安全性總覽- Cloud Volumes Service Google Cloud中的NetApp解決方案（CVS）

NetApp Solutions

NetApp
April 12, 2024

目錄

安全性總覽- Cloud Volumes Service Google Cloud中的NetApp解決方案（CVS）

TR-4918：安全性總覽- Google Cloud Volumes Service Cloud中的NetApp功能

Oliver Krause、Justin Parisi、NetApp

文件範圍

安全性、尤其是在基礎架構不受儲存管理員控制的雲端環境中、對於信任您的資料、以提供由雲端供應商提供的服務而言、是非常重要的。本文檔概述NetApp提供的安全產品 "支援Google Cloud Cloud Volumes Service"。

目標對象

本文件的目標對象包括但不限於下列角色：

- 雲端供應商
- 儲存管理員
- 儲存架構設計師
- 現場資源
- 企業決策者

如果您對本技術報告內容有任何疑問、請參閱一節 "「聯絡我們」。"

縮寫	定義
CVS軟體	支援服務類型CVS Cloud Volumes Service
CVS效能	Cloud Volume Service、服務類型CVs-Performance
PSA	

Google Cloud的功能介紹如何保護資料安全Cloud Volumes Service

在Google Cloud中使用支援多種方式、以原生方式保護資料安全。Cloud Volumes Service

安全的架構與租戶模式

透過分割不同端點的服務管理（控制面板）和資料存取（資料面板）、提供Google Cloud中的安全架構、使兩者都不會影響其他端點（請參閱一節）Cloud Volumes Service "「架構」Cloud Volumes Service"）。它使用Google的 "私有服務存取" （PSA）架構以提供服務。此架構可區分由NetApp提供及營運的服務供應商、以及客戶專案中的虛擬私有雲端（VPC）服務消費者、這些客戶是想要存取Cloud Volumes Service VMware檔案共享的客戶。

在此架構中、租戶（請參閱一節 "「租賃模式」"）定義為Google Cloud專案、除非使用者明確連線、否則這些專案彼此之間完全隔離。租戶可利用Cloud Volumes Service 這個功能、將資料磁碟區、外部名稱服務及解決方案的其他重要部分、與其他租戶完全隔離在一起。由於此平台是透過VPC對等連接、因此隔離也適用於此平台。Cloud Volumes Service您Cloud Volumes Service 可以使用共享VPC、在多個專案之間共用一個支援區塊（請參閱一節）"「共享VPC」"）。您可以將存取控制套用至SMB共用和NFS匯出、以限制可以檢視或修改資料集的人員或內容。

針對控制面板提供強大的身分識別管理功能

在執行不完整組態的控制面板Cloud Volumes Service 中、使用管理身分識別管理 "身分識別存取管理（IAM）"。IAM是一項標準服務、可讓您控制Google Cloud專案執行個體的驗證（登入）和授權（權限）。所有組態都是透過Cloud Volumes Service 使用TLS 1.2加密的安全HTTPS傳輸來執行、而驗證則是使用JWT權杖來執行、以提高安全性。Google Console UI Cloud Volumes Service for the取消功能、可將使用者輸入內容轉譯為Cloud Volumes Service 使用者對功能不整的API呼叫。

安全強化：限制攻擊面

有效安全性的一部分是限制服務中可用的攻擊面數量。攻擊面可能包括各種內容、包括閒置資料、飛行傳輸、登入及資料集本身。

託管服務可移除設計中固有的部分攻擊面。基礎架構管理、如一節所述 "「服務營運、」" 由專屬團隊處理、並自動化以減少人員實際接觸組態的次數、有助於減少刻意和非蓄意的錯誤數量。網路已被隔離、因此只有必要的服務才能彼此存取。加密會被納入資料儲存設備、只有資料層需要Cloud Volumes Service 得到資訊管理員的安全注意。藉由將大部分的管理隱藏在API介面之後、可藉由限制攻擊面來實現安全性。

零信任模式

過去、IT安全理念一直是信任、但卻是驗證、而且只是仰賴外部機制（例如防火牆和入侵偵測系統）來減輕威脅。然而、攻擊與入侵事件演變成透過網路釣魚、社交工程、內部威脅及其他驗證方法、規避環境中的驗證、進而進入網路並造成嚴重破壞。

零信任已成為安全性的新方法、目前的宗旨是「在驗證一切的同時、不信任任何事物」。 因此、預設不允許任何存取。這項強制原則有多種執行方式、包括標準防火牆和入侵偵測系統（IDS）、也有下列方法：

- 強式驗證方法（例如AES加密的Kerberos或JWT權杖）
- 單一強身分識別來源（例如Windows Active Directory、輕量型目錄存取傳輸協定（LDAP）和Google IAM）
- 網路區隔和安全的多租戶共享（預設只允許租戶存取）
- 以最低權限存取原則進行精細的存取控制
- 專屬且值得信賴的小型專屬系統管理員清單、提供數位稽核與書面記錄

在Google Cloud上執行的解決方案採用零信任模式、實作「無信任、驗證一切」的立場。Cloud Volumes Service

加密

加密閒置資料（請參閱一節 "「閒置時的資料加密」"）搭配NetApp Volume Encryption（NVE）和線上使用XTS-AES-256密碼 "「SMB加密」" 或NFS Kerberos 5p支援。瞭解跨區域複寫傳輸受到TLS 1.2加密保護、讓您高枕無憂（請參閱一節）"「跨區域複寫」"）。此外、Google網路也提供加密通訊（請參閱一節 "「傳輸中的資料加密」"）提供額外的保護層、防範攻擊。如需傳輸加密的詳細資訊、請參閱一節 "「Google Cloud Network」"。

資料保護與備份

安全性不只是預防攻擊而已。這也與我們如何在攻擊發生時或發生時從攻擊中恢復有關。此策略包括資料保護與備份。提供在停電時複製到其他地區的方法（請參閱一節Cloud Volumes Service "「跨區域複寫」"）或資料集受到勒索軟體攻擊的影響。也Cloud Volumes Service 可以使用、將資料非同步備份到非執行個體的位置 "支援Cloud Volumes Service"。透過定期備份、降低安全事件的時間、節省成本、並使系統管理員感到焦慮。

利用領先業界的**Snapshot**複本、快速緩解勒索軟體

除了資料保護與備份、Cloud Volumes Service 支援不可變的Snapshot複本（請參閱一節） "「可永久保存的Snapshot複本」"）允許從勒索軟體攻擊中恢復的磁碟區（請參閱一節 "「服務營運」"）在發現問題的幾秒鐘內、並將中斷時間降至最低。恢復時間與影響取決於Snapshot排程、但您可以建立Snapshot複本、在勒索軟體攻擊中提供最少一小時的差異。Snapshot複本對效能和容量使用率的影響微乎其微、是保護資料集的低風險高報酬方法。

安全考量與攻擊面

瞭解如何保護資料安全的第一步、就是找出風險和潛在的攻擊面。

其中包括（但不限於）下列項目：

- 系統管理與登入
- 閒置資料
- 資料傳輸中
- 網路和防火牆
- 勒索軟體、惡意軟體和病毒

瞭解攻擊面可協助您更妥善地保護環境安全。在Google Cloud中、不需進行任何管理互動、即可將許多主題納入考量、並在預設情況下實作安全功能。Cloud Volumes Service

確保安全登入

保護關鍵基礎架構元件的安全時、必須確保只有獲核准的使用者才能登入及管理您的環境。如果不良的使用者違反您的管理認證、他們就能擁有城堡的金鑰、而且可以執行任何他們想要的動作：變更組態、刪除磁碟區和備份、建立後端或停用Snapshot排程。

支援Google Cloud的解決方案可透過模糊化的儲存即服務（StaaS）、防止未經授權的系統管理登入。Cloud Volumes Service由雲端供應商完全維護、無法從外部登入。Cloud Volumes Service所有的設定和組態作業都是完全自動化的、因此除非情況非常罕見、否則人員管理員永遠不需要與系統互動。

如果需要登入、Cloud Volumes Service Google Cloud中的功能驗證可確保登入安全、只要維護一份可供登入系統之受信任系統管理員的簡短清單即可。這項網關保存功能有助於減少可能的不良使用者存取權。此外、Google Cloud網路也將系統隱藏在網路安全層的背後、只向外界公開所需的內容。如需Google Cloud Cloud Volumes Service 的資訊、請參閱「架構」一節 "「架構」Cloud Volumes Service 。"

叢集管理與升級

有潛在安全風險的兩個領域包括叢集管理（如果不良的使用者具有管理存取權限、會發生什麼事）和升級（如果軟體映像遭到破壞、會發生什麼事）。

儲存管理保護

儲存設備即服務可移除對雲端資料中心外部終端使用者的存取權限、進而移除管理員曝險的額外風險。而唯一的組態是由客戶進行資料存取。每個租戶都會管理自己的磁碟區、而且沒有租戶能夠觸及其他Cloud Volumes Service 的實體執行個體。此服務是由自動化管理、其中只有一小份受信任的系統管理員清單、可透過本節所述的程序存取系統 "「服務營運。」"

CVS效能服務類型提供跨區域複寫選項、可在區域故障時、為不同區域提供資料保護。在這些情況Cloud Volumes Service 下、可將無法存取的功能故障轉移至未受影響的區域、以維持資料存取。

服務升級

更新有助於保護易受影響的系統。每項更新都提供安全性增強功能和錯誤修正、可將攻擊面減至最低。軟體更新是從集中式儲存庫下載、並在允許更新之前驗證、以驗證是否使用正式映像、以及升級是否受到不良行為的影響。

有了NetApp、雲端供應商團隊就能處理更新、提供具備組態與升級能力的專家、並將程序自動化且經過完整測試、藉此消除系統管理員團隊面臨的風險風險。Cloud Volumes Service升級不會中斷營運、Cloud Volumes Service 而為了獲得最佳整體效果、我們會維護最新的更新。

如需執行這些服務升級之系統管理員團隊的相關資訊、請參閱一節 "「服務營運。」"

保護閒置資料的安全

當磁碟遭竊、退回或重新使用時、靜止資料加密對於保護敏感資料非常重要。使用軟體式加密、可保護靜態資料Cloud Volumes Service 。

- Google產生的金鑰用於CVs-SW。
- 如需CVS效能、每個Volume金鑰會儲存在Cloud Volumes Service 內建於支援核心的金鑰管理程式中、此管理程式使用NetApp ONTAP 還原資料模組來產生AES-256加密金鑰。CryptoModis會列在CMVP FIPS 140-2驗證模組清單中。請參閱 "FIPS 140-2認證編號4144"。

自2021年11月起、客戶管理的加密（CMEK）功能預覽已推出CVS效能。此功能可讓您使用Google金鑰管理服務（KMS）中所裝載的個別專案、每個區域的主要金鑰、來加密每個Volume金鑰。KMS可讓您附加外部金鑰管理程式。

如需如何設定KMS以獲得CVS效能的詳細資訊、 "請參閱Cloud Volumes Service 《》文件"。

如需架構的詳細資訊、請參閱一節 "「架構」Cloud Volumes Service 。"

保護資料傳輸安全

除了確保閒置資料的安全、Cloud Volumes Service 您也必須能夠在資料在執行個體與用戶端或複寫目標之間傳輸時、保護資料安全。利用加密方法（例如使用Kerberos的SMB加密、封包的簽署/密封、以及用於資料傳輸端點對端點加密的NFS Kerberos 5p）、為透過NAS傳輸的傳輸中資料提供加密功能。Cloud Volumes Service

利用AES-GCM加密方法、複寫Cloud Volumes Service 不中斷的實體磁碟區使用TLS 1.2。

預設會停用最不安全的傳輸協定、例如：Telnet、NDMP等。不過、DNS並非Cloud Volumes Service 由支援DNS的功能加密（不支援DNS安全）、因此應盡可能使用外部網路加密來加密。請參閱一節 "「傳輸中的資料加密」" 以取得更多關於保護資料傳輸安全的資訊。

如需NAS傳輸協定加密的相關資訊、請參閱一節 "「NAS傳輸協定」。"

NAS權限的使用者和群組

保護雲端資料的一部分是適當的使用者和群組驗證、其中存取資料的使用者會在環境中驗證為真實使用者、而群組則包含有效的使用者。這些使用者和群組提供初始共用和匯出存取、以及儲存系統中檔案和資料夾的權限驗證。

針對SMB共用和Windows型權限、使用標準的Active Directory型Windows使用者和群組驗證。Cloud Volumes Service此服務也能運用UNIX身分識別供應商、例如LDAP for UNIX使用者和群組進行NFS匯出、NFSv4 ID驗證、Kerberos驗證及NFSv4 ACL。

> 目前僅支援Active Directory LDAP Cloud Volumes Service 搭配「以供LDAP使用」功能。

偵測、防範及防範勒索軟體、惡意軟體及病毒

勒索軟體、惡意軟體和病毒是系統管理員持續面臨的威脅、企業組織最需要注意的是偵測、防範和防範這些威脅。關鍵資料集上的單一勒索軟體事件可能會花費數百萬美元、因此您可以採取最大程度的行動來降低風險。

雖然目前不包含原生偵測或預防措施、例如防毒保護或Cloud Volumes Service "自動勒索軟體偵測"、您可以透過啟用定期Snapshot排程、快速從勒索軟體事件中恢復。Snapshot複本是不可變更的、而且是檔案系統中變更區塊的唯讀指標、幾乎是即時性的、對效能的影響最小、而且只有在資料變更或刪除時才會佔用空間。您可以設定Snapshot複本的排程、以符合所需的可接受恢復點目標（RPO）/恢復時間目標（RTO）、而且每個Volume最多可保留1、024個Snapshot複本。

Snapshot支援不需額外付費（除了Snapshot複本所保留的變更區塊/資料的資料儲存費用）Cloud Volumes Service 、而且在發生勒索軟體攻擊時、也可在攻擊發生之前、用於回溯至Snapshot複本。快照還原只需幾秒鐘即可完成、之後您就能恢復正常的資料服務。如需詳細資訊、請參閱 "NetApp勒索軟體解決方案"。

若要防止勒索軟體影響您的業務、需要採用多層方法、其中包括下列一項或多項：

- 端點保護
- 透過網路防火牆防範外部威脅
- 偵測資料異常
- 關鍵資料集的多重備份（現場與異地）
- 定期還原備份測試
- 不可變的唯讀NetApp Snapshot複本
- 關鍵基礎架構的多因素驗證
- 系統登入的安全性稽核

這份清單遠非詳盡無遺、但在處理勒索軟體攻擊的可能性時、這是一個很好的藍圖。在Google Cloud中提供多種方法來保護勒索軟體事件、並減少其影響。Cloud Volumes Service

不可變的Snapshot複本

由於資料刪除或整個磁碟區遭到勒索軟體攻擊、因此本機可提供可自訂排程的不可變唯讀Snapshot複本、以便在資料刪除或整個磁碟區遭到勒索軟體攻擊時、快速進行時間點還原。Cloud Volumes Service快照還原至先前的良好Snapshot複本、可根據Snapshot排程和RTO/RPO的保留期間、迅速將資料遺失減至最低。Snapshot技

術的效能影響微乎其微。

由於VMware的Snapshot複本Cloud Volumes Service 是唯讀的、因此除非勒索軟體擴散到未注意到的資料集、而且Snapshot複本已被勒索軟體感染、否則這些複本將不會受到勒索軟體的感染。因此、您也必須考慮根據資料異常狀況來偵測勒索軟體。目前無法原生提供偵測功能、但您可以使用外部監控軟體。Cloud Volumes Service

備份與還原

支援標準NAS用戶端備份功能（例如透過NFS或SMB進行備份）Cloud Volumes Service 。

- CVS效能提供跨區域磁碟區複寫至其他CVS效能磁碟區的功能。如需詳細資訊、請參閱 "Volume複製" 請參閱Cloud Volumes Service 《》文件。
- CVS軟體提供服務原生Volume備份/還原功能。如需詳細資訊、請參閱 "雲端備份" 請參閱Cloud Volumes Service 《》文件。

Volume複寫提供確切的來源磁碟區複本、可在發生災難時（包括勒索軟體事件）進行快速容錯移轉。

跨區域複寫

CVS效能可讓您在Google雲端區域之間安全地複寫磁碟區、以便在NetApp控制的後端服務網路上使用TLS1.2 AES 256 GCM加密、並使用特定介面在Google網路上執行複寫、以保護資料及歸檔使用案例。主要（來源）Volume包含作用中正式作業資料、並複寫至次要（目的地）Volume、以提供主要資料集的確切複本。

初始複寫會傳輸所有區塊、但更新只會傳輸主磁碟區中變更的區塊。例如、如果將位於主要磁碟區上的1TB資料庫複寫到次要磁碟區、則初始複寫時會傳輸1TB的空間。如果該資料庫在初始化與下一個更新之間有幾百列（假設、幾MB）的變更、則只有變更列的區塊會複寫到次要（幾MB）。這有助於確保傳輸時間保持低、並降低複寫費用。

檔案和資料夾的所有權限都會複寫到次要磁碟區、但共用存取權限（例如匯出原則和規則、SMB共用和共用ACL）必須分開處理。在站台容錯移轉的情況下、目的地站台應利用相同的名稱服務和Active Directory網域連線、以一致的方式處理使用者和群組的身分識別和權限。當發生災難時、您可以使用次要Volume做為容錯移轉目標、方法是打破複寫關係、將次要Volume轉換為讀寫。

Volume複本為唯讀、可在異地提供不可改變的資料複本、以便在病毒感染資料或勒索軟體加密主要資料集的情況下、快速恢復資料。唯讀資料不會加密、但如果主要磁碟區受到影響並發生複寫、則受感染的區塊也會複寫。您可以使用較舊且不受影響的Snapshot複本進行還原、但SLA可能超出承諾的RTO/RPO範圍、視偵測到攻擊的速度而定。

此外、您也可以利用Google Cloud的跨區域複寫（CRR）管理功能、防止惡意的管理動作、例如磁碟區刪除、Snapshot刪除或Snapshot排程變更。這是透過建立自訂角色來完成、這些角色可分隔磁碟區管理員、這些管理員可以刪除來源磁碟區、但不能中斷鏡射、因此無法從CRR管理員刪除目的地磁碟區、因為他們無法執行任何Volume作業。請參閱 "安全考量" 關於每個系統管理員群組所允許的權限、請參閱Cloud Volumes Service 《參考資料》文件。

支援**Cloud Volumes Service**

雖然此功能可提供高資料持久性、但外部事件可能導致資料遺失。Cloud Volumes Service如果發生病毒或勒索軟體等安全事件、備份與還原對於及時恢復資料存取而言、將會變得非常重要。系統管理員可能不小心刪除Cloud Volumes Service 了一個聲音區。或者、使用者只是想保留資料的備份版本好幾個月、而在磁碟區內保留額外的Snapshot複本空間、就成為成本上的挑戰。雖然Snapshot複本應該是保留過去幾週備份版本以還原遺失資料的首選方法、但它們位於磁碟區內部、如果磁碟區消失、就會遺失。

基於上述所有理由、NetApp Cloud Volumes Service 支援透過提供備份服務 "支援Cloud Volumes Service"。

利用Google Cloud Storage（GCS）、即可在該磁碟區上產生一份複本。Cloud Volumes Service它只會備份儲存在磁碟區內的實際資料、而非可用空間。它的運作方式永遠是遞增的、也就是說、它只會在繼續備份變更的資料時、一次傳輸磁碟區內容、一次又一次從該處傳輸。相較於採用多個完整備份的傳統備份概念、它可節省大量備份儲存設備、進而降低成本。由於備份空間的每月價格比磁碟區低、因此是延長備份版本時間的理想選擇。

使用者可以使用Cloud Volumes Service 支援還原功能、將任何備份版本還原至相同區域內的相同或不同磁碟區。如果刪除來源磁碟區、則會保留備份資料、並需要獨立管理（例如刪除）。

支援的支援功能已內建於支援的選項中。Cloud Volumes Service Cloud Volumes Service使用者可依Cloud Volumes Service 每個Volume啟動「支援功能」備份、以決定要保護的磁碟區。請參閱 "支援的文件Cloud Volumes Service" 如需備份的相關資訊、請參閱 "支援的最大備份版本數"、排程和 "定價"。

專案的所有備份資料都儲存在GCS儲存區內、此儲存區由服務管理、使用者看不到。每個專案都使用不同的儲存庫。目前、這些庫位與Cloud Volumes Service 《非洲地理區（Sin the Same volume）」位於同一個區域、但我們正在討論更多選項。如需最新狀態、請參閱文件。

從資料庫傳輸Cloud Volumes Service 到GCS時、會使用內部服務的Google網路、搭配HTTPS和TLS1.2。資料會以Google管理的金鑰進行閒置加密。

若要管理Cloud Volumes Service 此功能（建立、刪除及還原備份）、使用者必須擁有 "角色/netappcloudVolumes.admin" 角色：

架構

總覽

信任雲端解決方案的一部分是瞭解架構及其安全性。本節說明Cloud Volumes Service Google中的各個環節、以協助您減輕資料安全的潛在疑慮、並指出可能需要採取額外組態步驟才能獲得最安全部署的領域。

整體的架構Cloud Volumes Service 可以分為兩個主要元件：控制面板和資料面板。

控制面

在這個過程中、由NetApp原生自動化軟體的管理員負責管理後端基礎架構。Cloud Volumes Service Cloud Volumes Service此架構對終端使用者完全透明、包括網路、儲存硬體、軟體更新等、有助於為Cloud Volumes Service 諸如更新的雲端解決方案提供價值。

資料平面

在資料架構Cloud Volumes Service 中、資料層面包括實際的資料量和Cloud Volumes Service 整體的支援（例如存取控制、Kerberos驗證等）。資料平面完全由Cloud Volumes Service 最終使用者和使用者控制。

