Oracle® ZFS Storage Appliance 安全指南 - 發行版本 OS8.8.x

文件號碼： **F39477-01**
2020 年 8 月

目錄

Oracle ZFS Storage Appliance 安全指南

本指南探討、複習以及說明建立安全系統所需的安全考量，並協助您全面瞭解您所需的安全目標。建議您在配置設備之前先閱讀本指南，以便充分利用現有的安全功能及建立所需的安全層次。

您也可以將本指南視為參考資料，藉以尋找與各種 Oracle ZFS Storage Appliance 功能安全考量相關的詳細資訊。如需設備組態程序的相關資訊，請參閱 *Oracle ZFS Storage Appliance Administration Guide*。

下列各節提供 Oracle ZFS Storage Appliance 安全功能與建議的描述：

- **第一步** - 描述在設備初始安裝期間的登入安全，以及對系統實體安全的建議。
- **管理模型** - 描述透過 BUI 和 CLI 的遠端存取、限制存取 BUI 和 CLI、系統修正模型、暫緩更新、支援組合以及組態備份。
- **設備使用者** - 描述管理角色、可以管理設備的人員以及管理使用者授權。
- **存取控制清單** - 描述用以允許或拒絕存取檔案和目錄的機制。
- **資料服務** - 描述設備支援的資料服務和其他資料服務所提供的安全。
- **目錄服務** - 描述可以在設備上設定的目錄服務及其安全相關問題。
- **系統設定值** - 描述系統設定值：Phone Home、服務標記、Kerberos、SMTP、SNMP、系統日誌、系統識別、磁碟檢測以及預防毀損。
- **安全日誌** - 描述與安全相關的日誌類型。

第一步

本節描述設備初始安裝期間的登入安全，以及對系統實體安全的建議。

初始安裝

Oracle ZFS Storage Appliance 出廠時已預先安裝設備軟體。由於無須安裝任何軟體，因此不會隨附任何媒體。

初始安裝使用預設帳戶名稱和密碼來完成，安裝後必須變更預設 root 密碼。如果將 Oracle ZFS Storage Appliance 重設為出廠預設值，則設備與服務處理器的 root 密碼也會同時重設為預設值。

在 Oracle ZFS Storage Appliance 的初始安裝期間會使用一組與系統服務處理器關聯的預設帳戶名稱和密碼。這個預設帳戶會讓系統管理員取得首次存取設備的權限，管理員必須利用此權限執行初始安裝步驟。其中一個必要步驟是設定新的設備管理員密碼，此動作接著會將預設服務處理器的密碼重設為相同的值。

實體安全

為控制對系統的存取，您必須維護電腦實體環境的安全。例如，登入後無人看管的系統非常容易遭到未經授權的存取。電腦的周圍環境和電腦硬體的實體必須隨時受到保護，才能避免未經授權的存取。

Oracle ZFS Storage Appliance 希望使用者能夠透過安全措施 (例如鑰匙、鎖、工具、識別證存取) 來管控並限制存取權限，而取得存取授權的人員必須瞭解限制存取權限的原因和必須採取的任何預防措施。

管理模型

本節描述 Oracle ZFS Storage Appliance 管理模型的安全。

遠端管理存取

本節描述 Oracle ZFS Storage Appliance 遠端存取安全。

瀏覽器使用者介面

瀏覽器使用者介面 (BUI) 用於一般的設備管理工作。您可以使用「BUI 服務畫面」來檢視及修改遠端存取服務和設定值。

管理動作會透過 HTTP 安全 (HTTPS) 瀏覽器階段作業來進行。HTTPS 階段作業會以自行簽署的憑證來加密，此憑證是在每個 Oracle ZFS Storage Appliance 系統初始安裝時產生的唯一憑證。使用者可自行定義 HTTPS 階段作業的逾時時間，預設的逾時時間為 15 分鐘。您可以前往 HTTPS 服務頁面，設定用於連線至 BUI 的 SSL/TLS 協定和加密方法。

指令行介面

指令行介面 (CLI) 可用於執行可以在 BUI 中執行的大部分管理動作。

「安全 Shell (SSH)」可讓使用者透過與 CLI 的「安全通訊端層 (SSL)」連線登入 Oracle ZFS Storage Appliance。SSH 也可以用來從遠端主機執行自動化命令檔，例如

擷取每日日誌或分析統計資料。您可以前往 SSH 服務頁面，設定用於連線至 CLI 的加密方法和 MAC。

限制的使用者授權

只有 root 使用者、定義中具有相關權限的本機管理員以及經由識別伺服器 (例如，輕量型目錄存取協定 (LDAP) 和網路資訊服務 (NIS)) 授權的使用者具有管理權限。

此外，當使用者使用 BUI、CLI 及 RESTful API 具備管理權限的身分登入，以及存取服務 (包括 NFS、HTTP、FTP、SFTP 以及 SSH) 時，設備可以透過 Kerberos 認證使用者。Kerberos 也可以用來設定使用 NFS 協定的個別共用安全，如「NFS 認證和加密選項」[11] 所述。

Oracle ZFS Storage Appliance RESTful API

Oracle ZFS Storage Appliance RESTful API 可用來管理 Oracle ZFS Storage Appliance。RESTful 架構的基礎是分層的用戶端-伺服器模型，可透過無用戶端配置的標準集線器、路由器和其他網路系統通透地將服務重新導向。

Oracle ZFS Storage Appliance RESTful API 使用與 BUI 和 CLI 相同的認證證明資料。所有來自外部用戶端的要求會各自使用設備證明資料認證，並且會透過連接埠 215 上的 HTTPS 連線進行。RESTful API 支援的 HTTPS 階段作業，其使用者可定義的預設逾時為 15 分鐘。

如需使用 RESTful API 管理 Oracle ZFS Storage Appliance 的相關資訊，請參閱 *Oracle ZFS Storage Appliance RESTful API Guide*。

