使用目錄服務
SANtricity 11.7

NetApp
February 12, 2024

目錄

使用目錄服務

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Unified Manager Web Services Proxy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*。

   此時將打開Add Directory Server（添加目錄服務器）對話框。

3. 在*伺服器設定*索引標籤中、輸入LDAP伺服器的認證資料。

欄位詳細資料

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（*username*@*domain*）、以指定要驗證的目錄伺服器。	伺服器URL
以的形式輸入存取LDAP 伺服器的 URL `ldap[s]://**host**:*port*`。	上傳憑證（選用）
此欄位只有在上述伺服器URL欄位中指定LDAPS傳輸協定時才會顯示。 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。	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「 bindacct 」、則您可以輸入例如的值 `CN=bindacct,CN=Users,DC=cpoc,DC=local`。	連結密碼（選用）

設定	說明
當您輸入連結帳戶時、會顯示此欄位。 輸入綁定帳戶的密碼。	在新增之前先測試伺服器連線
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。	權限設定
搜尋基礎DN	輸入要搜尋使用者的LDAP內容、通常是以的形式 `CN=Users, DC=cpoc, DC=local`。
使用者名稱屬性	輸入繫結至使用者ID以進行驗證的屬性。例如： `sAMAccountName`。
群組屬性	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`。

4. 按一下「角色對應」索引標籤。
5. 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
對應	群組 DN
指定要對應之LDAP使用者群組的群組辨別名稱（DN）。支援規則運算式。如果這些特殊的規則運算式字元不是規則運算式模式的一部分、則必須以反斜槓（\）轉義： \.[]{}()<>*+-=!?^$	
角色	按一下欄位、然後選取要對應至群組DN的其中一個本機使用者角色。您必須個別選取要納入此群組的每個角色。監控角色必須與其他角色搭配使用、才能登入SANtricity 到NetApp Unified Manager。對應的角色包括下列權限： • 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。

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*。

   此時將打開Directory Server Settings（目錄服務器設置）對話框。

5. 在*伺服器設定*索引標籤中、變更所需的設定。

欄位詳細資料

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（*username @domain*）、以指定要驗證的目錄伺服器。	伺服器URL
以下列形式存取LDAP伺服器的URL `ldap[s]://host:port`。	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）
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、通常採用的形式 `CN=Users, DC=cpoc, 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： `sAMAccountName`。
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。

欄位詳細資料

設定	說明
對應	群組 DN
要對應之LDAP使用者群組的網域名稱。支援規則運算式。如果這些特殊的規則運算式字元不是規則運算式模式的一部分、則必須以反斜槓（\）轉義： \.[]{}()<>*+-=!?^$	
角色	要對應至群組DN的角色。您必須個別選取要納入此群組的每個角色。監控角色必須與其他角色搭配使用、才能登入SANtricity 到NetApp Unified Manager。 這些角色包括： • 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。

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」。

   此時會開啟「移除目錄伺服器」對話方塊。

5. 類型 `remove` 在欄位中、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。