



存取管理 SANtricity 11.6

NetApp
February 12, 2024

This PDF was generated from <https://docs.netapp.com/zh-tw/e-series-santricity-116/um-certificates/how-access-management-works-unified.html> on February 12, 2024. Always check docs.netapp.com for the latest.

目錄

- 存取管理 1
 - 概念 1
 - 使用方法 4
 - 常見問題集 11

存取管理

概念

存取管理的運作方式

使用存取管理功能、在SANtricity 《統一化管理程式》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、使用者名稱「admin」會自動顯示、無法變更。「admin」使用者可完整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 and 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。
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套用SANtricity 至《統一化管理程式》。

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。
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SANtricity 功能、可在「統一化管理程式」中存取工作。

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SANtricity 在NetApp 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」使用者可完整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. *選用：*系統管理員會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 and 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SANtricity 使用包含安全管理員權限的使用者設定檔登入到NetApp的《統一化管理程式》。



「admin」使用者可完整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。

使用方法

檢視本機使用者角色

從本機使用者角色索引標籤、您可以檢視使用者與預設角色之間的對應。這些對應是在Web Services Proxy for SANtricity the Unified Manager中強制執行的RBAC（角色型存取控制）的一部分。

開始之前

- 您必須以包含安全管理員權限的使用者設定檔登入。否則、就不會顯示存取管理功能。

關於這項工作

無法變更使用者和對應。只能修改密碼。

步驟

1. 選擇*存取管理*。
2. 選取*本機使用者角色*索引標籤。

下表顯示使用者：

- 管理：擁有系統中所有功能存取權的超級管理員。此使用者包含所有角色。
- 儲存設備：負責所有儲存資源配置的管理員。此使用者包括下列角色：儲存管理員、支援管理員及監控。
- 安全性：負責安全性組態的使用者、包括存取管理和憑證管理。此使用者包括下列角色：安全性管理和監控。
- 支援：負責硬體資源、故障資料及韌體升級的使用者。此使用者包括下列角色：Support Admin和Monitor。
- 監控：擁有系統唯讀存取權的使用者。此使用者僅包含「監控」角色。
- * rw*（讀寫）-此使用者包括下列角色：儲存管理員、支援管理員及監控。
- * RO*（唯讀）-此使用者僅包含「監控」角色。

變更密碼

您可以在「存取管理」中變更每位使用者的使用者密碼。

開始之前

- 您必須以本機系統管理員的身分登入、其中包含root系統管理權限。
- 您必須知道本機系統管理員密碼。

關於這項工作

選擇密碼時請謹記以下準則：

- 任何新的本機使用者密碼必須符合或超過最小密碼的目前設定（在「檢視/編輯設定」中）。
- 密碼區分大小寫。
- 設定後置空格時、不會從密碼中移除。如果密碼中包含空格、請務必小心。
- 為了提高安全性、請使用至少15個英數字元、並經常變更密碼。

步驟

1. 選擇*存取管理*。
2. 選取*本機使用者角色*索引標籤。
3. 從表格中選取使用者。

「變更密碼」按鈕隨即可用。

4. 選擇*變更密碼*。

「變更密碼」對話方塊隨即開啟。

5. 如果未設定本機使用者密碼的最小密碼長度、您可以選取核取方塊、要求使用者輸入密碼才能存取系統。
6. 在兩個欄位中輸入所選使用者的新密碼。
7. 輸入您的本機系統管理員密碼以確認此作業、然後按一下*變更*。

結果

如果使用者目前登入、密碼變更會導致使用者的作用中工作階段終止。

變更本機使用者密碼設定

您可以設定所有新的或更新的本機使用者密碼所需的最小長度。您也可以允許本機使用者在不輸入密碼的情況下存取系統。

開始之前

- 您必須以本機系統管理員的身分登入、其中包含root系統管理權限。

關於這項工作

設定本機使用者密碼的最小長度時、請謹記下列準則：

- 設定變更不會影響現有的本機使用者密碼。
- 本機使用者密碼的最小長度設定必須介於0到30個字元之間。
- 任何新的本機使用者密碼必須符合或超過目前的最小長度設定。
- 如果您希望本機使用者在未輸入密碼的情況下存取系統、請勿設定密碼的最小長度。