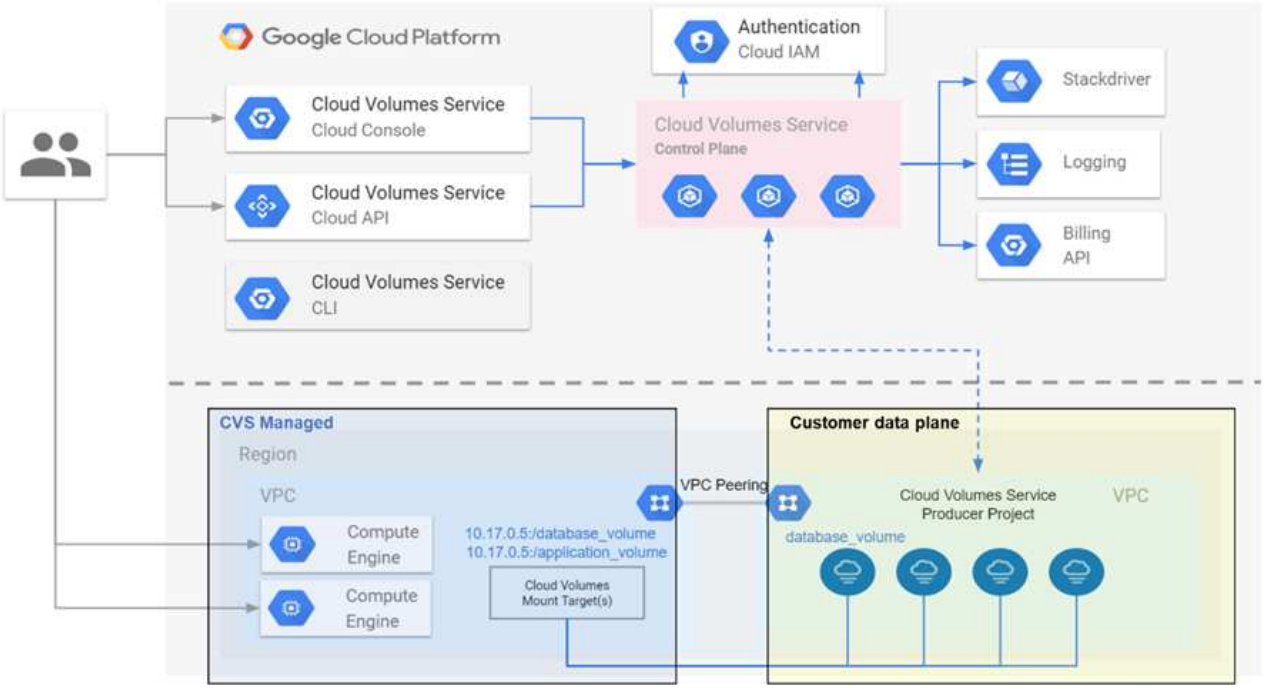
每個平面的安全與管理方式各有不同。以下各節涵蓋這些差異、從Cloud Volumes Service 架構概述開始。

架構**Cloud Volumes Service**

以類似其他Google Cloud原生服務的方式、例如CloudSQL、Google Cloud VMware

Engine（GCVE）和Filestore Cloud Volumes Service 、即用功能 "Google PSA" 以提供服務。在PSAA中、服務是建置於服務製造商專案內、此專案使用的 "VPC網路對等關係" 連線至服務使用者。服務製造商由NetApp提供及營運、服務消費者是客戶專案中的VPC、負責託管想要存取Cloud Volumes Service VMware檔案共享的客戶。

下圖、請參閱 "架構區段" 在本文件中Cloud Volumes Service 、顯示了高階檢視。



虛線上方的部分顯示服務的控制面、控制磁碟區生命週期。虛線下方的部分顯示資料平面。左藍色方塊描繪使用者VPC（服務消費者）、右藍色方塊則是NetApp提供的服務製造商。兩者都透過VPC對等連接。

租賃模式

在本例中、個別專案被視為獨特的租戶。Cloud Volumes Service這表示每個專案都會執行對磁碟區、Snapshot複本等的操作。換句話說、所有磁碟區都屬於在其中建立的專案、而且根據預設、只有該專案能管理及存取其中的資料。這被視為服務的控制面板檢視。

共享VPC

在資料平面檢視中Cloud Volumes Service 、無法連接至共享的VPC。您可以在託管專案或連接至共享VPC的其中一個服務專案中建立磁碟區。連接至該共享VPC的所有專案（主機或服務）都能到達網路層（TCP/IP）的磁碟區。由於在共享VPC上具有網路連線能力的所有用戶端都可能透過NAS傳輸協定存取資料、因此必須使用個別Volume上的存取控制（例如使用者/群組存取控制清單（ACL）和NFS匯出的主機名稱/ IP位址）來控制誰可以存取資料。

每個客戶專案最多可連接Cloud Volumes Service 到五部VPC。在控制面板上、專案可讓您管理所有建立的磁碟區、無論這些磁碟區連接到哪個VPC。在資料層面上、VPC彼此隔離、而且每個磁碟區只能連接至一個VPC。

個別磁碟區的存取是由特定傳輸協定（NFS/SMB）存取控制機制所控制。

換句話說、在網路層上、所有連線至共享VPC的專案都能看到該磁碟區、而在管理端、控制面板只能讓擁有者專

案查看該磁碟區。

VPC服務控制

VPC服務控管機制建立了Google Cloud服務周邊的存取控制、這些服務已連接至網際網路、可在全球各地存取。這些服務可透過使用者身分識別提供存取控制、但無法限制來自哪些網路位置要求。VPC服務控制功能引進限制存取已定義網路的功能、藉此彌補這項落差。

此資料平面並未連線至外部網際網路、而是連線至具有明確定義網路邊界（周邊）的私有VPC。Cloud Volumes Service在該網路中、每個磁碟區都使用特定於傳輸協定的存取控制。任何外部網路連線都是由Google Cloud專案管理員明確建立。然而、控制面板並未提供與資料面板相同的保護、任何人只要擁有有效的認證資料（"JWT權杖"）。

簡而言之Cloud Volumes Service 、不需要支援VPC服務控制、也不明確使用VPC服務控制、即可透過資料中心提供網路存取控制功能。

封包偵測/追蹤考量

封包擷取可用於疑難排解網路問題或其他問題（例如NAS權限、LDAP連線等）、但也可惡意用來取得網路IP位址、MAC位址、使用者和群組名稱、以及端點使用的安全層級等資訊。由於Google Cloud網路、VPC和防火牆規則的設定方式、如果沒有使用者登入認證或、就很難取得不必要的網路封包存取權 "JWT權杖" 雲端執行個體。封包擷取只能在端點（例如虛擬機器（VM））上進行、而且只能在VPC內部的端點上進行、除非使用共享VPC和（或）外部網路通道/ IP轉送來明確允許外部流量進入端點。無法從用戶端外部窺探流量。

使用共享VPC時、會使用NFS Kerberos和/或進行傳輸中加密 "SMB加密" 可以遮罩從追蹤中收集到的大部分資訊。不過、有些流量仍會以純文字形式傳送、例如 "DNS" 和 "LDAP查詢"。下圖顯示從Cloud Volumes Service來源於指令集的純文字LDAP查詢擷取的封包、以及可能公開的識別資訊。目前支援透過SSL加密或LDAP的Cloud Volumes Service LDAP查詢不支援。CVS效能支援LDAP簽署（若Active Directory要求）。CVS軟體不支援LDAP簽署。

> unixUserPassword是由LDAP查詢、不會以純文字傳送、而是以Salted雜湊傳送。根據預設、Windows LDAP不會填入unixUserPassword欄位。只有當您需要利用Windows LDAP透過LDAP互動登入用戶端時、才需要此欄位。不支援互動式LDAP登入執行個體。Cloud Volumes Service

下圖顯示NFS Kerberos對話擷取的封包擷取、位於透過AUTH_SYS擷取NFS的旁邊。請注意、追蹤中的可用資訊在兩者之間有何差異、以及啟用飛行中加密如何為NAS流量提供更高的整體安全性。

IP addresses of the NFS client and CVS instance

Genericized NFS call/reply

No.	Time	Source	Destination	Protocol	Length	Info
380	9.218014	10.193.67.225	10.193.67.219	NFS	346	V4 Call (Reply In 381)
381	9.218480	10.193.67.219	10.193.67.225	NFS	426	V4 Reply (Call In 380)
382	9.218641	10.193.67.225	10.193.67.219	NFS	370	V4 Call (Reply In 397)
397	9.369035	10.193.67.219	10.193.67.225	NFS	458	V4 Reply (Call In 382)

```
> Frame 381: 426 bytes on wire (3408 bits), 426 bytes captured (3408 bits)
> Ethernet II, Src: IntelCor_7f:da:bc (90:e2:ba:7f:da:bc), Dst: VMware_a0:2c:2d (00:50:56:a0:2c:2d)
> Internet Protocol Version 4, Src: 10.193.67.219, Dst: 10.193.67.225
> Transmission Control Protocol, Src Port: 2049, Dst Port: 738, Seq: 6305, Ack: 6569, Len: 360
> Remote Procedure Call, Type:Reply XID:0xef5e998d
v GSS-Wrap
    Length: 300
    GSS Data: 050407ff0000000000000000025913451ee1d43d298cf3031…
  > krb5_blob: 050407ff0000000000000000025913451ee1d43d298cf3031…
v Network File System
    [Program Version: 4]
    [V4 Procedure: COMPOUND (1)]
```

GSS wrapped NFS calls/replies with no other identifying information

IP addresses of the NFS client and CVS instance

Detailed NFS call types and file handle information

No.	Time	Source	Destination	Protocol	Length	Info
33	0.958480	10.193.67.201	10.193.67.204	NFS	458	V4 Reply (Call In 32) OPEN StateID: 0x0481
34	0.958784	10.193.67.204	10.193.67.201	NFS	306	V4 Call (Reply In 35) SETATTR FH: 0x6c07918a
35	0.959284	10.193.67.201	10.193.67.204	NFS	358	V4 Reply (Call In 34) SETATTR

```
> Opcode: PUTFH (22)
> Opcode: SETATTR (34)
v Opcode: GETATTR (9)
    Status: NFS4_OK (0)
  v Attr mask[0]: 0x0010011a (Type, Change, Size, FSID, FileId)
    > reqd_attr: Type (1)
    > reqd_attr: Change (3)
    > reqd_attr: Size (4)
    > reqd_attr: FSID (8)
    v reco_attr: FileId (20)
        fileid: 9232254136597092620
  v Attr mask[1]: 0x00b0a03a (Mode, NumLinks, Owner, Owner_Group, Space_Used, Time_Access, Time_Metadata, Time_Modify, Mounted_on_FileId)
    v reco_attr: Mode (33)
      > mode: 0644, Name: Unknown, Read permission for owner, Write permission for owner, Read permission for group, Read permission for others
    > reco_attr: NumLinks (35)
    v reco_attr: Owner (36)
      > fattr4_owner: root@NTAP.LOCAL
    v reco_attr: Owner_Group (37)
      > fattr4_owner_group: root@NTAP.LOCAL
    > reco_attr: Space_Used (45)
    > reco_attr: Time_Access (47)
    > reco_attr: Time_Metadata (52)
    > reco_attr: Time_Modify (53)
    > reco_attr: Mounted_on_FileId (55)
```

File ID

Permission information

Owner and group ID strings

VM網路介面

攻擊者可能會嘗試將新的網路介面卡（NIC）新增至中的VM "混雜模式" （連接埠鏡射）或在現有NIC上啟用雜亂模式、以利窺探所有流量。在Google Cloud中、新增NIC需要完全關閉虛擬機器、才能建立警示、因此攻擊者無法察覺。

此外、NIC完全無法設定為雜亂模式、而且會在Google Cloud中觸發警示。

控制面板架構

所有的功能都是透過API來執行。Cloud Volumes Service整合至GCP雲端主控台的BIOS管理也會使用此功能的Cloud Volumes Service Cloud Volumes Service

身分識別與存取管理

身分識別與存取管理 ("IAM"）是一項標準服務、可讓您控制Google Cloud專案執行個體的驗證（登入）和授權（權限）。Google IAM提供完整的權限授權與移除稽核追蹤。目前Cloud Volumes Service 無法提供控制面板稽核。

授權/權限總覽

IAM提供Cloud Volumes Service 內建的精細權限來執行功能。您可以找到 "請在此填寫詳細權限清單"。

IAM也提供兩種預先定義的角色：「netappcloudVolumes.admin」和「netappcloudVolumes.viewer」。這些角色可指派給特定使用者或服務帳戶。

指派適當的角色和權限、讓IAM使用者能夠管理Cloud Volumes Service 功能。

使用精細權限的範例包括：

- 建立只有「Get / List / cred/ update」權限的自訂角色、讓使用者無法刪除磁碟區。
- 使用僅具有「napshot.*」權限的自訂角色、建立用於建置應用程式一致Snapshot整合的服務帳戶。
- 建立自訂角色、將「volumereplication*」委派給特定使用者。

服務帳戶

透過Cloud Volumes Service 指令碼或進行功能不均的API呼叫 "Terraform"、您必須建立角色為「角色/netappcloudVolumes.admin」的服務帳戶。您可以使用此服務帳戶、以Cloud Volumes Service 兩種不同的方式產生驗證申請表API要求所需的JWT權杖：

- 產生Json金鑰、並使用Google API從其衍生JWT權杖。這是最簡單的方法、但需要手動管理機密（Json金鑰）。
- 使用 "服務帳戶模擬" 使用角色/iam.serviceAccountTokenCreator`。程式碼（指令碼、Terraform等）會與一起執行 "應用程式預設認證" 並模擬服務帳戶以取得其權限。這種方法反映了Google的最佳安全實務做法。

請參閱 "建立您的服務帳戶和私密金鑰" 如需詳細資訊、請參閱Google雲端文件。

部分**API Cloud Volumes Service**

利用HTTPS（TLSv1.2）作為基礎網路傳輸、藉此使用REST型API。Cloud Volumes Service您可以找到最新的API定義 "請按這裡" 以及如何使用API的相關資訊、請參閱 "Google雲端文件中的Cloud Volumes API"。

API端點由NetApp使用標準HTTPS（TLSv1.2）功能來操作及保護。

JWT權杖

API驗證是以JWT承載權杖執行 ("RFC-7519"）。必須使用Google Cloud IAM驗證來取得有效的JWT權杖。這必須透過提供服務帳戶Json金鑰、從IAM擷取權杖來完成。

稽核記錄

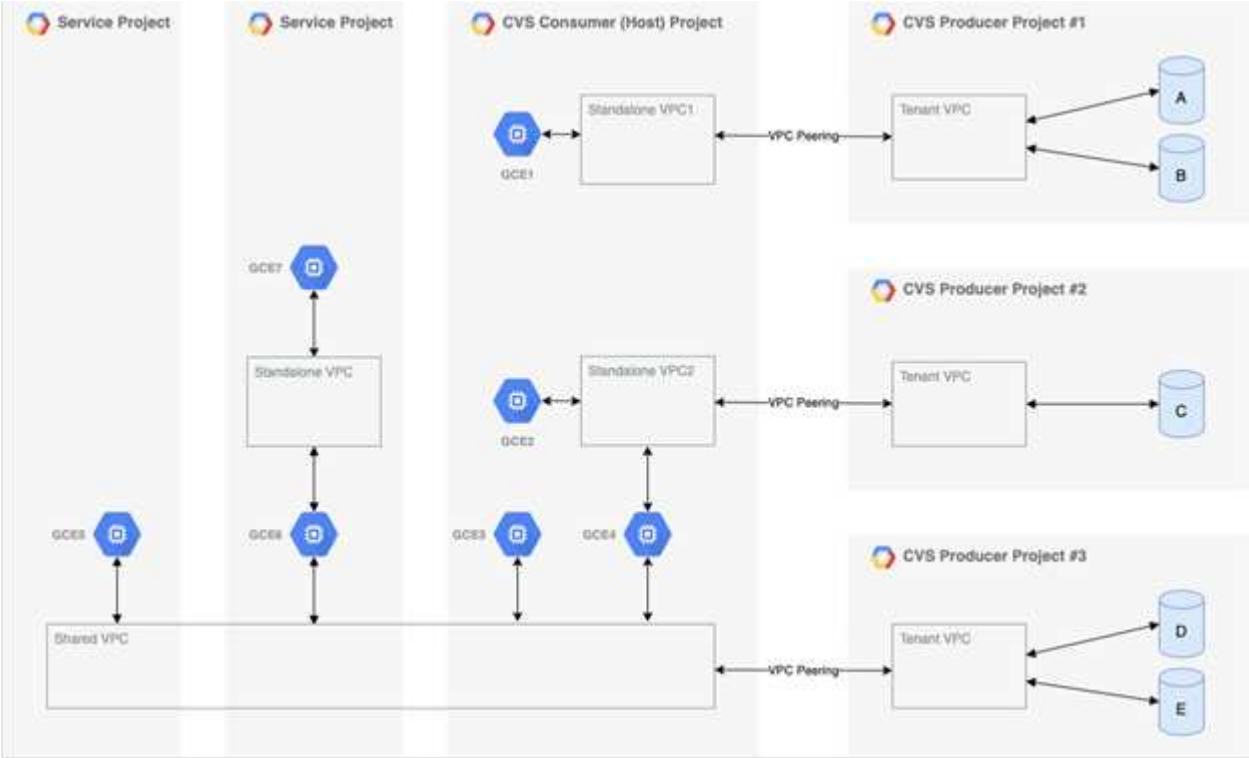
目前沒有使用者可存取的控制面板稽核記錄可供使用。

資料平面架構

適用於Google Cloud的解決方案運用Google Cloud Cloud Volumes Service "私有服務存取" 架構。在此架構中、使用者可以連線Cloud Volumes Service 到這個功能。此架構使用服務網路和VPC對等架構、如同其他Google Cloud服務、確保租戶之間完全隔離。

如需Cloud Volumes Service Google Cloud的架構總覽、請參閱 "架構Cloud Volumes Service"。

使用者VPC（獨立式或共享）會在Cloud Volumes Service 託管的代管租戶專案中連接至VPC、以裝載這些磁碟區。



上圖顯示一個專案（中間是CVS消費者專案）、其中三個VPC網路連接Cloud Volumes Service 到多個運算引擎VM（GCE1-7）共用磁碟區：

- VPC1允許GCE1存取磁碟區A和B
- VPC2可讓GCE2和GCE4存取Volume C
- 第三個VPC網路是共享的VPC、與兩個服務專案共用。它可讓GCE3、GCE4、GCE5和GCE6存取Volume D和E共享VPC網路僅支援CVS效能服務類型的磁碟區。

GCE7無法存取任何Volume。

資料可在傳輸中（使用Kerberos和/或SMB加密）加密、Cloud Volumes Service 也可在支援中加密。

傳輸中的資料加密

傳輸中的資料可在NAS傳輸協定層加密、Google Cloud網路本身也會加密、如下列各節所述。

Google Cloud網路

Google Cloud會加密網路層級的流量、如所述 "傳輸中加密" 在Google文件中。如「Cloud Volumes Services Architecture」一節所述、Cloud Volumes Service NetApp控制的PSAPa生產商專案將提供此功能。

在CVs-SW的情況下、生產商租戶會執行Google VM來提供服務。Google Cloud Volumes Service 會自動加密使用者VM和不支援的VM之間的流量。

雖然CVS效能的資料路徑在網路層上並未完全加密、但NetApp與Google仍使用這種組合 "IEEE 802.1AE加密（MAC安全）"、 "封裝" （資料加密）和實體受限的網路、以保護Cloud Volumes Service 資料在整個過程中在整個過程中在靜止CVS效能服務類型和Google Cloud之間傳輸。

NAS傳輸協定

NFS和SMB NAS傳輸協定可在傳輸協定層提供選用的傳輸加密。

SMB加密

"SMB加密" 提供SMB資料的端點對端點加密、並保護資料免於在不受信任的網路上遭人竊取。您可以啟用用戶端/伺服器資料連線（僅適用於支援SMB3.x的用戶端）和伺服器/網域控制器驗證的加密。

啟用SMB加密時、不支援加密的用戶端將無法存取共用區。

支援RC4-HMAC、AES-122-CTS-HMA-SHA1和AES-256-CTS-HMA-SHA1安全密碼、以進行SMB加密。Cloud Volumes ServiceSMB會交涉至伺服器支援的最高加密類型。

NFSv4.1 Kerberos

對於NFSv4.1、CVS效能提供如所述的Kerberos驗證 "RFC7530"。您可以針對每個磁碟區啟用Kerberos。

Kerberos目前最強大的加密類型是AES-256-CTS-HMA-SHA1。NetApp Cloud Volumes Service 支援AES-256-CTS-HMA-SHA1、AES-123-CTS-HMA-SHA1、DES3和DES for NFS。它也支援CIFS/SMB流量的ARCFOUR-HMAC（RC4）、但不支援NFS。

Kerberos為NFS裝載提供三種不同的安全性層級、可讓您選擇Kerberos安全性的強度。

根據RedHat "通用掛載選項" 文件：

```
sec=krb5 uses Kerberos V5 instead of local UNIX UIDs and GIDs to
authenticate users.
sec=krb5i uses Kerberos V5 for user authentication and performs integrity
checking of NFS operations using secure checksums to prevent data
tampering.
sec=krb5p uses Kerberos V5 for user authentication, integrity checking,
and encrypts NFS traffic to prevent traffic sniffing. This is the most
secure setting, but it also involves the most performance overhead.
```

一般而言、Kerberos安全性層級越高、效能就越差、因為用戶端和伺服器花費時間來加密和解密所傳送的每個封包的NFS作業。許多用戶端和NFS伺服器都支援AES-NI卸載至CPU、以獲得更好的整體體驗、但Kerberos 5p（完整端對端加密）的效能影響遠高於Kerberos 5（使用者驗證）的影響。