系統更新

為使用最新的安全改良功能，Oracle 建議您將系統軟體保持在最新狀態。

套用系統更新時會一次更換所有的系統軟體二進位檔。更新之前，會先製作一個執行中系統集區的快照。這樣可以讓管理員在必要時倒回至先前的版本。

暫緩更新

暫緩更新是系統更新中的一種功能或局部功能，但此功能在執行系統更新時不會啟動。管理員可以決定套用暫緩更新的時間或是否要套用。系統更新時未套用的更新，仍然可以在後續系統更新時加以套用。您無法個別選取要套用的更新，當您選擇套用暫緩更新

時，只能選擇套用所有更新或不套用任何更新。套用更新之後，您將無法倒回之前的系統軟體版本。

支援組合

如果您的系統已註冊 Phone Home 支援，在發生重大錯誤時，系統狀態將會傳送到 My Oracle Support，而工程支援人員將針對收到的問題加以檢驗並建立支援組合。傳送到 My Oracle Support 的系統狀態資訊不會包含使用者資料；只會傳送配置資訊。

配置備份

系統配置可以儲存在本機上供日後回復之用。這些備份不會包含使用者資料；只會儲存配置設定值。

設備使用者

有兩種類型的 Oracle ZFS Storage Appliance 使用者：

- **資料服務使用者** – 使用支援的協定 (例如，網路檔案系統 (NFS)、伺服器訊息區塊 (SMB)、光纖通道、網際網路小型電腦系統介面 (Internet Small Computer System Interface, iSCSI)、超文字傳輸協定 (HTTP) 及檔案傳輸協定 (FTP)) 存取檔案和區塊資源的用戶端。
- **管理使用者** - 在設備上管理配置和服務的使用者。

本節僅適用於管理使用者。

管理使用者角色

您可以透過指定自訂角色給管理員的方式，將權限授予管理員。角色是一個可以指定給管理員的權限集合。您可以建立具備不同授權層次的多個管理員和操作員角色。您應該根據員工需求指定適當的角色給員工成員，而不要指定非必要的權限。

使用角色會比共用具有完整存取權的管理員密碼 (例如，將 root 密碼提供給每個人員) 更加安全。角色會將使用者的存取權限定為一組已定義的授權。此外，使用者角色可以追蹤至稽核日誌中的個別使用者名稱。系統預設會提供一個稱為「基本管理」的角色，這個角色包含最基本的授權。

管理使用者角色可以是：

- **本機使用者** – 其所有帳戶資訊都儲存在 Oracle ZFS Storage Appliance 上。

- **目錄使用者** – 使用現有的 NIS 或 LDAP 帳戶，而補充的授權設定值會儲存在設備上。需將設備的存取權明確授予現有的 NIS/LDAP 使用者，他們才能登入和管理設備。存取權無法透過預設方式授予。

管理範圍

授權可以讓使用者執行特定工作，例如，建立共用、將設備重新開機以及更新系統軟體。多個授權的群組稱為範圍。每個範圍都會有一組可以縮減授權數量的選擇性篩選。例如，不讓授權重新啟動所有服務，而是使用篩選以限制只能重新啟動 HTTP 服務。

存取控制清單

Oracle ZFS Storage Appliance 透過存取控制清單 (ACL) 來提供檔案存取控制。ACL 是允許或拒絕存取特定檔案或目錄的機制。

Oracle ZFS Storage Appliance 提供的 ACL 模型是以 NFSv4 ACL 模型 (此模型衍生自 Windows ACL 語意) 為基礎。這個豐富的 ACL 模型能夠精密地控制檔案和目錄的存取權。儲存設備內的每個檔案和目錄都有 ACL，而 SMB 和 NFS 兩者的所有存取控制決策都將透過相同的演算法，來判斷允許或拒絕要存取檔案和目錄的人員。

ACL 由一或多個存取控制項目 (ACE) 所組成。每個 ACE 都包含一個代表 ACE 授權或拒絕的項目、要套用 ACE 的人員以及要使用的繼承層次旗標。

ACL 繼承

NFSv4 ACL 會讓新建的文件和目錄能夠繼承個別的 ACE。ACE 繼承由多個繼承層次旗標所控制，管理員會在初始設定時於 ACL 上設定這些旗標。

判斷 ACL 存取權

NFSv4 ACL 會依序由上而下進行處理。當某個權限被授予後，後續的 ACE 將無法取消此權限。當某個權限被拒絕後，後續的 ACE 將無法再授予該權限。

SMB 共用層次 ACL

SMB 共用層次 ACL 會結合共用中的檔案或目錄 ACL，並藉此來判斷檔案的有效權限。共用層次 ACL 會在檔案 ACL 之上提供另一層的存取控制，進而提供更精確的存取控制

配置。使用 SMB 協定匯出檔案系統時，就會設定共用層次 ACL。如果不是使用 SMB 協定匯出檔案系統，則設定共用層次 ACL 將不會有任何作用。共用層次 ACL 預設會授予每個人完整的控制權。

ZFS ACL 特性

ACL 行為和繼承特性只適用於 NFS 用戶端。SMB 用戶端使用嚴格的 Windows 語意，而且優先順序高於 ZFS 特性。這兩者的差異在於 NFS 利用的是 POSIX 語意，而 SMB 用戶端不是。此特性大致上與 POSIX 相容。

資料服務

下表提供每項資料服務的描述和使用的連接埠。

表 1 資料服務

服務	描述	使用的連接埠
NFS	透過 NFSv3 和 NFSv4 協定存取檔案系統	111 和 2049
iSCSI	透過 iSCSI 協定存取 LUN	3260 和 3205
SMB	透過 SMB 協定存取檔案系統	SMB-over-NetBIOS 為 139 SMB-over-TCP 為 445 NetBIOS 資料封包為 138 NetBIOS 名稱服務為 137
病毒掃描	檔案系統病毒掃描	
FTP	透過 FTP 協定存取檔案系統	21
HTTP	透過 HTTP 協定存取檔案系統	80
HTTPS	內送安全連線	443
NDMP	NDMP 主機服務	10000
遠端複製	遠端複製	216 和 217
加密	檔案系統和 LUN 使用通透的加密	
陰影移轉	陰影資料移轉	
SFTP	透過 SFTP 協定存取檔案系統	218
TFTP	透過 TFTP 協定存取檔案系統	
儲存區域網路	儲存區域網路目標和啟動器群組	

