



# 管理叢集管理員使用者帳戶

## Element Software

NetApp  
November 19, 2025

This PDF was generated from [https://docs.netapp.com/zh-tw/element-software-127/storage/concept\\_system\\_manage\\_manage\\_ldap.html](https://docs.netapp.com/zh-tw/element-software-127/storage/concept_system_manage_manage_ldap.html) on November 19, 2025. Always check [docs.netapp.com](https://docs.netapp.com) for the latest.

# 目錄

管理叢集管理員使用者帳戶	1
儲存叢集管理員帳戶類型	1
檢視叢集管理詳細資料	1
建立叢集管理員帳戶	2
編輯叢集管理員權限	3
變更叢集管理員帳戶的密碼	3
如需詳細資訊、請參閱	3
管理 LDAP	3
完成LDAP支援的預先組態步驟	4
使用元素使用者介面啟用LDAP驗證	4
使用Element API啟用LDAP驗證	6
檢視 LDAP 詳細資料	8
測試LDAP組態	9
停用 LDAP	11
如需詳細資訊、請參閱	11

# 管理叢集管理員使用者帳戶

您可以SolidFire 建立、刪除及編輯叢集管理員帳戶、變更叢集管理員密碼、以及設定LDAP設定來管理使用者的系統存取、藉此管理適用於整個儲存系統的叢集管理員帳戶。

## 儲存叢集管理員帳戶類型

執行NetApp Element 下列兩種類型的系統管理員帳戶可存在於執行此軟件的儲存叢集：主叢集系統管理員帳戶和叢集系統管理員帳戶。

- 主叢集管理員帳戶

此管理員帳戶是在建立叢集時建立的。此帳戶是主要管理帳戶、具有最高層級的叢集存取權。此帳戶類似於Linux系統中的root使用者。您可以變更此系統管理員帳戶的密碼。

- 叢集管理員帳戶

您可以為叢集管理員帳戶提供有限的管理存取權限、以便在叢集中執行特定工作。指派給每個叢集管理員帳戶的認證資料、用於驗證儲存系統內的API和元素UI要求。



需要本機（非LDAP）叢集管理員帳戶、才能透過每節點UI存取叢集中的作用中節點。存取尚未屬於叢集一部分的節點時、不需要帳戶認證。

## 檢視叢集管理詳細資料

1. 若要建立全叢集（非LDAP）叢集管理員帳戶、請執行下列動作：
  - a. 按一下「使用者>\*叢集管理員\*」。
2. 在「使用者」索引標籤的「叢集管理員」頁面上、您可以檢視下列資訊。
  - \* ID\*：指派給叢集管理員帳戶的連續編號。
  - 使用者名稱：建立叢集管理員帳戶時所指定的名稱。
  - 存取：指派給使用者帳戶的使用者權限。可能值：
    - 讀取
    - 報告
    - 節點
    - 磁碟機
    - 磁碟區
    - 帳戶
    - 叢集管理員
    - 系統管理員
    - SupportAdmin



系統管理員存取類型可使用所有權限。

- 類型：叢集管理員的類型。可能值：
  - 叢集
  - LDAP
- 屬性：如果叢集管理員帳戶是使用元素API建立、則此欄會顯示使用該方法設定的任何名稱值配對。  
請參閱。"《軟件API參考》NetApp Element"

## 建立叢集管理員帳戶

您可以建立具有權限的新叢集管理員帳戶、以允許或限制存取儲存系統的特定區域。當您設定叢集管理員帳戶權限時、系統會針對您未指派給叢集管理員的任何權限、授予唯讀權限。

如果您想要建立LDAP叢集管理員帳戶、請先確定已在叢集上設定LDAP、然後再開始。

### "[使用元素使用者介面啟用LDAP驗證](#)"

您可以稍後變更叢集管理員帳戶的報告權限、節點、磁碟機、磁碟區、帳戶、和叢集層級存取。當您啟用權限時、系統會指派該層級的寫入存取權。系統會針對您未選取的層級、授予系統管理員使用者唯讀存取權。

