



NetApp StorageGRID與 Splunk SmartStore

NetApp artificial intelligence solutions

NetApp
August 18, 2025

目錄

NetApp StorageGRID與 Splunk SmartStore	1
TR-4869：NetApp StorageGRID與 Splunk SmartStore	1
概況	1
關於NetApp StorageGRID	1
關於Splunk Enterprise	3
關於Splunk SmartStore	3
解決方案概述	3
NetAppStorageGRID	3
Splunk Enterprise	3
Splunk SmartStore	4
此解決方案的優勢	4
Splunk 架構	4
關鍵定義	4
Splunk 分散式部署	5
Splunk SmartStore	6
Splunk SmartStore 資料流	7
軟體需求	8
單站點和多站點要求	8
硬體需求	10
Splunk 設計	12
適用於 Splunk SmartStore 的靈活StorageGRID功能	14
使用網格管理器進行簡單管理	14
適用於 Splunk 的NetApp StorageGRID應用程式	15
ILM 策略	15
表現	15
負載平衡器和端點配置	15
智慧分層和成本節約	16
單站點 SmartStore 效能	16
配置	19
SmartStore遠端商店效能驗證	19
StorageGRID性能	24
StorageGRID硬體使用量	25
採用NetApp儲存控制器的 SmartStore - 為客戶帶來好處	26
結論	27
在哪裡可以找到更多信息	27

NetApp StorageGRID與 Splunk SmartStore

TR-4869：NetApp StorageGRID與 Splunk SmartStore

Splunk Enterprise 是市場領先的安全資訊和事件管理 (SIEM) 解決方案，可推動安全、IT 和 DevOps 團隊取得成果。

概況

數據量持續以指數級增長，為能夠利用這一巨大資源的企業創造了巨大的機會。Splunk Enterprise 在更廣泛的使用案例中被廣泛採用。隨著用例的成長，Splunk Enterprise 提取和處理的資料量也在增加。Splunk Enterprise 的傳統架構是分散式橫向擴展設計，提供出色的資料存取和可用性。然而，使用這種架構的企業面臨著與擴展相關的成本不斷增長的問題，以滿足快速增長的資料量。

採用NetApp StorageGRID的 Splunk SmartStore 透過提供計算和儲存分離的新部署模型解決了這個難題。該解決方案還允許客戶跨單一和多個站點進行擴展，從而為 Splunk Enterprise 環境提供無與倫比的規模和彈性，同時透過允許運算和儲存獨立擴展並為經濟高效的基於雲端的 S3 物件儲存添加智慧分層來降低成本。

該解決方案在保持搜尋效能的同時優化了本地儲存的資料量，允許按需擴展運算和儲存。SmartStore 會自動評估資料存取模式，以確定哪些資料需要即時分析，哪些資料應該駐留在成本較低的 S3 物件儲存中。

本技術報告概述了NetApp為 Splunk SmartStore 解決方案帶來的優勢，同時示範了在您的環境中設計和調整 Splunk SmartStore 大小的框架。最終結果是一個簡單、可擴展且有彈性的解決方案，可提供極具吸引力的 TCO。StorageGRID提供可擴展且經濟高效的基於 S3 協定/API 的物件儲存（也稱為遠端儲存），使組織能夠以較低的成本擴展其 Splunk 解決方案，同時提高彈性。



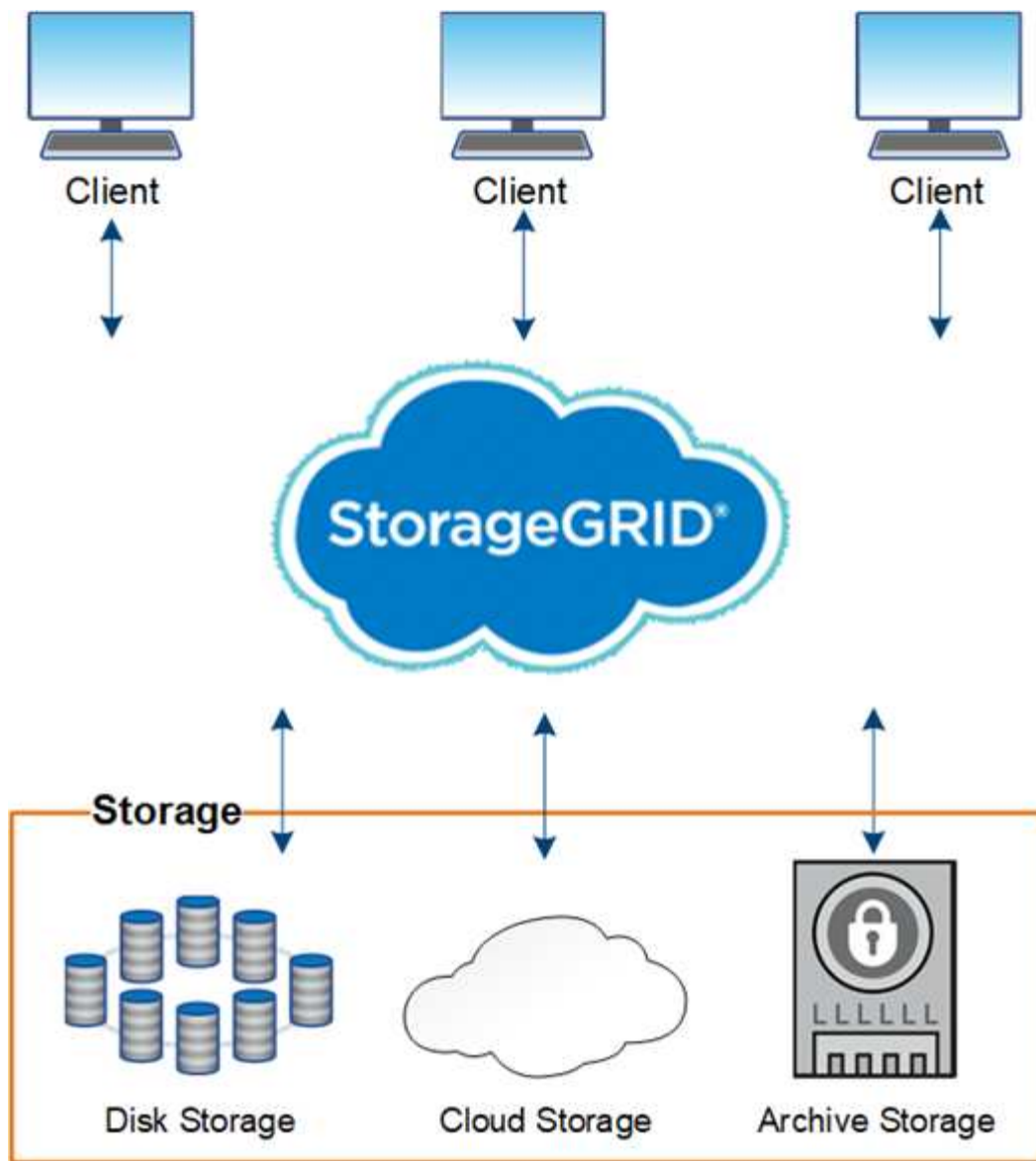
Splunk SmartStore 將物件儲存稱為遠端儲存或遠端儲存層。

關於NetApp StorageGRID

NetApp StorageGRID是一種軟體定義的物件儲存解決方案，適用於大型檔案、媒體儲存庫和 Web 資料儲存。借助StorageGRID，NetApp利用二十年來提供業界領先的創新和資料管理解決方案的經驗，同時幫助組織管理和最大化其內部以及公共、私有或混合雲部署中的資訊價值。

StorageGRID為大規模非結構化資料提供安全、持久的儲存。整合的、元資料驅動的生命週期管理策略可最佳化資料在整個生命週期中的儲存位置。將內容放置在正確的位置、正確的時間以及正確的儲存層以降低成本。單一命名空間允許透過單一呼叫存取數據，而不管StorageGRID儲存的地理位置如何。客戶可以在資料中心之間和雲端基礎設施中部署和管理多個StorageGRID實例。

StorageGRID系統由全球分佈、冗餘、異質的節點組成，可與現有和下一代用戶端應用程式整合。



IDC MarketScape 最近在最新報告《IDC MarketScape：2019 年全球基於物件的儲存供應商評估》中將NetApp 評為領導者。StorageGRID擁有近 20 年在要求最嚴格的行業中進行生產部署的經驗，是非結構化資料領域公認的領導者。

使用StorageGRID，您可以實現以下目標：

- 部署多個StorageGRID實例，透過可輕鬆擴展到數百 PB 的單一命名空間存取資料中心和雲端之間任何位置的資料。
- 提供跨基礎設施部署和集中管理的靈活性。
- 利用分層擦除編碼 (EC) 提供無與倫比的耐用性，耐用性達到 15 個 9。
- 透過與 Amazon S3 Glacier 和 Azure Blob 進行驗證的集成，實現更多混合多雲功能。
- 透過防篡改資料保留滿足監管義務並促進合規性，無需專有 API 或供應商鎖定。

有關StorageGRID如何幫助您解決最複雜的非結構化資料管理問題的更多信息，請參閱 ["NetApp StorageGRID 主頁"](#)。

關於Splunk Enterprise

Splunk Enterprise 是一個將資料轉化為行動的平台。日誌檔案、網站、裝置、感測器和應用程式等各種來源產生的資料會傳送到 Splunk Indexer 並由其解析，使您可以從資料中獲得豐富的見解。它可能識別資料外洩、指出客戶和產品趨勢、尋找優化基礎架構的機會或在各種用例中創建可操作的見解。

關於Splunk SmartStore

Splunk SmartStore 擴展了 Splunk 架構的優勢，同時簡化了其經濟高效擴展的能力。計算和儲存資源的分離導致索引器節點針對 I/O 進行了最佳化，並且儲存需求顯著減少，因為它們僅將一部分資料儲存為快取。當只需要其中一種資源時，您不必添加額外的計算或儲存，從而可以實現顯著的成本節約。您可以使用經濟高效且易於擴展的基於 S3 的物件儲存，這進一步簡化了環境、降低了成本並允許您維護更龐大的資料集。

Splunk SmartStore 為組織帶來巨大價值，包括：

- 透過將熱數據移至成本優化的 S3 物件儲存來降低儲存成本
- 透過分離儲存和運算實現無縫擴展
- 利用彈性雲原生儲存簡化業務連續性

解決方案概述

本頁介紹了完成此解決方案所使用的元件，包括NetApp StorageGRID、Splunk Enterprise 和 Splunk SmartStore。

NetAppStorageGRID

NetApp StorageGRID是一個高效能且經濟高效的物件儲存平台。它使用分散式、基於節點的網格架構提供智慧、策略驅動的全球資料管理。它透過其無所不在的全域物件命名空間與複雜的資料管理功能結合，簡化了 PB 級非結構化資料和數十億個物件的管理。單次呼叫物件存取可跨站點擴展，並簡化高可用性架構，同時確保無論站點或基礎設施是否中斷，都能持續進行物件存取。

多租戶允許多個雲端和企業非結構化資料應用程式在同一網格內安全地服務，從而增加了StorageGRID的投資回報率和用例。可以使用元資料驅動的物件生命週期策略來建立多個服務級別，從而優化跨多個地區的耐用性、保護性、效能和局部性。隨著需求的變化，使用者可以調整策略並且無中斷地重新調整資料格局。