最低連接埠需求

您可以建立防火牆來提供網路安全。建立防火牆需要使用連接埠號碼，連接埠號碼同時也是透過指定主機和服務所進行之網路交易的唯一識別。

下列為建立防火牆時的最低連接埠需求：

內送連接埠

- icmp/0-65535 (PING)
- tcp/1920 (EM)
- tcp/215 (BUI)
- tcp/22 (SSH)
- udp/161 (SNMP)

如果使用 HTTP 檔案共用，還需要其他內送連接埠 (一般並不使用)

- tcp/443 (SSL WEB)
- tcp/80 (WEB)

外送連接埠

- tcp/80 (WEB)

注意 - 若是進行複製，請儘可能使用 Generic Routing Encapsulation (GRE) 通道。這可讓流量在後端介面執行，避免經過防火牆而導致流量變慢。如果無法在 NFS 核心使用 GRE 通道，您就必須透過前端介面執行複製。在此情況下，還必須開放連接埠 216 和連接埠 217。

NFS 認證和加密選項

除了設備可以使用 Kerberos 來對使用者的管理登入和服務的存取權進行認證之外，Kerberos 也可以用來設定使用 NFS 協定的個別共用安全。

NFS 共用預設使用 AUTH_SYS RPC 認證配置。您也可以將它們設定為透過 Kerberos 安全共用。如果使用 AUTH_SYS 認證，NFS 伺服器在網路上傳送的為未經認證的用戶端 UNIX 使用者 ID (UID) 和群組 ID (GID)。此種認證機制很容易就能夠被用戶端上任何具備 root 存取權的人所破解，因此最好使用另一種安全模式。

您可以針對每個共用分別指定額外的存取控制，以便允許或不允許存取共用的特定主機、DNS 網域或網路。

安全模式

安全模式可在每個共用上個別設定。下列清單描述可用的 Kerberos 安全設定值：

- **krb5** - 透過 Kerberos V5 進行一般使用者認證
- **krb5i** - krb5 加上完整性保護 (防止資料封包遭到竄改)
- **krb5p** - krb5 加上私密性保護 (防止資料封包遭到竄改並予以加密)

您也可以在安全模式設定中指定各種 Kerberos 類型的組合。組合安全模式可以讓用戶端掛載任何列出的 Kerberos 類型。

Kerberos 類型

- **sys** - 系統認證
- **krb5** - 僅 Kerberos v5，用戶端必須使用此類型來掛載
- **krb5:krb5i** - Kerberos v5 以及完整性，用戶端可以使用列出的任何類型來掛載
- **krb5i** - 僅 Kerberos v5 完整性，用戶端必須使用此類型來掛載
- **krb5:krb5i:krb5p** - Kerberos v5 以及完整性或私密性，用戶端可以使用列出的任何類型來掛載
- **krb5p** - 僅 Kerberos v5 私密性，用戶端必須使用此類型來掛載

iSCSI 資料服務

當您在 Oracle ZFS Storage Appliance 上設定 LUN 時，您可以透過 iSCSI 目標來匯出該磁碟區。iSCSI 服務讓 iSCSI 啟動器可以使用 iSCSI 協定來存取目標。

此服務支援使用 iSNS 協定來進行尋找、管理以及組態。iSCSI 服務支援使用「查問交握式認證協定 (Challenge-Handshake Authentication Protocol, CHAP)」來進行單向 (目標認證啟動器) 和雙向 (目標和啟動器相互認證) 認證。再者，此服務支援「遠端認證撥入使用者服務 (Remote Authentication Dial-In User Service, RADIUS)」資料庫中的 CHAP 認證資料管理。

系統會先執行認證後再予以授權，這是兩個獨立的步驟。如果本機啟動器有 CHAP 名稱和 CHAP 密碼，系統就會執行認證。如果本機啟動器沒有 CHAP 特性，則系統不會執行任何認證，因此所有啟動器都可取得授權。

iSCSI 服務可讓您指定啟動器的全域清單，您可以在啟動器群組內使用此清單。使用 iSCSI 和 CHAP 認證時，RADIUS 可以作為 iSCSI 協定將所有 CHAP 認證委託給所選的 RADIUS 伺服器。

RADIUS 支援

RADIUS 系統會使用集中式伺服器來代替儲存節點執行 CHAP 認證。使用 iSCSI 和 CHAP 認證時，您可以選取 RADIUS 作為 iSCSI 協定 (iSCSI 和 iSCSI Extensions for RDMA (iSER) 皆適用)，然後將所有 CHAP 認證傳送給選取的 RADIUS 伺服器。

若要允許 Oracle ZFS Storage Appliance 使用 RADIUS 執行 CHAP 認證，必須符合下列條件：

- 設備必須指定與此 RADIUS 伺服器通訊時要使用的 RADIUS 伺服器位址與密碼。
- RADIUS 伺服器必須有一個能夠指定設備位址和上述密碼的項目 (例如，在其用戶端檔案中)。
- RADIUS 伺服器必須有一個能夠提供每個啟動器之 CHAP 名稱和相符 CHAP 密碼的項目 (例如，在其使用者檔案中)。
- 如果啟動器使用其 IQN 名稱作為 CHAP 名稱 (這是建議的配置)，且設備不需要在每個「啟動器」方塊使用不同的「啟動器」項目，則 RADIUS 伺服器可以執行所有的認證步驟。
- 如果啟動器使用不同的 CHAP 名稱，則設備在啟動器中就必須有一個指定 IQN 名稱與 CHAP 名稱對應的「啟動器」項目。此「啟動器」項目不需要指定啟動器的 CHAP 密碼。