下表顯示每個層級在安全性和效能方面的差異。

安全性層級	安全性	效能
NFSv3—系統	• 最不安全；純文字、含數字使用者ID /群組ID • 能夠檢視UID、GID、用戶端IP位址、匯出路徑、檔案名稱、封包擷取的權限	• 最適合大多數情況
NFSv4.x—系統	• 比NFSv3（用戶端ID、名稱字串/網域字串比對）更安全、但仍是純文字 • 能夠檢視UID、GID、用戶端IP位址、名稱字串、網域ID、 在封包擷取中匯出路徑、檔案名稱、權限	• 適合連續工作負載（例如VM、資料庫、大型檔案） • 高檔案數/高中繼資料的不良（差30-50%）
NFS—KRB5	• 每個NFS封包中的認證Kerberos加密：在GSS包裝程式的RPC呼叫中、將使用者/群組的UID/GID封包起來 • 要求存取掛載的使用者需要有效的Kerberos票證（透過使用者名稱/密碼或手動金鑰索引標籤交換）；票證會在指定的時間段後過期、使用者必須重新驗證才能存取 • 不加密NFS作業或掛載/連接埠對應器/ NLM等輔助通訊協定（可參閱匯出路徑、IP位址、檔案處理、權限、檔案名稱、 封包擷取的時間/時間）	• 在大多數情況下最佳的Kerberos；比AUTH_SYS更糟

安全性層級	安全性	效能
NFS：krb5i	• 每個NFS封包中的認證Kerberos加密：在GSS包裝程式的RPC呼叫中、將使用者/群組的UID/GID封包起來 • 要求存取掛載的使用者需要有效的Kerberos票證（透過使用者名稱/密碼或手動金鑰索引標籤交換）；票證會在指定的時間段後過期、使用者必須重新驗證才能存取 • 不加密NFS作業或掛載/連接埠對應器/ NLM等輔助通訊協定（可參閱匯出路徑、IP位址、檔案處理、權限、檔案名稱、 封包擷取的時間/時間） • 每個封包都會新增Kerberos GSS Checksum、以確保不會攔截封包。如果校驗和相符、則允許對話。	• 優於krb5p、因為NFS有效負載未加密；只有與krb5相比、新增的額外負荷才是完整性Checksum。krb5i的效能不會比krb5差很多、但會有一些降低。
NFS–krb5p	• 每個NFS封包中的認證Kerberos加密：在GSS包裝程式的RPC呼叫中、將使用者/群組的UID/GID封包起來 • 要求存取掛載的使用者需要有效的Kerberos票證（透過使用者名稱/密碼或手動Keytab交換）；票證會在指定的時間段後過期、而且使用者必須重新驗證才能存取 • 所有NFS封包有效負載都會使用GSS包裝進行加密（無法在封包擷取中看到檔案處理代碼、權限、檔案名稱、atime/mtime）。 • 包括完整性檢查。 • NFS作業類型可見（Fsinfo, access, GetAttr等）。 • 輔助通訊協定（掛載、連接埠對應、NLM等）未加密-（請參閱匯出路徑、IP位址）	• 安全性層級效能最差；krb5p必須加密/解密更多資料。 • 使用NFSv4.x的效能優於krb5p、適用於高檔案數工作負載。

在VMware中、已設定的Active Directory伺服器會做為Kerberos伺服器和LDAP伺服器（從RFC2307相容架構查詢使用者身分）Cloud Volumes Service 。不支援其他Kerberos或LDAP伺服器。NetApp強烈建議您使用LDAP進行Cloud Volumes Service 身分識別管理。如需有關NFS Kerberos如何顯示在封包擷取中的資訊、請參閱一節"「封包偵測/追蹤考量。」"

閒置資料加密

所有的流通量Cloud Volumes Service 均使用AES-256加密進行閒置加密、這表示寫入媒體的所有使用者資料都會加密、而且只能使用每個磁碟區的金鑰來解密。

- 在CVS軟體中、會使用Google產生的金鑰。
- 如需CVS效能、每個Volume金鑰會儲存在Cloud Volumes Service 內建於此功能的關鍵管理程式中。

自2021年11月起、客戶管理的加密金鑰（CMEK）功能已可供預覽。這可讓您使用裝載於的每個專案個別區域主金鑰來加密每個Volume金鑰 "Google金鑰管理服務（KMS）。" KMS可讓您附加外部金鑰管理程式。

如需設定KMS以獲得CVS效能的相關資訊、請參閱 "設定客戶管理的加密金鑰"。

防火牆

可公開多個TCP連接埠以服務NFS和SMB共用：Cloud Volumes Service

- "NFS存取所需的連接埠"
- "SMB存取所需的連接埠"

此外、SMB、含LDAP的NFS（包括Kerberos）及雙傳輸協定組態、都需要存取Windows Active Directory網域。Active Directory連線必須是 "已設定" 以每個區域為基礎。Active Directory網域控制器（DC）是使用來識別 "DNS型DC探索" 使用指定的DNS伺服器。系統會使用任何傳回的DC。指定Active Directory站台可限制合格的DC清單。

使用分配給的CIDR範圍內的IP位址、即可將其移出Cloud Volumes Service `gcloud compute address` 命令的同時 "登入Cloud Volumes Service 時"。您可以使用此CIDR做為來源位址、為Active Directory網域控制器設定傳入防火牆。

Active Directory網域控制器必須具備 "請依照Cloud Volumes Service 此處所述、將連接埠公開給這些開發署"。

NAS傳輸協定

NAS傳輸協定總覽

NAS傳輸協定包括NFS（v3和v4.1）和SMB/CIFS（2.x和3.x）。這些通訊協定是CVS如何允許跨多個NAS用戶端共用存取資料。此外Cloud Volumes Service 、支援同時存取NFS和SMB/CIFS用戶端（雙傳輸協定）、同時遵守NAS共用中檔案和資料夾的所有身分識別和權限設定。為了維持最高的資料傳輸安全性、Cloud Volumes Service 支援使用SMB加密和NFS Kerberos 5p的傳輸協定加密。

> ⓘ 雙傳輸協定僅適用於CVs-Performance。

NAS傳輸協定的基本概念

NAS傳輸協定是讓網路上的多個用戶端存取儲存系統上相同資料的方法、例如Cloud Volumes Service GPC上的NFS和SMB是定義的NAS傳輸協定、可在Cloud Volumes

Service 客戶端/伺服器上運作、其中的伺服器是由支援服務器使用。用戶端會傳送存取、讀取和寫入要求給伺服器、伺服器負責協調檔案的鎖定機制、儲存權限、以及處理身分識別和驗證要求。

例如、如果NAS用戶端想要在資料夾中建立新檔案、則會遵循下列一般程序。

1. 用戶端會要求伺服器提供目錄的相關資訊（權限、擁有者、群組、檔案ID、可用空間、 等）；如果要求的用戶端和使用者對父資料夾擁有必要的權限、伺服器就會回應該資訊。
2. 如果目錄上的權限允許存取、則用戶端會詢問伺服器所建立的檔案名稱是否已存在於檔案系統中。如果檔案名稱已在使用中、建立就會失敗。如果檔案名稱不存在、伺服器會讓用戶端知道它可以繼續。
3. 用戶端會呼叫伺服器、以使用目錄處理和檔案名稱來建立檔案、並設定存取和修改時間。伺服器會對檔案發出唯一的檔案ID、以確保沒有以相同的檔案ID建立其他檔案。
4. 用戶端會在寫入作業之前傳送呼叫來檢查檔案屬性。如果權限允許、用戶端就會寫入新檔案。如果傳輸協定/應用程式使用鎖定、用戶端會要求伺服器提供鎖定、以防止其他用戶端在鎖定時存取檔案、以避免資料毀損。

NFS

NFS是一種分散式檔案系統傳輸協定、是在Request for Comments（RFC）中定義的開放式IETF標準、可讓任何人實作該傳輸協定。

透過匯出可供用戶端或一組用戶端存取的路徑、將位於此功能的Volume Cloud Volumes Service 共享給NFS用戶端。掛載這些匯出的權限是由匯出原則和規則所定義、Cloud Volumes Service 這些原則和規則可由資訊管理員設定。

NetApp NFS實作被視為傳輸協定的黃金標準、可用於無數的企業NAS環境。以下各節涵蓋Cloud Volumes Service 支援的NFS和特定安全功能、以及如何實作這些功能。

預設的本機**UNIX**使用者和群組

包含多個預設UNIX使用者和群組、可提供各種基本功能。Cloud Volumes Service這些使用者和群組目前無法修改或刪除。目前無法將新的本機使用者和群組新增Cloud Volumes Service 至無法更新的功能。外部LDAP名稱服務必須提供預設使用者和群組以外的UNIX使用者和群組。

下表顯示預設使用者和群組及其對應的數字ID。NetApp建議不要在LDAP或重新使用這些數字ID的本機用戶端上建立新的使用者或群組。

預設使用者：數字**ID**	預設群組：數字**ID**
• 根目錄：0 • pcuser:65534 • 無人：65535	• 根目錄：0 • 精靈：1. • pcuser:65534 • 無人：65535

> 使用NFSv4.1時、root使用者在NFS用戶端上執行列出命令的目錄時、可能會顯示為nobnobody。這是因為用戶端的ID網域對應組態。請參閱「」一節 NFSv4.1和nobody使用者/群組 以取得此問題的詳細資訊及解決方法。

root使用者

在Linux中、root帳戶可以存取Linux型檔案系統中的所有命令、檔案和資料夾。由於此帳戶的強大功能、安全性最佳實務做法通常會要求root使用者停用或限制某種方式。在NFS匯出中、root使用者對檔案和資料夾的控制能力、可Cloud Volumes Service 透過匯出原則和規則、以及稱為root squash的概念、在整個過程中加以控制。

root使用者之間的衝突可確保存取NFS掛載的root使用者被擠到匿名的數字使用者65534（請參閱「」一節）[匿名使用者]」）、目前僅適用於使用CVS效能的情況、方法是在建立匯出原則規則期間選取「Off」（關閉）進行root存取。如果root使用者被擠到匿名使用者、就無法再執行chown或 "setuid/setgid命令（sticky位元）" 在NFS掛載的檔案或資料夾上、root使用者建立的檔案或資料夾會將anon UID顯示為擁有者/群組。此外、NFSv4 ACL無法由root使用者修改。不過、root使用者仍可存取不具有明確權限的chmod和刪除檔案。如果您想限制root使用者的檔案和資料夾權限存取、請考慮使用具有NTFS ACL的磁碟區、建立名為「root」的Windows使用者、並將所需權限套用至檔案或資料夾。

匿名使用者

匿名（anon）使用者ID會指定對應至用戶端要求的UNIX使用者ID或使用者名稱、而該用戶端要求沒有有效的NFS認證。使用root使用者時、這可能包括root使用者。Anon的Cloud Volumes Service 使用者是65534。

此UID通常與Linux環境中的使用者名稱「nobnob」或「nfsnobn」相關聯。也使用65534作為本機UNIX使用者的pcuser'（請參閱「Cloud Volumes Service預設的本機UNIX使用者和群組」）、這也是Windows到UNIX名稱對應的預設後援使用者、但LDAP中找不到有效的相符UNIX使用者。

由於Linux使用者名稱與Cloud Volumes Service 適用於UID 65534的使用者名稱不同、因此使用NFSv4.1時對應至65534的使用者名稱字串可能不相符。因此、您可能會在某些檔案和資料夾上看到「無人」的使用者身分。請參閱「」一節NFSv4.1和nobody使用者/群組」以取得此問題的相關資訊及解決方法。

存取控制/匯出

NFS裝載的初始匯出/共用存取是透過匯出原則中包含的主機型匯出原則規則來控制。定義主機IP、主機名稱、子網路、網路群組或網域、以允許存取掛載NFS共用區、以及允許存取主機的層級。匯出原則規則組態選項取決於Cloud Volumes Service 哪些方面。

對於CVS軟體、下列選項可用於匯出原則組態：

- *用戶端相符*以逗號分隔的IP位址清單、以逗號分隔的主機名稱、子網路、網路群組、網域名稱清單。
- * RO/RW存取規則。*選取「讀取/寫入」或「唯讀」來控制對EXPE/CVs-Performance的存取層級、提供下列選項：
- *用戶端相符*以逗號分隔的IP位址清單、以逗號分隔的主機名稱、子網路、網路群組、網域名稱清單。
- * RO/RW存取規則。*選取「讀取/寫入」或「唯讀」以控制匯出的存取層級。
- *根存取權（開啟/關閉）。*設定根分區（請參閱「[root使用者]」的詳細資料）。
- *傳輸協定類型。*這會將NFS掛載的存取限制為特定的傳輸協定版本。為Volume指定NFSv3和NFSv4.1時、請將兩者留白或同時勾選兩個方塊。
- * Kerberos安全性層級（選取「啟用Kerberos」時）。*提供krb5、krb5i及/或krb5p選項、以進行唯讀或讀寫存取。

變更擁有權（**chown**）和變更群組（**chgrp**）

NFS on Cloud Volumes Service 支援僅允許root使用者在檔案和資料夾上執行chown / chgrp。其他使用者也會看到「不允許操作」錯誤、即使是他們自己擁有的檔案也一樣。如果您使用root quash（如一節中所述）[root使

用者]」）時、root會被擠到非root使用者、且不允許存取chown和chgrp。目前在不允許非root使用者使用chown和chgrp的因應措施Cloud Volumes Service 。如果需要變更擁有權、請考慮使用雙傳輸協定磁碟區、並將安全樣式設定為NTFS、以便從Windows端控制權限。

權限管理

支援兩種模式位元（例如rwx的644、777等）和NFSv4.1 ACL、以控制使用UNIX安全型態之磁碟區在NFS用戶端上的權限。Cloud Volumes Service標準權限管理用於這些項目（例如、chmod、chown或nfs4_setfacl）、並可與任何支援這些項目的Linux用戶端搭配使用。

此外、當使用設為NTFS的雙傳輸協定磁碟區時、NFS用戶端可以利用Cloud Volumes Service 指向Windows使用者的名稱對應功能來解析NTFS權限。這需要LDAP連線Cloud Volumes Service 至才能提供數字ID對使用者名稱的轉譯、因為Cloud Volumes Service 需要有效的UNIX使用者名稱才能正確對應至Windows使用者名稱。

為**NFSv3**提供精細的**ACL**

模式位元權限僅涵蓋語義中的擁有者、群組及其他所有人、這表示基本NFSv3沒有精細的使用者存取控制。由於不支援POSIX ACL、也不支援擴充屬性（例如chatr）、因此使用NFSv3時、只有在下列情況下才能使用精細的ACL：Cloud Volumes Service

- NTFS安全型磁碟區（需要CIFS伺服器）、具有有效的UNIX至Windows使用者對應。
- 使用管理用戶端掛載NFSv4.1套用NFSv4.1 ACL以套用ACL。

這兩種方法都需要LDAP連線才能進行UNIX身分識別管理、並填入有效的UNIX使用者和群組資訊（請參閱一節"「LDAP」"）和僅適用於CVS效能執行個體。若要將NTFS安全型磁碟區搭配NFS使用、您必須使用雙傳輸協定（SMB和NFSv3）或雙傳輸協定（SMB和NFSv4.1）、即使沒有建立SMB連線。若要在NFSv3掛載中使用NFSv4.1 ACL、您必須選取「兩者（NFSv3/NFSv4.1）」作為傳輸協定類型。

一般UNIX模式位元在權限方面的精細度與NTFS或NFSv4.x ACL所提供的精細度不同。下表比較NFSv3模式位元與NFSv4.1 ACL之間的權限精細度。如需NFSv4.1 ACL的相關資訊、請參閱 "nfs4_ACL - NFSv4存取控制清單"。

NFSv3模式位元	NFSv4.1 ACL
• 設定執行時的使用者ID • 設定執行時的群組ID • 儲存交換的文字（未在POSIX中定義） • 擁有者的讀取權限 • 擁有者的寫入權限 • 對檔案擁有者執行權限；或在目錄中查詢（搜尋）擁有者權限 • 群組的讀取權限 • 群組的寫入權限 • 對檔案上的群組執行權限；或查詢（搜尋）目錄中的群組權限 • 其他人的讀取權限 • 其他人的寫入權限 • 對檔案上的其他人執行權限；或查詢（搜尋）目錄中的其他人權限	存取控制項目（ACE）類型（允許/拒絕/稽核）*繼承旗標*目錄繼承*檔案繼承*不傳播繼承*僅繼承 權限*讀取資料（檔案）/ list-directory（目錄）寫入資料（檔案）/建立檔案（目錄）*附加資料（檔案）/create子目錄（目錄）*執行（檔案）/變更目錄（目錄）*刪除*刪除子項目*讀取屬性*寫入屬性*讀取命名屬性*寫入命名屬性*寫入命名屬性 ACL

最後、根據RPC封包限制、NFS群組成員資格（NFSv3和NFSv4.x）的AUTH_SYS預設上限為16。NFS Kerberos最多可提供32個群組、NFSv4 ACL則可透過精細的使用者和群組ACL（每個ACE最多可容納1024個項目）來移除限制。

此外Cloud Volumes Service 、支援範圍更廣泛、最多可將支援的群組數量擴充至32個。這需要LDAP連線至包含有效UNIX使用者和群組身分識別的LDAP伺服器。如需設定此項目的詳細資訊、請參閱 "建立及管理NFS磁碟區" 在Google文件中。

NFSv3使用者與群組ID

NFSv3使用者和群組ID會以數字ID而非名稱的形式出現在線路上。使用NFSv3時、由於UNIX安全型磁碟區只使用模式位元、因此無法針對這些數字ID進行使用者名稱解析。Cloud Volumes Service當NFSv4.1 ACL存在時、即使使用NFSv3、仍需要數字ID查詢和/或名稱字串查詢、才能正確解析ACL。使用NTFS安全型磁碟區時Cloud Volumes Service 、必須先將數字ID解析為有效的UNIX使用者、然後對應至有效的Windows使用者以協商存取權限。

NFSv3使用者與群組ID的安全性限制

使用NFSv3時、用戶端和伺服器永遠不需要確認使用者使用數字ID進行讀取或寫入、這只是隱含信任而已。如此一來、只要偽造任何數字ID、檔案系統就會遭受潛在的資料外洩。為了避免這類安全漏洞、Cloud Volumes Service 我們提供一些選項供大家選擇。

- 實作Kerberos for NFS會強制使用者使用使用者名稱和密碼或Keytab檔案進行驗證、以取得Kerberos票證、以便存取掛載。Kerberos適用於CVS效能執行個體、僅適用於NFSv4.1。
- 限制匯出原則規則中的主機清單、會限制NFSv3用戶端存取Cloud Volumes Service 該卷的權限。
- 使用雙傳輸協定磁碟區並將NTFS ACL套用至磁碟區、會強制NFSv3用戶端將數字ID解析為有效的UNIX使用者名稱、以便正確驗證以存取裝載。這需要啟用LDAP並設定UNIX使用者和群組身分識別。

- 浪費root使用者的力量可限制root使用者對NFS掛載所造成的損害、但並不會完全消除風險。如需詳細資訊、請參閱「」一節[root使用者]。」

最後、NFS安全性僅限於您所使用的傳輸協定版本。NFSv3的整體效能比NFSv4.1高、但提供的安全性層級卻不相同。

NFSv4.1

NFSv4.1提供比NFSv3更高的安全性與可靠性、原因如下：

- 透過租賃型機制進行整合式鎖定
- 狀態工作階段
- 單一連接埠上的所有NFS功能（2049）
- 僅TCP
- ID網域對應
- Kerberos整合（NFSv3可以使用Kerberos、但僅適用於NFS、而非用於NLM等輔助傳輸協定）

NFSv4.1相依性

由於NFSv4.1還有額外的安全功能、因此不需要使用NFSv3（類似於SMB需要相依性（例如Active Directory）的方式）、也會涉及一些外部相依性。

NFSv4.1 ACL

支援NFSv4.x ACL、相較於一般的POSIX式權限、可提供明顯的優勢、例如：Cloud Volumes Service

- 精細控制使用者對檔案和目錄的存取
- 更好的NFS安全性
- 改善與CIFS/SMB的互通性
- 使用AUTH_SYS安全性移除每位使用者16個群組的NFS限制
- ACL不需要群組ID（GID）解析、因此能有效移除GID限制NFSv4.1 ACL、而非Cloud Volumes Service 從無法更新的NFS用戶端控制。若要使用NFSv4.1 ACL、請確定用戶端的軟體版本支援這些ACL、並已安裝適當的NFS公用程式。

NFSv4.1 ACL與SMB用戶端之間的相容性

NFSv4 ACL與Windows檔案層級ACL（NTFS ACL）不同、但具有類似的功能。不過、在多重傳輸協定NAS環境中、如果有NFSv4.1 ACL、而且您使用的是雙傳輸協定存取（NFS和SMB位於同一個資料集）、則使用SMB2.0及更新版本的用戶端將無法從Windows安全性索引標籤檢視或管理ACL。

NFSv4.1 ACL的運作方式

下列術語為參考定義：

- *存取控制清單（ACL）。*權限項目清單。
- *存取控制項目（ACE）。*清單中的權限項目。

當用戶端在設定作業期間、在檔案上設定NFSv4.1 ACL時、Cloud Volumes Service 會將物件上的ACL設定為由

任何現有的ACL取代。如果檔案上沒有ACL、則檔案的模式權限會從Owner@、group @和任何人@計算。如果檔案上有任何現有的SUID/SGID/便利貼位元、則不會受到影響。

當用戶端在GetAttr作業期間取得檔案的NFSv4.1 ACL時、Cloud Volumes Service 會讀取與物件相關聯的NFSv4.1 ACL、建構ACE清單、並將清單傳回用戶端。如果檔案具有NT ACL或模式位元、則會從模式位元建構ACL並傳回用戶端。

如果ACL中存在拒絕的ACE、則會拒絕存取；如果存在允許的ACE、則會授予存取權。不過、如果ACL中沒有任何ACE、也會拒絕存取。

安全性描述元由安全性ACL（SACL）和判別ACL（DACL）組成。當NFSv4.1與CIFS/SMB互操作時、DACL會以一對一的方式對應NFSv4和CIFS。DACL由允許和拒絕的ACE組成。

如果在已設定NFSv4.1 ACL的檔案或資料夾上執行基本的「chmod」、則會保留現有的使用者和群組ACL、但會修改預設的「擁有者」、「群組@」、「每個人@」ACL。

使用NFSv4.1 ACL的用戶端可以設定及檢視系統上檔案和目錄的ACL。當在具有ACL的目錄中建立新檔案或子目錄時、該物件會繼承ACL中已標記適當的所有ACE "繼承旗標"。

