# 部署後設定SolidFire 系統選項

Element Software

NetApp
January 15, 2024

# 目錄

# 部署後設定SolidFire 系統選項

設定SolidFire 完整套系統之後、您可能會想要執行一些選用的工作。

如果您變更系統中的認證資料、您可能會想知道對其他元件的影響。

此外、您也可以設定多因素驗證、外部金鑰管理及聯邦資訊處理標準（FIPS）安全性的設定。您也應該視需要更新密碼。

## 如需詳細資訊、請參閱

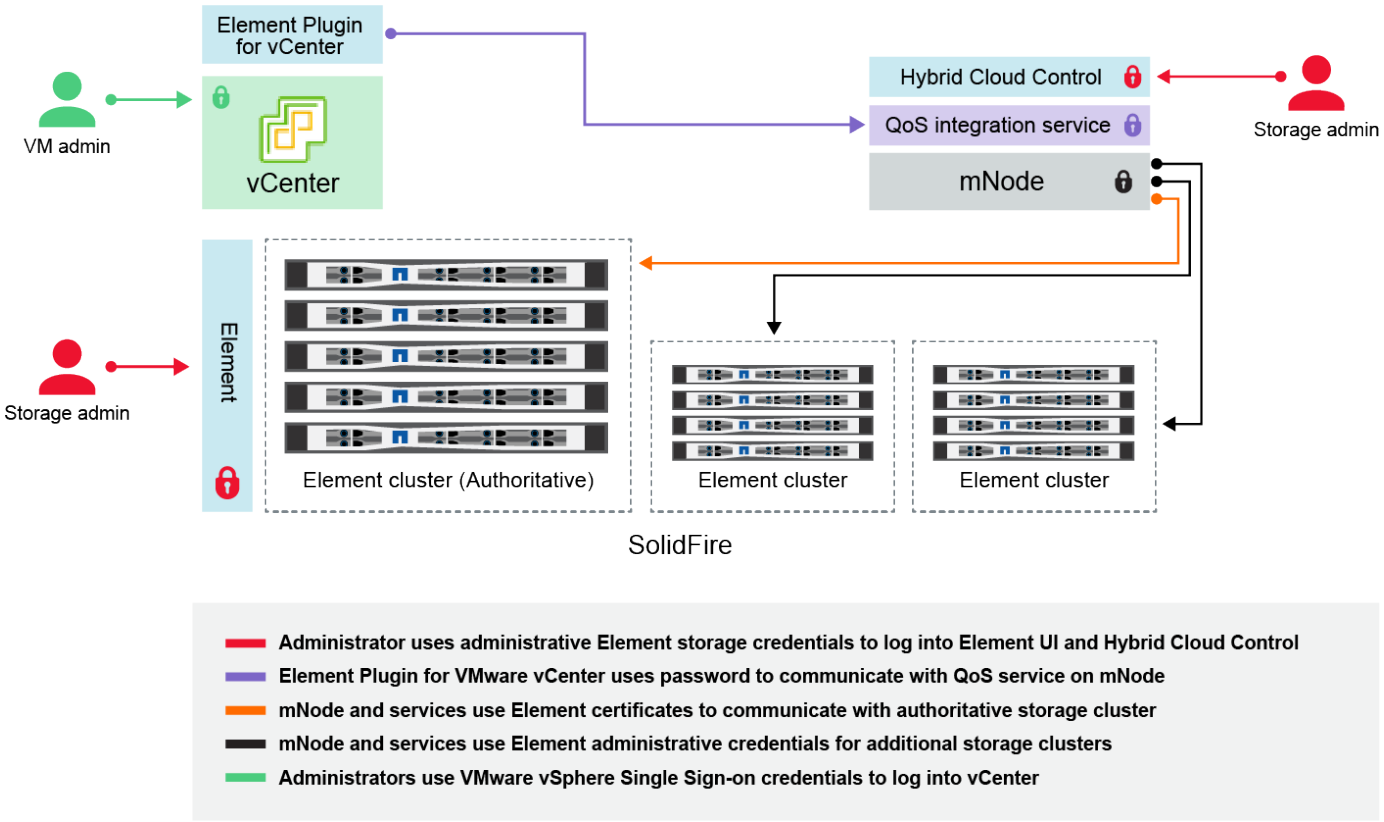
- "變更NetApp HCI 身分證明資料、請至NetApp SolidFire 解決方案"
- "變更Element軟體預設SSL憑證"
- "變更節點的IPMI密碼"
- "啟用多因素驗證"
- "開始使用外部金鑰管理"
- "建立支援FIPS磁碟機的叢集"

## 變更NetApp HCI 身分證明資料、請至NetApp SolidFire 解決方案

視部署NetApp HCI 了NetApp或NetApp SolidFire 的組織安全政策而定、變更認證或密碼通常是安全實務的一部分。在變更密碼之前、您應該瞭解部署中其他軟體元件的影響。