SMB 資料服務

SMB 協定 (也稱為「通用網際網路檔案系統 (CIFS)」) 主要在 Microsoft Windows 網路上提供檔案的共用存取權。它也提供認證作業。

下列 SMB 選項有一些安全考量：

- **限制不能以匿名方式存取共用清單** - 此選項會要求用戶端在接收共用清單之前，先使用 SMB 進行認證。如果停用此選項，則匿名用戶端就可以存取共用清單。此選項預設為停用。
- **啟用 SMB 簽署** - 此選項會啟用與 SMB 用戶端 (使用 SMB 簽署功能) 的互通性。如果啟用此選項，將會驗證已簽署封包的簽章。如果停用此選項，則會在不驗證簽章的情況下接受未簽署的封包。此選項預設為停用。
- **需要 SMB 簽署** - 需要 SMB 簽署時即可使用此選項。啟用此選項時，所有 SMB 封包都必須經過簽署，否則將被拒絕。不支援 SMB 簽署的用戶端將無法連線伺服器。此選項預設為關閉。
- **啟用存取權的列舉** - 設定此選項會根據用戶端的證明資料來篩選目錄項目。當用戶端不具備某個檔案或目錄的存取權時，傳回該用戶端的項目清單中將會省略該檔案。此選項預設為停用。

Active Directory 網域模式認證

在「網域模式」下，使用者定義於 Microsoft Active Directory (AD) 中。SMB 用戶端可以使用 Kerberos 或 NTLM 認證連線到 Oracle ZFS Storage Appliance。

當使用者透過完整 Oracle ZFS Storage Appliance 主機名稱連線時，相同網域或信任網域中的 Windows 用戶端將會使用 Kerberos 認證，而其他則會使用 NTLM 認證。

SMB 用戶端使用 NTLM 認證連線至設備時，使用者的證明資料會轉送到 AD 網域控制站進行認證。這稱為傳遞式 (pass-through) 認證。

如果 Windows 安全原則中定義了禁止使用 NTLM 認證，則 Windows 用戶端必須透過完整主機名稱才能連線至設備。如需詳細資訊，請參閱此 Microsoft Developer Network 文章：

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/jj865668(v=ws.10)?redirectedfrom=MSDN

認證後，將針對使用者的 SMB 階段作業建立「安全相關資訊環境」。此安全相關資訊環境所代表的使用者會具有唯一「安全描述元 (SID)」。此 SID 代表檔案擁有權，可用來判斷檔案的存取權限。

工作群組模式認證

在工作群組模式下使用者定義於 Oracle ZFS Storage Appliance 的本機中。當 SMB 用戶端以「工作群組模式」連線至設備時，會使用該使用者的使用者名稱和密碼雜湊在本機認證該使用者。

LAN Manager (LM) 相容性層次可指定設備在「工作群組模式」時用於認證的協定。

下列清單顯示每個 LM 相容性層次的 Oracle ZFS Storage Appliance 行為：

- 層次 2：接受 LM、NTLM 以及 NTLMv2 認證
- 層次 3：接受 LM、NTLM 以及 NTLMv2 認證
- 層次 4：接受 NTLM 和 NTLMv2 認證
- 層次 5：只接受 NTLMv2 認證

「工作群組使用者」成功認證後，就會建立安全相關資訊環境。系統會使用機器 SID 和使用者 UID 的組合，為設備中定義的使用者建立唯一的 SID。所有本機使用者都會定義為 UNIX 使用者。

本機群組和權限

本機群組是可提供額外權限給使用者的網域使用者群組。「管理員」可以略過檔案權限並變更檔案的擁有權。「備份操作員」可以略過檔案存取控制並備份和回復檔案。

透過 Microsoft 管理主控台的管理作業

為了確保只有適當的使用者可以存取管理作業，使用者在遠端使用 Microsoft 管理主控台 (MMC) 執行作業時會有存取限制。

下列清單顯示使用者及其允許的作業：

- **一般使用者** - 列出共用的項目。
- **Administrators 群組的成員** - 列出開啟的檔案和關閉的檔案、中斷使用者連線、檢視服務和事件日誌。Administrators 群組的成員也可以設定和修改共用層次 ACL。

病毒掃描

「病毒掃描」服務會在檔案系統層次掃描病毒。不論透過任何協定存取檔案，「病毒掃描」服務都會先掃描檔案，如果發現病毒，該檔案將被拒絕存取並加以隔離。這個掃描是由 Oracle ZFS Storage Appliance 連線的外部引擎執行。此外部引擎未包括在設備軟體中。

使用最新的病毒定義掃描檔案後，該檔案直到下次修改之後才會被重新掃描。病毒掃描功能的適用對象主要是可能引進病毒的 SMB 用戶端。NFS 用戶端也可以使用病毒掃描，不過，由於 NFS 協定運作的方式，可能無法像 SMB 用戶端一樣快速地偵測出病毒。

時序攻擊的延遲引擎

SMB 不會實作防止時序攻擊的延遲引擎。它仰賴的是 Oracle Solaris 加密架構。

纜線上的資料加密

SMB 服務使用版本 1 的 SMB 協定，而此協定不支援纜線上的資料加密。

FTP 資料服務

FTP 可以讓 FTP 用戶端存取檔案系統。FTP 服務不允許匿名登入，使用者必須使用設定的名稱服務進行認證。

FTP 支援下列安全設定值。啟用 FTP 協定存取的所有檔案系統皆共用下列設定值：

- **啟用 SSL/TLS** - 允許 SSL/TLS 加密的 FTP 連線，並確定 FTP 交易經過加密。此選項預設為停用。FTP 伺服器使用自行簽署的安全憑證或客戶提供的憑證。
- **SSL/TLS 版本和加密方法** - FTP 連線適用的 SSL/TLS 協定版本和加密方法。預設值為 TLSv1.1、TLSv1.2 與其關聯的加密方法。基於安全考量，預設不會啟用 TLSv1.0，但是可以啟用以提供回溯相容性。BUI 中的加密方法清單會依選取的版本而有所不同。部分選取的 SSL/TLS 協定版本和 (或) 加密方法在軟體升級後若不再受到支援，就會被移除。除非情況特殊或在 Oracle 客戶服務部的指示下而改用其他設定之外，請維持使用預設值，以避免發生服務無法使用的情形。