步驟

1. 選擇*存取管理*。
2. 選取*本機使用者角色*索引標籤。
3. 選取*檢視/編輯設定*。

「本機使用者密碼設定」對話方塊隨即開啟。

4. 執行下列其中一項：
 - 若要允許本機使用者存取系統而不輸入密碼、請清除「要求所有本機使用者密碼至少為」核取方塊。
 - 若要設定所有本機使用者密碼的最小密碼長度、請選取「要求所有本機使用者密碼至少為」核取方塊、然後使用微調方塊設定所有本機使用者密碼的最小長度要求。

任何新的本機使用者密碼必須符合或超過目前設定。

5. 按一下「*儲存*」。

新增目錄伺服器

若要設定存取管理驗證、您需要在LDAP伺服器和執行Web Services Proxy for SANtricity the Unified Manager的主機之間建立通訊。然後將LDAP使用者群組對應至本機使用者角色。

開始之前

- 您必須以包含安全管理員權限的使用者設定檔登入。否則、就不會顯示存取管理功能。
- 必須在目錄服務中定義使用者群組。
- LDAP伺服器認證必須可用、包括網域名稱、伺服器URL、以及可選的連結帳戶使用者名稱和密碼。
- 對於使用安全傳輸協定的LDAPS伺服器、LDAP伺服器的憑證鏈結必須安裝在本機機器上。

關於這項工作

新增目錄伺服器的程序分為兩個步驟。首先輸入網域名稱和URL。如果您的伺服器使用安全傳輸協定、則如果CA憑證是由非標準簽署授權單位簽署、您也必須上傳該憑證以進行驗證。如果您有綁定帳戶的認證、也可以輸入使用者帳戶名稱和密碼。接下來、您可以將LDAP伺服器的使用者群組對應至本機使用者角色。

步驟

1. 選擇*存取管理*。
2. 從*目錄服務*索引標籤、選取*新增目錄伺服器*。

「新增目錄伺服器」對話方塊隨即開啟。

3. 在*伺服器設定*索引標籤中、輸入LDAP伺服器的認證資料。

設定	說明
組態設定	網域
輸入LDAP伺服器的網域名稱。若為多個網域、請在以逗號分隔的清單中輸入網域。網域名稱用於登入 (<i>username@domain</i>)、以指定要驗證的目錄伺服器。	伺服器URL
以「LDAP[s]//host:port」的形式輸入存取LDAP伺服器的URL。	上傳憑證 (選用)
<div data-bbox="245 905 302 957"></div> <p data-bbox="358 779 477 1083">此欄位只有在上述伺服器URL欄位中指定LDAP S傳輸協定時才會顯示。</p> <p data-bbox="212 1136 513 1272">按一下*瀏覽*並選取要上傳的CA憑證。這是用於驗證LDAP伺服器的信任憑證或憑證鏈結。</p>	連結帳戶 (選用)
輸入唯讀使用者帳戶、以便針對LDAP伺服器進行搜尋查詢、並在群組內進行搜尋。以LDAP類型格式輸入帳戶名稱。例如、如果繫結使用者稱為「bindacc」、則您可以輸入「c=bindacct,cn=uss,c=cpoc,dc=local」之類的值。	連結密碼 (選用)