如果您變更NetApp HCI 了某個元件的驗證資料、請SolidFire 參閱下表、瞭解決對其他元件的影響。

NetApp SolidFire 元件互動
：




| 認證類型和圖示 | 由管理員使用 | 請參閱這些指示 |
|---|---|---|
| 元素認證 | 適用於 NetApp HCI SolidFire<br><br>系統管理員使用這些認證登入：<br><br>• Element儲存叢集上的Element使用者介面<br>• 管理節點（mNode）上的混合雲控制<br><br>當混合雲控制管理多個儲存叢集時、它只會接受儲存叢集的管理認證、也就是當初設定mNode的_驗證叢集_。稍後新增至混合雲控制的儲存叢集、mNode會安全地儲存管理認證資料。如果變更後續新增儲存叢集的認證資料、也必須使用mNode API在mNode中更新認證資料。 | • "更新儲存叢集管理密碼。"<br>• 使用更新mNode中的儲存叢集管理認證 "修改叢集管理API"。 |
| vSphere單一登入認證 | 適用於：NetApp HCI 僅限參考<br><br>系統管理員會使用這些認證來登入VMware vSphere Client。當vCenter是NetApp HCI 安裝過程的一部分時、認證資料會在NetApp部署引擎中設定如下：<br><br>• 使用指定密碼的username@vple.eril、以及<br>• 使用指定密碼的管理員@vple.estil。當現有vCenter用於部署NetApp HCI 功能時、vSphere單一登入認證會由IT VMware管理員管理。 | "更新vCenter和ESXi認證資料"。 |

| 認證類型和圖示 | 由管理員使用 | 請參閱這些指示 |
| --- | --- | --- |
| 基礎板管理控制器（BMC）認證 | 適用於：NetApp HCI 僅限參考<br><br>系統管理員使用這些認證資料登入NetApp HCI 到NetApp運算節點的BMC、以進行支援。BMC提供基本的硬體監控和虛擬主控台功能。<br><br>每個NetApp運算節點的BMC（有時稱為_IPMI_）認證會安全地儲存在NetApp HCI 資源開發環境的mNode上。NetApp混合式雲端控制使用服務帳戶容量中的BMC認證、在運算節點韌體升級期間與運算節點中的BMC通訊。<br><br>變更BMC認證後、必須同時在mNode上更新個別運算節點的認證資料、才能保留所有混合雲控制功能。 | • "為NetApp HCI 每個節點設定IPMI"。<br>• 對於H410C、H610C和H615C節點、 "變更預設IPMI密碼"。<br>• 對於H410S和H610S節點、"變更預設的ipm密碼"。<br>• "變更管理節點上的BMC認證"。 |
| ESXi認證 | 適用於：NetApp HCI 僅限參考<br><br>管理員可以使用SSH或本機DCUI（使用本機根帳戶）登入ESXi主機。在部署中、使用者名稱為「root」、密碼是在NetApp部署引擎中初次安裝該運算節點時指定的。NetApp HCI<br><br>每個NetApp運算節點的ESXi根認證均安全地儲存在NetApp HCI VMware部署的mNode上。NetApp混合雲控制系統會使用服務帳戶容量中的認證資料、在運算節點韌體升級和健全狀況檢查期間、直接與ESXi主機通訊。<br><br>當ESXi根認證由VMware管理員變更時、必須在mNode上更新個別運算節點的認證資料、才能保留混合雲控制功能。 | "更新vCenter和ESXi主機的認證資料"。 |
| QoS整合密碼 | 適用於：NetApp HCI 不SolidFire 適用*：不適用*<br><br>不適用於管理員的互動式登入。<br><br>VMware vSphere與Element軟體之間的QoS整合可透過下列方式啟用：<br><br>• vCenter Server的Element外掛程式、以及<br>• mNode上的QoS服務。<br><br>對於驗證、QoS服務會使用此內容中專屬使用的密碼。QoS密碼是在初始安裝Element Plug-in for vCenter Server期間指定、或NetApp HCI 是在進行VMware vCenter部署時自動產生。<br><br>不會影響其他元件。 | "更新NetApp Element vCenter Server的VMware vCenter外掛程式中的QoSSIOC認證"。<br><br>vCenter Server SIOC密碼的「功能」外掛程式也稱為_QoSSIOC密碼。NetApp Element<br><br>檢閱｛url-peak｝[Element Plug-In for vCenter Server KB文章]。 |

| 認證類型和圖示 | 由管理員使用 | 請參閱這些指示 |
|---|---|---|
| vCenter Service Appliance認證資料 | 適用於：NetApp HCI 僅當NetApp部署引擎設定時才適用<br><br>管理員可以登入vCenter Server應用裝置虛擬機器。在進行內部部署時、使用者名稱為「root」、密碼是在NetApp部署引擎中初次安裝該運算節點時指定的。NetApp HCI根據部署的VMware vSphere版本、vSphere單一登入網域中的特定管理員也可以登入應用裝置。<br><br>不會影響其他元件。 | 無需變更。 |
| NetApp管理節點管理認證 | 適用於：NetApp HCI 不SolidFire 適用*：不適用*<br><br>管理員可以登入NetApp管理節點虛擬機器、以進行進階組態和疑難排解。根據部署的管理節點版本、預設不會啟用透過SSH登入。<br><br>在進行元件部署時、使用者在NetApp部署引擎中初次安裝運算節點時、會指定使用者名稱和密碼。NetApp HCI<br><br>不會影響其他元件。 | 無需變更。 |