- **允許 root 登入** - 允許 root 使用者登入 FTP。此選項預設為關閉，因為 FTP 認證使用純文字，而這很可能會引發網路竊聽 (sniffing) 攻擊的安全威脅。
- **允許的登入嘗試次數上限** - FTP 連線中斷前允許的登入嘗試失敗次數，在此之後，使用者必須重新連線才能再次嘗試。預設值為 3。
- **記錄日誌層級** - 日誌的詳細程度。

FTP 支援下列日誌：

- **proftpd** - 包括成功和失敗之登入嘗試的 FTP 事件
- **proftpd_xfer** - 檔案傳輸日誌
- **proftpd_tls** - 與 SSL/TLS 加密相關的 FTP 事件

HTTP 資料服務

HTTP 透過使用 HTTP 和 HTTPS 協定以及 HTTP 擴充功能 Web 型分工編寫及版本管理 (Web based Distributed Authoring and Versioning, WebDAV) 來存取檔案系統。這可讓用戶端透過 Web 瀏覽器或以本機檔案系統的形式 (如果其用戶端軟體支援的話) 存取共用檔案系統。

HTTPS 伺服器使用自行簽署的安全憑證或客戶提供的憑證。若要取得客戶提供的憑證，您必須產生「憑證簽署要求 (CSR)」，並將它傳送到「憑證授權機構 (CA)」以取得簽章。從 CA 傳回簽署過的憑證之後，便可將它安裝在設備上。如果憑證是由非根 CA 簽署，則還必須取得第二層和更高層 CA 的憑證。如需關於憑證管理的詳細資訊，請參閱 *Oracle ZFS Storage Appliance Administration Guide*。

提供的特性如下：

- **要求用戶端登入** - 用戶端必須先經過認證才能允許存取共用，而這些用戶端建立的檔案也會由他們所擁有。如果沒有設定此選項，則建立的檔案會由 HTTP 服務所擁有，而使用者將標示為 "nobody"。
- **協定** - 選取要支援的存取方法：HTTP、HTTPS 或兩者。
- **HTTP 連接埠 (內送連線)** - HTTP 連接埠，預設值為連接埠 80。
- **HTTPS 連接埠 (內送安全連線)** - HTTPS 連接埠，預設連接埠為 443。
- **SSL/TLS 版本和加密方法** - HTTP 連線適用的 SSL/TLS 協定版本和加密方法。預設值為 TLSv1.1、TLSv1.2 與其關聯的加密方法。基於安全考量，預設不會啟用 TLSv1.0，但是可以啟用以提供回溯相容性。BUI 中的加密方法清單會依選取的版本而有所不同。部分選取的 SSL/TLS 協定版本和 (或) 加密方法在軟體升級後若不再受到支援，就會被移除。除非情況特殊或在 Oracle 客戶服務部的指示下而改用其他設定之外，請維持使用預設值，以避免發生服務無法使用的情形。

啟用「要求用戶端登入」時，若本機使用者、NIS 使用者或 LDAP 使用者未提供有效的認證證明資料，Oracle ZFS Storage Appliance 將會拒絕這些用戶端的存取。不支援 Active Directory 認證。只支援基本 HTTP 認證。除非使用 HTTPS，否則傳輸的使用

者和密碼將不會加密，這對於所有環境來說都是不適當的。如果停用「要求用戶端登入」，則設備不會嘗試認證證明資料。

無論認證與否，建立的檔案和目錄都不會遮罩權限。所有人都會具備新建檔案的讀取和寫入權限。而所有人也都會具備新建目錄的讀取、寫入以及執行權限。

NDMP 資料服務

網路資料管理協定 (NDMP) 讓 Oracle ZFS Storage Appliance 可以參與由遠端 NDMP 用戶端 (稱為「資料管理應用程式 (DMA)」) 控制的 NDMP 式備份與回復作業。使用 NDMP 時，設備使用者資料 (例如，設備中儲存於管理員建立之共用內的資料) 可以同時備份與回復到與本機連接的裝置 (例如，磁帶機) 和遠端系統。與本機連接的裝置也可以透過 DMA 進行備份與回復。

遠端複製資料服務

Oracle ZFS Storage Appliance 遠端複製可協助您提升專案和共用的複製作業。此服務可讓您檢視哪些設備將資料複製到某個特定設備，並控制某個特定設備可以複製到哪些設備。

啟用此服務時，設備會接收來自其他設備的複製更新，並根據設定的動作傳送本機專案和共用的複製更新。停用此服務時，內送複製更新會失敗，且不會複製任何本機專案和共用。

配置設備的遠端複製目標時需要使用遠端設備的 root 密碼。這些目標可用來設定已啟用設備通訊的複製對等連線。

建立目標期間，將使用 root 密碼來確認要求的真實性，並產生及交換安全金鑰 (此金鑰將在後續通訊中用於識別設備)。

產生的金鑰會永久儲存為設備配置的一部分。root 密碼一律不會永久儲存，也不會以未加密的形式傳送。所有設備通訊 (包括此初始識別交換) 皆使用 SSL 保護。

Oracle ZFS Storage Appliance 的離線複製功能可減少在透過有限頻寬的網路複製大型資料集時所需的時間、資源以及可能發生的資料錯誤。離線複製會將複製串流匯出成 NFS 伺服器上的檔案，如此便能夠以物理方式移動至遠端目標位置，或是選擇將它複製到外部媒體加以運送。在目標位置這邊，管理員可將包含複製串流的檔案匯入目標設備。

若要限制存取匯出的複製串流，請僅對來源和目標設備的 IP 位址顯示 NFS 共用。若要加密此資料，請對 NFS 伺服器的 NFS 共用啟用磁碟加密。請參閱您的 NFS 伺服器文件瞭解詳細資訊。請注意，設備一律不會對匯出的複製串流加密。

使用資料加密

注意 - 對某些型號而言，加密是授權的功能。如需詳細資訊，請參閱 "Oracle Software License Agreement ("SLA") and Entitlement for Hardware Systems with Integrated Software Options"，以及軟體發行版本的 Licensing Information User Manual。