SmartStore 利用StorageGRID作為遠端儲存層，並允許客戶部署多個地理分佈的站點，以實現強大的可用性和耐用性，並以單一物件命名空間的形式呈現。這使得 Splunk SmartStore 能夠利用StorageGRID的高效能、高密度容量以及使用單一 URL 與物件互動擴展到多個實體網站上的數百個節點的能力。此單一 URL 還允許在不中斷的情況下進行儲存擴充、升級和修復，甚至超越單一網站。StorageGRID獨特的資料管理策略引擎提供了最佳化的效能和耐用性水平，並符合資料局部性要求。

Splunk Enterprise

Splunk 是機器生成資料收集和分析的領導者，透過其營運分析功能幫助簡化和現代化 IT。它還擴展到商業分析、安全性和物聯網用例。儲存是成功部署 Splunk 軟體的關鍵因素。

機器產生的數據是成長最快的大數據類型。其格式難以預測，並且來自許多不同的來源，通常速率很高且數量巨大。這些工作負載特徵通常被稱為數位排氣。Splunk SmartStore 有助於理解這些資料並提供智慧資料分層，以便在最具成本效益的儲存層上優化放置熱資料和溫資料。

Splunk SmartStore

Splunk SmartStore 是一種索引器功能，它使用物件儲存（也稱為遠端儲存或遠端儲存層）例如StorageGRID透過 S3 協定儲存熱資料。

隨著部署的資料量增加，對儲存的需求通常會超過對電腦資源的需求。SmartStore 可讓您透過分別擴展運算和儲存來經濟高效地管理索引器儲存和運算資源。

SmartStore 引入了使用 S3 協定的遠端儲存層和快取管理器。這些功能允許資料駐留在本機索引器或遠端儲存上。快取管理器位於索引器上，負責管理索引器和遠端儲存層之間的資料移動。資料與儲存桶元資料一起儲存在儲存桶（熱和溫）中。

使用 SmartStore，您可以將索引器儲存佔用空間降至最低，並選擇 I/O 最佳化的運算資源，因為大多數資料都駐留在遠端儲存層上。索引器維護一個本地緩存，代表返回請求和預測結果所需的最少資料量。本地快取包含熱儲存桶、參與活動或最近搜尋的熱儲存桶副本以及儲存桶元資料。

具有StorageGRID的 Splunk SmartStore 使客戶能夠透過高效能且經濟高效的遠端儲存逐步擴展環境，同時為整體解決方案提供高度的彈性。這使得客戶可以在任何給定時間添加任何給定數量的任何組件（熱儲存和/或溫 S3 存儲），無論他們是需要更多索引器、更改資料保留，還是在不造成任何中斷的情況下增加攝取率。

此解決方案的優勢

此解決方案允許添加運算、熱儲存或 S3 資源，以滿足單一站點和多站點部署中使用者數量或攝取率不斷增長的需求。

- ***表現。** * Splunk SmartStore 和NetApp StorageGRID的結合使用物件儲存在熱儲存桶和溫儲存桶之間實現資料的快速遷移。StorageGRID透過為大型物件工作負載提供快速效能來加速遷移過程。
- ***多站點就緒。** * StorageGRID分散式架構允許 Splunk SmartStore 透過單一全域命名空間擴展跨單一和多個站點的部署，無論資料位於何處，都可以從任何網站存取資料。
- ***提高了可擴展性。** *獨立於運算資源擴展儲存資源，以滿足 Splunk 環境中不斷變化的需求，從而提供更好的 TCO。
- ***容量。** *使用StorageGRID將單一命名空間擴展到 560PB 以上，滿足 Splunk 部署中快速成長的容量。
- ***數據可用性。** *使用元資料驅動的策略來優化資料可用性、效能、地理分佈、保留、保護和儲存成本，這些策略可以隨著資料的業務價值的發展而動態調整。

使用 SmartStore 快取提高效能，它是索引器的一個元件，負責處理本地（熱）儲存和遠端（溫）儲存之間的儲存桶副本傳輸。此解決方案的 Splunk 規模基於 ["Splunk 提供的指南"](#)。此解決方案允許添加運算、熱儲存或 S3 資源，以滿足單一站點和多站點部署中使用者數量或攝取率不斷增長的需求。

Splunk 架構

本節介紹 Splunk 架構，包括關鍵定義、Splunk 分散式部署、Splunk SmartStore、資料流、硬體和軟體需求、單一站點和多站點需求等。

關鍵定義

接下來的兩個表格列出了分散式 Splunk 部署中使用的 Splunk 和NetApp元件。

此表列出了分散式 Splunk Enterprise 配置的 Splunk 硬體元件。

Splunk 元件	任務
索引器	Splunk Enterprise 資料儲存庫
通用轉發器	負責提取資料並將資料轉發給索引器
搜尋頭	用於在索引器中搜尋資料的使用者前端
叢集主節點	管理索引器和搜尋頭的 Splunk 安裝
監控控制台	整個部署中使用的集中監控工具
許可證主控	許可證管理員處理 Splunk Enterprise 許可
部署伺服器	更新配置並將應用程式分發到處理組件
儲存組件	任務
NetApp AFF	用於管理熱層資料的全快閃儲存。也稱為本地儲存。
NetAppStorageGRID	用於管理熱層資料的 S3 物件儲存。SmartStore 使用它在熱層和溫層之間移動資料。也稱為遠端儲存。

下表列出了 Splunk 儲存架構中的元件。

Splunk 元件	任務	負責組件
智慧商店	為索引器提供將資料從本機儲存分層到物件儲存的能力。	Splunk
熱的	通用轉發器放置新寫入資料的著陸點。儲存是可寫的，資料是可搜尋的。此資料層通常由 SSD 或快速 HDD 組成。	ONTAP
快取管理器	管理索引資料的本地緩存，在搜尋時從遠端儲存中獲取熱數據，並從快取中逐出最不常用的數據。	智慧商店
溫暖的	資料按邏輯捲動到儲存桶，首先從熱層重新命名為暖層。此層內的資料受到保護，與熱層一樣，可以由更大容量的 SSD 或 HDD 組成。使用常見的資料保護解決方案支援增量備份和完整備份。	StorageGRID

Splunk 分散式部署

為了支援資料來自多台機器的更大環境，您需要處理大量資料。如果許多使用者需要搜尋數據，您可以透過在多台機器上分發 Splunk Enterprise 實例來擴展部署。這被稱為分散式部署。

在典型的分散式部署中，每個 Splunk Enterprise 執行個體執行一項專門的任務，並駐留在與主要處理功能相對應的三個處理層之一上。

下表列出了 Splunk Enterprise 處理層。

層級	成分	描述
資料輸入	貨運代理	轉發器消費數據，然後將數據轉發給一組索引器。
索引	索引器	索引器對通常從一組轉發器接收的傳入資料進行索引。索引器將資料轉換為事件並將事件儲存在索引中。索引器也會根據搜尋頭的搜尋請求搜尋索引資料。
搜尋管理	搜尋頭	搜尋頭是搜尋的中心資源。叢集中的搜尋頭是可互換的，並且可以從搜尋頭叢集的任何成員存取相同的搜尋、儀表板、知識對像等。

下表列出了在分散式 Splunk Enterprise 環境中使用的重要元件。

成分	描述	責任
索引集群主節點	協調索引器集群的活動和更新	索引管理
索引集群	配置為相互複製資料的 Splunk Enterprise 索引器組	索引
搜尋頭部署器	處理叢集主控的部署與更新	搜尋頭管理
搜尋頭集群	一組搜尋頭，作為搜尋的中心資源	搜尋管理
負載平衡器	由叢集元件使用，以處理搜尋頭、索引器和 S3 目標不斷增長的需求，從而在叢集元件之間分配負載。	叢集元件的負載管理

請參閱 Splunk Enterprise 分散式部署的以下優點：

- 存取多樣化或分散的資料來源
- 提供處理任何規模和複雜程度的企業資料需求的功能
- 透過資料複製和多站點部署實現高可用性並確保災難復原

Splunk SmartStore

SmartStore 是一種索引器功能，它使遠端物件儲存（如 Amazon S3）能夠儲存索引資料。隨著部署的資料量增加，對儲存的需求通常會超過對運算資源的需求。SmartStore 可讓您透過單獨擴充這些資源來經濟高效地管理索引器儲存和運算資源。

SmartStore 引入了遠端儲存層和快取管理器。這些功能允許資料駐留在本機索引器上或遠端儲存層。快取管理器管理索引器和索引器上配置的遠端儲存層之間的資料移動。

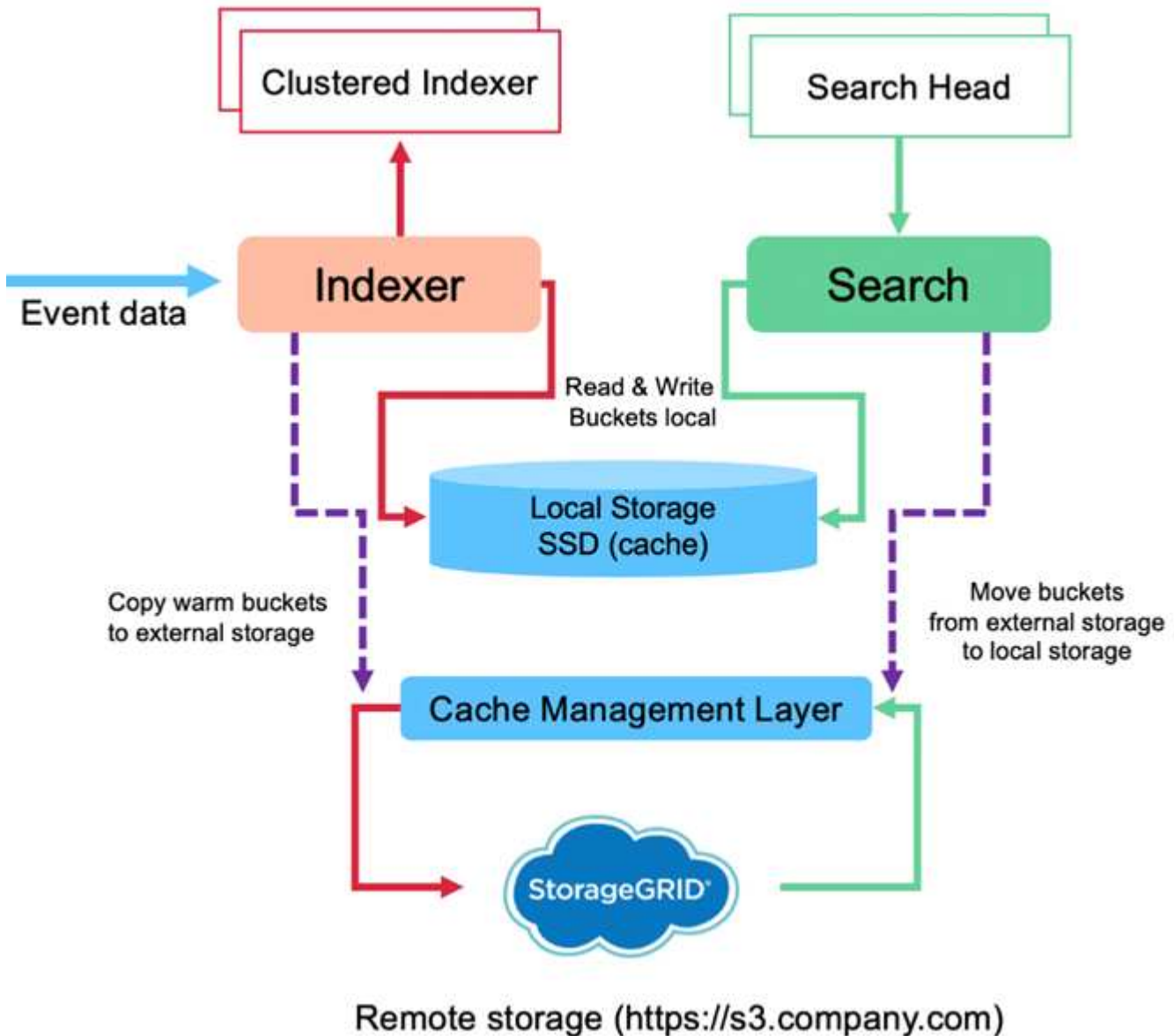
使用 SmartStore，您可以將索引器儲存佔用空間降至最低，並選擇針對 I/O 最佳化的運算資源。大多數資料駐留在遠端儲存上。索引器維護一個包含最少量資料的本地快取：熱儲存桶、參與活動或最近搜尋的熱儲存桶副本以及儲存桶元資料。

