Oracle® ZFS 儲存設備安全指南

ORACLE®

Oracle ZFS 儲存設備安全簡介

本指南探討、複習以及說明建立安全儲存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 儲存設備 (ZFSSA) 功能安全考量相關的詳細資訊。如需設備配置程序的相關資訊，請參閱 Oracle ZFS Storage System Administration Guide。

下列各節提供 ZFSSA 安全功能的描述：

- **初始安裝** - 描述如何設定管理存取、如何建立 root 帳戶以及將 ZFSSA 重設為出廠設定的影響。
- **實體安全** - 描述 ZFSSA 的實體安全環境。
- **管理模型** - 描述限制存取 CLI 和 BUI、系統修正模型、暫緩更新、支援組合以及配置備份。
- **ZFSSA 使用者** - 描述管理角色、可以管理 ZFSSA 的人員以及管理使用者授權。
- **存取控制清單 (ACL)** - 描述用以允許或拒絕存取檔案和目錄的機制。
- **儲存區域網路 (SAN)** - 描述邏輯單位號碼 (LUN)、相關的啟動器群組以及啟動器認證選項和預設值。
- **資料服務** - 描述 ZFSSA 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 ZFSSA 上配置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、SMTP、SNMP、系統日誌、系統識別、磁碟檢測以及預防毀損。
- **遠端管理存取** - 描述透過 BUI 和 CLI 的遠端存取。
- **日誌** - 描述與安全相關的日誌類型。

初始安裝

ZFSSA 在出貨給客戶時已預先安裝 ZFSSA 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 密嗎。如果將 ZFSSA 重設為出廠預設值，則 ZFSSA 和服務處理器的 root 密碼也會同時重設為預設值。

在 ZFSSA 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 ZFSSA 的權限，管理員接著必須利用此權限執行系統的初始安裝步驟。其中一個必要步驟是設定新的 ZFSSA 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。

ZFSSA 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 ZFSSA 管理模型的安全。

限制存取 (CLI 和 BUI)

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)) 授權的使用者可以管理「瀏覽器使用者介面 (BUI)」和「指令行介面 (CLI)」。

管理動作會透過安全通訊端層 (SSL) 指令行登入或 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 ZFSSA 初始安裝時產生的唯一憑證。HTTPS 階段作業的使用者可定義預設階段作業逾時為 15 分鐘。

系統更新

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

當您的系統註冊 Phone Home 支援後，如果系統發生重大錯誤，系統狀態將會傳送到 My Oracle Support，而工程支援人員將針對收到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。

ZFSSA 使用者

ZFSSA 使用者可分為兩種：

- **資料服務使用者** – 使用支援的協定 (例如，NFS、SMB、光纖通道、iSCSI、http 以及 FTP) 存取檔案和區塊資源的用戶端。
- **管理使用者** - 在 ZFSSA 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

透過指派自訂角色給管理員的方式即可將權限授予管理員。角色是一個可以指派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派適當的角色給員工成員，而不要指派非必要的權限。

使用角色比使用可獲得完整存取權的共用管理員密碼 (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 ZFSSA 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 ZFSSA 上。這樣可以讓現有的 NIS/LDAP 使用者登入並管理 ZFSSA，但現有的 NIS/LDAP 使用者預設是無法登入 ZFSSA 的。您必須將存取權明確授予 ZFSSA 才行。

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 ZFSSA 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小授權數量的選擇性篩選。例如，讓授權不會重新啟動所有服務，而是使用篩選讓授權只能重新啟動 HTTP 服務。

存取控制清單 (ACL)

ZFSSA 可以透過存取控制清單 (ACL) 來控制檔案的存取。存取控制清單是允許或拒絕存取特定檔案或目錄的一種機制。

ZFSSA 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。這個種豐富的 ACL 模型能夠精密地控制檔案和目錄的存取權。儲存體 ZFSSA 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，來判斷允許或拒絕存取檔案和目錄的人員。

ACL 由一或多個 ACE (存取控制項目) 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，管理員會在初始安裝時於 ACL 上設定這些旗標。

判斷 ACL 存取權

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

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。

儲存區域網路 (SAN)

在 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：如果使用預設啟動器群組，可能會將 LUN 暴露給不想使用或相衝突的啟動器。

資料服務

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
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
NDMP	NDMP 主機服務	10000
遠端複製	遠端複製	216
陰影移轉	陰影資料移轉	
SFTP	透過 SFTP 協定存取檔案系統	218
SRP	透過 SRP 協定存取區塊	
TFTP	透過 TFTP 協定存取檔案系統	
病毒掃描	檔案系統病毒掃描	