Oracle ZFS Storage Appliance 為個別的共用 (檔案系統和 LUN) 和在專案內建立的共用提供通透的資料加密方式。從軟體發行版本 OS8.8.0 開始，可以在儲存集區建立時，設定要求對所有專案和內送複製串流加密。當設定集區對專案啟用加密時，預設共用將會繼承集區的加密設定。初始設備安裝期間或重設為出廠設定後的重新設定組態期間，無法設定集區加密特性，因為此時尚未設定任何金鑰存放區。

管理加密金鑰

設備包含內建的 LOCAL 金鑰存放區，並且可連線至 Oracle Key Manager (OKM) 系統。每個加密的專案或共用皆需要 LOCAL 或 OKM 金鑰存放區的包裝金鑰。資料加密金鑰由儲存設備所管理，並且由 LOCAL 或 OKM 金鑰存放區的包裝金鑰以加密方式永久儲存。

OKM 是一個全面的金鑰管理系統 (KMS)，可因應企業對儲存體資料加密的快速成長需求。由於和開放式標準相容，此功能可在散布各處的異質儲存架構中提供集中管理加密金鑰所需的能力、擴充性和互通性。

OKM 可滿足儲存體金鑰管理的獨特需求，包括：

- **長期保留金鑰** - OKM 可確保歸檔資料始終可供使用，並在完整資料週期中安全地保留加密金鑰。
- **互通性** - OKM 的單一儲存體金鑰管理服務，可提供支援連接至大型主機或開放式系統的多種儲存裝置所需的互通性。
- **高可用性** - 具有主動式 N-node 叢集、動態負載平衡及自動化容錯移轉的特性，因此無論設備是設置在一起或分佈於全球各地，OKM 皆可提供高可用性。
- **大容量**- OKM 可管理大量儲存裝置，甚至是更多的儲存體金鑰。單一叢集的設備可為成千上萬個儲存裝置和數百萬個儲存體金鑰提供金鑰管理服務。
- **彈性金鑰配置** - 每個 OKM 叢集都會自動產生金鑰，或是個別建立 LOCAL 或 OKM 金鑰存放區。安全管理員負責提供要與金鑰存放區結合的金鑰名稱，將指定的包裝金鑰與專案或共用相關聯。

維護金鑰

使用停用狀態之 OKM 金鑰的共用和專案仍然可供存取。若要禁止使用某 OKM 金鑰，OKM 管理員必須明確刪除該金鑰。

若要確保加密的共用和專案可供存取，請備份您的設備配置和 LOCAL 金鑰存放區金鑰值。如果金鑰無法使用，則使用該金鑰的任何共用或專案也將無法存取。如果專案金鑰無法使用，便無法在該專案中建立新的共用。

金鑰可能因為下列情形而無法使用：

- 金鑰已刪除
- 倒回至不支援加密的版本
- 倒回至尚未配置這些金鑰的版本
- 重設為出廠設定
- OKM 伺服器無法使用

加密金鑰生命週期

加密金鑰的生命週期具有彈性，因為您隨時可在不使資料服務離線的情況下變更金鑰。

當金鑰自金鑰存放區刪除後，便會卸載使用該金鑰的所有共用，其資料也將無法存取。應使用 OKM 備份服務來執行 OKM 金鑰存放區中的金鑰備份。LOCAL 金鑰存放區中的金鑰，會在執行「系統配置備份」時一併備份。對於 LOCAL 金鑰存放區，還可在建立時依值提供金鑰以允許在外部系統中託管，如此可提供替代的依金鑰備份/回復功能。

陰影移轉資料服務

陰影移轉允許來自外部或內部來源的自動資料移轉，並控制自動背景移轉。不論是否啟用此服務，頻內要求的資料都會同步移轉。此服務的主要目的是允許使用者調整背景移轉專用的繫線數目。

掛載在 NFS 來源上的 NFS 不是由 Oracle ZFS Storage Appliance 使用者所控制。因此，陰影移轉掛載並不安全；如果伺服器應使用 Kerberos 或是要進行類似要求，則來源掛載將被拒絕。

SFTP 資料服務

SSH 檔案傳輸協定 (SFTP) 可允許 SFTP 用戶端存取檔案系統。不允許匿名登入，因此使用者必須使用設定的名稱服務進行認證。

建立 SFTP 金鑰時，您必須包括使用者特性和有效的使用者指定項目。SFTP 金鑰依使用者分組，並透過 SFTP 根據使用者名稱加以認證。

注意 - 儘管現有 SFTP 金鑰仍將進行認證，但基於安全理由，請重新建立未包含使用者特性的現有 SFTP 金鑰。

SFTP 支援下列安全設定值。啟用 SFTP 協定存取的所有檔案系統皆共用下列設定值：

- **加密方法** - SFTP 連線適用的加密方法。
- **MAC** - SFTP 連線的訊息認證碼 (MAC)。

TFTP 資料服務

「檔案傳輸協定 (TFTP)」是簡易的傳輸檔案協定。這個協定小型且容易實作，但缺乏 FTP 的大部分安全功能。TFTP 只能讀取和寫入遠端伺服器的檔案。它無法列出目錄，且目前不提供使用者認證功能。

儲存區域網路

在「儲存區域網路 (SAN)」中，目標和啟動器群組會定義多組可以和「邏輯單位號碼 (LUN)」關聯的目標和啟動器。與目標群組關聯的 LUN 只能透過這些群組的目標進行存取。與啟動器群組關聯的 LUN 也只能由這些群組的啟動器進行存取。建立 LUN 時，您會將啟動器群組和目標群組套用至 LUN。您必須定義至少一個目標群組和一個啟動器群組，才能順利建立 LUN。

除了只有在使用 iSCSI/iSER 啟動器存取時能夠選取的「查問交握式認證協定 (Challenge-Handshake Authentication Protocol, CHAP)」認證之外，不會執行其他認證。