設定	說明
 <p>當您輸入連結帳戶時、會顯示此欄位。</p> <p>輸入綁定帳戶的密碼。</p>	<p>在新增之前先測試伺服器連線</p>
<p>如果您要確保系統能夠與您輸入的LDAP伺服器組態通訊、請選取此核取方塊。按一下對話方塊底部的*「Add*（新增*）」之後、就會進行測試。如果選取此核取方塊且測試失敗、則不會新增組態。您必須解決錯誤或取消選取核取方塊、才能跳過測試並新增組態。</p>	<p>**權限設定</p>
<p>搜尋基礎DN</p>	<p>輸入要搜尋使用者的LDAP內容、通常格式為「CN=Users、DC=cOPC、DC=local」。</p>
<p>使用者名稱屬性</p>	<p>輸入繫結至使用者ID以進行驗證的屬性。例如：「AMAccountName」。</p>
<p>群組屬性</p>	<p>輸入使用者的群組屬性清單、以用於群組對角色對應。例如：「memberof、managedObjects」。</p>

- 按一下「**角色對應」索引標籤。
- 將LDAP群組指派給預先定義的角色。一個群組可以有多個指派的角色。

欄位詳細資料

設定	說明
<p>對應</p>	<p>群組DN</p>
<p>指定要對應之LDAP使用者群組的群組辨別名稱(DN)。</p>	<p>角色</p>



所有使用者（包括系統管理員）都必須具備「監控」角色。

6. 如有需要、請按一下*新增其他對應*、以輸入更多群組對角色對應。
7. 完成對應後、按一下*「Add*（新增*）」。

系統會執行驗證、確保儲存陣列和LDAP伺服器能夠通訊。如果出現錯誤訊息、請檢查在對話方塊中輸入的認證資料、並視需要重新輸入資訊。

編輯目錄伺服器設定和角色對應

如果您先前在Access Management中設定了目錄伺服器、則可以隨時變更其設定。設定包括伺服器連線資訊和群組對角色對應。

開始之前

- 您必須以包含安全管理員權限的使用者設定檔登入。否則、就不會顯示存取管理功能。
- 必須定義目錄伺服器。

步驟

1. 選擇*存取管理*。
2. 選取*目錄服務*索引標籤。
3. 如果定義了多個伺服器、請從表格中選取您要編輯的伺服器。
4. 選取*檢視/編輯設定*。

此時會開啟「目錄伺服器設定」對話方塊。

5. 在*伺服器設定*索引標籤中、變更所需的設定。

設定	說明
組態設定	網域
LDAP伺服器的網域名稱。若為多個網域、請在以逗號分隔的清單中輸入網域。網域名稱用於登入（ <i>username@domain</i> ）、以指定要驗證的目錄伺服器。	伺服器URL
以「LDAP[s]//host:port」形式存取LDAP伺服器的URL。	連結帳戶（選用）
用於針對LDAP伺服器進行搜尋查詢及在群組內搜尋的唯讀使用者帳戶。	連結密碼（選用）

設定	說明
綁定帳戶的密碼。（輸入連結帳戶時、會顯示此欄位。）	儲存前先測試伺服器連線
檢查系統是否能與LDAP伺服器組態通訊。按一下「儲存」之後、就會進行測試。如果選取此核取方塊且測試失敗、則不會變更組態。您必須解決錯誤或清除核取方塊、才能跳過測試並重新編輯組態。	權限設定
搜尋基礎DN	要搜尋使用者的LDAP內容、通常格式為「CN=Users、DC=cOPC、DC=local」。
使用者名稱屬性	繫結至使用者ID以進行驗證的屬性。例如：「AMAccountName」。
群組屬性	使用者上的群組屬性清單、用於群組對角色對應。例如：「memberof、managedObjects」。

6. 在*角色對應*索引標籤中、變更所需的對應。

設定	說明
對應	群組DN
要對應之LDAP使用者群組的網域名稱。	角色



所有使用者（包括系統管理員）都必須具備「監控」角色。

7. 如有需要、請按一下*新增其他對應*、以輸入更多群組對角色對應。

8. 按一下「* 儲存 *」。

結果

完成此工作之後、任何作用中的使用者工作階段都會終止。只會保留目前的使用者工作階段。

移除目錄伺服器

若要中斷目錄伺服器與Web服務Proxy之間的連線、您可以從「存取管理」頁面移除伺服器資訊。如果您設定了新的伺服器、然後想要移除舊的伺服器、則可能需要執行此工作。