如果檔案或目錄具有NFSv4.1 ACL、則無論使用哪種傳輸協定來存取檔案或目錄、該ACL都能用來控制存取。

只要將ACE標記為正確的繼承旗標、檔案和目錄就會從父目錄的NFSv4 ACL繼承ACE（可能需要適當的修改）。

當檔案或目錄是因NFSv4要求而建立時、產生的檔案或目錄上的ACL取決於檔案建立要求是否包含ACL或僅包含標準UNIX檔案存取權限。ACL也取決於父目錄是否具有ACL。

- 如果要求包含ACL、則會使用該ACL。
- 如果要求僅包含標準UNIX檔案存取權限、且父目錄沒有ACL、則會使用用戶端檔案模式來設定標準UNIX檔案存取權限。
- 如果要求僅包含標準UNIX檔案存取權限、且父目錄具有不可繼承的ACL、則會針對新物件設定以傳遞至要求的模式位元為基礎的預設ACL。
- 如果要求僅包含標準UNIX檔案存取權限、但父目錄具有ACL、則只要將ACE標記為適當的繼承旗標、父目錄ACL中的ACE就會由新檔案或目錄繼承。

ACE權限

NFSv4.1 ACL權限使用一系列大小寫字母值（例如「raptncy」）來控制存取。如需這些字母值的詳細資訊、請參閱 "使用方法：使用NFSv4 ACL"。

具有umask和ACL繼承的NFSv4.1 ACL行為

"NFSv4 ACL可提供ACL繼承功能"。ACL繼承意味著在使用NFSv4.1 ACL集的物件下建立的檔案或資料夾、可以根據的組態來繼承ACL "ACL繼承旗標"。

"umask" 用於控制在目錄中建立檔案和資料夾的權限等級、而無需系統管理員互動。根據預設Cloud Volumes Service 、支援使用者使用支援功能來覆寫繼承的ACL、這是預期的行為 "RFC 5661"。

ACL格式化

NFSv4.1 ACL具有特定格式化。下列範例是檔案上的ACE設定：

```
A::ldapuser@domain.netapp.com:rwatTnNcCy
```

上述範例遵循下列ACL格式準則：

```
type:flags:principal:permissions
```

一種「A」表示「允許」。 在此情況下不會設定繼承旗標、因為主體不是群組、不包含繼承。此外、由於ACE不是稽核項目、因此不需要設定稽核旗標。如需NFSv4.1 ACL的詳細資訊、請參閱 "http://linux.die.net/man/5/nfs4_acl"。

如果NFSv4.1 ACL設定不正確（或用戶端和伺服器無法解析名稱字串）、則ACL可能無法如預期般運作、或ACL變更可能無法套用及拋出錯誤。

範例錯誤包括：

```
Failed setxattr operation: Invalid argument
Scanning ACE string 'A:: user@rwaDxtTnNcCy' failed.
```

明確拒絕

NFSv4.1權限可包含擁有者、群組及所有人的明確拒絕屬性。這是因為NFSv4.1 ACL是預設拒絕ACL、這表示如果某個ACL未由ACE明確授予、就會拒絕該ACL。明確拒絕屬性會覆寫任何明確或不明確的存取ACE。

拒絕ACE的屬性標籤設定為「D」。

在以下範例中、允許群組@擁有所有讀取和執行權限、但拒絕所有寫入權限。

```
sh-4.1$ nfs4_getfacl /mixed
A::ldapuser@domain.netapp.com:ratTnNcCy
A::OWNER@:rwaDxtTnNcCy
D::OWNER@:
A:g:GROUP@:rxtncy
D:g:GROUP@:waDTC
A::EVERYONE@:rxtncy
D::EVERYONE@:waDTC
```

應盡可能避免使用拒絕的ACE、因為它們可能會造成混淆和複雜；允許不明確定義的ACL被隱含拒絕。當設定拒絕ACE時、使用者預期會被授予存取權限時、可能會被拒絕存取。

上述一組ACE相當於模式位元中的755、這表示：

- 擁有者擁有完整權利。
- 群組具有唯讀。
- 其他人則為唯讀。

不過、即使權限調整為等同的775個權限、仍會因為每個人都設定明確的拒絕權限而拒絕存取。

NFSv4.1 ID網域對應相依性

NFSv4.1利用ID網域對應邏輯做為安全層、協助驗證嘗試存取NFSv4.1掛載的使用者確實是他們宣稱的對象。在這些情況下、來自NFSv4.1用戶端的使用者名稱和群組名稱會附加名稱字串、並傳送至Cloud Volumes Service該實例。如果該使用者名稱/群組名稱和ID字串組合不相符、則使用者和（或）群組會被擠到用戶端上「/etc/idmapd.conf」檔案中指定的預設nober使用者。

此ID字串是適當遵循權限的必要條件、尤其是使用NFSv4.1 ACL和/或Kerberos時。因此、需要使用名稱服務伺服器相依性（例如LDAP伺服器）來確保用戶端之間的一致性、Cloud Volumes Service 以及使用者和群組名稱身分識別解析是否正確。

使用靜態預設ID網域名稱值「defaultv4iddomain.com」Cloud Volumes Service 。NFS用戶端的ID網域名稱設定預設為DNS網域名稱、但您可以在「/etc/idmapd.conf」中手動調整ID網域名稱。

如果在Cloud Volumes Service 支援功能中啟用LDAP、Cloud Volumes Service 則當NFS ID網域在DNS中變更為搜尋網域所設定的項目時、不需要修改用戶端、除非他們使用不同的DNS網域搜尋名稱。

當能夠解析本機檔案或LDAP中的使用者名稱或群組名稱時、會使用網域字串、而非相符的網域ID則會對nobnobody進行儲存。Cloud Volumes Service如果Cloud Volumes Service 無法在本機檔案或LDAP中找到使用者名稱或群組名稱、則會使用數字ID值、NFS用戶端會正確解析名稱（這與NFSv3行為類似）。

在不變更用戶端的NFSv4.1 ID網域以符合Cloud Volumes Service 使用的功能的情況下、您會看到下列行為：

- UNIX使用者和群組的本機項目Cloud Volumes Service （例如root、如本機UNIX使用者和群組所定義）會被浪費在nobnobody值。
- 如果Cloud Volumes Service DNS網域不同於NFS用戶端和Cloud Volumes Service 更新、則UNIX使用者和在LDAP中有項目的群組（如果將Sfuse設定為使用LDAP）會被浪費給任何人。
- 沒有本機項目或LDAP項目的UNIX使用者和群組會使用數字ID值、並解析為NFS用戶端上指定的名稱。如果用戶端上不存在名稱、則只會顯示數字ID。

以下顯示上述案例的結果：

```
# ls -la /mnt/home/prof1/nfs4/
total 8
drwxr-xr-x 2 nobody nobody 4096 Feb  3 12:07 .
drwxrwxrwx 7 root   root   4096 Feb  3 12:06 ..
-rw-r--r-- 1   9835   9835    0 Feb  3 12:07 client-user-no-name
-rw-r--r-- 1 nobody nobody    0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 nobody nobody    0 Feb  3 12:06 root-user-file
```

當用戶端和伺服器ID網域相符時、相同的檔案清單看起來就像這樣：

```
# ls -la
total 8
drwxr-xr-x 2 root   root         4096 Feb  3 12:07 .
drwxrwxrwx 7 root   root         4096 Feb  3 12:06 ..
-rw-r--r-- 1   9835         9835    0 Feb  3 12:07 client-user-no-name
-rw-r--r-- 1 apache apache-group    0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 root   root            0 Feb  3 12:06 root-user-file
```

如需此問題及其解決方法的詳細資訊、請參閱「」一節NFSv4.1和nobody使用者/群組。」

Kerberos相依性

如果您打算使用Kerberos搭配NFS、Cloud Volumes Service 則必須搭配下列功能搭配使用才能使用：

- 適用於Kerberos Distribution Center服務（Kdc）的Active Directory網域
- Active Directory網域中的使用者和群組屬性會填入UNIX資訊以供LDAP功能使用（Cloud Volumes Service 在列舉NFS Kerberos時、需要使用者的SPN-UNIX使用者對應才能正常運作）。
- LDAP已在Cloud Volumes Service 實例上啟用
- DNS服務的Active Directory網域

NFSv4.1和nobody使用者/群組

NFSv4.1組態最常見的問題之一、就是檔案或資料夾列在使用「ls」的清單中、顯示為「user:group」的「nobnon:nobnobnone」組合。

例如：

```
sh-4.2$ ls -la | grep prof1-file
-rw-r--r-- 1 nobody nobody    0 Apr 24 13:25 prof1-file
```

數字ID是「99」。

```
sh-4.2$ ls -lan | grep prof1-file
-rw-r--r-- 1 99 99    0 Apr 24 13:25 prof1-file
```

在某些情況下、檔案可能會顯示正確的擁有者、但不會顯示「nobody」為群組。

```
sh-4.2$ ls -la | grep newfile1
-rw-r--r-- 1 prof1  nobody    0 Oct  9  2019 newfile1
```

誰是無人？

NFSv4.1中的「nobn」使用者與「nfsnobnobn」使用者不同。您可以執行「id」命令來檢視NFS用戶端如何查

看每位使用者：

```
# id nobody
uid=99(nobody) gid=99(nobody) groups=99(nobody)
# id nfsnobody
uid=65534(nfsnobody) gid=65534(nfsnobody) groups=65534(nfsnobody)
```

使用NFSv4.1時、「noban」使用者是由「idmapd.conf」檔案定義的預設使用者、可定義為任何您要使用的使用者。

```
# cat /etc/idmapd.conf | grep nobody
#Nobody-User = nobody
#Nobody-Group = nobody
```

為什麼會發生這種情況？

由於透過名稱字串對應來確保安全性是NFSv4.1作業的重要宗旨、因此名稱字串不適當時的預設行為是將該使用者分成通常無法存取使用者和群組所擁有之檔案和資料夾的使用者。

當您在檔案清單中看到使用者和（或）群組的「nobnoby」時、這通常表示NFSv4.1中的某些項目設定錯誤。區分大小寫的功能可在此處發揮。

例如、如果user1@CVSDEM.LOSLL（uid、1234、gid、1234）正在存取匯出、Cloud Volumes Service 則必須找到user1@CVSDEM.LOSLL（uid、gid、1234）。如果Cloud Volumes Service 使用者在支援資料的範本中是USER1@CVSDEMO.在許多情況下、您可以在用戶端的訊息檔案中看到下列內容：

```
May 19 13:14:29 centos7 nfsidmap[17481]: nss_getpwnam: name
'root@defaultv4iddomain.com' does not map into domain 'CVSDEMO.LOCAL'
May 19 13:15:05 centos7 nfsidmap[17534]: nss_getpwnam: name 'nobody' does
not map into domain 'CVSDEMO.LOCAL'
```

用戶端和伺服器必須都同意使用者確實是他們聲稱的對象、因此您必須檢查下列項目、以確保用戶端看到的使用者擁有Cloud Volumes Service 與此使用者相同的資訊。

- * NFSv4.x ID網域。*用戶端：「idmapd.conf」檔案；Cloud Volumes Service 使用「defaultv4iddomain.com」、無法手動變更。如果將LDAP搭配NFSv4.1使用、Cloud Volumes Service 則將ID網域變更為DNS搜尋網域所使用的網域、與AD網域相同。
- *使用者名稱和數字ID。*這會決定用戶端尋找使用者名稱的位置、並運用名稱服務交換器組態：用戶端：「nsswitch.conf」和（或）本機密碼和群組檔案；Cloud Volumes Service 不允許對此進行修改、但會在啟用時自動將LDAP新增至組態。
- *群組名稱和數字ID。*這會決定用戶端尋找群組名稱的位置、並運用名稱服務交換器組態（用戶端：「nsswitch.conf」和/或本機密碼和群組檔案）；Cloud Volumes Service 不允許對此進行修改、但會在啟用時自動將LDAP新增至組態。

在幾乎所有的情況Cloud Volumes Service 下、如果您在用戶端的使用者和群組清單中看到「nobnoby」、問題在於使用者或群組名稱網域ID轉譯功能會在更新到NFS用戶端之間進行。若要避免這種情況發生、請使用LDAP

來解決用戶端和Cloud Volumes Service 客戶端之間的使用者和群組資訊。

在用戶端上檢視NFSv4.1的名稱ID字串

如果您使用NFSv4.1、NFS作業期間會發生名稱字串對應、如前所述。

除了使用「/var/log/Messages」來找出NFSv4 ID的問題、您也可以使用 "nfsidmap -l" NFS用戶端上的命令、可檢視哪些使用者名稱已正確對應至NFSv4網域。

例如、此命令會在用戶端找到使用者之後輸出、Cloud Volumes Service 並由用戶端存取NFSv4.x掛載：

```
# nfsidmap -l
4 .id_resolver keys found:
  gid:daemon@CVSDEMO.LOCAL
  uid:nfs4@CVSDEMO.LOCAL
  gid:root@CVSDEMO.LOCAL
  uid:root@CVSDEMO.LOCAL
```

如果未正確對應至NFSv4.1 ID網域的使用者（在此案例中為「NetApp-user」）嘗試存取相同的掛載、並接觸檔案、就會依照預期指派「nobnan:nobnobnobn」。

```
# su netapp-user
sh-4.2$ id
uid=482600012(netapp-user), 2000(secondary)
sh-4.2$ cd /mnt/nfs4/
sh-4.2$ touch newfile
sh-4.2$ ls -la
total 16
drwxrwxrwx  5 root   root   4096 Jan 14 17:13 .
drwxr-xr-x. 8 root   root     81 Jan 14 10:02 ..
-rw-r--r--  1 nobody nobody    0 Jan 14 17:13 newfile
drwxrwxrwx  2 root   root   4096 Jan 13 13:20 qtree1
drwxrwxrwx  2 root   root   4096 Jan 13 13:13 qtree2
drwxr-xr-x  2 nfs4   daemon 4096 Jan 11 14:30 testdir
```

nfidmap -l輸出顯示螢幕上的使用者為「pcuser"、但不是「NetApp-user"；這是我們的匯出原則規則（「65534」）中的匿名使用者。

```
# nfsidmap -l
6 .id_resolver keys found:
  gid:pcuser@CVSDEMO.LOCAL
  uid:pcuser@CVSDEMO.LOCAL
  gid:daemon@CVSDEMO.LOCAL
  uid:nfs4@CVSDEMO.LOCAL
  gid:root@CVSDEMO.LOCAL
  uid:root@CVSDEMO.LOCAL
```

中小企業

"中小企業" 是由Microsoft開發的網路檔案共用傳輸協定、可透過乙太網路為多個SMB用戶端提供集中式使用者/群組驗證、權限、鎖定及檔案共用。檔案和資料夾會以共用的方式呈現給用戶端、您可以設定各種共用內容、並透過共用層級權限來提供存取控制。SMB可以呈現給任何支援該傳輸協定的用戶端、包括Windows、Apple和Linux用戶端。

支援SMB 2.1和3.x版的傳輸協定。Cloud Volumes Service

存取控制/**SMB**共用區

- 當Windows使用者名稱要求存取Cloud Volumes Service 到此卷時、Cloud Volumes Service 功能區會使用Cloud Volumes Service 由管理員設定的方法尋找UNIX使用者名稱。
- 如果已設定外部UNIX身分識別供應商（LDAP）、且Windows / UNIX使用者名稱相同、則Windows使用者名稱會將1：1對應至UNIX使用者名稱、而不需要任何額外的組態。啟用LDAP時、會使用Active Directory來裝載使用者和群組物件的UNIX屬性。
- 如果Windows名稱和UNIX名稱不一致、則必須將LDAP設定為允許Cloud Volumes Service 使用LDAP名稱對應組態（請參閱一節）"「使用LDAP進行非對稱名稱對應」"）。
- 如果未使用LDAP、則Windows SMB使用者會對應至Cloud Volumes Service 預設的本地UNIX使用者、名稱為「pcuser" in fuse」。這表示在Windows中、對應到「pcuser'」的使用者所寫入的檔案、會在多重傳輸協定NAS環境中、將UNIX擁有權顯示為「pcuser'」。這裏的「pcuser」實際上是Linux環境中的「nobnobody」使用者（UID 65534）。

在僅使用SMB的部署中、「pcuser'」對應仍會發生、但這並不重要、因為Windows使用者和群組擁有權已正確顯示、而且不允許NFS存取SMB專屬磁碟區。此外、純SMB磁碟區在建立之後、不支援轉換成NFS或雙傳輸協定磁碟區。

Windows利用Kerberos與Active Directory網域控制器進行使用者名稱驗證、這需要與Cloud Volumes Service AD DC交換使用者名稱/密碼、此區段是由實例外部的。當SMB用戶端使用「\伺服器名稱」的UNC路徑時、就會使用Kerberos驗證、下列情況為真：

- 伺服器名稱存在DNS A/Aaaa項目
- 伺服器名稱具有SMB / CIFS存取的有效SPN

建立一個支援功能的SMB Volume時、會依區段中的定義建立機器帳戶名稱Cloud Volumes Service "「Cloud Volumes Service 如何在Active Directory中顯示此功能。」" 該機器帳戶名稱也會成為SMB共用存取路徑、因為Cloud Volumes Service 它利用動態DNS（DDNS）在DNS中建立必要的A/AAAA和PTr項目、以及在機器帳戶主體上建立必要的SPN-s項目。

若要建立PTr項目、Cloud Volumes Service DNS伺服器上必須存在適用於此實例IP位址的反向對應區域。

例如Cloud Volumes Service 、此Sesvvolume使用下列的UNC共用路徑：「\cs-east- 433d.cvsdemo.local'」。

在Active Directory中、這些是Cloud Volumes Service產生的SPN項目：

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
        HOST/cvs-east-433d.cvsdemo.local
        HOST/CVS-EAST-433D
```

這是DNS轉送/反轉查詢結果：

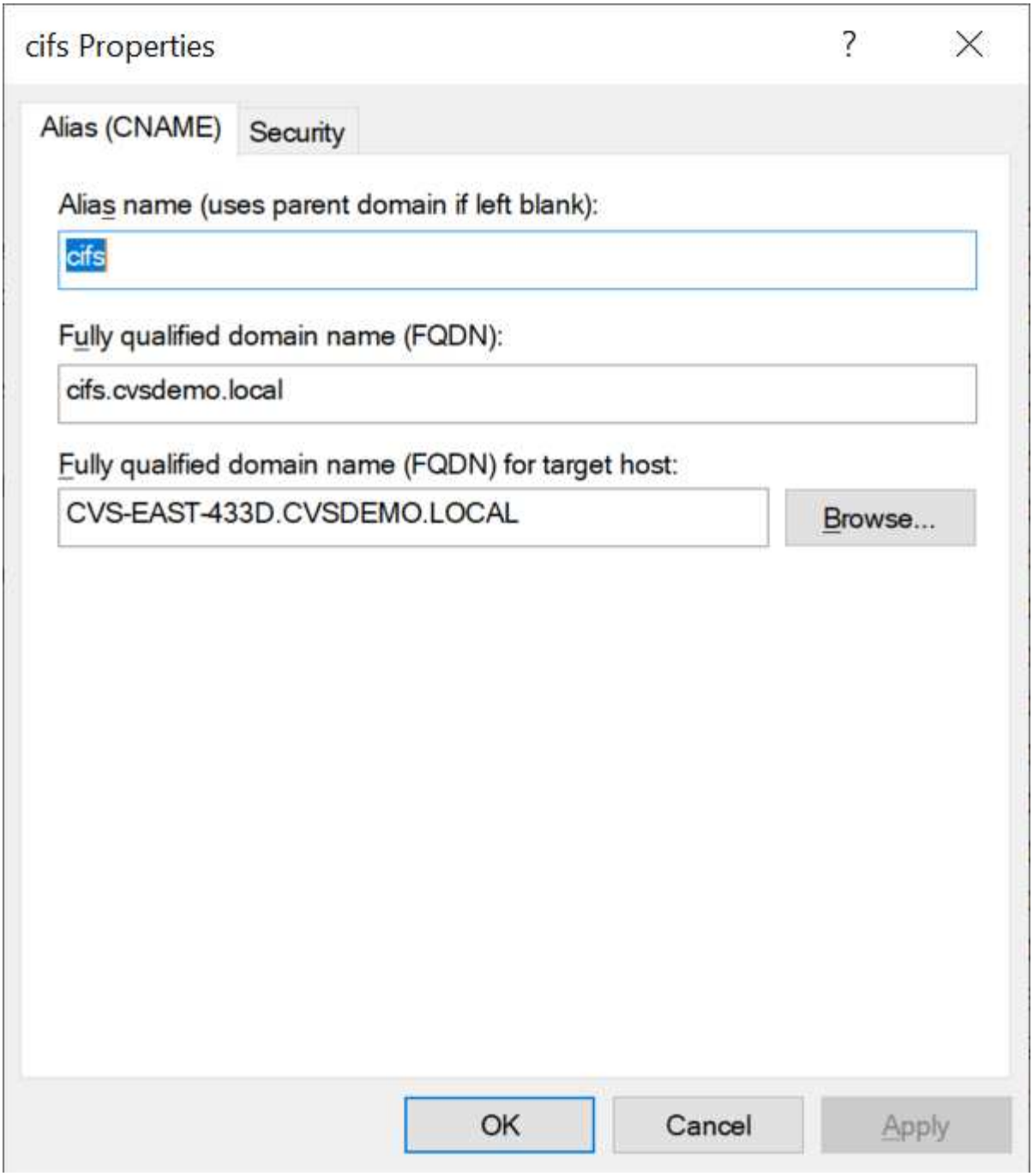
```
PS C:\> nslookup CVS-EAST-433D
Server:  activedirectory. region. lab. internal
Address:  10. xx.0. xx
Name:    CVS-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
PS C:\> nslookup 10. xxx.0. x
Server:  activedirectory.region.lab.internal
Address:  10.xx.0.xx
Name:    CVS-EAST-433D.CVSDEMO.LOCAL
Address:  10. xxx.0. x
```

或者、啟用Cloud Volumes Service /要求SMB加密以利執行更多存取控制、以利執行支援。如果其中一個端點不支援SMB加密、則不允許存取。

使用SMB名稱別名

在某些情況下、終端使用者可能會擔心安全問題、因為他們知道Cloud Volumes Service 使用中的機器帳戶名稱以供使用。在其他情況下、您可能只想提供更簡單的存取路徑給終端使用者。在這些情況下、您可以建立SMB別名。

如果您想要為SMB共用路徑建立別名、可以利用DNS中稱為「CNAME-」記錄的名稱。例如、如果您想要使用名稱「\CIFS」來存取共享區、而不是「\CVS東- 433d.cvsdemo.local」、但仍想要使用Kerberos驗證、DNS中的一種命名為「CNAME」、指向現有的A/AAAA記錄、以及新增至現有機器帳戶的其他SPN-s、則可提供Kerberos存取。



這是在新增CNAME:

```
PS C:\> nslookup cifs
Server:  ok-activedirectory.us-east4-a.c.cv-solution-architect-
lab.internal
Address:  10. xx.0. xx
Name:    CVS-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
Aliases:  cifs.cvsdemo.local
```

這是新增SPN後產生的SPN查詢：

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
        cifs/cifs.cvsdemo.local
        cifs/cifs
        HOST/cvs-east-433d.cvsdemo.local
        HOST/CVS-EAST-433D
```

在封包擷取中、我們可以使用與CNAMA相關的SPN來查看工作階段設定要求。

```
431 4.156722                                    SMB2    308 Negotiate Protocol Response
432 4.156785                                    SMB2    232 Negotiate Protocol Request
434 4.158108                                    SMB2    374 Negotiate Protocol Response
435 4.160977                                    SMB2   1978 Session Setup Request
437 4.166224                                    SMB2    322 Session Setup Response
438 4.166891                                    SMB2    152 Tree Connect Request Tree: \\cifs\IPC$
439 4.168063                                    SMB2    138 Tree Connect Response
```

```
    realm: CVSDEMO.LOCAL
  ⌄ sname
      name-type: kRB5-NT-SRV-INST (2)
    ⌄ sname-string: 2 items
        SNameString: cifs
        SNameString: cifs
  ⌄ enc-part
      etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
```

SMB驗證的語言

支援下列項目Cloud Volumes Service "方言" SMB驗證：

- LM
- NTLM
- NTLMv2
- Kerberos

SMB共用存取的Kerberos驗證是您可以使用的最安全驗證層級。啟用AES和SMB加密後、安全層級會進一步提升。

支援LM和NTLM驗證的向下相容性。Cloud Volumes Service當Kerberos設定錯誤時（例如建立SMB別名時）、共用存取會回復到較弱的驗證方法（例如：NTLMv2）。由於這些機制較不安全、因此在某些Active Directory環境中會停用這些機制。如果停用較弱的驗證方法、但未正確設定Kerberos、則共用存取會失敗、因為沒有有效的驗證方法可以還原。

如需在Active Directory中設定/檢視支援的驗證層級的相關資訊、請參閱 "網路安全性：LAN Manager驗證層級"。

權限模式

NTFS/檔案權限

NTFS權限是指套用至檔案系統中符合NTFS邏輯的檔案和資料夾。您可以在「基本」或「進階」中套用NTFS權限、並可設定為「允許」或「允許」以進行存取控制。

基本權限包括：

- 完全控制
- 修改
- 讀取與執行
- 讀取
- 寫入

當您設定使用者或群組的權限（稱為ACE）時、該使用者或群組會駐留在ACL中。NTFS權限使用與UNIX模式位元相同的讀取/寫入/執行基礎、但也可延伸至更精細且延伸的存取控制（也稱為特殊權限）、例如「取得所有權」、「建立資料夾/附加資料」、「寫入屬性」等。

標準UNIX模式位元提供的精細度與NTFS權限不同（例如、能夠設定ACL中個別使用者和群組物件的權限、或是設定延伸屬性）。不過NFSv4.1 ACL確實提供與NTFS ACL相同的功能。

NTFS權限比共用權限更為特定、可搭配共用權限使用。使用NTFS權限結構時、會套用最嚴格的限制。因此、在定義存取權限時、明確拒絕使用者或群組甚至會覆寫「完全控制」。

NTFS權限由Windows SMB用戶端控制。

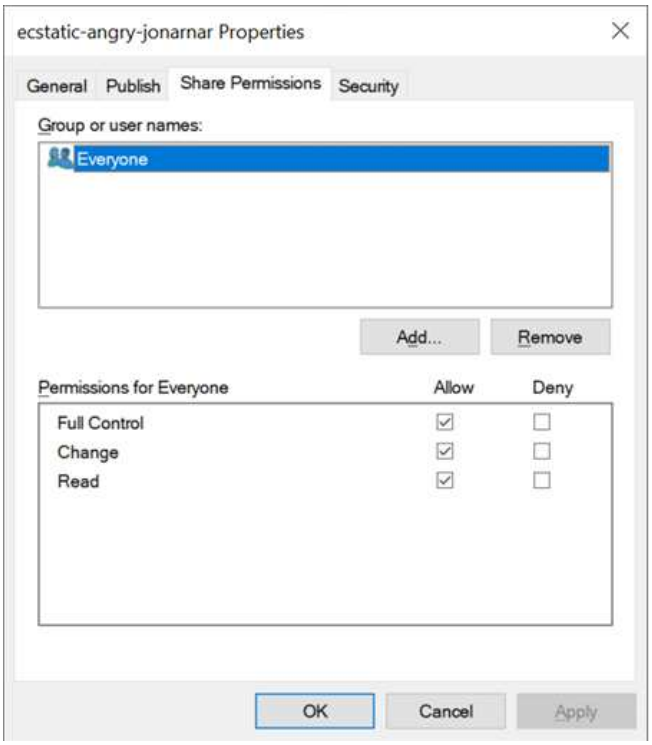
共用權限

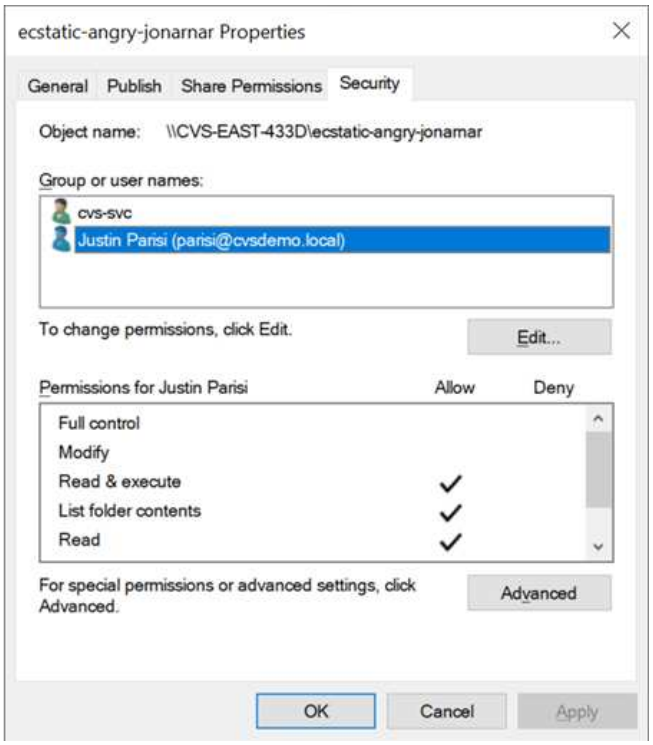
共用權限比NTFS權限更為一般（唯讀/變更/完全控制）、並控制SMB共用的初始項目、類似於NFS匯出原則規則的運作方式。

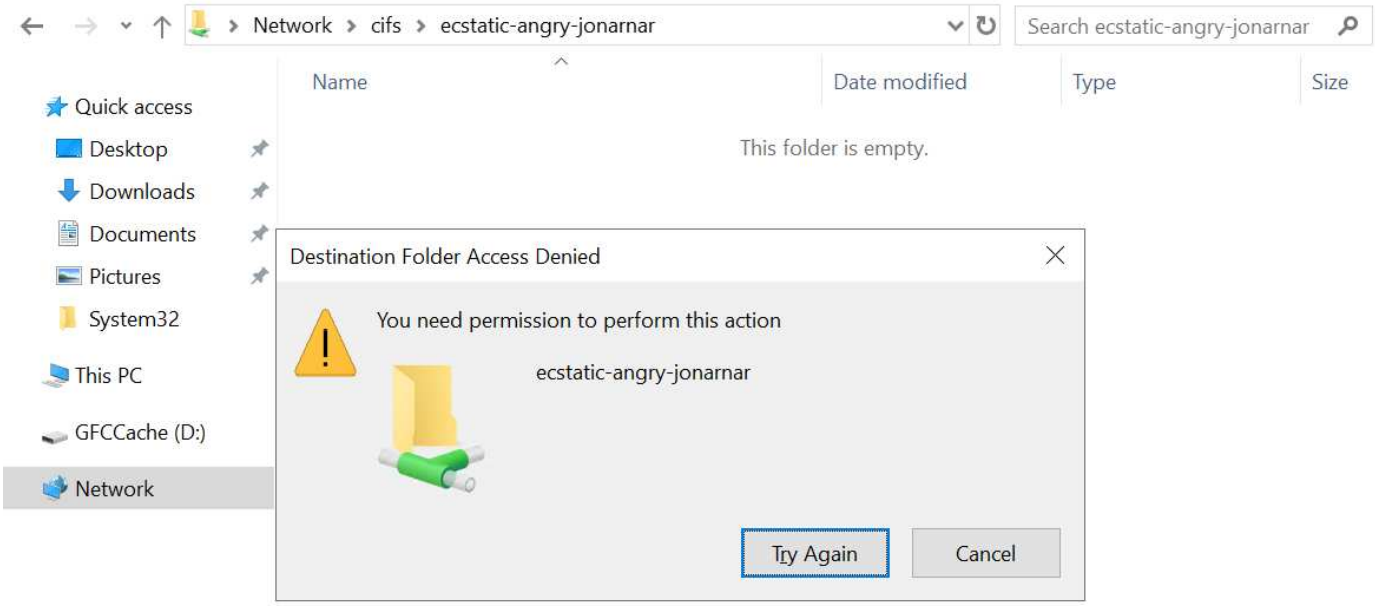
雖然NFS匯出原則規則可透過主機型資訊（例如IP位址或主機名稱）來控制存取、但SMB共用權限可以使用共用ACL中的使用者和群組ACE來控制存取。您可以從Windows用戶端或Cloud Volumes Service 從功能區管理UI設定共用ACL。

根據預設、共用ACL和初始Volume ACL包括「完全控制的每個人」。檔案ACL應該變更、但共用權限會被共用區中物件的檔案權限所取代。

例如、如果使用者只能讀取Cloud Volumes Service 對此實體磁碟區檔案ACL的存取權、則即使共用ACL設定為「擁有完全控制權的所有人」、仍無法存取建立檔案和資料夾、如下圖所示。







若要獲得最佳的安全性結果、請執行下列步驟：

- 從共用和檔案ACL中移除「所有人」、改為設定使用者或群組的共用存取權。
- 使用群組進行存取控制、而非個別使用者、以利管理、並更快移除/新增使用者、透過群組管理來共用ACL。
- 允許對共用權限上的ACE進行較少限制、較為一般的共用存取、並鎖定具有檔案權限的使用者和群組存取、以達到更精細的存取控制。
- 避免一般使用明確拒絕ACL、因為它們會覆寫允許ACL。限制使用者或群組的明確拒絕ACL、以防止他們快速存取檔案系統。
- 請務必注意 "ACL繼承" 修改權限時的設定；在目錄或磁碟區的最上層設定具有高檔案計數的繼承旗標、表示該目錄或磁碟區下方的每個檔案都已新增繼承權限、 這可能會在調整每個檔案時產生不必要的行為、例如非

預期的存取/拒絕、以及冗長的權限修改。

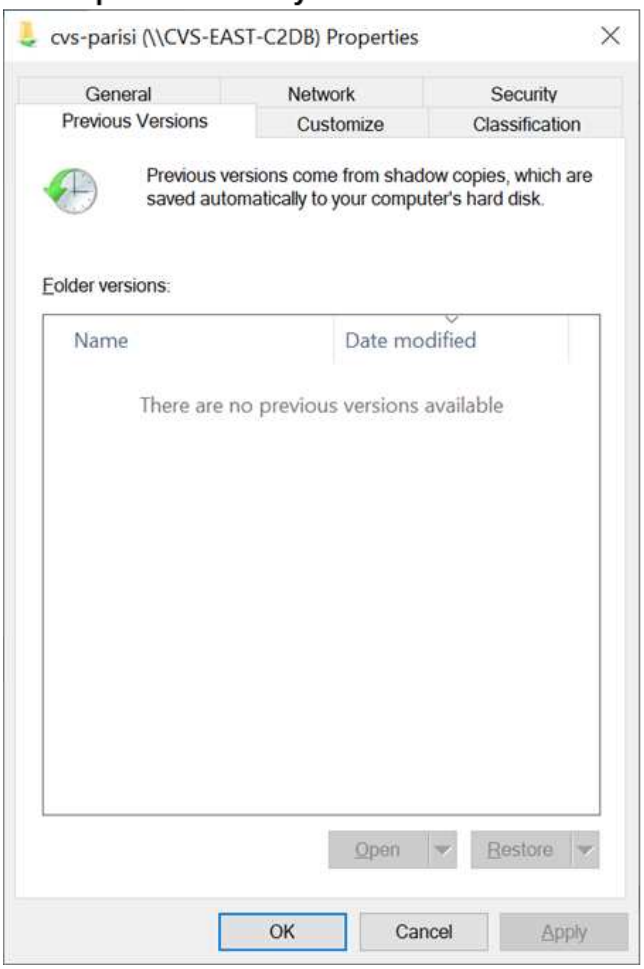
SMB共享安全功能

當您第一次在Cloud Volumes Service 支援SMB存取的情況下建立Volume時、系統會提供一系列的選項來保護該Volume。

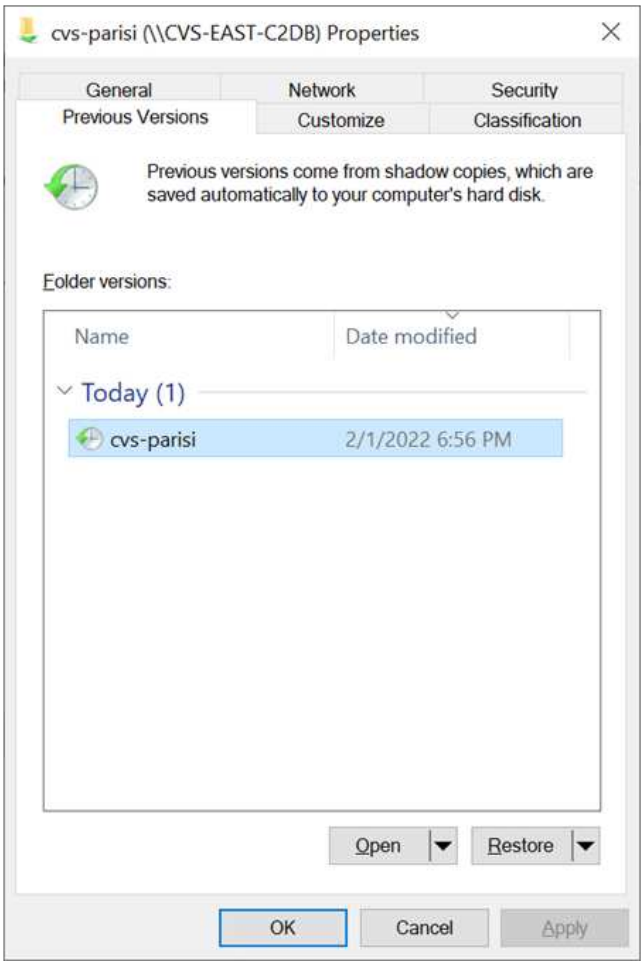
這些選項中的部分取決於Cloud Volumes Service 「樣層」（「效能」或「軟體」）、選項包括：

- *使Snapshot目錄可見（同時適用於CVs-Performance和CVs-SW）。*此選項控制SMB用戶端是否可以存取SMB共用區（「\伺服器\共用~snapshot」和/或「舊版」索引標籤）中的Snapshot目錄。未核取預設設定、這表示磁碟區預設為隱藏及不允許存取「~snapshot」目錄、而且磁碟區的「舊版」索引標籤不會顯示Snapshot複本。

Snapshot directory visible: Unchecked



Snapshot directory visible: Checked



基於安全理由、效能理由（將這些資料夾隱藏在AV掃描之外）或偏好、可能需要從終端使用者處隱藏Snapshot複本。由於「支援快照」是唯讀的、因此即使這些快照可見、終端使用者仍無法刪除或修改Snapshot目錄中的檔案。Cloud Volumes Service應用Snapshot複本時、檔案或資料夾的檔案權限。如果檔案或資料夾的權限在Snapshot複本之間變更、則變更也會套用至Snapshot目錄中的檔案或資料夾。使用者和群組可以根據權限存取這些檔案或資料夾。雖然無法刪除或修改Snapshot目錄中的檔案、但仍可將檔案或資料夾從Snapshot目錄中複製出來。

- 啟用**SMB**加密（同時適用於**CVs-Performance**和**CVs-SW**）。 SMB加密預設為停用（未核取）。核取此方塊可啟用SMB加密、這表示SMB用戶端與伺服器之間的流量會在傳輸中加密、並以議定的最高支援加密層級進行加密。支援高達AES-256的SMB加密。Cloud Volumes Service啟用SMB加密確實會造成效能損失、而

您的SMB用戶端可能會或可能不會察覺到這種情況、範圍大致介於10-20%之間。NetApp強烈建議測試、以瞭解效能損失是否可接受。

- *隱藏SMB共用區（同時適用於CVS效能和CVS軟體）。*設定此選項會隱藏SMB共用路徑、使其無法正常瀏覽。這表示不知道共用路徑的用戶端在存取預設的UNC路徑（例如：「\CVS SMB」）時、無法看到共用區。核取此核取方塊時、只有明確知道SMB共用路徑或由群組原則物件定義共用路徑的用戶端才能存取該路徑（透過混淆來確保安全）。
- *啟用存取型列舉（ABE）（僅限CVs-SW）。*這類似於隱藏SMB共用區、但共用區或檔案只會隱藏在沒有存取物件權限的使用者或群組中。例如、如果不允許Windows使用者「Joe」透過權限至少讀取存取權、則Windows使用者「Joe」根本看不到SMB共用區或檔案。此功能預設為停用、您可以選取核取方塊來啟用此功能。如需ABE的詳細資訊、請參閱NetApp知識庫文章 "存取型列舉（ABE）如何運作？"
- 啟用持續可用的（**CA**）共用支援（僅限**CVS**效能）。 "持續可用的SMB共用" 透過在Cloud Volumes Service 整個節點之間複寫鎖定狀態、將容錯移轉事件期間的應用程式中斷降至最低。這不是一項安全功能、但確實能提供更好的整體恢復能力。目前、此功能僅支援SQL Server和FSLogix應用程式。

預設隱藏共用

當SMB伺服器是以Cloud Volumes Service 支援功能建立時、就會出現這種情況 "隱藏的管理共用" （使用$命名慣例）、這是在資料Volume SMB共用區之外建立的。其中包括C$（命名空間存取）和IPC$（共用具名管道、用於程式之間的通訊、例如用於Microsoft管理主控台（MMC）存取的遠端程序呼叫（RPC））。

IPC$共用區不含共用ACL、無法修改、嚴格用於RPC呼叫和 "Windows預設不允許匿名存取這些共用"。

依預設、C$共用可讓BUILTIN/系統管理員存取、但Cloud Volumes Service 由於能夠存取C$共用區、因此無法檢視Cloud Volumes Service 所有安裝於此的磁碟區、因此無法存取共享ACL。因此、嘗試瀏覽至「\SERVER\C$」失敗。

具有本機**/BUILTIN/**系統管理員**/**備份權限的帳戶

由於本機群組（例如BUILTIN\Administrator）會套用存取權限給選取的網域使用者和群組、因此、支援SMB伺服器的功能與一般Windows SMB伺服器類似。Cloud Volumes Service

當您指定要新增至備份使用者的使用者時、該使用者會新增至Cloud Volumes Service 使用該Active Directory連線的執行個體中BUILTIN\Backup Operators群組、然後取得 "SeBackup權限和Se恢復 權限"。

當您將使用者新增至「安全性權限使用者」時、系統會將SeSecurityPrivilege賦予使用者、這在某些應用程式使用案例（例如）中很有用 "SMB共用上的SQL Server"。

Backup Users

Provide a comma separated list of domain users or a domain group name that require elevated privileges to access volumes created by Cloud Volumes Service.