注意 - 使用預設的啟動器群組可能會導致使用不想使用或相衝突的 LUN 啟動器。

目錄服務

本節描述可以在設備上設定的目錄服務及其安全相關問題。

網路資訊服務

網路資訊服務 (NIS) 是集中目錄管理的名稱服務。Oracle ZFS Storage Appliance 可以作為使用者和群組的 NIS 用戶端，因此 NIS 使用者可以登入 FTP 和 HTTP/WebDAV。NIS 使用者也可以取得設備管理的權限。設備將使用本身的權限設定值來補充 NIS 資訊。

輕量型目錄存取協定

Oracle ZFS Storage Appliance 使用「輕量型目錄存取協定 (LDAP)」來認證管理使用者和部分資料服務使用者 (FTP、HTTP)。設備支援 LDAP-over-SSL 安全。LDAP 可用來擷取使用者和群組的相關資訊，其使用方式如下：

- 提供用以接受及顯示使用者和群組名稱的使用者介面。
- 針對使用名稱的資料協定 (例如 NFSv4) 提供使用者和群組名稱的對應。
- 定義存取控制中使用的群組成員身分。
- (選擇性) 攜帶用於管理和資料存取認證的認證資料。

LDAP 連線可以作為認證機制使用。例如，當使用者嘗試向 ZFS Storage Appliance 認證時，設備可以嘗試向 LDAP 伺服器認證該使用者，這就是使用 LDAP 連線來驗證使用者認證的機制。

LDAP 連線安全有多種控制方式：

- 設備到伺服器認證：
  - 設備為匿名
  - 設備利用使用者的 Kerberos 證明資料進行認證
  - 設備利用指定的「代理」使用者和密碼進行認證
- 伺服器到設備的認證 (確認連線至正確的伺服器)：
  - 不受保護
  - 伺服器使用 Kerberos 進行認證
  - 伺服器使用 TLS 憑證進行認證

如果使用的是 Kerberos 或 TLS，則透過 LDAP 連線攜帶的資料會經過加密，除此之外則不會加密。使用 TLS 時，於配置期間進行的第一次連線不是安全連線。伺服器的憑證會在該期間收集，並用來認證後續的實際執行連線。

您無法匯入一個用來認證多個 LDAP 伺服器的「憑證授權機構」憑證，也無法手動匯入特定 LDAP 伺服器的憑證。

只支援原始 TLS (LDAPS)。不支援 STARTTLS 連線 (此連線會在不安全的 LDAP 連線上開始，然後變更為安全的連線)。不支援需要用戶端憑證的 LDAP 伺服器。

識別對應

用戶端可以使用 SMB 或 NFS 在 Oracle ZFS Storage Appliance 存取檔案資源，每個用戶端都有唯一的使用者 ID。SMB/Windows 使用者有「安全描述元 (SID)」，而 UNIX/

Linux 使用者有「使用者 ID (UID)」。使用者也可以是群組的成員，這些群組由「群組 SID」(Windows 使用者) 或「群組 ID (GID)」(UNIX/Linux 使用者) 來加以識別。

在使用兩種協定存取檔案資源的環境中，通常會希望建立識別同等性，例如 UNIX 使用者等同於 Active Directory 使用者。這一點對判斷設備上檔案資源的存取權而言非常重要。

與「目錄服務」(例如，Active Directory、LDAP 以及 NIS) 相關的識別有多種類型。使用目錄服務時，請謹慎遵循安全性的最佳應用。

Identity Management for UNIX

Microsoft 提供一種稱為 Identity Management for UNIX (IDMU) 的功能。此軟體適用於 Windows Server 2003，並隨附於 Windows Server 2003 R2 和更新版本。此功能在未隨附於軟體時屬於 Services for UNIX 的一部分。

IDMU 的主要用途是支援 Windows 作為 NIS/NFS 伺服器。IDMU 讓管理員可以指定多個 UNIX 相關參數：UID、GID、登入 Shell、本位目錄以及與前述類似的群組項目。透過類似於 (但不完全相同) RFC 2307 的綱要與透過 NIS 服務，就可以利用 AD 來使用這些參數。

使用 IDMU 對應模式時，識別對應服務會使用這些 UNIX 屬性來建立 Windows 和 UNIX 識別之間的對應。這個方法非常類似於目錄式對應，但識別對應服務會查詢由 IDMU 軟體建立的特性綱要，而非允許自訂綱要。使用此方法時，就不能使用其他目錄式對應。

目錄式對應

目錄式對應會在 LDAP 或 Active Directory 物件中加註關於如何將識別對應到相對平台之同等識別的資訊。您必須配置這些與物件關聯的額外屬性。

名稱式對應

名稱式對應會建立各種依名稱對應識別的規則。這些規則會建立 Windows 識別和 UNIX 識別之間的同等性。

暫時對應

如果某個特定使用者沒有套用名稱式對應規則，則該使用者會透過暫時對應來取得暫時證明資料，除非使用者遭到拒絕對應的封鎖。使用暫時 UNIX 名稱的 Windows 使用者在系統上建立檔案時，使用 SMB 存取該檔案的 Windows 用戶端會看到此檔案是由該 Windows 識別所擁有。不過，NFS 用戶端則會看到檔案是由 “nobody” 所擁有。

系統設定值

後續各節描述可用的系統安全設定值。

Phone Home

Phone Home 服務的功用為管理 Oracle ZFS Storage Appliance 註冊以及 Phone Home 遠端支援服務。這些訊息中不會傳送任何使用者資料或描述資料。

註冊會將您的 Oracle ZFS Storage Appliance 連線到 Oracle 的產品目錄入口網站，您可以透過此網站管理您的 Oracle 設備。您必須先註冊才能使用 Phone Home 服務。

Phone Home 服務會與 Oracle Support 通訊並提供下列功能：

- **錯誤報告** - 系統會向 Oracle 報告作用中的問題，並取得自動化服務回應。視錯誤的本質而定，支援案例可能會維持在未結案狀態。
- **活動訊號** - 每日活動訊號訊息會傳送給 Oracle 以指示該系統目前啟動並在執行中。當已啟動的系統在一段時間內未傳送活動訊號時，Oracle 客戶服務部會通知此帳戶的技術聯絡人員。
- **系統組態** - 定期傳送訊息給 Oracle，這些訊息描述目前軟體及硬體的版本和組態，以及儲存組態。