開始之前

- 您必須以包含安全管理員權限的使用者設定檔登入。否則、就不會顯示存取管理功能。

關於這項工作

完成此工作之後、任何作用中的使用者工作階段都會終止。只會保留目前的使用者工作階段。

步驟

1. 選擇*存取管理*。
2. 選取*目錄服務*索引標籤。
3. 從清單中選取您要刪除的目錄伺服器。
4. 按一下「移除」。

「移除目錄伺服器」對話方塊隨即開啟。

5. 在欄位中輸入「移除」、然後按一下「移除」。

目錄伺服器組態設定、權限設定和角色對應都會移除。使用者無法再使用此伺服器的認證登入。

常見問題集

為什麼我無法登入？

如果您在嘗試登入SANtricity 時收到錯誤訊息、請檢閱這些可能的原因。

Unified Manager的登入錯誤可能是因為下列原因之一：

- 您輸入的使用者名稱或密碼不正確。
- 您的權限不足。
- 目錄伺服器（若已設定）可能無法使用。如果是這種情況、請嘗試以本機使用者角色登入。
- 您嘗試多次登入失敗、這會觸發鎖定模式。請等待10分鐘以重新登入。

由於下列原因之一、可能會發生遠端儲存陣列鏡射工作的登入錯誤：

- 您輸入的密碼不正確。
- 您嘗試多次登入失敗、這會觸發鎖定模式。請等待10分鐘再登入一次。
- 控制器上使用的用戶端連線數量已達上限。檢查多個使用者或用戶端。

新增目錄伺服器之前、我需要知道什麼？

在Access Management中新增目錄伺服器之前、您必須符合特定需求。

- 必須在目錄服務中定義使用者群組。
- LDAP伺服器認證必須可用、包括網域名稱、伺服器URL、以及可選的連結帳戶使用者名稱和密碼。
- 對於使用安全傳輸協定的LDAPS伺服器、LDAP伺服器的憑證鏈結必須安裝在本機機器上。

我需要知道哪些關於對應至儲存陣列角色的資訊？

在將群組對應至角色之前、請先檢閱準則。

RBAC（角色型存取控制）功能包括下列角色：

- 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。



所有使用者（包括系統管理員）都必須具備「監控」角色。

如果您使用的是LDAP（輕量型目錄存取傳輸協定）伺服器 and 目錄服務、請確定：

- 系統管理員已在目錄服務中定義使用者群組。
- 您知道LDAP使用者群組的群組網域名稱。

什麼是本機使用者？

本機使用者會在系統中預先定義、並包含特定權限。

本機使用者包括：

- 管理：擁有系統中所有功能存取權的超級管理員。此使用者包含所有角色。首次登入時必須設定密碼。
- 儲存設備：負責所有儲存資源配置的管理員。此使用者包括下列角色：儲存管理員、支援管理員及監控。在設定密碼之前、此帳戶會停用。
- 安全性：負責安全性組態的使用者、包括存取管理和憑證管理。此使用者包括下列角色：安全性管理和監控。在設定密碼之前、此帳戶會停用。
- 支援：負責硬體資源、故障資料及韌體升級的使用者。此使用者包括下列角色：Support Admin和Monitor。在設定密碼之前、此帳戶會停用。
- 監控：擁有系統唯讀存取權的使用者。此使用者僅包含「監控」角色。在設定密碼之前、此帳戶會停用。
- * rw*（讀寫）-此使用者包括下列角色：儲存管理員、支援管理員及監控。在設定密碼之前、此帳戶會停用。
- * RO*（唯讀）-此使用者僅包含「監控」角色。在設定密碼之前、此帳戶會停用。

版權資訊

Copyright © 2024 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。