## 如需詳細資訊、請參閱

- "變更Element軟體預設SSL憑證"
- "變更節點的IPMI密碼"
- "啟用多因素驗證"
- "開始使用外部金鑰管理"
- "建立支援FIPS磁碟機的叢集"

# 變更Element軟體預設SSL憑證

## 您可以使用NetApp Element NetApp API變更叢集中儲存節點的預設SSL憑證和私密金鑰。

建立一個支援功能的軟體叢集時、叢集會建立一個獨特的自我簽署安全通訊端層（SSL）憑證和私密金鑰、用於透過元素UI、每節點UI或API進行所有HTTPS通訊。NetApp ElementElement軟體支援自我簽署的憑證、以及由信任的憑證授權單位（CA）核發和驗證的憑證。

您可以使用下列API方法取得有關預設SSL憑證的詳細資訊、並進行變更。

- * GetSSLCertificate *

  您可以使用 "GetSSLCertificate方法" 擷取目前安裝之SSL憑證的相關資訊、包括所有憑證詳細資料。

- * SetSSLCertificate *

您可以使用 "SetSSLCertificate方法" 可將叢集和每節點SSL憑證設為您提供的憑證和私密金鑰。系統會驗證憑證和私密金鑰、以防止套用無效的憑證。

- *遠端SSLCertificate *

  。 "遠端SSLCertificate方法" 移除目前安裝的SSL憑證和私密金鑰。然後叢集會產生新的自我簽署憑證和私密金鑰。

> 叢集SSL憑證會自動套用至新增至叢集的所有新節點。從叢集移除的任何節點都會還原為自我簽署的憑證、而且所有使用者定義的憑證和金鑰資訊都會從節點移除。

### 如需詳細資訊、請參閱

- "變更管理節點的預設SSL憑證"
- "在Element Software中設定自訂SSL憑證有哪些要求？"
- "零件與元件軟體文件SolidFire"
- "vCenter Server的VMware vCenter外掛程式NetApp Element"

# 變更節點的預設IPMI密碼

## 您可以在遠端IPMI存取節點後、立即變更預設的智慧型平台管理介面（IPMI）管理員密碼。如果有任何安裝更新、您可能會想要這麼做。

如需設定節點的ipm存取的詳細資訊、請參閱 "為每個節點設定IPMI"。

您可以變更這些節點的ipm密碼：

- H410S節點
- H610S節點

### 變更H410S節點的預設IPMI密碼

設定IPMI網路連接埠後、您應該立即變更每個儲存節點上IPMI系統管理員帳戶的預設密碼。

#### 您需要的產品

您應該已為每個儲存節點設定IPMI IP位址。

#### 步驟

1. 在可連線到IPMI網路的電腦上開啟網頁瀏覽器、然後瀏覽至該節點的IPMI IP位址。
2. 在登入提示中輸入使用者名稱「admin」和密碼「admin」。
3. 登入後、按一下*組態*索引標籤。
4. 按一下「使用者」。
5. 選取「管理」使用者、然後按一下「修改使用者」。
6. 選取*變更密碼*核取方塊。

7. 在*密碼*和*確認密碼*欄位中輸入新密碼。
8. 按一下「修改」、然後按一下「確定」。
9. 對於任何其他使用預設IPMI密碼的H410S節點、請重複此程序。

## 變更H610S節點的預設IPMI密碼

設定IPMI網路連接埠後、您應該立即變更每個儲存節點上IPMI系統管理員帳戶的預設密碼。

您需要的產品

您應該已為每個儲存節點設定IPMI IP位址。

步驟

1. 在可連線到IPMI網路的電腦上開啟網頁瀏覽器、然後瀏覽至該節點的IPMI IP位址。
2. 在登入提示中輸入使用者名稱「root」和密碼「calvin」。
3. 登入後、按一下頁面左上角的功能表導覽圖示、即可開啟側邊列抽屜。
4. 按一下 * 設定 * 。
5. 按一下*使用者管理*。
6. 從清單中選取*系統管理員*使用者。
7. 啟用「變更密碼」核取方塊。
8. 在「密碼」和「確認密碼」欄位中輸入新的強式密碼。
9. 按一下頁面底部的*「Save"（儲存）*。
10. 對於任何其他使用預設IPMI密碼的H610S節點、請重複此程序。

## 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"