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。

NFS 認證和加密選項

NFS 共用預設使用 AUTH_SYS RPC 認證配置。您也可以將它們配置為透過 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 uid 和 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)
- krb5i - 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

當您在 ZFSSA 上配置 LUN 時，您可以透過「網際網路小型電腦系統介面 (Internet Small Computer System Interface, 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、管理以及配置。iSCSI 服務支援使用 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 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

「遠端認證撥入使用者服務 (Remote Authentication Dial-In User Service, 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 ZFSSA 使用 RADIUS 執行 CHAP 認證，必須符合下列條件：

- ZFSSA 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 (例如，在其用戶端檔案中) 必須有一個能夠指定 ZFSSA 位址和上述密碼的項目。
- RADIUS 伺服器 (例如，在其使用者檔案中) 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。
- 如果啟動器使用其 IQN 名稱作為 CHAP 名稱 (這是建議的配置)，且 ZFSSA 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 ZFSSA 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。

伺服器訊息區塊 (SMB)

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 (AD) 網域模式認證

在「網域模式」下，使用者定義於 Active Directory 中。SMB 用戶端可以使用 Kerberos 或 NTLM 認證連線到 ZFSSA。

當使用者透過完整 ZFSSA 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 ZFSSA 時，使用者的證明資料會轉送到 AD 網域控制器進行認證。這稱為傳遞式認證。

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 ZFSSA。如需詳細資訊，請參閱這份 MSDN 文章：http://technet.microsoft.com/en-us/library/jj865668%28v=ws.10%29.aspx。

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 ZFSSA 的本機中。SMB 用戶端在「工作群組模式」中連線 ZFSSA 時，會利用使用者的使用者名稱和密碼雜湊在本機上認證該使用者。

LAN Manager (LM) 相容性層次可指定 ZFSSA 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 ZFSSA 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，來針對 ZFSSA 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 (MMC) 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 MMC 執行作業時會有一些存取限制。

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
- Administrator 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
- Administrator 群組的成員也可以設定/修改共用層次 ACL
- Administrator 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

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。這個掃描是由支援 ZFSSA 的外部引擎執行。此外部引擎未包括在 ZFSSA 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 不會實作任何防止時序攻擊的引擎。它仰賴的是 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。

檔案傳輸協定 (FTP)

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

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

- 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。
- 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 認證使用的是純文字，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。
- 記錄日誌層次 - 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

超文字傳輸協定 (HTTP)

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。這樣可以讓用戶端透過網頁瀏覽器存取共用的檔案系統，或將共用的檔案系統當作本機檔案系統 (如果用戶端軟體支援的話)。HTTPS 伺服器使用自行簽署的安全憑證。

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。

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，ZFSSA 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 ZFSSA 不會嘗試進行認證。

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。

網路資料管理協定 (NDMP)

NDMP 讓 ZFSSA 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，ZFSSA 使用者資料 (例如，ZFSSA 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

ZFSSA 遠端複製可協助您提升專案和共用的複製作業。此服務可讓您檢視將資料複製到此 ZFSSA 的其他 ZFSSA，並且配置此 ZFSSA 可以複製到哪些 ZFSSA。

啟用此服務時，ZFSSA 會接收來自其他 ZFSSA 的複製更新，並根據配置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 ZFSSA 的遠端複製目標時需要使用遠端 ZFSSA 的 root 密碼。這些目標可用來設定已啟用 ZFSSA 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 ZFSSA)。

產生的金鑰會永久儲存為 ZFSSA 配置的一部分。root 密碼一律不會永久儲存。root 密碼一律不會以純文字傳送。所有 ZFSSA 通訊 (包括此初始識別交換) 皆使用 SSL 保護。

陰影移轉

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 ZFSSA 使用者來控制。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。

SSH 檔案傳輸協定 (SFTP)

SFTP 可以讓 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配置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派項目。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。

Trivial 檔案傳輸協定 (TFTP)

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。

目錄服務

網路資訊服務 (NIS)

NIS 是集中目錄管理的名稱服務。ZFSSA 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 ZFSSA 管理的權限。ZFSSA 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 (LDAP)

ZFSSA 使用 LDAP 來認證管理使用者和部分資料服務使用者 (ftp、http)。ZFSSA 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 ZFSSA 認證時，ZFSSA 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)：
  1. 不受保護
  2. 伺服器使用 Kerberos 進行認證
  3. 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 ZFSSA 上存取檔案資源，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 ZFSSA 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。