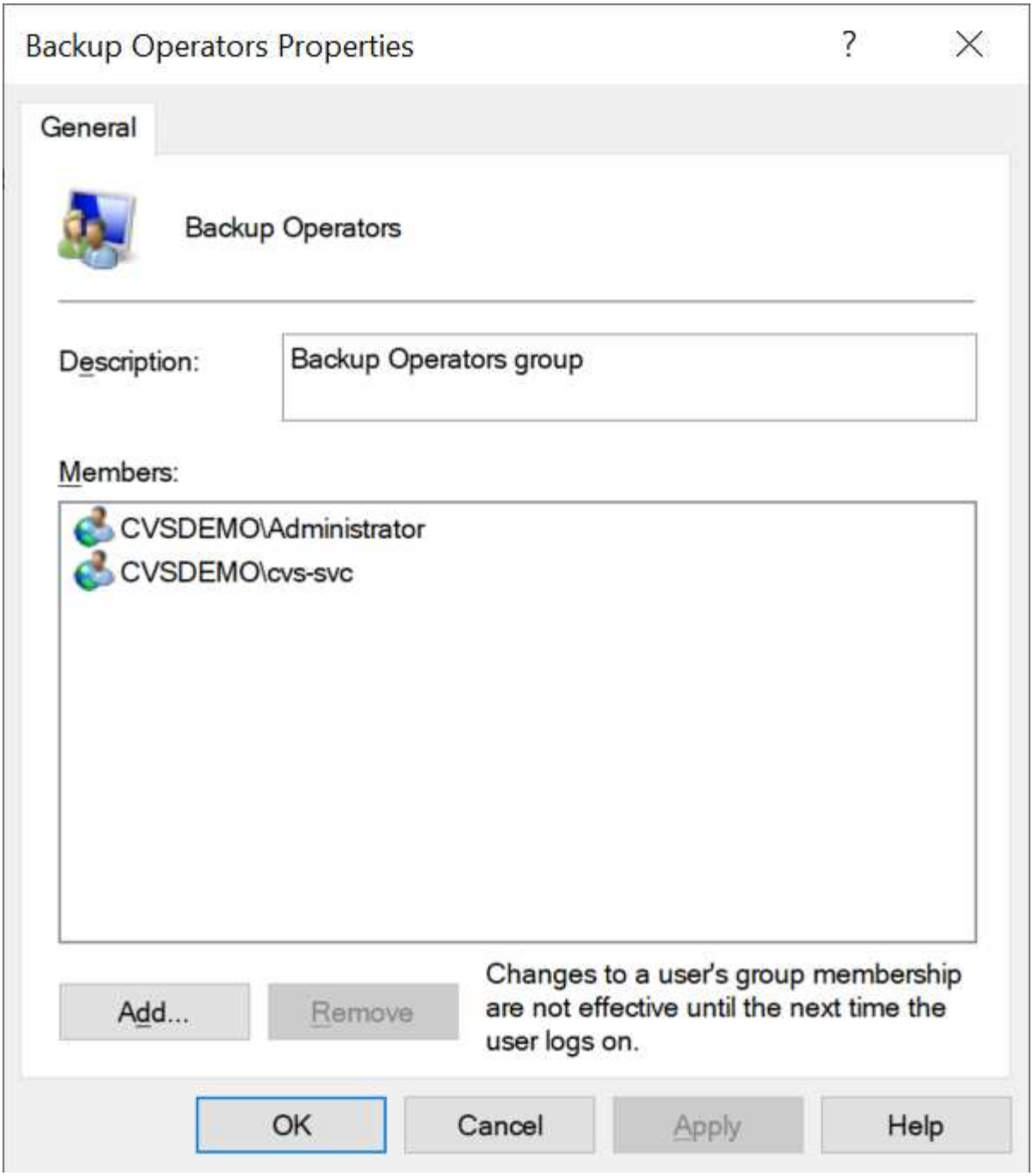
Accountnames
administrator,cvs-svc

Security Privilege Users

Provide a list of comma separated domain user accounts that require elevated privileges to manage security log for the Active Directory associated with Cloud Volumes Service.

Accountnames
administrator,cvs-svc

您可以Cloud Volumes Service 透過具有適當權限的MMC檢視本地的群組成員資格。下圖顯示使用Cloud Volumes Service 者已透過使用此功能新增的使用者。

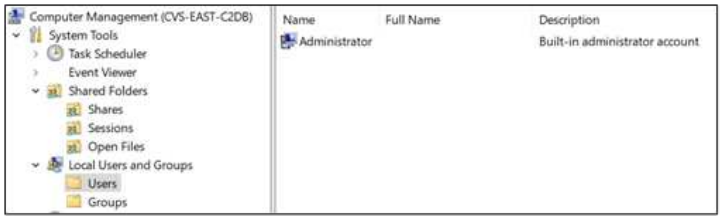


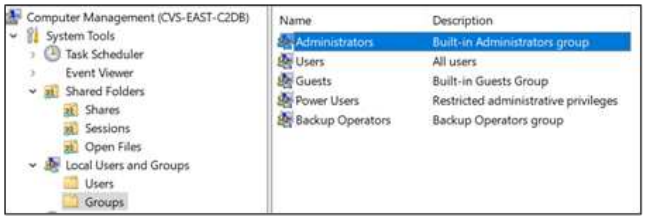
下表顯示預設BUILTIN群組清單、以及預設新增的使用者/群組。

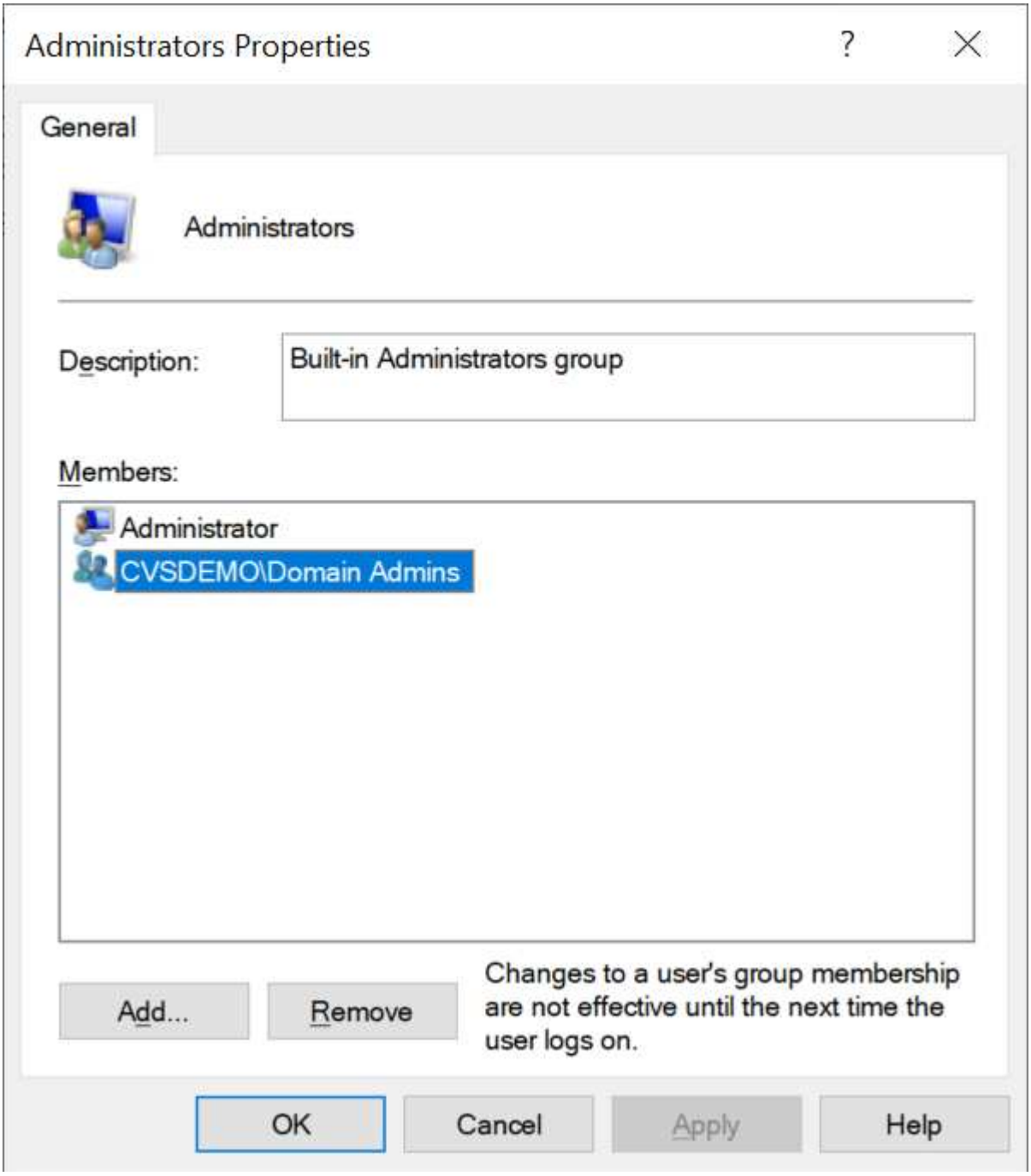
本機/**BUILTIN.**群組	預設成員
內建\系統管理員*	網域\網域管理員
內建\備份操作員*	無
內建\訪客	網域\網域來賓
內建\超級使用者	無
內建\網域使用者	網域\網域使用者

*群組成員資格是由Cloud Volumes Service 不實Active Directory連線組態所控制。

您可以在MMC視窗中檢視本機使用者和群組（及群組成員）、但無法從這個主控台新增或刪除物件或變更群組成員資格。根據預設、Cloud Volumes Service 只有Domain Admins群組和Administrator會新增至功能區的BUILTIN\Administrator群組。目前您無法修改此項目。







MMC/電腦管理存取

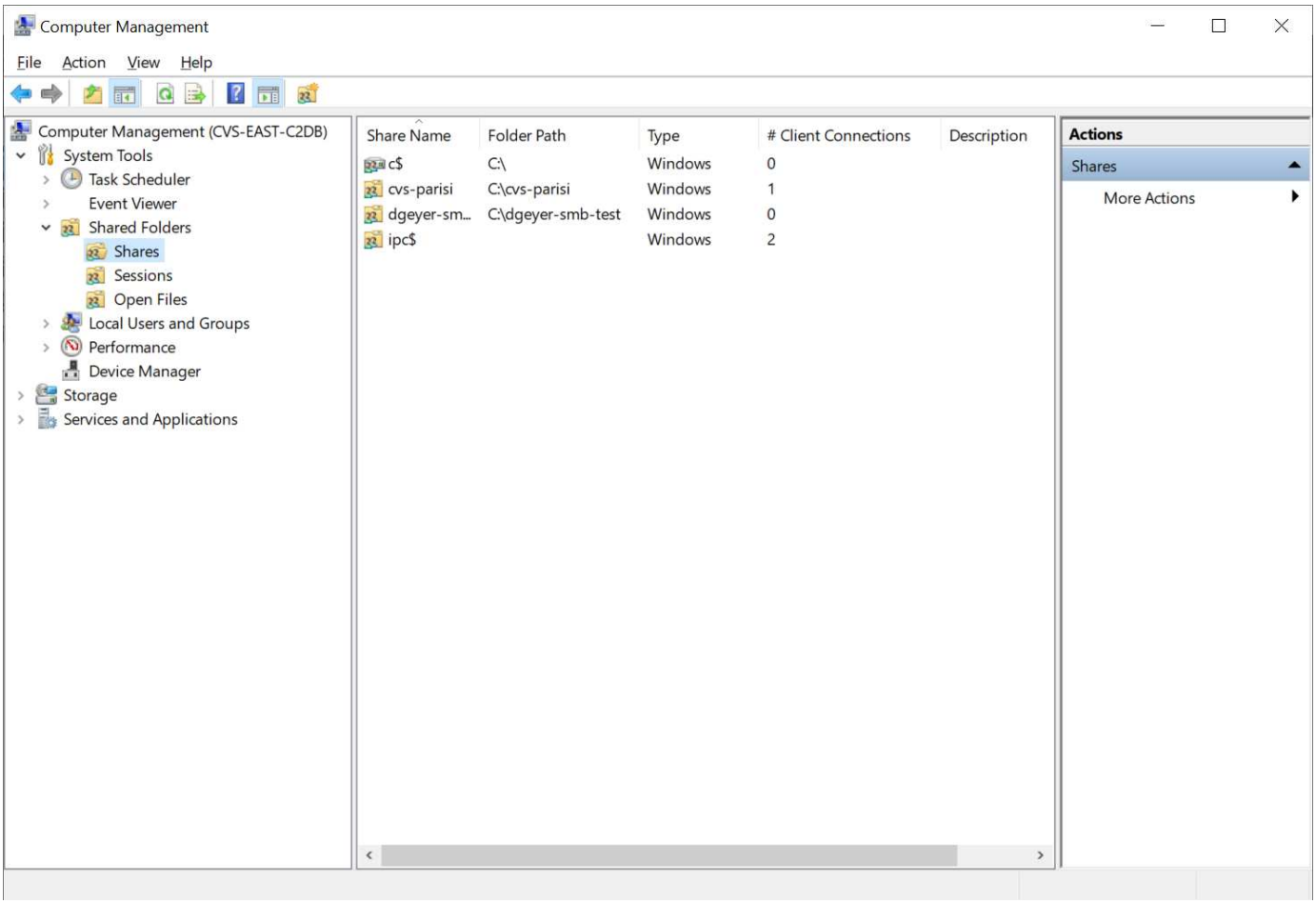
SMB存取Cloud Volumes Service 功能可連線至電腦管理MMC、讓您檢視共用區、管理共用ACL、以及檢視/管理SMB工作階段和開啟檔案。

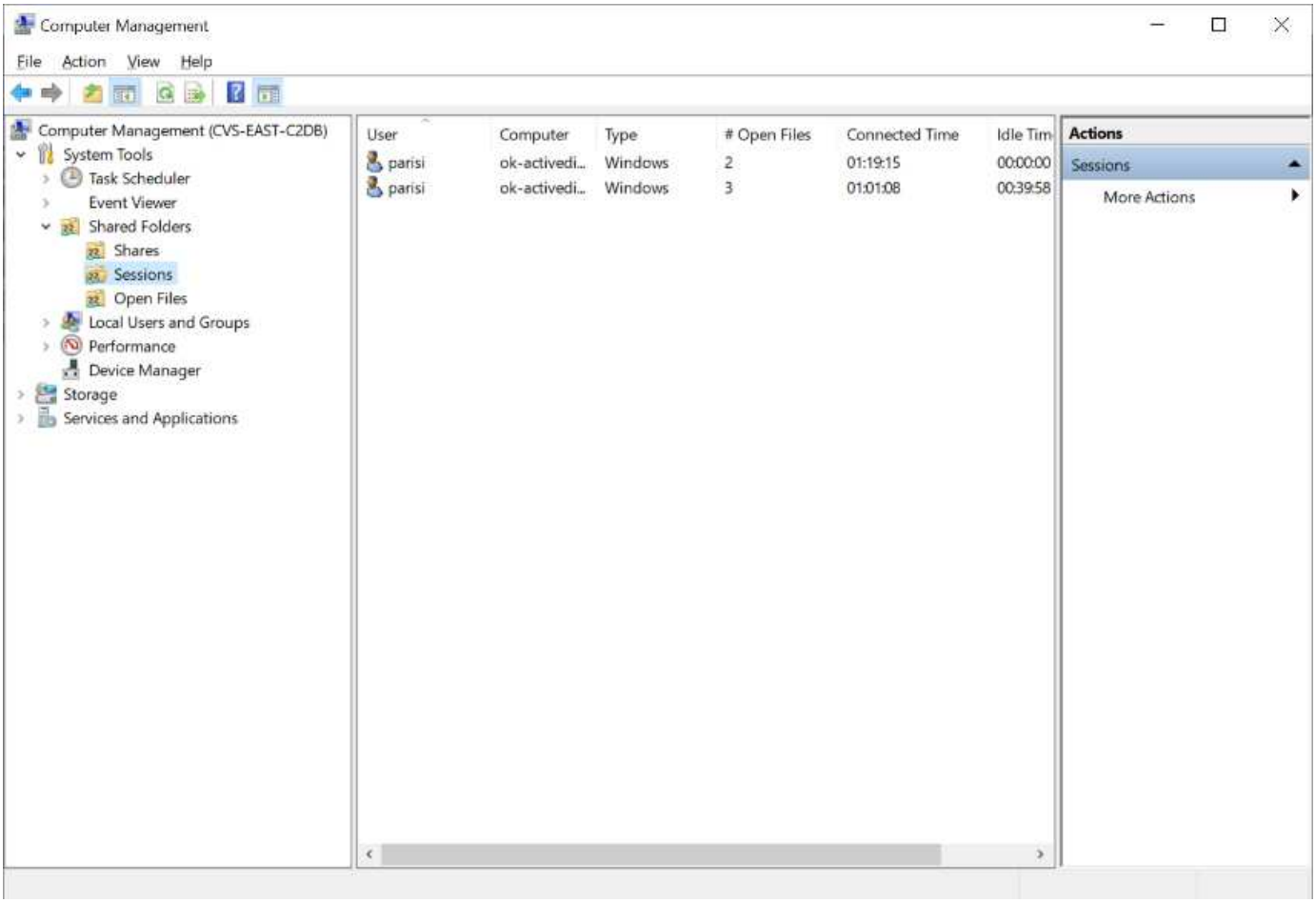
若要使用MMC來檢視Cloud Volumes Service SMB共用區和Sessions、目前登入的使用者必須是網域管理員。其他使用者可以從MMC檢視或管理SMB伺服器、並在嘗試檢視Cloud Volumes Service 有關Sisb執行個體的共用或工作階段時、收到「您沒有權限」對話方塊。

若要連線至SMB伺服器、請開啟「電腦管理」、在「電腦管理」上按一下滑鼠右鍵、然後選取「連線至其他電腦」。這會開啟「Select Computer（選取電腦）」對話方塊、您可以在其中輸入SMB伺服器名稱（可在Cloud Volumes Service 《支援資料》資料冊中找到）。

當您檢視具有適當權限的SMB共用時、Cloud Volumes Service 您會看到共享Active Directory連線的所有可用共享區。若要控制這種行為、請在Cloud Volumes Service 現象區執行個體上設定隱藏SMB共用選項。

請記住、每個地區只允許一個Active Directory連線。





下表顯示MMC支援/不支援的功能清單。

支援的功能	不支援的功能
• 檢視共享區 • 檢視作用中的SMB工作階段 • 檢視開啟的檔案 • 檢視本機使用者和群組 • 檢視本機群組成員資格 • 列舉系統中的工作階段、檔案和樹狀結構連線清單 • 關閉系統中開啟的檔案 • 關閉開啟的工作階段 • 建立/管理共用	• 建立新的本機使用者/群組 • 管理/檢視現有的本機使用者/群組 • 檢視事件或效能記錄 • 管理儲存設備 • 管理服務與應用程式

SMB伺服器安全性資訊

本產品的SMB伺服器Cloud Volumes Service 使用一系列選項來定義SMB連線的安全性原則、包括Kerberos時鐘偏移、票證存留期、加密等。

下表列出這些選項、其功能、預設組態、以及是否可以使用Cloud Volumes Service 更新。部分選項不適用

於Cloud Volumes Service 此功能。

安全選項	它的作用	預設值	可以改變嗎？
Kerberos時鐘最大偏差（分鐘）	最大Cloud Volumes Service 程度地縮短了在各個領域控制器之間的時間偏差。如果時間偏移超過5分鐘、Kerberos驗證就會失敗。這會設為Active Directory預設值。	5.	否
Kerberos票證壽命（小時）	Kerberos票證在要求續約之前保持有效的最長時間。如果在10小時之前沒有續約、您必須取得新的通知單。系統會自動執行這些續約作業。Cloud Volumes Service10小時為Active Directory預設值。	10.	否
Kerberos票證續約上限（天）	在需要新授權要求之前、可以續約Kerberos票證的最大天數。自動更新SMB連線的問題單。Cloud Volumes ServiceActive Directory預設值為七天。	7.	否
Kerberos Kdc連線逾時（秒）	Kdc連線逾時前的秒數。	3.	否
需要簽署傳入的SMB流量	設定為需要SMB流量的簽署。如果設為true、則不支援簽署的用戶端會失敗連線。	錯	
本機使用者帳戶需要密碼複雜度	用於本機SMB使用者的密碼。由於不支援建立本機使用者、因此此選項不適用於支援。Cloud Volumes Service Cloud Volumes Service	是的	否
Active Directory LDAP連線使用start_tls	用於啟用Active Directory LDAP的啟動TLS連線。目前不支援啟用此功能。Cloud Volumes Service	錯	否
為啟用Kerberos的AES-128和AES-256加密	這會控制AES加密是否用於Active Directory連線、並在建立/修改Active Directory連線時、使用「啟用Active Directory驗證的AES加密」選項加以控制。	錯	是的

安全選項	它的作用	預設值	可以改變嗎？
LM相容層級	Active Directory連線所支援的驗證語言層級。請參閱「」一節SMB驗證的語言」以取得更多資訊。	vLMvb-krb	否
傳入CIFS流量需要SMB加密	所有共用都需要SMB加密。這不是Cloud Volumes Service 由靜止使用；而是根據每個磁碟區設定加密（請參閱「」一節）SMB共享安全功能」）。	錯	否
用戶端工作階段安全性	設定LDAP通訊的簽署和/或密封。目前未在Cloud Volumes Service 不必要的情況下設定、但未來版本可能需要此功能來解決此問題。因Windows修補程式而導致的LDAP驗證問題補救措施將在一節中說明"「LDAP通道繫結。」"。	無	否
SMB2可啟用DC連線	使用SMB2進行DC連線。預設為啟用。	系統預設值	否
LDAP轉介追蹤	使用多個LDAP伺服器時、如果第一個伺服器中找不到項目、參照追蹤功能可讓用戶端參照清單中的其他LDAP伺服器。目前不支援此功能Cloud Volumes Service 。	錯	否
使用LDAPS進行安全的Active Directory連線	啟用LDAP over SSL。目前不受Cloud Volumes Service 支援。	錯	否
DC連線需要加密	需要加密才能成功建立DC連線。在功能不完整的情況下、預設為停用Cloud Volumes Service 。	錯	否

雙傳輸協定/多傳輸協定

支援將相同的資料集共享給SMB和NFS用戶端、同時維持適當的存取權限Cloud Volumes Service ("雙傳輸協定"）。這是透過協調不同傳輸協定之間的身分識別對應、以及使用集中式後端LDAP伺服器、將UNIX身分識別提供Cloud Volumes Service 給支援中心來完成。您可以使用Windows Active Directory為Windows和UNIX使用者提供方便使用的功能。

存取控制

- *共享存取控制。*決定哪些用戶端和（或）使用者和群組可以存取NAS共用區。對於NFS、匯出原則和規則會控制用戶端對匯出的存取。NFS匯出是從Cloud Volumes Service 整個過程中管理。SMB使用CIFS/SMB

共用和共用ACL、在使用者和群組層級提供更精細的控制。您只能使用從SMB用戶端設定共用層級ACL "MMC/電腦管理" 擁有Cloud Volumes Service 管理員權限的帳戶（請參閱一節） "「擁有本機/BUILTIN/系統管理員/備份權限的帳戶。」"）。

- *檔案存取控制。*控制檔案或資料夾層級的權限、且永遠從NAS用戶端進行管理。NFS用戶端可以使用傳統模式位元（rwx）或NFSv4 ACL。SMB用戶端運用NTFS權限。