Splunk SmartStore 資料流

當來自各個來源的資料到達索引器時，資料會被索引並本地保存在熱儲存桶中。索引器還將熱儲存桶資料複製到目標索引器。到目前為止，資料流與非 SmartStore 索引的資料流相同。

當熱桶變暖時，資料流就會分叉。來源索引器將熱儲存桶複製到遠端物件儲存（遠端儲存層），同時將現有副本保留在其快取中，因為搜尋往往會遇到最近索引的資料。但是，目標索引器會刪除其副本，因為遠端儲存無需維護多個本機副本即可提供高可用性。儲存桶的主副本現在位於遠端儲存中。

下圖顯示了 Splunk SmartStore 資料流。



索引器上的快取管理器是 SmartStore 資料流的核心。它根據需要從遠端儲存中獲取儲存桶的副本來處理搜尋請求。它還會從快取中逐出較舊或搜尋較少的儲存桶副本，因為它們參與搜尋的可能性會隨著時間的推移而降低。

快取管理器的工作是優化可用快取的使用，同時確保搜尋可以立即存取所需的儲存桶。

軟體需求

下表列出了實施該解決方案所需的軟體元件。解決方案實施過程中所使用的軟體元件可能會根據客戶要求而有所不同。

產品系列	產品名稱	產品版本	作業系統
NetAppStorageGRID	StorageGRID物件存儲	11.6	無
CentOS	CentOS	8.1	CentOS 7.x
Splunk Enterprise	Splunk Enterprise 與 SmartStore	8.0.3	CentOS 7.x

單站點和多站點要求

在企業 Splunk 環境（中型和大型部署）中，資料源自多台機器，許多使用者需要搜尋數據，您可以透過在單一和多個網站上分發 Splunk Enterprise 實例來擴展部署。

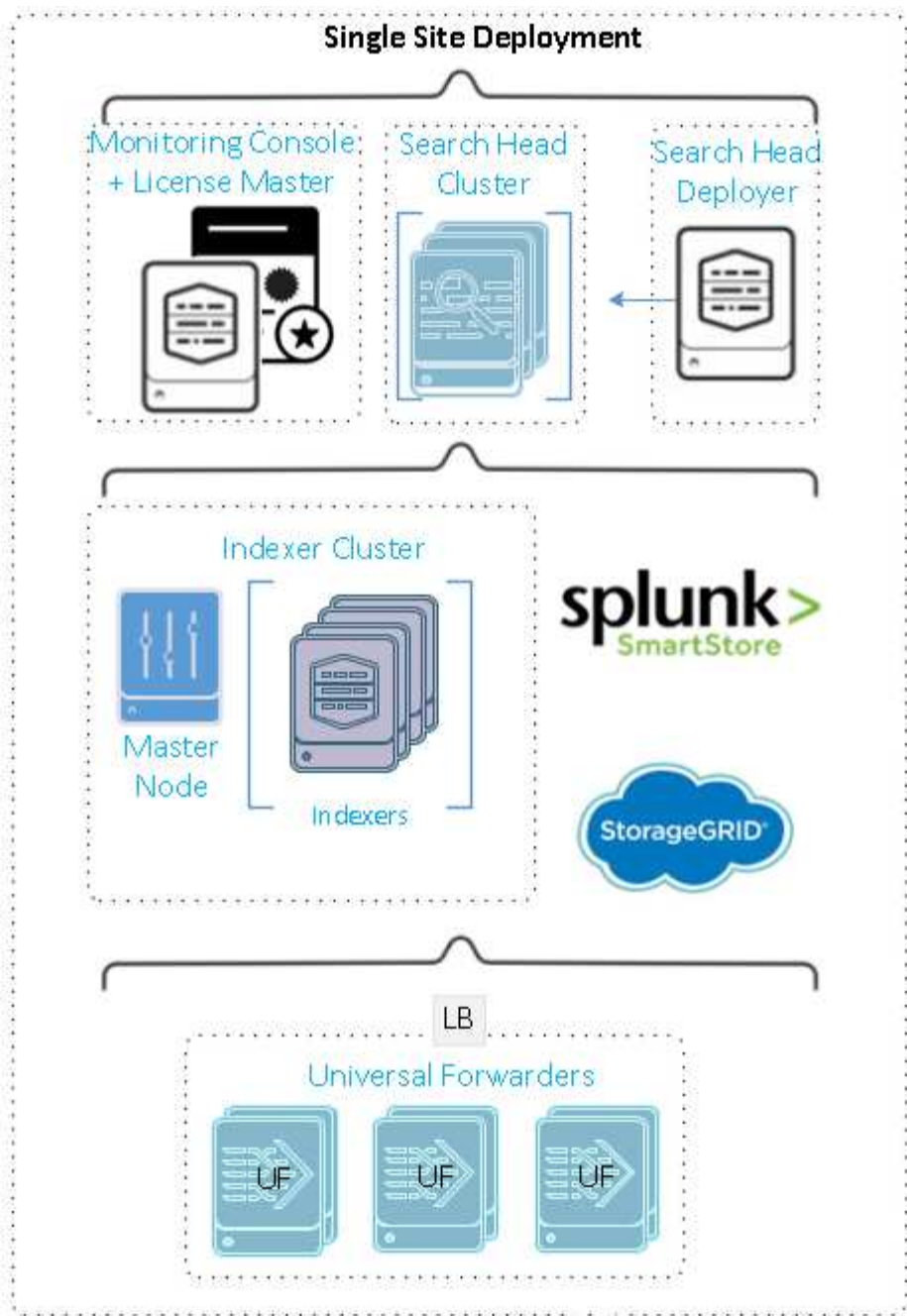
請參閱 Splunk Enterprise 分散式部署的以下優點：

- 存取多樣化或分散的資料來源
- 提供處理任何規模和複雜程度的企業資料需求的功能
- 透過資料複製和多站點部署實現高可用性並確保災難復原

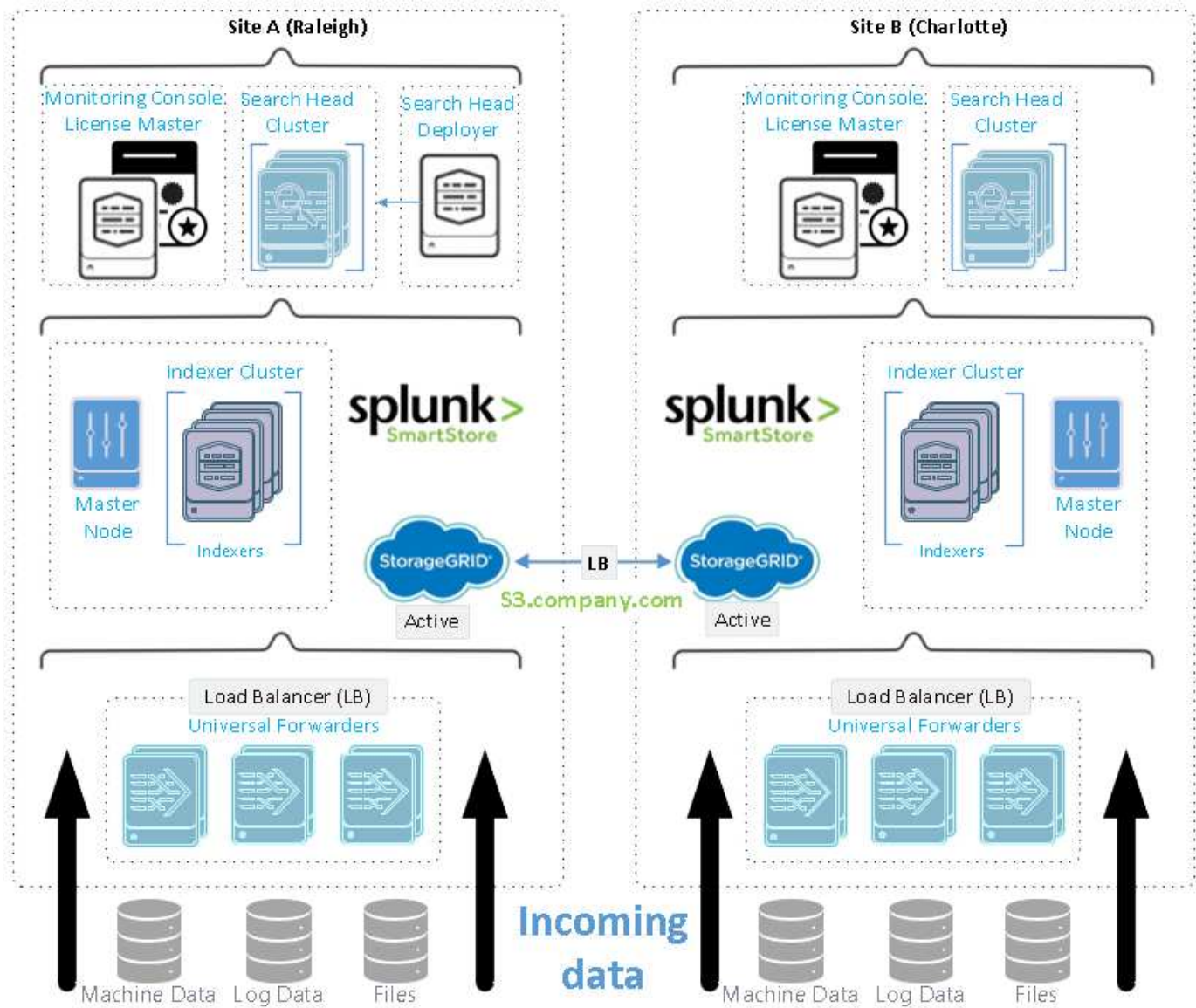
下表列出了在分散式 Splunk Enterprise 環境中使用的元件。

成分	描述	責任
索引集群主節點	協調索引器集群的活動和更新	索引管理
索引集群	配置為相互複製資料的 Splunk Enterprise 索引器組	索引
搜尋頭部署器	處理叢集主控的部署與更新	搜尋頭管理
搜尋頭集群	一組搜尋頭，作為搜尋的中心資源	搜尋管理
負載平衡器	由叢集元件使用，以處理搜尋頭、索引器和 S3 目標不斷增長的需求，從而在叢集元件之間分配負載。	叢集元件的負載管理