您也可以稍後移除系統管理員所建立的任何叢集管理員使用者帳戶。您無法移除建立叢集時所建立的主要叢集管理員帳戶。

1. 若要建立全叢集（非LDAP）叢集管理員帳戶、請執行下列動作：
  - a. 按一下「使用者>\*叢集管理員\*」。
  - b. 按一下「建立叢集管理」。
  - c. 選取\*叢集\*使用者類型。
  - d. 輸入帳戶的使用者名稱和密碼、然後確認密碼。
  - e. 選取要套用至帳戶的使用者權限。
  - f. 勾選核取方塊以同意終端使用者授權合約。
  - g. 按一下「建立叢集管理」。
2. 若要在LDAP目錄中建立叢集管理員帳戶、請執行下列動作：
  - a. 按一下\*叢集\*>\* LDAP \*。
  - b. 確認已啟用LDAP驗證。
  - c. 按一下\*測試使用者驗證\*、然後複製顯示給使用者或使用者所屬群組之一的辨別名稱、以便稍後貼上。
  - d. 按一下「使用者>\*叢集管理員\*」。
  - e. 按一下「建立叢集管理」。
  - f. 選取LDAP使用者類型。
  - g. 在辨別名稱欄位中、依照文字方塊中的範例輸入使用者或群組的完整辨別名稱。或者、也可以貼上您先前複製的辨別名稱。

如果辨別名稱是群組的一部分、則LDAP伺服器上屬於該群組成員的任何使用者都將擁有此管理員帳戶的權限。

若要新增LDAP叢集管理使用者或群組、使用者名稱的一般格式為「LDAP : <完整辨別名稱>」。

- a. 選取要套用至帳戶的使用者權限。
- b. 勾選核取方塊以同意終端使用者授權合約。
- c. 按一下「建立叢集管理」。

## 編輯叢集管理員權限

您可以變更叢集管理員帳戶的報告權限、節點、磁碟機、磁碟區、帳戶、和叢集層級存取。當您啟用權限時、系統會指派該層級的寫入存取權。系統會針對您未選取的層級、授予系統管理員使用者唯讀存取權。

1. 按一下「使用者>\*叢集管理員」。
2. 針對您要編輯的叢集管理員、按一下「動作」圖示。
3. 按一下 \* 編輯 \*。
4. 選取要套用至帳戶的使用者權限。
5. 按一下\*儲存變更\*。

## 變更叢集管理員帳戶的密碼

您可以使用Element UI來變更叢集管理員密碼。

1. 按一下「使用者>\*叢集管理員」。
2. 針對您要編輯的叢集管理員、按一下「動作」圖示。
3. 按一下 \* 編輯 \*。
4. 在變更密碼欄位中、輸入新密碼並加以確認。
5. 按一下\*儲存變更\*。

## 如需詳細資訊、請參閱

- "[使用元素使用者介面啟用LDAP驗證](#)"
- "[停用 LDAP](#)"
- "[零件與元件軟體文件SolidFire](#)"
- "[vCenter Server的VMware vCenter外掛程式NetApp Element](#)"

## 管理 LDAP

您可以設定輕量型目錄存取傳輸協定（LDAP）、以啟用SolidFire 安全的目錄型登入功能、以利進行資料儲存。您可以在叢集層級設定LDAP、並授權LDAP使用者和群組。

管理LDAP包括使用SolidFire 現有的Microsoft Active Directory環境、設定LDAP驗證至某個叢集、並測試組態。



您可以同時使用IPv4和IPv6位址。

啟用LDAP涉及下列詳細說明的高層級步驟：

1. 完成**LDAP**支援的預先設定步驟。驗證您是否擁有設定LDAP驗證所需的所有詳細資料。
2. 啟用**LDAP**驗證。使用Element UI或Element API。
3. 驗證**LDAP**組態。或者、您也可以執行GetLdapConfiguration API方法或使用元素UI檢查LTAP組態、檢查叢集是否設定正確的值。
4. \* 測試 LDAP 驗證 \* (與使用者一 `readonly` 起)。執行TestLdapAuthentication API方法或使用Element UI來測試LDAP組態是否正確。在此初始測試中、請使用使用者的使用者名稱「`shAMAccountName`」` ` `readonly`。這將驗證您的叢集是否已正確設定 LDAP 驗證、並驗證認證和存取是否 `readonly` 正確。如果此步驟失敗、請重複步驟1至3。
5. 測試**LDAP**驗證 (使用您要新增的使用者帳戶)。使用您要新增為元素叢集管理員的使用者帳戶重複設定4。複製 `distinguished` 名稱 (DN) 或使用者 (或群組)。此DN將在步驟6中使用。
6. 新增**LDAP**叢集**admin** (從「測試LDAP驗證」步驟複製並貼上DN)。使用Element UI或AddLdapClusterAdmin API方法、建立具有適當存取層級的新叢集管理使用者。對於使用者名稱、請貼上您在步驟5中複製的完整DN。如此可確保DN格式正確。
7. 測試叢集管理存取。使用新建立的LDAP叢集管理使用者登入叢集。如果您新增了LDAP群組、則可以以該群組中的任何使用者身分登入。