將資料提供給NFS和SMB的磁碟區存取控制權取決於使用中的傳輸協定。如需雙協定權限的相關資訊、請參閱「」一節[權限模式]。」

使用者對應

當用戶端存取Volume時Cloud Volumes Service 、嘗試將傳入的使用者對應至相反方向的有效使用者。這是確定跨傳輸協定適當存取的必要條件、並確保要求存取的使用者確實是他們聲稱的對象。

例如、如果名為「Joe」的Windows使用者嘗試透過SMB存取具有UNIX權限的Volume、Cloud Volumes Service 則會執行搜尋、尋找名為「Joe」的對應UNIX使用者。如果存在、則以Windows使用者「Joe」的身分寫入SMB共用區的檔案會顯示為來自NFS用戶端的UNIX使用者「Joe」。

或者、如果名為「Joe」的UNIX使用者嘗試以Cloud Volumes Service Windows權限存取某個Windows Volume、則UNIX使用者必須能夠對應至有效的Windows使用者。否則、將拒絕存取磁碟區。

目前、只有Active Directory支援使用LDAP進行外部UNIX身分識別管理。如需設定此服務存取權的詳細資訊、請參閱 "建立AD連線"。

權限模式

使用雙傳輸協定設定時Cloud Volumes Service 、利用磁碟區的安全樣式來判斷ACL的類型。這些安全型態是根據所指定的NAS傳輸協定來設定、或是在建立Cloud Volumes Service 完實體磁碟區時選擇使用雙傳輸協定。

- 如果您只使用NFS、Cloud Volumes Service 則Sfelles Volume會使用UNIX權限。
- 如果您只使用SMB、Cloud Volumes Service 則支援使用NTFS權限的功能。

如果要建立雙傳輸協定磁碟區、您可以在建立磁碟區時選擇ACL樣式。這項決定應以所需的權限管理為基礎。如果使用者管理來自Windows / SMB用戶端的權限、請選取NTFS。如果您的使用者偏好使用NFS用戶端和chmod/chown、請使用UNIX安全性樣式。

建立**Active Directory**連線的考量事項

支援將您的實例連接至外部Active Directory伺服器、以便同時為SMB和UNIX使用者進行身分識別管理。Cloud Volumes Service Cloud Volumes Service建立Active Directory連線是Cloud Volumes Service 在支援功能方面使用SMB的必要條件。

此設定提供多種選項、需要考量安全性。外部Active Directory伺服器可以是內部部署執行個體或原生雲端。如果您使用的是內部部署的Active Directory伺服器，請勿將網域暴露給外部網路（例如使用DMZ或外部IP位址）。而是使用安全的私有通道或VPN、單向樹系信任或內部部署網路專用的網路連線 "私有 Google 存取"。如需詳細資訊、請參閱Google Cloud文件 "在Google Cloud中使用Active Directory的最佳實務做法"。

> CVS軟體要求Active Directory伺服器位於同一個地區。如果嘗試在CVs-SW中連線至其他地區、嘗試就會失敗。使用CVs-SW時、請務必建立包含Active Directory DC的Active Directory網站、然後在Cloud Volumes Service 其中指定站台、以避免跨區域DC連線嘗試。

Active Directory認證

啟用SMB或LDAP for NFS時Cloud Volumes Service 、支援使用者可與Active Directory控制器互動、以建立機器帳戶物件來進行驗證。這與Windows SMB用戶端加入網域的方式並不不同、而且需要對Active Directory中的組織單位（OU）擁有相同的存取權限。

在許多情況下、安全性群組不允許在Cloud Volumes Service 外部伺服器上使用Windows系統管理員帳戶、例如在某些情況下、Windows系統管理員使用者會完全停用、這是安全性最佳實務做法。

建立SMB機器帳戶所需的權限

若要新增Cloud Volumes Service 物件至Active Directory、則該帳戶具有網域的管理權限或擁有 "委派權限以建立及修改機器帳戶物件" 需要指定的OU。您可以透過Active Directory中的委派控制精靈來執行此作業、方法是建立自訂工作、讓使用者以提供下列存取權限來存取電腦物件的建立/刪除：

- 讀取/寫入
- 建立/刪除所有子物件
- 讀取/寫入所有內容
- 變更/重設密碼

這樣做會自動將已定義使用者的安全ACL新增至Active Directory中的OU、並將Active Directory環境的存取權限減至最低。在委派使用者之後、此視窗中的使用者名稱和密碼可提供為Active Directory認證。

> 傳遞至Active Directory網域的使用者名稱和密碼會在機器帳戶物件查詢和建立期間、運用Kerberos加密技術來提高安全性。

Active Directory連線詳細資料

。 "Active Directory連線詳細資料" 提供欄位給系統管理員、以提供機器帳戶放置的特定Active Directory架構資訊、例如：

- * Active Directory連線類型。*用於指定區域中的Active Directory連線是用於Cloud Volumes Service 供應各種類型的SView或CVS效能服務的磁碟區。如果現有連線的設定不正確、使用或編輯時可能無法正常運作。
- 網域。 Active Directory網域名稱。
- *站台。*將Active Directory伺服器限制為特定站台、以確保安全性和效能 "考量"。當多個Active Directory伺服器橫跨多個區域時、這是必要的、因為Cloud Volumes Service 目前不支援將Active Directory驗證要求允許在Cloud Volumes Service 不同於此執行個體的區域內執行Active Directory伺服器。（例如、Active Directory網域控制器所在的區域僅支援CVs-Performance、但您想要在CVs-SW執行個體中使用SMB共用區）。
- * DNS伺服器。* DNS伺服器、用於名稱查詢。
- * NetBios名稱（選用）。*如果需要、則為伺服器的NetBios名稱。這是使用Active Directory連線建立新機器帳戶時所使用的功能。例如、如果將NetBios名稱設為CVs-East、則機器帳戶名稱將為CVs-East-{12334}。請參閱一節 "如何在Active Directory中顯示此功能Cloud Volumes Service" 以取得更多資訊。
- *組織單位（OU）。*建立電腦帳戶的特定OU。如果您要將機器帳戶的控制權委派給使用者至特定OU、這很有用。
- * AES Encryption。*您也可以勾選或取消勾選「啟用AD驗證的AES加密」核取方塊。啟用AES加密以進行Active Directory驗證、可在Cloud Volumes Service 使用者和群組查詢期間、提供額外的安全性、以利執行功能以進行通訊。啟用此選項之前、請先洽詢您的網域管理員、確認Active Directory網域控制器支援AES

驗證。

> 根據預設、大部分的Windows伺服器不會停用較弱的密碼（例如：Des或RC4-HMAC）、但如果您選擇停用較弱的密碼、請確認Cloud Volumes Service 已設定「更新Active Directory」連線以啟用AES。否則會發生驗證失敗。啟用AES加密並不會停用較弱的密碼、而是將AES密碼的支援新增至Cloud Volumes Service 該SMB機器帳戶。

Kerberos領域詳細資料

此選項不適用於SMB伺服器。而是在設定NFS Kerberos for Cloud Volumes Service the Sing系統時使用。填入這些詳細資料時、NFS Kerberos領域會設定（類似於Linux上的krb5..conf檔案）、並在Cloud Volumes Service 建立實體磁碟區時指定NFS Kerberos時使用、因為Active Directory連線會做為NFS Kerberos發佈中心（kdc）。

> 非Windows KDC目前不支援Cloud Volumes Service 搭配使用。

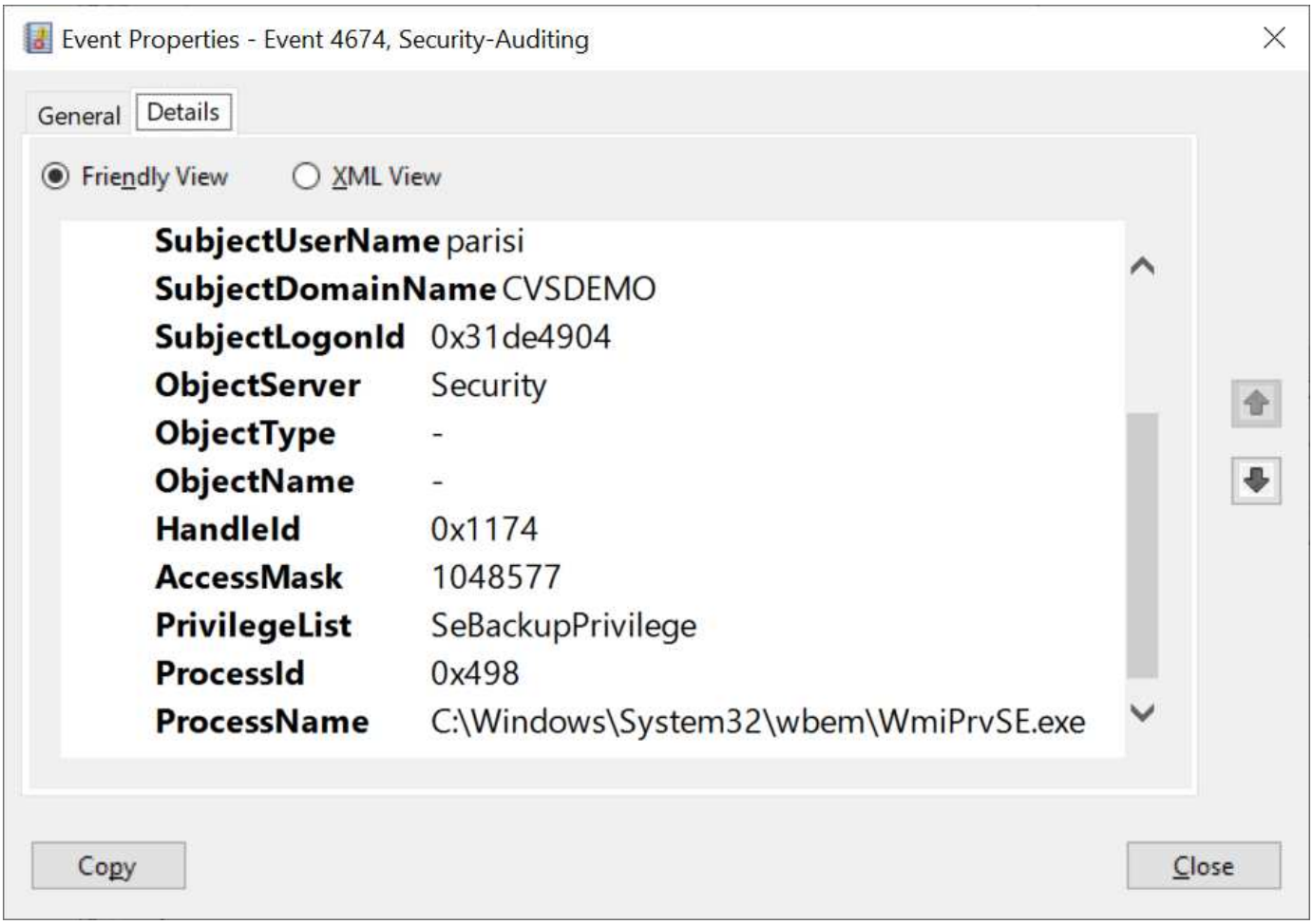
區域

區域可讓您指定Active Directory連線所在的位置。此區域必須與Cloud Volumes Service 《非洲地理區：

- *本機NFS使用者搭配LDAP.*本節中、也有允許本機NFS使用者搭配LDAP的選項。如果您想要將UNIX使用者群組成員資格支援延伸到NFS（延伸群組）的16群組限制之外、則必須取消選取此選項。不過、使用延伸群組時、需要設定用於UNIX身分識別的LDAP伺服器。如果您沒有LDAP伺服器、請取消選取此選項。如果您有LDAP伺服器、而且想要使用本機UNIX使用者（例如root）、請選取此選項。

備份使用者

此選項可讓您指定對Cloud Volumes Service 該Windows Volume具有備份權限的Windows使用者。某些應用程式必須具備備份權限（SeBackup權限）、才能在NAS磁碟區中正確備份及還原資料。此使用者擁有大量的磁碟區資料存取權限、因此您應該考慮 "啟用該使用者存取的稽核"。啟用後、稽核事件會顯示在「事件檢視器」>「Windows記錄」>「安全性」中。



安全性權限使用者

此選項可讓您指定Windows使用者、這些使用者具有Cloud Volumes Service 對此功能進行安全性修改的權限。某些應用程式需要安全性權限（SeSecurityPrivilege）（"例如SQL Server"）在安裝期間正確設定權限。管理安全性記錄時需要此權限。雖然此權限不如SeBackup權限強大、但NetApp建議您使用 "稽核使用者存取權限" 如果需要、請使用此權限層級。

如需詳細資訊、請參閱 "指派給新登入的特殊權限"。

如何在**Active Directory**中顯示此功能**Cloud Volumes Service**

在Active Directory中顯示為一般機器帳戶物件。Cloud Volumes Service命名慣例如下。

- CIFS/SMB和NFS Kerberos會建立個別的機器帳戶物件。
- 啟用LDAP的NFS會在Active Directory中建立機器帳戶、以進行Kerberos LDAP繫結。
- 具有LDAP的雙傳輸協定磁碟區會共用CIFS/SMB機器帳戶、以供LDAP和SMB使用。
- CIFS/SMB機器帳戶的機器帳戶命名慣例為：名稱-1234（隨機四位數ID、加上連字號、加上<10個字元名稱）。您可以使用Active Directory連線上的[NetBios名稱]設定來定義名稱（請參閱「」一節）Active Directory連線詳細資料」）。
- NFS Kerberos使用NFS-name-1234作為 命名慣例（最多15個字元）。如果使用超過15個字元、則名稱為nfs -截短名稱-1234.
- 僅NFS的CVS效能執行個體若啟用LDAP、則會建立SMB機器帳戶、以與CIFS/SMB執行個體相同的命名慣

例來繫結至LDAP伺服器。

- 建立SMB機器帳戶時、預設的隱藏管理共用區（請參閱一節 "「預設隱藏共用」"）也會建立（c$、admin$、ipc$）、但這些共用區並未指派ACL、因此無法存取。
- 依預設、機器帳戶物件會放置在CN=電腦中、但您可以在必要時指定不同的OU。請參閱「」一節建立SMB機器帳戶所需的權限」、以瞭解新增/移除Cloud Volumes Service 機器帳戶物件所需的存取權限。

當將SMB機器帳戶新增至Active Directory時Cloud Volumes Service 、會填入下列欄位：

- （使用指定的SMB伺服器名稱）
- dnsHostName（含SMBserver.domain.com）
- MSDS-SupportedEncryptionTypes（如果未啟用AES加密、則允許使用DES_CBC_MD5、RC4 _HMAC_MD5；如果啟用AES加密、則允許使用DES_CBC_MD5、RC4 _HMAC_MD5、AES128 _CTs_HMAC_SHA1_96、AES256_CTs_HMAC_SHA1_96進行Kerberos票證交換）
- 名稱（使用SMB伺服器名稱）
- SamAccountName（含SMBserver$）
- servicePrincipalName（含主機/smbserver.domain.com和主機/smbserver SPN for Kerberos）

如果您要停用機器帳戶上較弱的Kerberos加密類型（加密類型）、可以將機器帳戶上的MSDS-SupportedEncryptionTypes值變更為下表中的其中一個值、以僅允許AES。

msDS-SupportedEncryptionTypes值	已啟用**EncType**
2.	ds_CBC_MD5
4.	RC4_HMAC
8.	僅限AES122_CTs_HMAC_SHA1_96
16	僅限AES256_CTs_HMAC_SHA1_96
24	AES122_CTs_HMAC_SHA1_96 與AES256_CTs_HMAC_SHA1_96
30	DES_CBC_MD5、RC4_HMAC、AES122_CTs_HMAC_SHA1_96和AES256_CTs_HMAC_SHA1_96

若要啟用SMB機器帳戶的AES加密、請在建立Active Directory連線時按一下「啟用AD驗證的AES加密」。

若要啟用NFS Kerberos的AES加密、 "請參閱Cloud Volumes Service 《》文件"。

其他**NAS**基礎架構服務相依性（**Kdc**、**LDAP**和**DNS**）

使用Cloud Volumes Service 適用於NAS共享的功能時、可能需要外部相依性才能正常運作。在特定情況下、這些相依關係仍在發揮。下表顯示各種組態選項、以及必要的相依性（如果有）。

組態	所需相依性
僅限NFSv3	無
僅NFSv3 Kerberos	Windows Active Directory：* kdc * DNS * LDAP

組態	所需相依性
僅限NFSv4.1	用戶端ID對應組態（/etc/idmap.conf）
僅NFSv4.1 Kerberos	• 用戶端ID對應組態（/etc/idmap.conf） • Windows Active Directory：Kdc DNS LDAP
僅限SMB	Active Directory：* kdc * dns
多重傳輸協定NAS（NFS和SMB）	• 用戶端ID對應組態（僅限NFSv4.1；/etc/idmap.conf） • Windows Active Directory：Kdc DNS LDAP

機器帳戶物件的**Kerberos Keytab**旋轉/密碼重設

利用SMB機器帳戶Cloud Volumes Service 、此資訊可排定SMB機器帳戶的定期密碼重設。這些密碼會使用Kerberos加密進行重設、並在晚上11點到凌晨1點之間的隨機時間、於每四個星期日的排程中運作。這些密碼重設會變更Kerberos金鑰版本、旋轉Cloud Volumes Service 儲存在支援系統上的金鑰索引標籤、並協助維護執行Cloud Volumes Service 於支援更新版本的SMB伺服器的安全性。機器帳戶密碼是隨機配置的、系統管理員不知道。

對於NFS Kerberos機器帳戶、密碼重設只會在建立新的金鑰索引標籤並與Kdc交換時進行。目前Cloud Volumes Service 無法在不執行此動作的情況下進行。

用於**LDAP**和**Kerberos**的網路連接埠

使用LDAP和Kerberos時、您應該判斷這些服務所使用的網路連接埠。您可以在中找到Cloud Volumes Service 一份完整的清單、其中列出了供列舉使用的連接埠 "安全考量的相關文件Cloud Volumes Service"。

LDAP

充當LDAP用戶端、並使用標準LDAP搜尋查詢來查詢UNIX身分識別的使用者和群組。Cloud Volumes Service如果您想要使用Cloud Volumes Service 超出由供應之標準預設使用者的使用者和群組、則必須使用LDAP。如果您打算搭配使用者主體使用NFS Kerberos（例如user1@domain.com）、也必須使用LDAP。目前僅支援使用Microsoft Active Directory的LDAP。

若要將Active Directory當作UNIX LDAP伺服器使用、您必須在要用於UNIX身分識別的使用者和群組上填入必要的UNIX屬性。使用預設的LDAP架構範本來查詢屬性Cloud Volumes Service "RFC-2307-bis"。因此、下表顯示使用者和群組所需的最低Active Directory屬性、以及每個屬性的用途。

如需在Active Directory中設定LDAP屬性的詳細資訊、請參閱 "管理雙傳輸協定存取。"

屬性	它的作用
UID*	指定UNIX使用者名稱
uidNumber*	指定UNIX使用者的數字ID
gidNumber*	指定UNIX使用者的主要群組數字ID
objectClass *	指定要使用的物件類型；Cloud Volumes Service 物件類別清單中必須包含「使用者」（預設會包含在大部分的Active Directory部署中）。

屬性	它的作用
名稱	帳戶的一般資訊（真實姓名、電話號碼等、也稱為gecos）
unixUserPassword	無需設定、不適用於NAS驗證的UNIX身分識別查詢。設定此選項會將設定的unixUserPassword值設為純文字。
unixHomeDirectory	當使用者從Linux用戶端驗證LDAP時、定義UNIX主目錄的路徑。如果您要使用LDAP來執行UNIX主目錄功能、請設定此選項。
LoginShell	當使用者根據LDAP驗證時、定義Linux用戶端的Basash/profile Shell路徑。

*表示屬性是使用Cloud Volumes Service 功能不正確的必要條件。其餘屬性僅供用戶端使用。

屬性	它的作用
CN*	指定UNIX群組名稱。使用Active Directory for LDAP時、會在第一次建立物件時設定此選項、但稍後可加以變更。此名稱不得與其他物件相同。例如、如果您的UNIX使用者user1屬於Linux用戶端上名為user1的群組、則Windows不允許兩個具有相同CN屬性的物件。若要解決此問題、請將Windows使用者重新命名為唯一名稱（例如user-UNIX）；Cloud Volumes Service LDAP in Wesc使用UNIX使用者名稱的uid屬性。
gidNumber*	指定UNIX群組的數字ID。
objectClass *	指定要使用的物件類型；Cloud Volumes Service 使用物件類別清單時、需要將群組包含在物件類別清單中（此屬性預設會包含在大部分的Active Directory部署中）。
memberUid	指定哪些UNIX使用者是UNIX群組的成員。在Active Directory LDAP Cloud Volumes Service 的不實情況下、此欄位是不必要的。「支援組成員資格」功能使用「成員」欄位Cloud Volumes Service 。
成員*	群組成員資格/次要UNIX群組所需。此欄位是透過新增Windows使用者至Windows群組來填入。但是，如果Windows群組未填入UNIX屬性，則不會包含在UNIX使用者的群組成員資格清單中。任何需要在NFS中使用的群組、都必須填入此表格中所列的必要UNIX群組屬性。

*表示屬性是使用Cloud Volumes Service 功能不正確的必要條件。其餘屬性僅供用戶端使用。

LDAP連結資訊

若要查詢LDAP中的使用者、Cloud Volumes Service 必須將（登入）連結至LDAP服務。此登入具有唯讀權限、可用於查詢LDAP UNIX屬性以進行目錄查詢。目前只能使用SMB機器帳戶來進行LDAP連結。

您只能針對「CVS效能」執行個體啟用LDAP、並將其用於NFSv3、NFSv4.1或雙傳輸協定磁碟區。Active Directory連線必須與Cloud Volumes Service 支援LDAP的Volume在相同的地區建立、才能成功部署。