IDMU

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) RFC2307 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

下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 ZFSSA 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 ZFSSA 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 Support 會通知此帳戶的技術聯絡人員。
  - 系統配置 - 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配置，以及儲存配置。

服務標記

「服務標記」會透過查詢 ZFSSA 的下列資料來提供產品清查功能和支援：

- 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。

SMTP

SMTP 會傳送 ZFSSA 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 ZFSSA 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 ZFSSA 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 ZFSSA 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 (SNMP)

SNMP 在 ZFSSA 上提供兩種功能；SNMP 可以提供 ZFSSA 狀態資訊，並可以將警示配置為傳送 SNMP 設陷。同時提供 SNMP 版本 1 和 2c。

系統日誌

「系統日誌」訊息是小型的事件訊息，可從 ZFSSA 傳送到一或多個遠端系統。「系統日誌」提供兩種 ZFSSA 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
- ZFSSA 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」可以配置為使用 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 ZFSSA 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配置。如果 ZFSSA 移至不同的網路位置或改變了用途，則可能需要變更這些內容。

磁碟檢測 (Disk Scrubbing)

磁碟檢測應定期執行，讓 ZFSSA 可以偵測並更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 ZFSSA 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。

遠端管理存取

本節描述 ZFSSA 遠端存取安全。

瀏覽器使用者介面 (BUI)

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。

安全 Shell (SSH)

SSH 讓使用者可以透過「指令行介面 (CLI)」登入 ZFSSA，並執行可以在 BUI 中執行的大部分管理動作。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。

日誌

本節描述與安全有關的記錄日誌功能。

稽核

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
2009-10-12 05:20:24	root	galaxy	停用 FTP 服務	
2009-10-12 03:17:05	root	galaxy	使用者登入	
2009-10-11 22:38:56	root	galaxy	瀏覽器階段作業逾時	
2009-10-11 21:13:35	root	<console>	啟用 FTP 服務	

Phone Home

如果使用 Phone Home，此日誌將會顯示與 Oracle Support 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
2009-10-12 05:24:09	上傳檔案 'cores/ak.45e5ddd1-ce92-c16e-b5eb-9cb2a8091f1c.tar.gz' 給 Oracle Support	正常

其他資訊

按一下每個 ZFSSA「瀏覽器使用者介面 (BUI)」頁面中位於左上角的「說明」按鈕，即可找到關於每個頁面特定相關資訊環境的線上說明。

您可以在下列位置找到關於 Oracle ZFS 儲存設備的完整產品資訊：

www.oracle.com/us/products/servers-storage/storage/nas/overview

文件對應

使用下表尋找 ZFSSA 每個服務、配置或其他功能的詳細文件。使用 BUI 來配置 ZFSSA 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。

表 4 服務

服務	文件位置
Active Directory	Services:Active_Directory

服務	文件位置
識別對應	Services:Identity_Mapping
DNS	Services:DNS
動態路由	Services:Dynamic_Routing
IPMP	Services:IPMP
NTP	Services:NTP
Phone Home	Services:Phone_Home
服務標記	Services:Service_Tags
SMTP	Services:SMTP
SNMP	Services:SNMP
系統日誌	Services:Syslog
系統識別	Services:System_Identity
SSH	Services:SSH

表 5 配置

配置	文件位置
SAN	Configuration:SAN
SAN:FC	Configuration:SAN:FC
SAN:iSCSI	Configuration:SAN:iSCSI
SAN:SRP	Configuration:SAN:SRP
叢集	Configuration:Cluster
使用者	Configuration:Users
偏好設定	Configuration:Preferences
警示	Configuration:Alerts
儲存	Configuration:Storage

表 6 儲存

儲存	文件位置
共用	Shares
概念	Shares:Concepts
Shadow_Migration	Shares:Shadow_Migration
Space_Management	Shares:Space_Management
File system_Namespace	Shares:File system_Namespace
共用	Shares:Shares
一般	Shares:Shares:General
協定	Shares:Shares:Protocols
存取	Shares:Shares:Access
快照	Shares:Shares:Snapshots

儲存	文件位置
專案	Shares:Projects
Projects:General	Shares:Projects:General
Projects:Protocols	Shares:Projects:Protocols
Projects:Replication	Shares:Projects:Replication
綱要	Shares:Schema

ORACLE