該圖描繪了單站點分散式部署的範例。



該圖描繪了多站點分散式部署的範例。



硬體需求

下表列出了實施該解決方案所需的最少硬體組件數量。解決方案具體實施中使用的硬體組件可能會根據客戶要求而有所不同。



無論您在單一網站或多個網站部署了 Splunk SmartStore 和 StorageGRID，所有系統都透過 StorageGRID GRID Manager 在單一玻璃窗格中進行管理。有關更多詳細信息，請參閱“使用網絡管理器進行簡單管理”部分。

該表列出了單一站點使用的硬體。

硬體	數量	磁碟	可用容量	筆記
StorageGRID SG1000	1	無	無	管理節點和負載平衡器
StorageGRID SG6060	4	x48，8TB（NL-SAS 硬碟）	1PB	遠端儲存

下表列出了用於多站點配置（每個站點）的硬體。

硬體	數量	磁碟	可用容量	筆記
StorageGRID SG1000	2	無	無	管理節點和負載平衡器
StorageGRID SG6060	4	x48，8TB（NL-SAS 硬碟）	1PB	遠端儲存

NetApp StorageGRID負載平衡器：SG1000

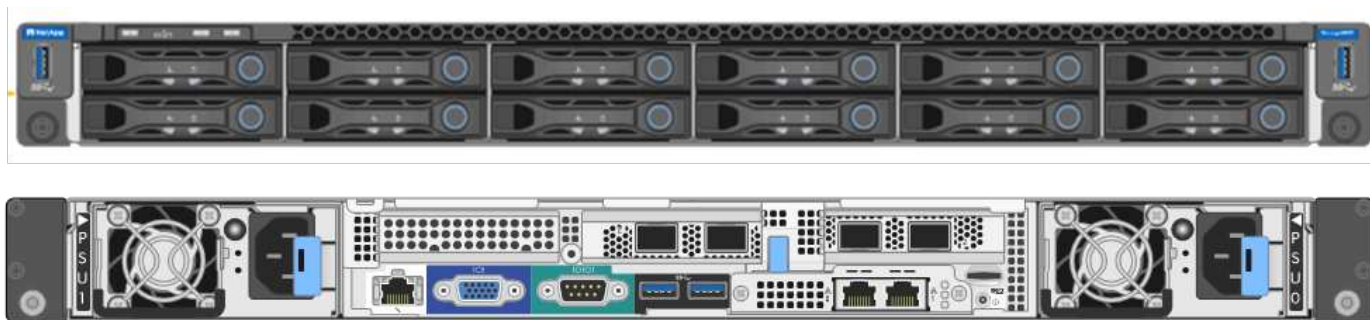
物件儲存需要使用負載平衡器來呈現雲端儲存命名空間。StorageGRID支援來自 F5 和 Citrix 等領先供應商的第三方負載平衡器，但許多客戶選擇企業級StorageGRID平衡器以實現簡單性、彈性和高效能。StorageGRID負載平衡器可作為虛擬機器、容器或專用設備使用。

StorageGRID SG1000 有助於使用高可用性 (HA) 群組和 S3 資料路徑連接的智慧負載平衡。沒有其他內部部署物件儲存系統提供客製化的負載平衡器。

SG1000 設備提供以下功能：

- StorageGRID系統的負載平衡器和管理節點（選用）功能
- StorageGRID Appliance Installer 可簡化節點部署與配置
- 簡化 S3 端點和 SSL 的配置
- 專用頻寬（而不是與其他應用程式共用第三方負載平衡器）
- 高達 4 x 100Gbps 聚合乙太網路頻寬

下圖顯示了 SG1000 網關服務設備。



SG6060

StorageGRID SG6060 設備包括一個運算控制器（SG6060）和一個儲存控制器架（E 系列 E2860），其中包含兩個儲存控制器和 60 個磁碟機。本設備具有以下功能：

- 在單一命名空間中擴展到 400PB。
- 高達 4x 25Gbps 的聚合乙太網路頻寬。
- 包括StorageGRID Appliance Installer，以簡化節點部署和配置。
- 每個 SG6060 設備可以有一個或兩個額外的擴充架，總共可容納 180 個驅動器。

- 兩個 E 系列 E2800 控制器（雙工配置）提供儲存控制器故障轉移支援。
- 五抽屜驅動器架，可容納 60 個 3.5 吋驅動器（兩個固態驅動器和 58 個 NL-SAS 驅動器）。

下圖顯示了 SG6060 設備。



Splunk 設計

下表列出了單一網站的 Splunk 配置。

Splunk 元件	任務	數量	核心	記憶	作業系統
通用轉發器	負責提取資料並將資料轉發給索引器	4	16 核	32 GB 內存	CentOS 8.1
索引器	管理用戶數據	10	16 核	32 GB 內存	CentOS 8.1
搜尋頭	用戶前端在索引器中搜尋數據	3	16 核	32 GB 內存	CentOS 8.1
搜尋頭部署器	處理搜尋頭集群的更新	1	16 核	32 GB 內存	CentOS 8.1
叢集主節點	管理 Splunk 安裝和索引器	1	16 核	32 GB 內存	CentOS 8.1
監控控制台和許可證主控器	對整個 Splunk 部署進行集中監控並管理 Splunk 許可證	1	16 核	32 GB 內存	CentOS 8.1

下表描述了多站點配置的 Splunk 配置。

下表列出了多站點配置（站點 A）的 Splunk 配置。

Splunk 元件	任務	數量	核心	記憶	作業系統
通用轉發器	負責提取資料並將資料轉發給索引器。	4	16 核	32 GB 內存	CentOS 8.1
索引器	管理用戶數據	10	16 核	32 GB 內存	CentOS 8.1
搜尋頭	用戶前端在索引器中搜尋數據	3	16 核	32 GB 內存	CentOS 8.1
搜尋頭部署器	處理搜尋頭集群的更新	1	16 核	32 GB 內存	CentOS 8.1
叢集主節點	管理 Splunk 安裝和索引器	1	16 核	32 GB 內存	CentOS 8.1
監控控制台和許可證主控器	對整個 Splunk 部署進行集中監控並管理 Splunk 許可證。	1	16 核	32 GB 內存	CentOS 8.1

下表列出了多站點配置（站點 B）的 Splunk 配置。

Splunk 元件	任務	數量	核心	記憶	作業系統
通用轉發器	負責提取資料並將資料轉發給索引器	4	16 核	32 GB 內存	CentOS 8.1
索引器	管理用戶數據	10	16 核	32 GB 內存	CentOS 8.1

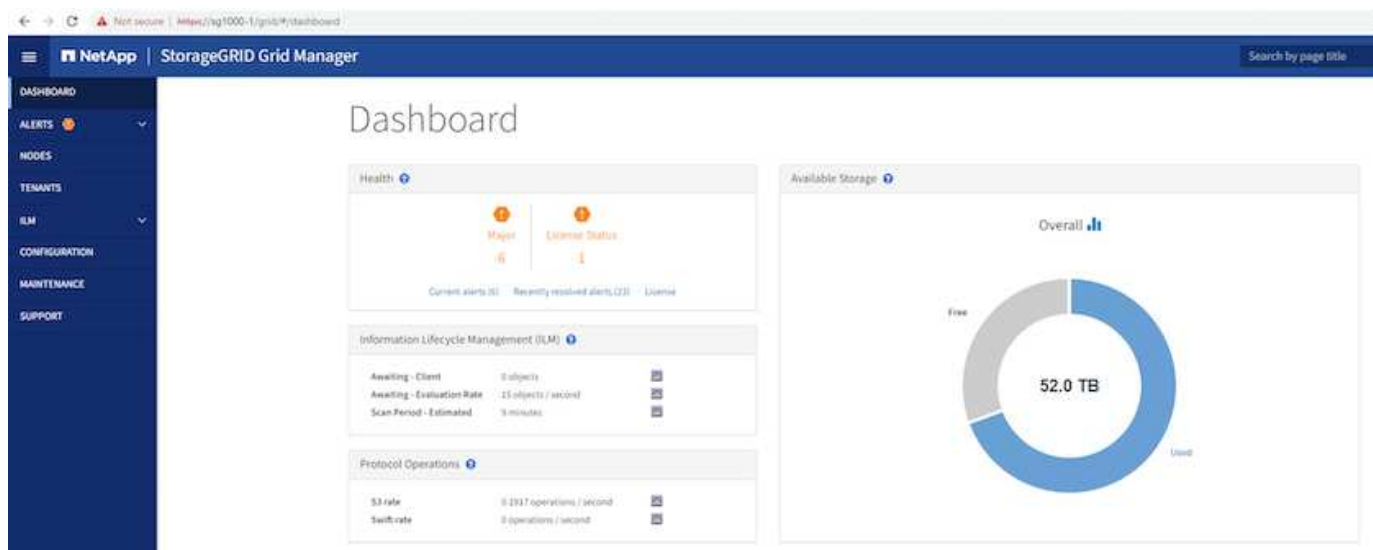
Splunk 元件	任務	數量	核心	記憶體	作業系統
搜尋頭	用戶前端在索引器中搜尋數據	3	16 核	32 GB 內存	CentOS 8.1
叢集主節點	管理 Splunk 安裝和索引器	1	16 核	32 GB 內存	CentOS 8.1
監控控制台和許可證主控器	對整個 Splunk 部署進行集中監控並管理 Splunk 許可證	1	16 核	32 GB 內存	CentOS 8.1

適用於 Splunk SmartStore 的靈活StorageGRID功能

StorageGRID具有多種功能，使用者可以利用這些功能並根據不斷變化的環境進行自訂。從部署到擴展您的 Splunk SmartStore，您的環境需要快速適應變化，並且不應對 Splunk 造成乾擾。StorageGRID靈活的資料管理策略 (ILM) 和流量分類器 (QoS) 讓您可以規劃並適應您的環境。