## 完成**LDAP**支援的預先組態步驟

在元素中啟用**LDAP**支援之前、您應該先設定Windows Active Directory伺服器、並執行其他的預先設定工作。

### 步驟

1. 設定Windows Active Directory伺服器。
2. \*選用：\*啟用**LDAPS**支援。
3. 建立使用者和群組。
4. 建立唯讀服務帳戶 (例如「`sfreadonly`」)、以用於搜尋**LDAP**目錄。

## 使用元素使用者介面啟用**LDAP**驗證

您可以設定儲存系統與現有**LDAP**伺服器的整合。這可讓**LDAP**管理員集中管理使用者的儲存系統存取。

您可以使用元素使用者介面或元素API來設定**LDAP**。本程序說明如何使用Element UI設定**LDAP**。

本範例說明如何在 SolidFire 上設定 **LDAP** 驗證、並將其用 `SearchAndBind` 作驗證類型。範例使用單一Windows Server 2012 R2 Active Directory伺服器。

### 步驟

1. 按一下\*叢集\*>\* **LDAP** \*。
2. 按一下「是」以啟用**LDAP**驗證。
3. 按一下\*「新增伺服器」\*。

4. 輸入\*主機名稱/IP位址\*。



您也可以輸入選用的自訂連接埠號碼。

例如、若要新增自訂連接埠號碼、請輸入：

5. 選用：\*選取\*使用**LDAPS**傳輸協定。

6. 在\*一般設定\*中輸入必要資訊。

#### LDAP Servers

Host Name/IP Address 192.168.9.99

[Remove](#)

Use LDAPS Protocol

[Add a Server](#)

#### General Settings

Auth Type Search and Bind

Search Bind DN msmyth@thesmyths.ca

Search Bind Password *e.g. password*

Show password

User Search Base DN OU=Home users,DC=thesmyths,DC=ca

User Search Filter (&(objectClass=person)(|(sAMAccountName=%USER

Group Search Type Active Directory

Group Search Base DN OU=Home users,DC=thesmyths,DC=ca

[Save Changes](#)

7. 按一下 \* 啟用 LDAP\* 。
8. 如果您要測試使用者的伺服器存取、請按一下\*測試使用者驗證\*。
9. 複製建立叢集管理員時、顯示的辨別名稱和使用者群組資訊、以供日後使用。
10. 按一下\*儲存變更\*以儲存任何新設定。
11. 若要在此群組中建立使用者、讓任何人都能登入、請完成下列步驟：  
a. 按一下\*使用者\*>\*檢視\*。

## Create a New Cluster Admin



### Select User Type

Cluster  LDAP

### Enter User Details

#### Distinguished Name

CN=StorageAdmins,OU=Home  
users,DC=thesmyths,DC=ca

### Select User Permissions

- |                                    |  |
|------------------------------------|--|
| <input type="checkbox"/> Reporting | <input type="checkbox"/> Volumes       |
| <input type="checkbox"/> Nodes     | <input type="checkbox"/> Accounts      |
| <input type="checkbox"/> Drives    | <input type="checkbox"/> Cluster Admin |

### Accept the Following End User License Agreement

- b. 對於新使用者、請按一下「使用者類型」的「\* LDAP\*」、然後將複製的群組貼到「辨別名稱」欄位。
- c. 選取權限、通常是所有權限。
- d. 向下捲動至「使用者授權合約」、然後按一下「我接受」。
- e. 按一下「建立叢集管理」。