服務標記

「服務標記」可透過允許查詢 Oracle ZFS Storage Appliance 的下列資料來簡化產品目錄與支援：

- 系統序號
- 系統類型
- 軟體版本號碼

您可以向 Oracle Support 註冊「服務標記」，這樣做可讓您輕鬆追蹤您的 Oracle 設備並加速服務電話的作業。預設會啟用服務標記。

Kerberos 服務

搭配 Kerberos 環境一起使用時，Kerberos 服務會為設備管理登入和服務的存取權 (例如 NFS、HTTP、FTP、SFTP 以及 SSH) 提供認證。設備使用者必須具有相同名稱的 Kerberos 主體，以針對這些服務使用 Kerberos 認證。Kerberos 也可以用來設定使用 NFS 協定的個別共用安全，如「NFS 認證和加密選項」[11] 所述。

Kerberos 和 Active Directory 具有不同的範圍和金鑰，因此可以同時啟用。若兩者均為作用中，則預設值為 Kerberos 範圍。若僅 Active Directory 為作用中，則預設值為 Active Directory 範圍。

簡易郵件傳輸協定

「簡易郵件傳輸協定 (SMTP)」會傳送 Oracle ZFS Storage Appliance 產生的所有郵件 (通常是根據配置的警示所產生的回應)。SMTP 不接受外部郵件；它只會傳送由設備本身自動產生的郵件。

SMTP 服務預設使用 DNS (MX 記錄) 來判斷要將郵件傳送到哪裡。如果設備的網域沒有配置 DNS，或者外送郵件的目的地網域沒有正確配置 DNS MX 記錄，則設備可以配置為透過外送郵件伺服器來轉送所有郵件。

簡易網路管理協定

「簡易網路管理協定 (SNMP)」在 Oracle ZFS Storage Appliance 上提供兩種功能：SNMP 可以提供設備狀態資訊，並可以將警示設定為傳送 SNMP 設陷。當啟用此項服務時，可使用 SNMP v1、v2c 及 v3 版本。設備最多可支援 128 個實體和邏輯網路介面。

系統日誌訊息

系統日誌訊息是小型的事件訊息，可從 Oracle ZFS Storage Appliance 傳送到一或多個遠端系統。系統日誌提供兩種設備功能：

- 警示可以配置為傳送系統日誌訊息給一或多個遠端系統
- 設備上具備系統日誌功能的服務可以將其系統日誌訊息轉送給遠端系統

系統日誌可以設定為使用 RFC 3164 描述的傳統輸出格式；或是使用 RFC 5424 所描述的更新版本輸出格式。系統日誌訊息可以用 UDP 資料封包方式傳送。因此，如果傳送系統的記憶體不足或網路擁塞時，這些封包可能會被網路捨棄，或者根本就不會傳送。所以，管理員應該要假設訊息在發生網路複雜失敗情況時可能會遺失與被捨棄。

訊息包含下列元素：

- 設備 - 描述發送訊息的系統元件類型
- 嚴重性 - 描述訊息相關狀況的嚴重性
- 時戳 - 描述事件的相關時間 (UTC 格式)
- 主機名稱 - 描述設備正規名稱
- 標記 - 描述發送訊息的系統元件名稱

- 訊息 - 描述事件本身

系統識別

此服務提供系統名稱和位置的組態。如果將 Oracle ZFS Storage Appliance 系統移至其他網路位置或改變用途，則可能需要變更系統名稱和位置。

磁碟檢測

磁碟檢測應定期執行，讓 Oracle ZFS Storage Appliance 可以偵測並修正磁碟上損壞的資料。磁碟檢測是一個背景處理作業，它會在磁碟閒置期間讀取磁碟，以偵測非經常存取磁區中無法修正的讀取錯誤。即時偵測到這類的潛在磁區錯誤將會減少資料的損失。

預防毀損

啟用「預防毀損」功能後，共用或專案就不會被毀棄。這包括下列情況：透過相依複製毀棄共用、毀棄專案中的共用或毀棄複製套件。不過，此功能對透過複製更新所發生的共用毀棄沒有作用。如果 Oracle ZFS Storage Appliance 系統上損毀的共用是複製來源，則目標上對應的共用將被毀棄 (即使已經設定此特性)。

若要毀棄共用，必須先在個別步驟中明確關閉此特性。此特性預設為關閉。

安全日誌

本節描述與安全有關的記錄日誌功能。

稽核日誌

稽核日誌會記錄使用者活動事件，包括登入及登出 BUI 和 CLI 以及管理動作。下表顯示範例稽核日誌項目在 BUI 中顯示的外觀：

表 2 稽核日誌記錄

時間	使用者	主機	摘要	階段作業註解
2021-10-12 05:20:24	root	galaxy	停用 FTP 服務	

時間	使用者	主機	摘要	階段作業註解
2021-10-12 03:17:05	root	galaxy	使用者登入	
2021-10-11 22:38:56	root	galaxy	瀏覽器階段作業逾時	
2021-10-11 21:13:35	root	<console>	啟用 FTP 服務	

Phone Home 日誌

如果使用 Phone Home，此日誌將會顯示與 Oracle 客戶服務部的通訊事件。下表是範例 Phone Home 項目在 BUI 中顯示的外觀：

表 3 Phone Home 日誌記錄

時間	描述	結果
2021-10-12 05:24:09	上傳檔案 'cores/ak.45e5ddd1-ce92-c16e-b5eb-9cb2a8091f1c.tar.gz' 至 Oracle Support	正常

其他資訊

您可以在下列位置找到關於 Oracle ZFS Storage Appliance 的完整產品資訊：

https://docs.oracle.com/en/storage/

使用 BUI 來設定 Oracle ZFS Storage Appliance 時，您可以按一下任一畫面右上角的「說明」連結來顯示該畫面的說明。