使用網格管理器進行簡單管理

Grid Manager 是基於瀏覽器的圖形介面，可讓您在單一玻璃窗格中配置、管理和監控全球分佈位置的StorageGRID系統，如下圖所示。



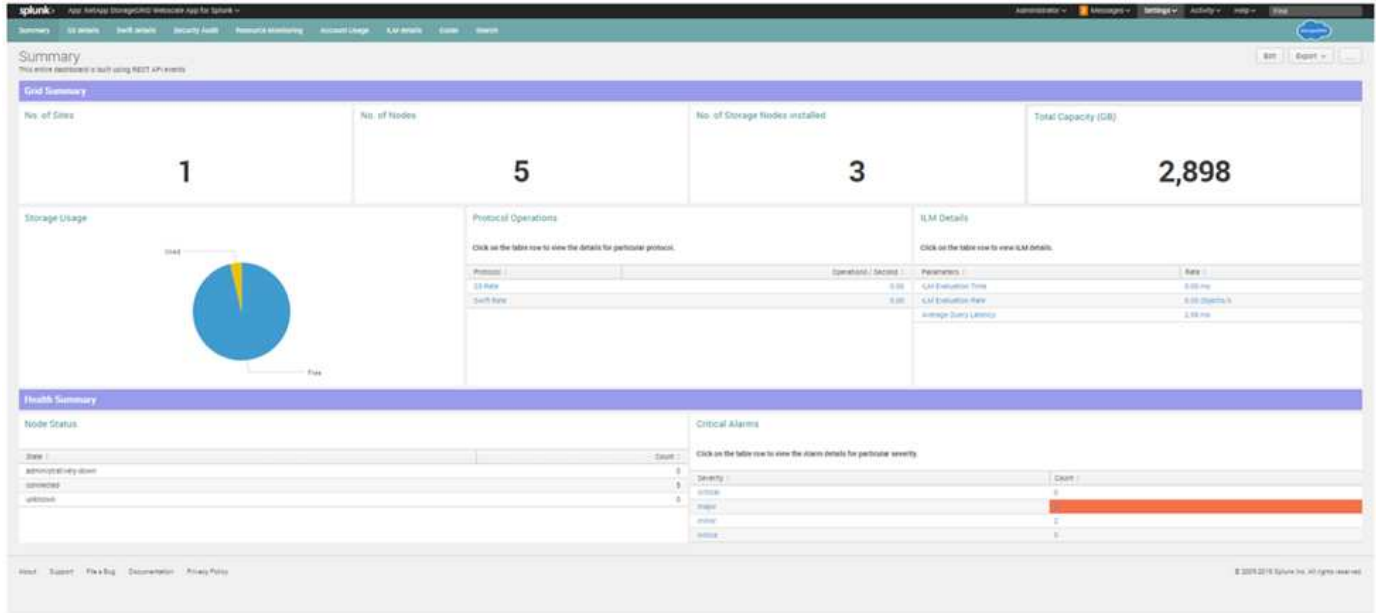
使用網格管理器介面執行以下任務：

- 管理全球分佈的 PB 級物件儲存庫，例如影像、影片和記錄。
- 監控網格節點和服務以確保物件可用性。
- 使用資訊生命週期管理 (ILM) 規則來管理物件資料隨時間推移的放置。這些規則控制著物件資料被攝取後會發生什麼、如何防止資料遺失、物件資料儲存在何處以及儲存多長時間。
- 監控系統內的交易、效能和操作。

適用於 Splunk 的 NetApp StorageGRID 應用程式

NetApp StorageGRID App for Splunk 是專用於 Splunk Enterprise 的應用程式。此應用程式與 Splunk 的 NetApp StorageGRID 附加元件搭配使用。它提供對 StorageGRID 健康狀況、帳戶使用資訊、安全審計詳細資訊、資源使用情況和監控等方面的可見性。

下圖顯示了適用於 Splunk 的 StorageGRID 應用程式。



ILM 策略

StorageGRID 具有靈活的資料管理策略，包括保留對象的多個副本，並使用 2+1 和 4+2（以及許多其他）等 EC（擦除編碼）方案來儲存對象，具體取決於特定的效能和資料保護要求。由於工作負載和需求隨時間而變化，ILM 策略通常也必須隨時間而變化。修改 ILM 策略是一項核心功能，可讓 StorageGRID 客戶快速輕鬆地適應不斷變化的環境。

表現

StorageGRID 透過增加更多節點來擴展效能，這些節點可以是虛擬機器、裸機或專用設備，如 SG5712、SG5760、SG6060 或 SGF6024。在我們的測試中，我們使用 SG6060 設備以最小尺寸的三節點網格超出了 SmartStore 關鍵效能要求。當客戶使用附加索引器擴展其 Splunk 基礎架構時，他們可以添加更多儲存節點來提高效能和容量。

負載平衡器和端點配置

StorageGRID 中的管理節點提供網格管理器 UI（使用者介面）和 REST API 端點來檢視、設定和管理您的 StorageGRID 系統，以及稽核日誌來追蹤系統活動。為了為 Splunk SmartStore 遠端儲存提供高可用性 S3 端點，我們實作了 StorageGRID 負載平衡器，它作為管理節點和網關節點上的服務運作。此外，負載平衡器還管理本地流量並與 GSLB（全域伺服器負載平衡）對話以協助進行災難復原。

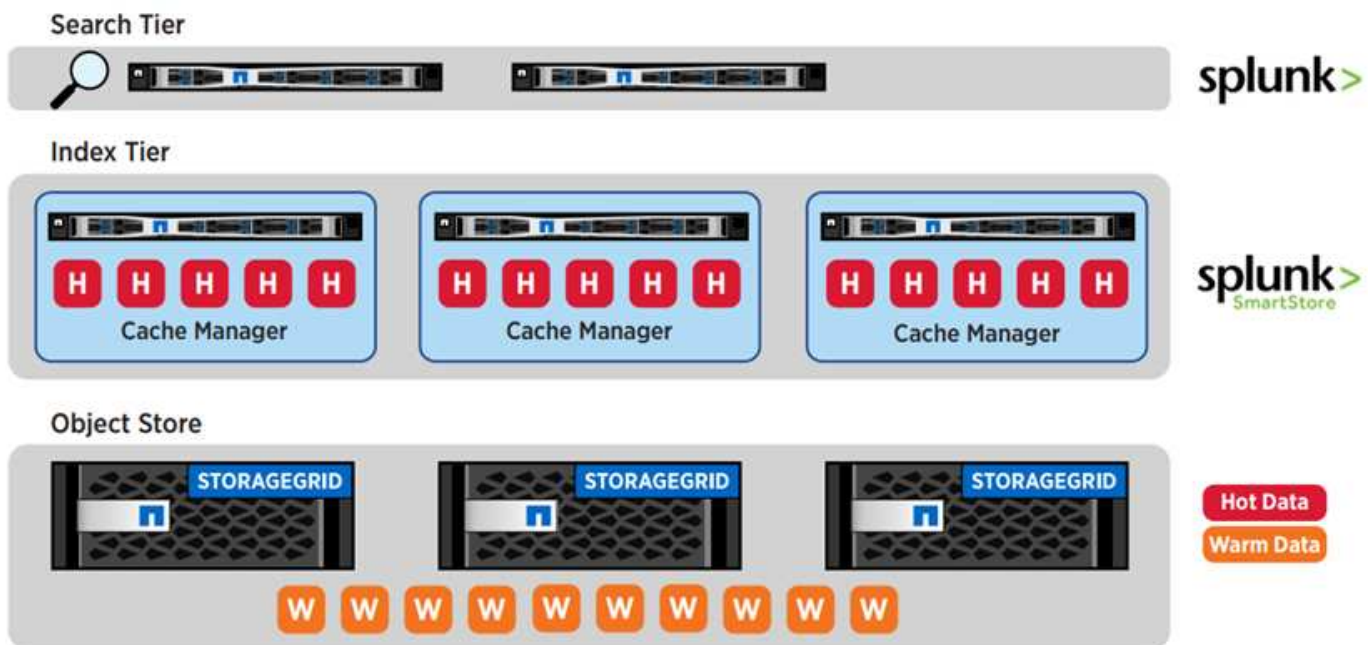
為了進一步增強端點配置，StorageGRID 提供了內建於管理節點的流量分類策略，讓您監控工作負載流量，並對工作負載套用各種服務品質 (QoS) 限制。流量分類策略應用於網關節點和管理節點的 StorageGRID 負載平衡器服務上的端點。這些策略可以幫助限制和監控流量。

智慧分層和成本節約

當客戶意識到 Splunk 數據分析的強大功能和易用性時，他們自然希望索引不斷增長的數據量。隨著資料量的增長，服務資料所需的運算和儲存基礎設施也在增長。由於舊資料的引用頻率較低，因此投入相同數量的運算資源並消耗昂貴的主儲存變得越來越低效。為了大規模運營，客戶可以將熱數據移動到更具成本效益的層，從而釋放熱數據的運算和主儲存。

具有StorageGRID 的Splunk SmartStore 為組織提供了可擴展、高效且經濟高效的解決方案。由於 SmartStore 具有資料感知能力，它會自動評估資料存取模式，以確定哪些資料需要即時分析（熱資料），哪些資料應該駐留在低成本的長期儲存中（溫資料）。SmartStore 動態且智慧地使用業界標準的 AWS S3 API，將資料放置在StorageGRID提供的 S3 儲存體中。StorageGRID靈活的橫向擴展架構允許熱資料層根據需要以經濟高效的方式進行成長。StorageGRID基於節點的架構確保效能和成本需求最佳滿足。