現在您的使用者擁有Active Directory群組的值。

若要測試、請登出Element UI、然後以該群組中的使用者身分重新登入。

### 使用Element API啟用LDAP驗證

您可以設定儲存系統與現有LDAP伺服器的整合。這可讓LDAP管理員集中管理使用者的儲存系統存取。

您可以使用元素使用者介面或元素API來設定LDAP。本程序說明如何使用Element API設定LDAP。

若要在 SolidFire 叢集上使用 LDAP 驗證、請先使用 API 方法在叢集上啟用 LDAP 驗證  
EnableLdapAuthentication。

#### 步驟

1. 請先使用 API 方法在叢集上啟用 LDAP 驗證 EnableLdapAuthentication。

2. 輸入所需資訊。

```
{  
    "method": "EnableLdapAuthentication",  
    "params": {  
        "authType": "SearchAndBind",  
        "groupSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net",  
        "groupSearchType": "ActiveDirectory",  
        "searchBindDN": "SFReadOnly@prodtest.solidfire.net",  
        "searchBindPassword": "ReadOnlyPW",  
        "userSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net ",  
        "userSearchFilter":  
            "(&(objectClass=person)(sAMAccountName=%USERNAME%))"  
        "serverURIs": [  
            "ldap://172.27.1.189",  
            [  
                ],  
            "id": "1"  
    }  
}
```

3. 變更下列參數的值：

使用的參數	說明
驗證類型：SearchAndBind	表示叢集將使用唯讀服務帳戶來先搜尋要驗證的使用者、然後在找到並驗證時連結該使用者。
群組SearchBaseDN : DC=prodtest,DC=solidfire,DC=net	指定LDAP樹狀結構中要開始搜尋群組的位置。在此範例中、我們使用了樹狀結構的根目錄。如果您的LDAP樹狀結構非常大、您可能想要將其設定為更精細的子樹狀結構、以縮短搜尋時間。
userSearchBaseDN : DC=prodtest,DC=solidfire,DC=net	指定LDAP樹狀結構中要開始搜尋使用者的位置。在此範例中、我們使用了樹狀結構的根目錄。如果您的LDAP樹狀結構非常大、您可能想要將其設定為更精細的子樹狀結構、以縮短搜尋時間。
群組搜尋類型：ActiveDirectory	使用Windows Active Directory伺服器做為LDAP伺服器。

使用的參數	說明
<pre data-bbox="208 192 802 297">userSearchFilter: "(&amp;(objectClass=person)(sAMAccountName=%USERNAME%))"</pre>	(SamAccountName=%username%) (userPrincipalName=%username%) )」 -
<p>若要使用userPrincipalName（登入電子郵件地址）, 您可以將userSearchFilter變更為：</p> <pre data-bbox="208 508 802 572">"(&amp;(objectClass=person)(userPrincipalName=%USERNAME%))"</pre>	
<p>或者、若要同時搜尋userPrincipalName和sAMAccountName, 您可以使用下列userSearchFilter：</p> <pre data-bbox="208 804 649 846">"(&amp;(objectClass=person)(</pre>	
<p>利用sAMAccountName作為我們的使用者名稱來登入SolidFire到這個叢集。這些設定可讓LDAP在sAMAccountName屬性中搜尋登入時指定的使用者名稱、並將搜尋範圍限制為在objectClass屬性中具有「person」值的項目。</p>	searchBindDN
<p>這是唯讀使用者的辨別名稱、用於搜尋LDAP目錄。對於Active Directory、通常最容易使用使用者的userPrincipalName（電子郵件地址格式）。</p>	searchBindPassword

若要測試、請登出Element UI、然後以該群組中的使用者身分重新登入。

## 檢視 LDAP 詳細資料

在「叢集」索引標籤的「LDAP」頁面上檢視LDAP資訊。



您必須啟用LDAP才能檢視這些LDAP組態設定。

1. 若要檢視含有元素UI的LDAP詳細資料、請按一下\*叢集\*>\* LDAP\*。
  - 主機名稱/IP位址：LDAP或LDAPS目錄伺服器的位址。
  - 驗證類型：使用者驗證方法。可能值：
    - 直接連結
    - 搜尋與連結