啟用LDAP時、會在特定情況下發生下列情況。

- 如果Cloud Volumes Service 僅將NFSv3或NFSv4.1用於該項目、則會在Active Directory網域控制器中建立新的機器帳戶、Cloud Volumes Service 而在其中的LDAP用戶端則會使用機器帳戶認證來繫結至Active Directory。不會為NFS磁碟區和預設的隱藏管理共用建立SMB共用區（請參閱一節）"「預設隱藏共用」"）刪除共享ACL。
- 如果Cloud Volumes Service 將雙傳輸協定磁碟區用於執行此項目、則Cloud Volumes Service 只會使用專為SMB存取所建立的單一機器帳戶、將位於的LDAP用戶端連結至Active Directory。不會建立其他機器帳戶。
- 如果專屬SMB磁碟區是分開建立（在啟用LDAP的NFS磁碟區之前或之後）、則LDAP繫結的機器帳戶會與SMB機器帳戶共用。
- 如果也啟用NFS Kerberos、則會建立兩個機器帳戶：一個用於SMB共用和（或）LDAP繫結、另一個用於NFS Kerberos驗證。

LDAP查詢

雖然LDAP繫結已加密、但LDAP查詢會使用通用LDAP連接埠389、以純文字形式透過線路傳送。這個廣為人知的連接埠目前無法在Cloud Volumes Service 更新過程中進行變更。因此、在網路中存取封包偵測功能的人可以看到使用者和群組名稱、數字ID和群組成員資格。

不過、Google Cloud VM無法窺探其他VM的單點傳播流量。只有主動參與LDAP流量（亦即能夠連結）的VM、才能看到來自LDAP伺服器的流量。如需Cloud Volumes Service 更多有關資料包偵測功能的資訊、請參閱一節"「封包偵測/追蹤考量。」"

LDAP用戶端組態預設值

在Cloud Volumes Service 某個實例中啟用LDAP時、預設會以特定組態詳細資料建立LDAP用戶端組態。在某些情況下、選項可能不適用於Cloud Volumes Service 不支援的功能（不支援）、也可能無法設定。

LDAP用戶端選項	它的作用	預設值	可以改變嗎？
LDAP伺服器清單	設定用於查詢的LDAP伺服器名稱或IP位址。這並不適用於Cloud Volumes Service 不適用。而是使用Active Directory網域來定義LDAP伺服器。	未設定	否
Active Directory網域	設定Active Directory網域用於LDAP查詢。利用DNS中的SRVs LDAP記錄、在網域中尋找LDAP伺服器。Cloud Volumes Service	設定為Active Directory連線中指定的Active Directory網域。	否
慣用的Active Directory伺服器	設定要用於LDAP的慣用Active Directory伺服器。不受Cloud Volumes Service 支援。而是使用Active Directory站台來控制LDAP伺服器選擇。	未設定。	否

LDAP用戶端選項	它的作用	預設值	可以改變嗎？
使用SMB伺服器認證進行連結	使用SMB機器帳戶連結至LDAP。目前Cloud Volumes Service 、唯一受支援的LDAP綁定方法就是支援的功能。	是的	否
架構範本	用於LDAP查詢的架構範本。	MS-AD-BIS	否
LDAP伺服器連接埠	用於LDAP查詢的連接埠號碼。目前僅使用標準LDAP連接埠389。Cloud Volumes Service目前不支援LDAPS/Port 636。	389	否
是否已啟用LDAPS	控制LDAP over Secure Socket Layer（SSL）是否用於查詢和連結。目前不受Cloud Volumes Service支援。	錯	否
查詢逾時（秒）	查詢逾時。如果查詢的時間超過指定值、查詢就會失敗。	3.	否
最小綁定驗證層級	支援的最低連結層級。由於使用機器帳戶進行LDAP連結、且Active Directory預設不支援匿名連結、因此此選項不適用於安全性。Cloud Volumes Service	匿名	否
連結DN	使用簡單繫結時用於繫結的使用者/辨別名稱（DN）。使用機器帳戶進行LDAP連結、目前不支援簡單的連結驗證。Cloud Volumes Service	未設定	否
基礎DN	用於LDAP搜尋的基礎DN。	Windows網域用於Active Directory連線、採用DN格式（亦即DC=DOWN, DC=local）。	否
基礎搜尋範圍	基礎DN搜尋的搜尋範圍。值可以包括base、onel海拔 或子樹狀結構。僅支援子樹狀結構搜尋。Cloud Volumes Service	子樹狀結構	否

LDAP用戶端選項	它的作用	預設值	可以改變嗎？
使用者DN	定義使用者開始搜尋LDAP查詢的DN。目前不支援Cloud Volumes Service使用此功能、因此所有使用者搜尋都從基礎DN開始。	未設定	否
使用者搜尋範圍	使用者DN搜尋的搜尋範圍。值可以包括base、onel海拔 或子樹狀結構。不支援設定使用者搜尋範圍。Cloud Volumes Service	子樹狀結構	否
群組DN	定義群組開始搜尋LDAP查詢的DN。目前不支援Cloud Volumes Service使用此功能、因此所有群組搜尋都會從基礎DN開始。	未設定	否
群組搜尋範圍	群組DN搜尋的搜尋範圍。值可以包括base、onel海拔 或子樹狀結構。不支援設定群組搜尋範圍。Cloud Volumes Service	子樹狀結構	否
網路群組DN	定義netgroup開始搜尋LDAP查詢的DN。目前不支援Cloud Volumes Service 使用此功能、因此所有網路群組搜尋都會從基礎DN開始。	未設定	否
網路群組搜尋範圍	netgroup DN搜尋的搜尋範圍。值可以包括base、onel海拔 或子樹狀結構。不支援設定netgroup搜尋範圍。Cloud Volumes Service	子樹狀結構	否
透過LDAP使用start_tls	利用Start TLS透過連接埠389進行憑證型LDAP連線。目前不受Cloud Volumes Service 支援。	錯	否
啟用各主機的網路群組查詢	可依主機名稱進行網路群組查詢、而非展開網路群組以列出所有成員。目前不受Cloud Volumes Service 支援。	錯	否

LDAP用戶端選項	它的作用	預設值	可以改變嗎？
網路群組的主機DN	定義netgroup by host開始搜尋LDAP查詢的DN。不支援Cloud Volumes Service 以主機為單位的netgroup。	未設定	否
Netgroup依主機搜尋範圍	netgroup by主機DN搜尋的搜尋範圍。值可以包括base、onel海拔 或子樹狀結構。不支援Cloud Volumes Service 以主機為單位的netgroup。	子樹狀結構	否
用戶端工作階段安全性	定義LDAP使用的工作階段安全性層級（簽署、認證或無）。如果Active Directory要求、則CVS效能可支援LDAP簽署。CVS軟體不支援LDAP簽署。目前不支援這兩種服務類型的密封。	無	否
LDAP參照追蹤	使用多個LDAP伺服器時、如果第一個伺服器中找不到項目、參照追蹤功能可讓用戶端參照清單中的其他LDAP伺服器。目前不支援此功能Cloud Volumes Service 。	錯	否
群組成員資格篩選器	提供自訂LDAP搜尋篩選器、以便在從LDAP伺服器查詢群組成員資格時使用。目前不支援Cloud Volumes Service 使用此功能。	未設定	否

使用**LDAP**進行非對稱名稱對應

根據預設、不需特殊組態、即可雙向對應具有相同使用者名稱的Windows使用者和UNIX使用者。Cloud Volumes Service只要Cloud Volumes Service 找到有效的UNIX使用者（使用LDAP）、就會產生1：1名稱對應。例如、如果使用Windows使用者「johnsmith」、Cloud Volumes Service 那麼如果在LDAP中找到名為「johnsmith」的UNIX使用者、則名稱對應會為該使用者成功、所有由「johnsmith」建立的檔案/資料夾都會顯示正確的使用者擁有權、 而影響「johnsmith」的所有ACL、無論使用的是哪種NAS傳輸協定、都是受到尊重的。這稱為對稱名稱對應。

非對稱名稱對應是指Windows使用者和UNIX使用者身分不相符的情況。舉例Cloud Volumes Service 來說、如果Windows使用者「johnsmith」的UNIX身分為「jsmith」、那麼就需要一種方式來瞭解這種差異。由於目前不支援建立靜態名稱對應規則、因此LDAP必須用於查詢Windows和UNIX身分識別的使用者身分、以確保檔案和資料夾擁有適當的所有權、以及預期的權限。Cloud Volumes Service

根據預設Cloud Volumes Service 、在名稱對應資料庫的n-switches中加入「LDAP」、以便使用LDAP提供非對稱名稱的名稱對應功能、您只需修改部分使用者/群組屬性、以反映Cloud Volumes Service 出本產品的外觀。

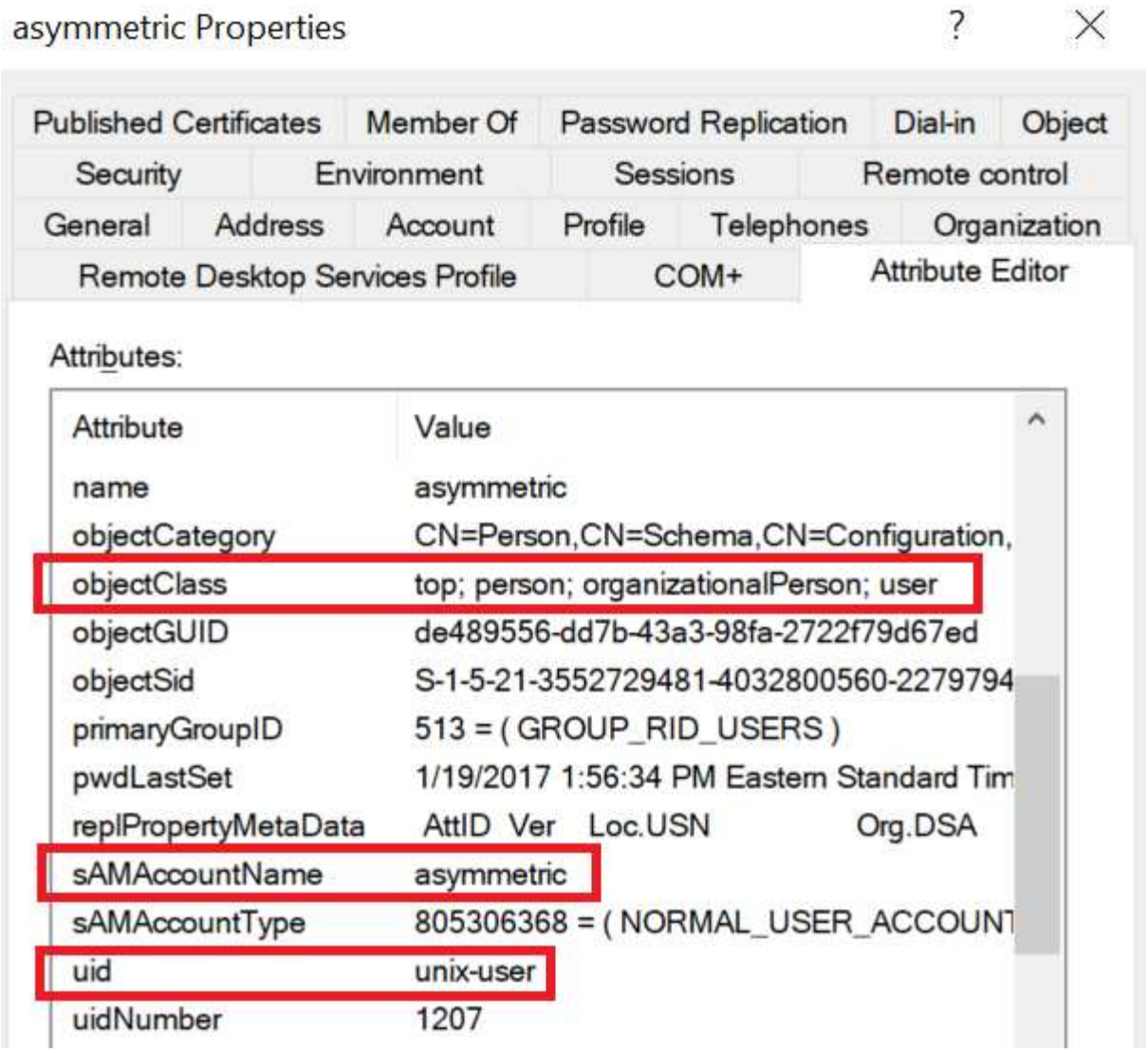
下表顯示在LDAP中必須填入哪些屬性才能使用非對稱名稱對應功能。在大多數情況下、Active Directory已設定為執行此作業。

屬性**Cloud Volumes Service**	它的作用	供名稱對應之用的值**Cloud Volumes Service**
Windows到UNIX的objectClass	指定要使用的物件類型。（也就是使用者、群組、posixAccount等）	必須包含使用者（如有需要、可包含多個其他值）。
Windows至UNIX屬性	定義建立時的Windows使用者名稱。可將此功能用於Windows到UNIX的查詢。Cloud Volumes Service	此處無需變更；sAMAccountName與Windows登入名稱相同。
UID	定義UNIX使用者名稱。	所需的UNIX使用者名稱。

由於目前無法在LDAP查詢中使用網域前置碼、因此多個網域LDAP環境無法在LDAP namemap查詢中正常運作。Cloud Volumes Service

以下範例顯示Windows名稱為「不對稱」、UNIX名稱為「UNIX使用者」的使用者、以及從SMB和NFS寫入檔案時所遵循的行為。

下圖顯示LDAP屬性從Windows伺服器的外觀。



從NFS用戶端、您可以查詢UNIX名稱、但不能查詢Windows名稱：

```
# id unix-user
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
# id asymmetric
id: asymmetric: no such user
```

從NFS將檔案寫入為「UNIX使用者」時、NFS用戶端會產生下列結果：

```
sh-4.2$ pwd
/mnt/home/ntfssh-4.2$ touch unix-user-file
sh-4.2$ ls -la | grep unix-user
-rwx------  1 unix-user sharedgroup     0 Feb 28 12:37 unix-user-nfs
sh-4.2$ id
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
```

從Windows用戶端、您可以看到檔案擁有者已設定為適當的Windows使用者：

```
PS C:\ > Get-Acl \\demo\home\ntfs\unix-user-nfs | select Owner
Owner
-----
NTAP\asymmetric
```

相反地、Windows使用者從SMB用戶端建立的「非對稱」檔案、會顯示適當的UNIX擁有者、如下文所示。

中小企業：

```
PS Z:\ntfs> echo TEXT > asymmetric-user-smb.txt
```

NFS：

```
sh-4.2$ ls -la | grep asymmetric-user-smb.txt
-rwx------  1 unix-user         sharedgroup   14 Feb 28 12:43 asymmetric-
user-smb.txt
sh-4.2$ cat asymmetric-user-smb.txt
TEXT
```

LDAP通道繫結

由於Windows Active Directory網域控制器存在弱點、 "Microsoft安全性摘要報告ADV190023" 變更DC允許LDAP繫結的方式。

對功能的影響Cloud Volumes Service 與對任何LDAP用戶端的影響相同。目前不支援通道連結。Cloud Volumes Service由於根據預設、透過協商來支援LDAP簽署、因此LDAP通道繫結不應成為問題。Cloud Volumes Service 如果您在啟用通道繫結的情況下、無法連結至LDAP、請遵循ADV190023的修正步驟、讓LDAP從Cloud Volumes Service 支援區連結成功。

DNS

Active Directory和Kerberos都依賴DNS來解析主機名稱與IP / IP之間的主機名稱。DNS需要開啟連接埠53。不修改DNS記錄、也不支援使用Cloud Volumes Service "動態DNS" 在網路介面上。

您可以設定Active Directory DNS、限制哪些伺服器可以更新DNS記錄。如需詳細資訊、請參閱 "安全的Windows DNS"。

請注意、Google專案中的資源預設為使用Google Cloud DNS、而Google Cloud DNS並未與Active Directory DNS連線。使用Cloud DNS的用戶端無法解析Cloud Volumes Service 由解決所傳回的UNC路徑。加入Active Directory網域的Windows用戶端已設定為使用Active Directory DNS、並可解析此類的UNC路徑。

若要將用戶端加入Active Directory、您必須將其DNS組態設定為使用Active Directory DNS。您也可以設定Cloud DNS、將要求轉送至Active Directory DNS。請參閱 "為什麼我的用戶端無法解析SMB NetBios名稱？" 以取得更多資訊。

目前不支援DNSSEC、DNS查詢則以純文字執行。Cloud Volumes Service

檔案存取稽核

目前不支援Cloud Volumes Service 使用此功能。

防毒保護

您必須在Cloud Volumes Service 用戶端執行「從位向至NAS共享區的」功能中的防毒掃描。目前沒有原生的防毒整合Cloud Volumes Service 功能可搭配使用。

服務營運

這個支援團隊負責管理Google Cloud的後端服務、並運用多種策略來保護平台安全、防止不必要的存取。Cloud Volumes Service

每位客戶都有自己專屬的子網路、預設會有與其他客戶隔離的存取權限、Cloud Volumes Service 而在這個子網路中、每個租戶都會獲得自己的命名空間和VLAN、以實現整體資料隔離。驗證使用者之後、服務交付引擎（SDE）只能讀取該租戶專屬的組態資料。

實體安全性

在適當的預先核准下、只有現場工程師和NetApp認可的現場支援工程師（FSE）才能存取機箱和機架進行實體工作。不允許進行儲存與網路管理。只有這些現場資源能夠執行硬體維護工作。

對於現場工程師、會提出一份工作說明書（SOW）的票證、其中包括機架ID和裝置位置（RU）、以及所有其他詳細資料均包含在票證中。對於NetApp FSE、必須向Colo出示網站參訪票證、票證中必須包含訪客的詳細資料、日期和時間、以供稽核之用。FSE的SOW會在內部傳達給NetApp。

營運團隊

支援此功能的營運團隊Cloud Volumes Service 由Production Engineering和Site可靠性工程師（SRE）組成、負責雲端Volume Services、以及NetApp現場支援工程師和硬體合作夥伴。所有營運團隊成員均已獲得Google Cloud認證、並會針對每張提出的問題單、維護詳細的工作記錄。此外、也有嚴格的變更控管與核准程序、確保每項決策都經過適當的審查。

SRE團隊負責管理控制面板、以及如何將資料從UI要求路由傳送至Cloud Volumes Service 支援的後端硬體和軟體。SRE團隊也會管理系統資源、例如磁碟區和inode上限。SRES不得與客戶資料互動或存取。SRES也能與退貨材料授權（RMA）協調、例如新磁碟或後端硬體的記憶體更換要求。

客戶責任

客戶負責管理組織的Active Directory和使用者角色管理、以及磁碟區和資料作業。Cloud Volumes Service客戶可以擁有管理角色、並可使用NetApp和Google Cloud提供的兩個預先定義角色（管理員和檢視者）、將權限委派給同一個Google Cloud專案中的其他終端使用者。

系統管理員可以對等客戶專案中的任何VPC、Cloud Volumes Service 使客戶認爲適當。客戶有責任管理其Google Cloud市場訂閱的存取權、以及管理可存取資料層面的VPC。

惡意SRE保護

可能會產生的一項疑慮是Cloud Volumes Service 、當發生惡意SRE或SRE認證遭入侵時、如何保護不受攻擊？

只有少數SRE人員能夠存取正式作業環境。系統管理權限進一步限制給少數經驗豐富的系統管理員。我們的安全資訊與事件管理（SIEM）威脅情報平台會記錄所有在整個流程環境中由任何人執行的行動Cloud Volumes Service 、並偵測到任何基礎異常或可疑活動。因此、在Cloud Volumes Service 對該後端造成太多損害之前、可以追蹤並減輕惡意行為。

Volume生命週期

僅管理服務中的物件、而非磁碟區內的資料。Cloud Volumes Service只有存取磁碟區的用戶端才能管理資料、ACL、檔案擁有者等。這些磁碟區中的資料會在閒置時加密、而且只能由Cloud Volumes Service 執行個體的租戶存取。

支援的Volume生命週期Cloud Volumes Service 是「cree-update-delete」。Volume會保留Volume的Snapshot複本、直到磁碟區被刪除為止、而且只有通過驗證Cloud Volumes Service 的NetApp管理員才能刪除Cloud Volumes Service 整個實體中的Volume。當系統管理員要求刪除磁碟區時、需要輸入磁碟區名稱的其他步驟來驗證刪除作業。刪除磁碟區後、磁碟區便會消失、無法恢復。

如果終止了某個方面的合約、NetApp會在特定時間段後將磁碟區標示為刪除。Cloud Volumes Service在該期間到期之前、您可以應客戶的要求來恢復磁碟區。

認證

Cloud Volumes Services for Google Cloud目前已通過ISO/IEC 27001：2013和ISO/IEC 27018：2019標準的認證。該服務最近也收到SOC2類型I證明報告。如需NetApp對資料安全性與隱私權承諾的相關資訊、請參閱 "法規遵循：資料安全與資料隱私"。

GDPR

我們對隱私權和遵守GDPR的承諾、已在我們的多個公司中提供 "客戶合約"、例如我們的 "客戶資料處理附錄"、其中包括 "標準合約條款" 由歐盟委員會提供。我們也會在隱私權政策中做出這些承諾、並以公司行為準則中所列的核心價值為後盾。

其他資訊和聯絡資訊

若要深入瞭解本文所述資訊、請檢閱下列文件和 / 或網站：

- Google Cloud文件Cloud Volumes Service

  "https://cloud.google.com/architecture/partners/netapp-cloud-volumes/"

- Google私有服務存取

  https://cloud.google.com/vpc/docs/private-services-access?hl=en_US

- NetApp產品文件

  "https://www.netapp.com/support-and-training/documentation/"

- 密碼編譯驗證模組方案—NetApp CryptoMod

  "https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4144"

- NetApp勒索軟體解決方案

  https://www.netapp.com/pdf.html?item=/media/16716-sb-3938pdf.pdf&v=202093745

- TR-4616：ONTAP NFS Kerberos in Sf2

  https://www.netapp.com/pdf.html?item=/media/19384-tr-4616.pdf

聯絡我們

請告訴我們如何改善這份技術報告。

請聯絡我們：mailto：doccomments@netapp.com doccomments@netapp.com。在主題行中加入技術報告4918。