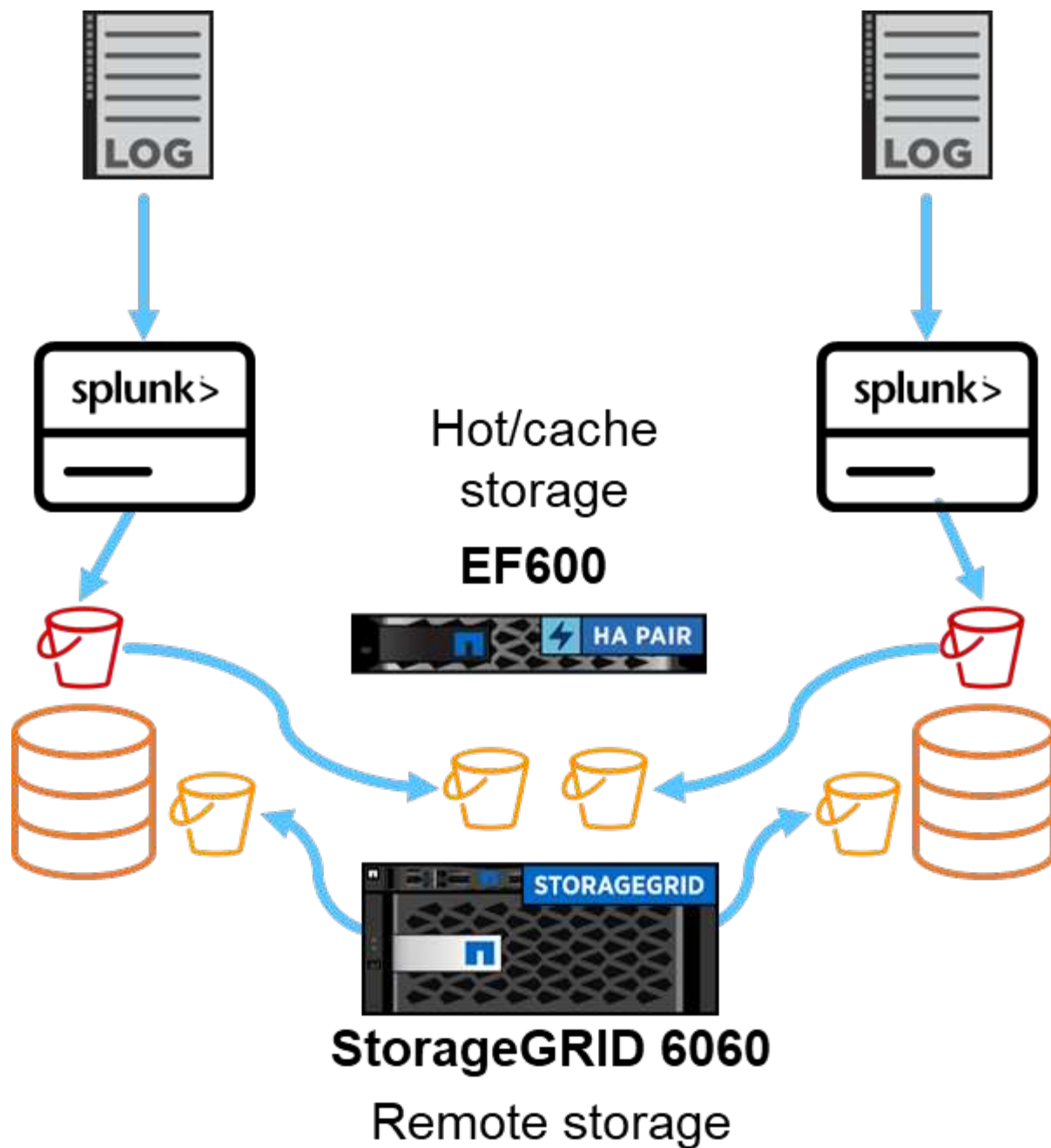
下圖說明了 Splunk 和StorageGRID分層。



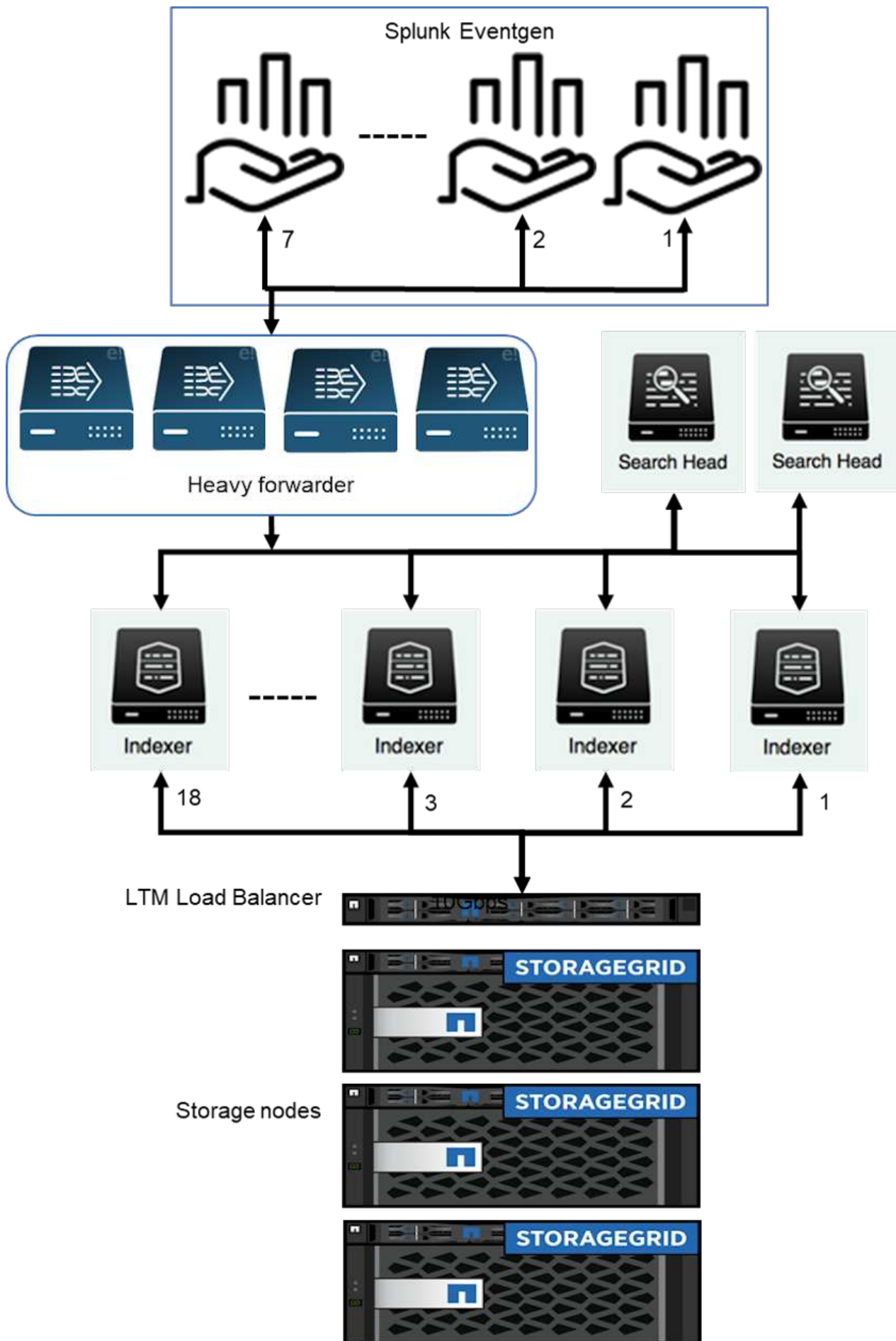
Splunk SmartStore 與NetApp StorageGRID的業界領先組合透過全端解決方案提供了解耦架構的優勢。

單站點 SmartStore 效能

本節介紹 Splunk SmartStore 在NetApp StorageGRID控制器上的效能。 Splunk SmartStore 將熱資料移至遠端儲存，在本例中是效能驗證中的StorageGRID物件儲存。



我們使用 EF600 作為熱/快取存儲，使用StorageGRID 6060 作為遠端儲存。我們使用以下架構進行效能驗證。我們使用了兩個搜尋頭、四個重型轉發器將數據轉發到索引器、七個 Splunk 事件產生器（Eventgens）來產生即時數據，以及 18 個索引器來儲存數據。



配置

下表列出了用於 SmartStorage 效能驗證的硬體。

Splunk 元件	任務	數量	核心	記憶	作業系統
重型貨運代理	負責提取資料並將資料轉發給索引器	4	16 核	32 GB 內存	SLED 15 SP2
索引器	管理用戶數據	18	16 核	32 GB 內存	SLED 15 SP2
搜尋頭	用戶前端在索引器中搜尋數據	2	16 核	32 GB 內存	SLED 15 SP2
搜尋頭部署器	處理搜尋頭集群的更新	1	16 核	32 GB 內存	SLED 15 SP2
叢集主節點	管理 Splunk 安裝和索引器	1	16 核	32 GB 內存	SLED 15 SP2
監控控制台和許可證主控器	對整個 Splunk 部署進行集中監控並管理 Splunk 許可證	1	16 核	32 GB 內存	SLED 15 SP2

SmartStore遠端商店效能驗證

在本次效能驗證中，我們在所有索引器的本機儲存中配置了 SmartStore 緩存，以保存 10 天的資料。我們啟用了 `maxDataSize=auto`（750MB 儲存桶大小）在 Splunk 叢集管理器中並將變更推送到所有索引器。為了測量上傳效能，我們在 10 天內每天攝取 10TB 的數據，並同時將所有熱儲存桶轉為熱儲存桶，並從 SmartStore 監控控制台儀表板擷取每個實例和整個部署的峰值和平均吞吐量。

此圖顯示了一天內攝取的數據。

Enterprise license group

Change license group

This server is configured to use licenses from the Enterprise license group.

Add license

Usage report

Alerts

Licensing alerts notify you of excessive indexing warnings and licensing misconfigurations. [Learn more](#)

Current

- 1 pool warning reported by 1 indexer Correct by midnight to avoid warning [Learn more](#)
- 1 pool quota overage warning reported by 1 indexer Correct by midnight to avoid warning [Learn more](#)

Permanent

- 48 pool quota overage warnings reported by 12 indexers 1 day ago

Splunk Internal License DO NOT DISTRIBUTE stack [Learn more](#)

Licenses	Volume	Expiration	Status
Splunk Internal License DO NOT DISTRIBUTE Notes	2,097,752 MB	Oct 15, 2021, 2:59:59 AM	expired Delete
Splunk Internal License DO NOT DISTRIBUTE Notes	10,485,760 MB	Jul 2, 2022, 2:59:59 AM	valid Delete

Effective daily volume 10,485,760 MB

Pools	Indexers	Volume used today
auto_generated_pool_enterprise		10,878,328 MB / 10,485,760 MB Edit / Delete
	rtp-idx0005	902,186 MB (8.604%)
	rtp-idx0006	766,053 MB (7.306%)
	rtp-idx0010	943,927 MB (9.002%)
	rtp-idx0008	931,854 MB (8.887%)
	rtp-idx0001	855,659 MB (8.16%)
	rtp-idx0012	949,412 MB (9.054%)
	rtp-idx0011	910,235 MB (8.681%)
	rtp-idx0002	906,379 MB (8.644%)
	rtp-idx0007	963,664 MB (9.19%)
	rtp-idx0009	949,847 MB (9.058%)
	rtp-idx0003	883,446 MB (8.425%)
	rtp-idx0004	915,666 MB (8.732%)

Add pool

Local server information

Indexer name	rtp-mc-lm
Volume used today	0 MB
Warning count	0
Debug information	All license details All indexer details

我們從叢集主節點執行以下命令（索引名稱是 eventgen-test）。然後，我們透過 SmartStore 監控控制台儀表板捕獲每個實例和整個部署的峰值和平均上傳吞吐量。

```
for i in rtp-idx0001 rtp-idx0002 rtp-idx0003 rtp-idx0004 rtp-idx0005 rtp-idx0006 rtp-idx0007 rtp-idx0008 rtp-idx0009 rtp-idx0010 rtp-idx0011 rtp-idx0012 rtp-idx0013011 rtdx0014 rtp-idx0015 rtp-idx0016 rtp-idx0017 rtp-idx0018 ; do ssh $i "hostname; date; /opt/splunk/bin/splunk _internal call /data/indexes/eventgen-test/roll-hot-buckets -auth admin:12345678; sleep 1 "; done
```



群集主機對所有索引器（rtp-idx0001...rtp-idx0018）均採用無密碼身份驗證。

為了測量下載效能，我們使用以下命令執行兩次 `evict CLI`，從快取中逐出所有資料。



我們從叢集主機執行以下命令，並從搜尋頭基於來自StorageGRID的遠端儲存的 10 天資料運行搜尋。然後，我們透過 SmartStore 監控控制台儀表板捕獲每個實例和整個部署的峰值和平均上傳吞吐量。

```
for i in rtp-idx0001 rtp-idx0002 rtp-idx0003 rtp-idx0004 rtp-idx0005 rtp-idx0006 rtp-idx0007 rtp-idx0008 rtp-idx0009 rtp-idx0010 rtp-idx0011 rtp-idx0012 rtp-idx0013 rtp-idx0014 rtp-idx0015 rtp-idx0016 rtp-idx0017 rtp-idx0018 ; do ssh $i " hostname; date; /opt/splunk/bin/splunk _internal call /services/admin/cacheman/_evict -post:mb 1000000000 -post:path /mnt/EF600 -method POST -auth admin:12345678; "; done
```

索引器配置是從 SmartStore 叢集主機推送的。群集主機對索引器有以下配置。

```
Rtp-cm01:~ # cat /opt/splunk/etc/master-apps/_cluster/local/indexes.conf
[default]
maxDataSize = auto
#defaultDatabase = eventgen-basic
defaultDatabase = eventgen-test
hotlist_recency_secs = 864000
repFactor = auto
[volume:remote_store]
storageType = remote
path = s3://smartstore2
remote.s3.access_key = U64TUHONBNC98GQGL60R
remote.s3.secret_key = UBoXNE0jmECie05Z7iCYVzbSB6WJFckiYLcdm2yg
remote.s3.endpoint = 3.sddc.netapp.com:10443
remote.s3.signature_version = v2
remote.s3.clientCert =
[eventgen-basic]
homePath = $SPLUNK_DB/eventgen-basic/db
coldPath = $SPLUNK_DB/eventgen-basic/colddb
thawedPath = $SPLUNK_DB/eventgen-basic/thawed
[eventgen-migration]
homePath = $SPLUNK_DB/eventgen-scale/db
coldPath = $SPLUNK_DB/eventgen-scale/colddb
thawedPath = $SPLUNK_DB/eventgen-scale/thaweddb
[main]
homePath = $SPLUNK_DB/$_index_name/db
coldPath = $SPLUNK_DB/$_index_name/colddb
thawedPath = $SPLUNK_DB/$_index_name/thaweddb
[history]
homePath = $SPLUNK_DB/$_index_name/db
coldPath = $SPLUNK_DB/$_index_name/colddb
```