- 搜尋連結DN：完整的DN、可用來登入以執行LDAP搜尋使用者（需要對LDAP目錄的連結層級存取）。
- 搜尋連結密碼：用於驗證LDAP伺服器存取的密碼。
- 使用者搜尋基礎DN：用於開始使用者搜尋的樹狀結構基礎DN。系統會從指定位置搜尋子樹狀結構。
- 使用者搜尋篩選器：使用您的網域名稱輸入下列內容：

```
(& (objectClass=person) (| (sAMAccountName=%USERNAME%) (userPrincipalName=%USERNAME%)) )
```

- 群組搜尋類型：控制所用預設群組搜尋篩選器的搜尋類型。可能值：
  - Active Directory：使用者所有LDAP群組的巢狀成員資格。
  - 無群組：無群組支援。
  - 成員DN：成員DN樣式群組（單層）。
- 群組搜尋基礎DN：用於開始群組搜尋的樹狀結構基礎DN。系統會從指定位置搜尋子樹狀結構。
- 測試使用者驗證：設定LDAP之後、請使用此選項來測試LDAP伺服器的使用者名稱和密碼驗證。輸入已存在的帳戶以進行測試。系統將顯示辨別名稱和使用者群組資訊、您可以複製這些資訊以供建立叢集管理員時使用。

## 測試LDAP組態

設定 LDAP 之後、您應該使用元素 UI 或元素 API 方法來測試 LDAP TestLdapAuthentication。

### 步驟

1. 若要使用Element UI測試LDAP組態、請執行下列步驟：
  - a. 按一下\*叢集\*>\* LDAP \*。
  - b. 按一下\*測試LDAP驗證\*。
  - c. 請使用下表中的資訊解決任何問題：

錯誤訊息	說明
xLDAPUserNotFound	<ul style="list-style-type: none"> <li>• 在設定的子樹狀結構中找不到要測試的使用者 userSearchBaseDN。</li> <li>• `userSearchFilter`設定不正確。</li> </ul>
xLDAPBindFailed (Error: Invalid credentials)	<ul style="list-style-type: none"> <li>• 正在測試的使用者名稱是有效的LDAP使用者、但提供的密碼不正確。</li> <li>• 正在測試的使用者名稱是有效的LDAP使用者、但帳戶目前已停用。</li> </ul>
xLDAPSearchBindFailed (Error: Can't contact LDAP server)	LDAP伺服器URI不正確。

錯誤訊息	說明
xLDAPSearchBindFailed (Error: Invalid credentials)	唯讀使用者名稱或密碼設定不正確。
xLDAPSearchFailed (Error: No such object)	`userSearchBaseDN`不是 LDAP 樹中的有效位置。
xLDAPSearchFailed (Error: Referral)	<ul style="list-style-type: none"> <li>`userSearchBaseDN`不是 LDAP 樹中的有效位置。</li> <li>`userSearchBaseDN`和 `groupSearchBaseDN`位於巢狀 OU 中。這可能會導致權限問題。因應措施是將 OU 納入使用者和群組基準 DN 項目中（例如：`ou=storage, cn=company, cn=com`）</li> </ul>

2. 若要使用Element API測試LDAP組態、請執行下列步驟：

a. 呼叫TestLdapAuthentication方法。

```
{
  "method": "TestLdapAuthentication",
  "params": {
    "username": "admin1",
    "password": "admin1PASS"
  },
  "id": 1
}
```

b. 檢閱結果。如果API呼叫成功、結果會包含指定使用者的辨別名稱、以及使用者所屬群組的清單。

```
{  
  "id": 1  
  "result": {  
    "groups": [  
  
      "CN=StorageMgmt,OU=PTUsers,DC=prodtest,DC=solidfire,DC=net"  
    ],  
    "userDN": "CN=Admin1  
Jones,OU=PTUsers,DC=prodtest,DC=solidfire,DC=net"  
  }  
}
```

## 停用 LDAP

您可以使用Element UI來停用LDAP整合。

在開始之前、您應該記下所有組態設定、因為停用LDAP會清除所有設定。

### 步驟

1. 按一下\*叢集\*>\* LDAP \*。
2. 按一下\*否\*。
3. 按一下\*停用LDAP\*。

### 如需詳細資訊、請參閱

- "[零件與元件軟體文件SolidFire](#)"
- "[vCenter Server的VMware vCenter外掛程式NetApp Element](#)"

## 版權資訊

Copyright © 2025 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 保留隨時變更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。