含網站擁有者的相關資訊、以及認證（簽署）此資訊的信任實體身分。
LDAP	輕量型目錄存取傳輸協定（LDAP）是用於存取及維護分散式目錄資訊服務的應用程式傳輸協定。此傳輸協定可讓許多不同的應用程式和服務連線至LDAP伺服器、以驗證使用者。
RBAC	角色型存取控制（RBAC）是一種根據個別使用者角色來管理電腦或網路資源存取的方法。Unified Manager包含預先定義的角色。
SAML	安全聲明標記語言（SAML）是兩個實體之間驗證與授權的XML型標準。SAML允許多因素驗證、使用者必須提供兩個或多個項目來證明身分（例如密碼和指紋）。儲存陣列的內嵌 SAML 功能符合 SAML2.0 標準、可用於識別聲明、驗證及授權。
SSO	單一登入（SSO）是一種驗證服務、可讓一組登入認證資料存取多個應用程式。
Web服務Proxy	Web服務Proxy可透過標準HTTPS機制提供存取、讓系統管理員能夠設定儲存陣列的管理服務。Proxy可安裝在Windows或Linux主機上。Unified Manager介面可與Web Services Proxy搭配使用。

對應角色的權限

RBAC（角色型存取控制）功能包括預先定義的使用者、其中有一或多個角色對應至他們。每個角色都包含存取Unified Manager工作的權限。

這些角色可讓使用者存取工作、如下所示：

- 儲存設備管理-完整讀寫陣列上的儲存物件存取權、但無法存取安全性組態。
- 安全管理：存取存取管理與憑證管理中的安全性組態。
- 支援**admin**：存取儲存陣列、故障資料及MEL事件上的所有硬體資源。無法存取儲存物件或安全性組態。

- 監控-對所有儲存物件的唯讀存取、但無法存取安全性組態。

如果使用者沒有特定功能的權限、則該功能可能無法選取、或不會顯示在使用者介面中。

具有本機使用者角色的存取管理

系統管理員可以使用Unified Manager中強制執行的RBAC（角色型存取控制）功能。這些功能稱為「本機使用者角色」。

組態工作流程

本機使用者角色是在系統中預先設定的。若要使用本機使用者角色進行驗證、系統管理員可以執行下列動作：

1. 系統管理員使用包含安全管理員權限的使用者設定檔登入Unified Manager。

> `admin`使用者可完全存取系統中的所有功能。

2. 系統管理員會檢閱預先定義且無法修改的使用者設定檔。
3. 系統管理員也可以為每個使用者設定檔指派新密碼。
4. 使用者使用指派的認證登入系統。

管理

只使用本機使用者角色進行驗證時、系統管理員可以執行下列管理工作：

- 變更密碼。
- 設定密碼的最小長度。
- 允許使用者不使用密碼登入。

使用目錄服務進行存取管理

系統管理員可以使用LDAP（輕量型目錄存取傳輸協定）伺服器和目錄服務、例如Microsoft的Active Directory。

組態工作流程

如果在網路中使用LDAP伺服器和目錄服務、則組態作業如下：

1. 系統管理員使用包含安全管理員權限的使用者設定檔登入Unified Manager。

> `admin`使用者可完全存取系統中的所有功能。

2. 系統管理員會輸入LDAP伺服器的組態設定。設定包括網域名稱、URL及連結帳戶資訊。
3. 如果LDAP伺服器使用安全傳輸協定（LDAPS）、則系統管理員會在LDAP伺服器和安裝Web服務Proxy的主機系統之間、上傳憑證授權單位（CA）憑證鏈結進行驗證。
4. 建立伺服器連線之後、系統管理員會將使用者群組對應至本機使用者角色。這些角色已預先定義、無法修改。
5. 系統管理員會測試LDAP伺服器與Web服務Proxy之間的連線。
6. 使用者使用指派的LDAP/Directory Services認證登入系統。

管理

使用目錄服務進行驗證時、系統管理員可以執行下列管理工作：

- 新增目錄伺服器。
- 編輯目錄伺服器設定。
- 將LDAP使用者對應至本機使用者角色。
- 移除目錄伺服器。
- 變更密碼。
- 設定密碼的最小長度。
- 允許使用者不使用密碼登入。

使用SAML進行存取管理

對於存取管理、系統管理員可以使用陣列內嵌的安全聲明標記語言（SAML）2.0功能。

組態工作流程

SAML組態運作方式如下：

1. 系統管理員使用包含安全管理員權限的使用者設定檔登入 Unified Manager 。

> `admin`使用者可完全存取 `System Manager` 中的所有功能。

2. 系統管理員會移至「存取管理」下的「* SAML」索引標籤。
3. 系統管理員會設定與身分識別供應商（IDP）的通訊。IDP是一種外部系統、用於向使用者要求認證、並判斷使用者是否已成功驗證。若要設定與儲存陣列的通訊、管理員會從 IDP 系統下載 IDP 中繼資料檔案、然後使用 Unified Manager 將檔案上傳至儲存陣列。
4. 系統管理員會在服務供應商與IDP之間建立信任關係。服務供應商會控制使用者授權；在此情況下、儲存陣列中的控制器會扮演服務供應商的角色。若要設定通訊、管理員可使用 Unified Manager 匯出控制器的服務供應商中繼資料檔案。接著、系統管理員會從 IDP 系統將中繼資料檔案匯入 IDP 。

> 系統管理員也應確保IDP支援在驗證時傳回名稱ID的功能。

5. 系統管理員會將儲存陣列的角色對應至IDP中定義的使用者屬性。為達此目的、管理員使用 Unified Manager 來建立對應。
6. 系統管理員會測試SSO登入IDP URL。此測試可確保儲存陣列與IDP之間的通訊。

> 一旦啟用SAML、您就無法透過使用者介面停用SAML、也無法編輯IDP設定。如果您需要停用或編輯SAML組態、請聯絡技術支援部門以取得協助。

7. 從 Unified Manager 、系統管理員可為儲存陣列啟用 SAML 。
8. 使用者使用SSO認證登入系統。

管理

使用SAML進行驗證時、系統管理員可以執行下列管理工作：

- 修改或建立新的角色對應
- 匯出服務供應商檔案

存取限制

啟用 SAML 時、使用者無法從舊版 Storage Manager 介面探索或管理該陣列的儲存設備。

此外、下列用戶端無法存取儲存陣列服務和資源：

- 企業管理所需時間（EMW）
- 命令列介面（CLI）
- 軟體開發人員套件（SDK）用戶端
- 頻內用戶端
- HTTP基本驗證REST API用戶端
- 使用標準REST API端點登入