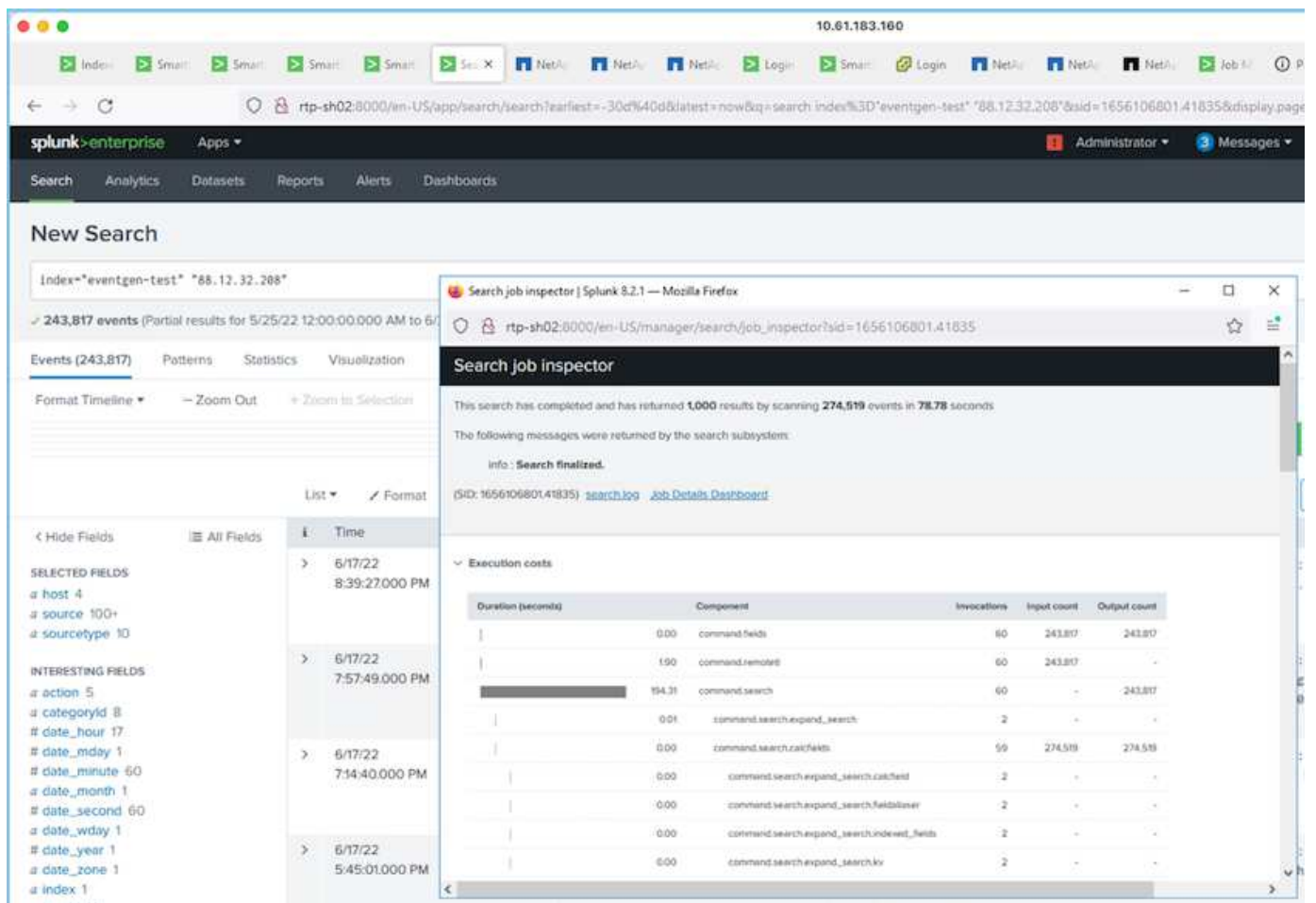


```

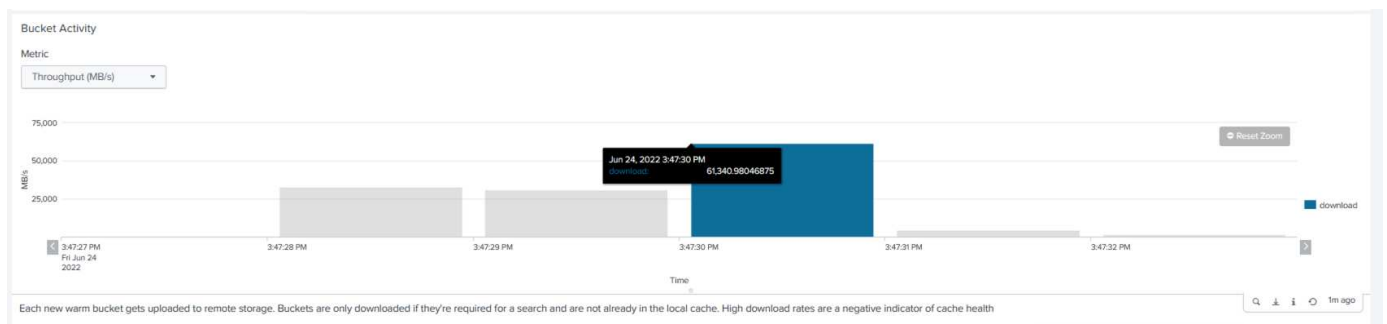
thawedPath = $$SPLUNK_DB/$_index_name/thaweddb
[summary]
homePath = $$SPLUNK_DB/$_index_name/db
coldPath = $$SPLUNK_DB/$_index_name/colddb
thawedPath = $$SPLUNK_DB/$_index_name/thaweddb
[remote-test]
homePath = $$SPLUNK_DB/$_index_name/db
coldPath = $$SPLUNK_DB/$_index_name/colddb
#for storagegrid config
remotePath = volume:remote_store/$_index_name
thawedPath = $$SPLUNK_DB/$_index_name/thaweddb
[eventgen-test]
homePath = $$SPLUNK_DB/$_index_name/db
maxDataSize=auto
maxHotBuckets=1
maxWarmDBCount=2
coldPath = $$SPLUNK_DB/$_index_name/colddb
#for storagegrid config
remotePath = volume:remote_store/$_index_name
thawedPath = $$SPLUNK_DB/$_index_name/thaweddb
[eventgen-evict-test]
homePath = $$SPLUNK_DB/$_index_name/db
coldPath = $$SPLUNK_DB/$_index_name/colddb
#for storagegrid config
remotePath = volume:remote_store/$_index_name
thawedPath = $$SPLUNK_DB/$_index_name/thaweddb
maxDataSize = auto_high_volume
maxWarmDBCount = 5000
rtp-cm01:~ #

```

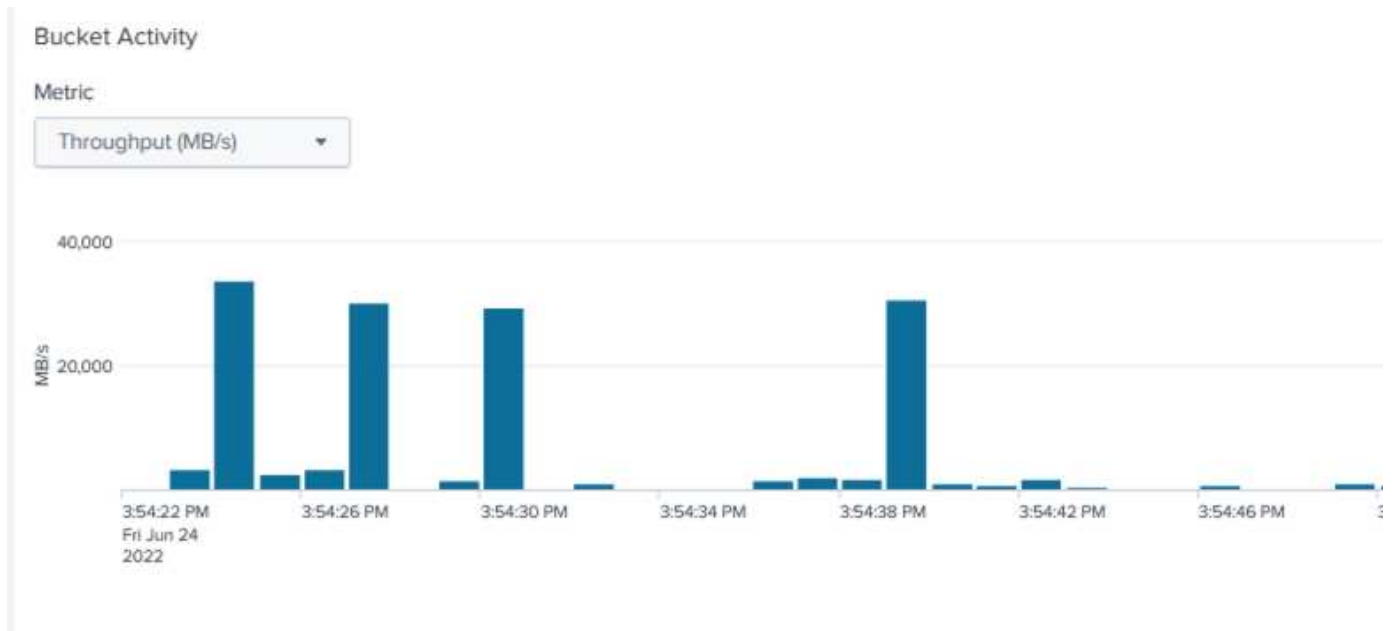
我們在搜尋頭上執行了以下搜尋查詢來收集效能矩陣。



我們從叢集主機收集了效能資訊。峰值性能為61.34GBps。



平均效能約 29GBps。

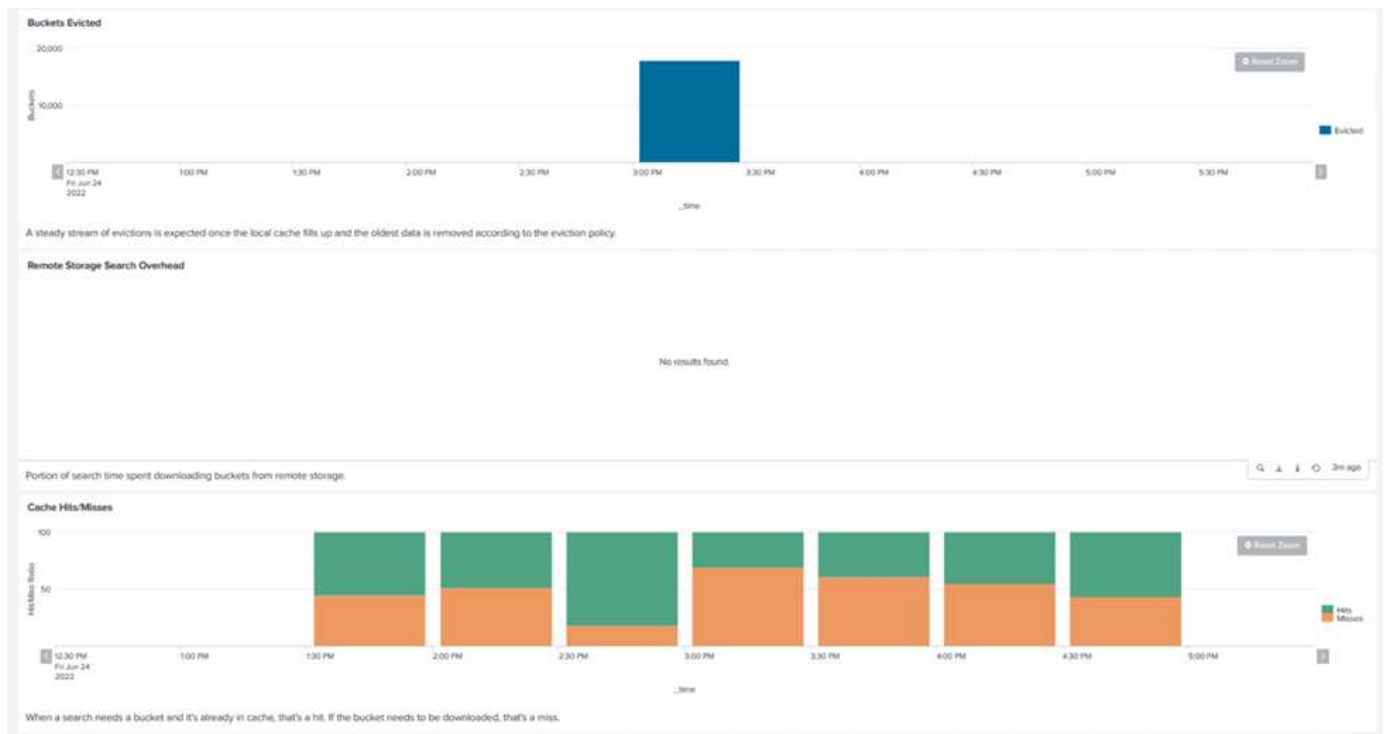


StorageGRID性能

SmartStore 的效能是基於從大量資料中搜尋特定的模式和字串。在此驗證中，事件是使用 "事件生成"透過搜尋頭在特定的 Splunk 索引 (eventgen-test) 上進行搜索，並且請求對於大多數查詢轉到StorageGRID。下圖顯示了查詢資料的命中和未命中情況。命中資料來自本機磁碟，未命中資料來自StorageGRID控制器。

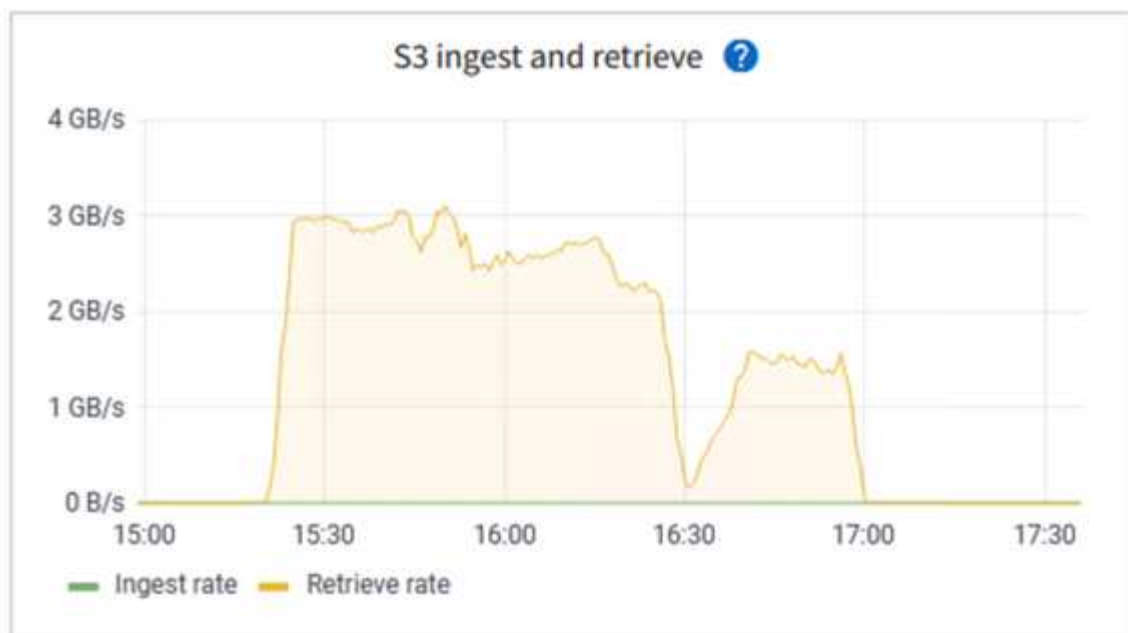


綠色顯示命中數據，橘色顯示未命中數據。



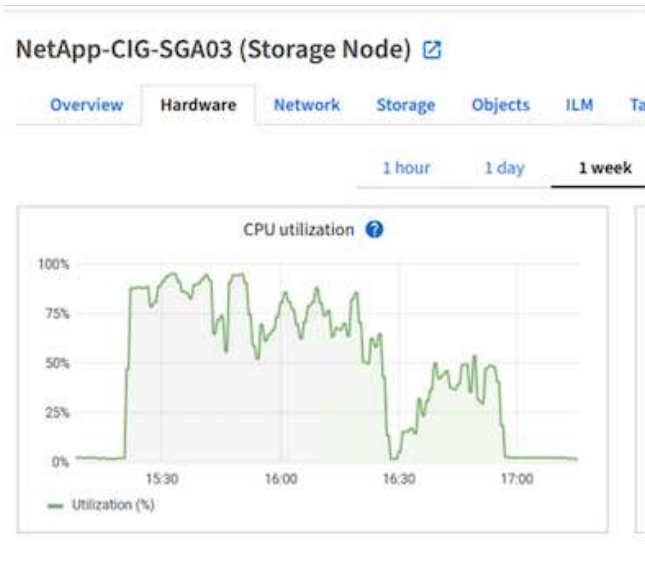
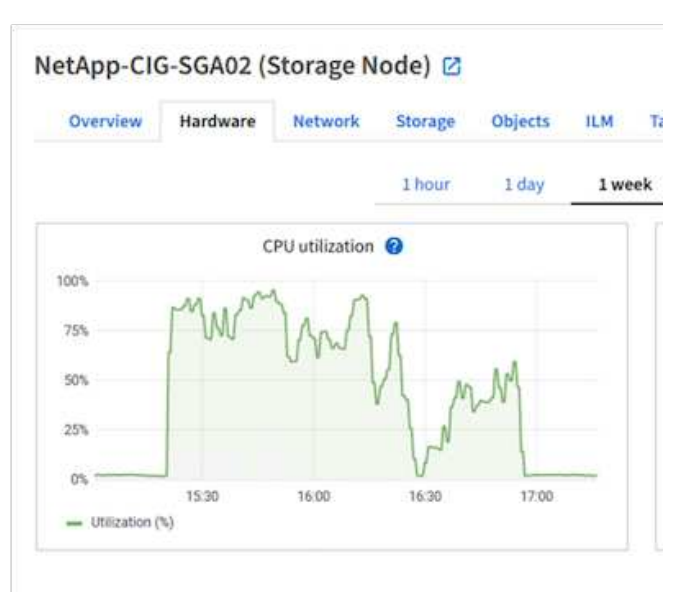
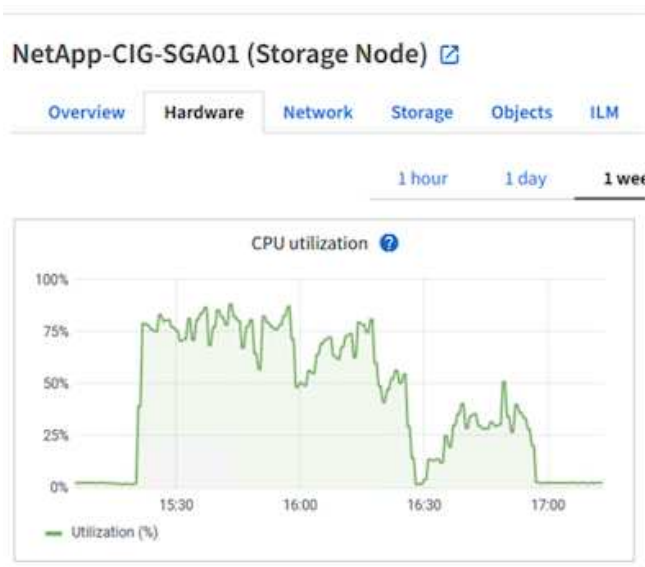
當在StorageGRID上執行搜尋查詢時，StorageGRID的 S3 擷取率的時間如下圖所示。

SmartStore-Site-1 (Site) [🔗](#)

[Network](#)[Storage](#)[Objects](#)[ILM](#)[Platform services](#)[Load b](#)[1 hour](#)[1 day](#)[1 week](#)

StorageGRID硬體使用量

StorageGRID實例有一個負載平衡器和三個StorageGRID控制器。所有三個控制器的 CPU 使用率均為 75% 至 100%。



採用NetApp儲存控制器的 **SmartStore** - 為客戶帶來好處

- *將計算和儲存分離。* Splunk SmartStore 將運算和儲存分離，幫助您獨立擴展它們。
- *按需提供資料。* SmartStore 使資料接近按需運算，並提供運算和儲存彈性和成本效率，以實現更長時間的大規模資料保留。
- *符合 AWS S3 API。* SmartStore 使用 AWS S3 API 與復原儲存進行通信，恢復儲存是符合 AWS S3 和 S3 API 的物件儲存，例如StorageGRID。
- *減少儲存需求和成本。* SmartStore 減少了老化資料（暖/冷）的儲存要求。它只需要一份資料副本，因為NetApp儲存提供資料保護並處理故障和高可用性。
- *硬體故障。* SmartStore 部署中的節點故障不會導致資料無法訪問，並且索引器從硬體故障或資料不平衡中恢復的速度更快。
- 應用程式和資料感知快取。
- 按需新增或刪除索引器以及設定或拆除叢集。
- 儲存層不再與硬體相關。

結論

Splunk Enterprise 是市場領先的 SIEM 解決方案，可推動安全、IT 和 DevOps 團隊取得成果。我們客戶組織中 Splunk 的使用量已顯著增加。因此，需要增加更多資料來源，同時保留更長的數據，從而給 Splunk 基礎設施帶來壓力。

Splunk SmartStore 和 NetApp StorageGRID 的結合旨在為組織提供可擴展的架構，以透過 SmartStore 和 StorageGRID 物件儲存實現更高的攝取效能，並提高跨多個地理區域的 Splunk 環境的可擴展性。

在哪裡可以找到更多信息

要了解有關本文檔中描述的信息的更多信息，請查看以下文檔和/或網站：

- ["NetApp StorageGRID 文件資源"](#)
- ["NetApp 產品文檔"](#)
- ["Splunk Enterprise 文檔"](#)
- ["Splunk Enterprise 關於 SmartStore"](#)
- ["Splunk Enterprise 分散式部署手冊"](#)
- ["Splunk Enterprise 管理索引器和索引器集群"](#)

版權資訊

Copyright © 2025 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。