



功能與安全性FlexPod FlexPod

NetApp
October 30, 2025

This PDF was generated from https://docs.netapp.com/zh-tw/flexpod/security/security-ransomware_what_is_ransomware.html on October 30, 2025. Always check docs.netapp.com for the latest.

目錄

功能與安全性FlexPod	1
解決方案FlexPod	1
TR-4802：FlexPod 《勒索軟體解決方案》	1
概述FlexPod	3
勒索軟體保護措施	4
保護FlexPod 及恢復資料	6
無需支付贖金即可繼續營運	19
結論	19
感謝	19
其他資訊	20
FIPS 140-2 FlexPod 安全性認證的醫療解決方案	20
TR-4892：FIPS 140-2安全性認證FlexPod 的醫療解決方案	20
醫療網路安全威脅	21
FIPS 140-2總覽	23
控制面與資料面	24
Cisco UCS運算與FIPS 140-2 FlexPod	24
Cisco網路與FIPS 140-2 FlexPod	25
NetApp的不二儲存和FIPS 140-2 FlexPod ONTAP	29
解決方案優勢FlexPod：融合式基礎架構	36
其他FlexPod 的安全考量	38
結論	40
感謝、版本歷程記錄、以及何處可以找到其他資訊	40

功能與安全性FlexPod

解決方案FlexPod

TR-4802：FlexPod 《勒索軟體解決方案》

Arvind Ramakrishnan、NetApp



與下列合作夥伴合作：

若要瞭解勒索軟體、必須先瞭解密碼編譯的幾個關鍵點。Cryptographical方法可利用共享的秘密金鑰（對稱金鑰加密）或一對金鑰（非對稱金鑰加密）來加密資料。其中一個金鑰是廣泛使用的公開金鑰、另一個是未揭露的私密金鑰。

勒索軟體是一種以密碼學為基礎的惡意軟體、這是使用密碼編譯來建置惡意軟體。此惡意軟體可同時使用對稱和非對稱金鑰加密來鎖定受害者的資料、並要求贖金提供金鑰來解密受害者的資料。

勒索軟體如何運作？

下列步驟說明勒索軟體如何使用密碼編譯來加密受害者的資料、而不需讓受害者有任何解密或恢復空間：

1. 攻擊者會產生金鑰配對、如同非對稱金鑰加密。產生的公開金鑰會放在惡意軟體中、然後再發行惡意軟體。
2. 惡意軟體進入受害者的電腦或系統後、會使用pseudorandom號碼產生器（PRNG）或任何其他可行的隨機數字產生演算法、產生隨機對稱金鑰。
3. 惡意軟體使用此對稱金鑰來加密受害者的資料。最後會使用內嵌於惡意軟體中的攻擊者公開金鑰來加密對稱金鑰。此步驟的輸出為加密對稱金鑰的非對稱加密文字、以及受害者資料的對稱加密文字。
4. 惡意軟體會將受害者的資料和用於加密資料的對稱金鑰歸零（清除）、因此無法進行還原。
5. 受害者現在會看到對稱金鑰的非對稱加密文字、以及必須支付的贖金值、以便取得用於加密資料的對稱金鑰。
6. 受害者支付贖金、並與攻擊者分享非對稱加密文字。攻擊者使用自己的私密金鑰來解密密碼文字、這會導致對稱金鑰。
7. 攻擊者與受害者共用此對稱金鑰、可用來解密所有資料、進而從攻擊中恢復。

挑戰

受到勒索軟體攻擊時、個人和組織會面臨下列挑戰：

- 最重要的挑戰是、組織或個人的生產力必須立即大幅提高。恢復正常狀態需要時間、因為所有重要檔案都必須重新取得、而且系統必須受到保護。
- 這可能導致資料外洩、其中包含屬於客戶或客戶的敏感機密資訊、並導致組織顯然想要避免的危機情況。
- 資料可能會落入不法之手或被完全刪除、這會導致無法回報的情況、對組織和個人而言可能是災難性的。
- 支付贖金之後、無法保證攻擊者會提供金鑰來還原資料。

- 無法保證攻擊者不會在支付贖金的情況下廣播敏感資料。
- 在大型企業中、找出導致勒索軟體攻擊的漏洞是一項繁瑣的工作、而保護所有系統的安全則需要付出許多努力。

誰有風險？

任何人都可能遭受勒索軟體攻擊、包括個人和大型組織。未實作明確定義的安全措施和實務做法的組織、更容易遭受此類攻擊。攻擊對大型組織的影響可能比個人承受的影響大幾倍。

勒索軟體約佔所有惡意軟體攻擊的28%。換句話說、四分之一以上的惡意軟體事件是勒索軟體攻擊。勒索軟體可透過網際網路自動且不加區分地散佈、一旦發生安全性問題、便可進入受害者的系統、繼續散佈到其他連線系統。攻擊者傾向於鎖定執行大量檔案共用、擁有大量敏感和關鍵資料的人員或組織、或是維持不適當的保護措施來防範攻擊。

攻擊者傾向專注於下列潛在目標：

- 大學與學生社群
- 政府辦公室與機構
- 醫院
- 銀行

這並非詳盡的目標清單。如果您不屬於這些類別、就無法安全防範攻擊。

勒索軟體如何進入系統或擴散？

勒索軟體可透過多種方式進入系統或擴散至其他系統。在當今世界中、幾乎所有系統都透過網際網路、LAN、WAN等方式彼此連線。在這些系統之間產生和交換的資料量只會增加。

勒索軟體的一些最常見傳播方式、包括我們每天用來共用或存取資料的方法：

- 電子郵件
- 點對點網路
- 檔案下載
- 社交網路
- 行動裝置
- 連線至不安全的公共網路
- 存取Web URL

資料遺失的後果

資料遺失的後果或影響可能比組織預期的影響更廣泛。影響可能會因停機時間或組織無法存取其資料的期間而有所不同。攻擊持續時間越長、對組織的營收、品牌和聲譽的影響就越大。組織也可能面臨法律問題、生產力大幅下降。

隨著這些問題持續不斷、它們開始擴大、最終可能改變組織的文化、視其對攻擊的回應方式而定。在當今世界中、資訊快速傳播、以及有關組織的負面新聞、可能會對組織的聲譽造成永久性損害。組織可能面臨資料遺失的重大損失、最終可能導致企業倒閉。

財務影響

根據最近的資料 "[McAfee報告](#)" 全球網路犯罪所造成的成本約為6、000億美元、約佔全球國內生產總值的0.8%。如果將這筆金額與全球不斷成長的4.2兆美元網際網路經濟進行比較、則相當於14%的成長稅。

勒索軟體在這筆財務成本中佔有相當大的比例。2018年、勒索軟體攻擊所造成的成本約為80億美元、預計2019年將達到115億美元。

解決方案為何？

只有實作主動式災難恢復計畫、才能在停機時間最短的情況下、從勒索軟體攻擊中恢復。從攻擊中恢復的能力很好、但完全預防攻擊是理想的做法。

雖然您必須從幾個方面進行審查和修正、以防止攻擊、但讓您預防或恢復攻擊的核心元件是資料中心。

資料中心的設計及其提供的保護網路、運算和儲存端點的功能、在打造安全環境以利日常營運方面扮演著關鍵角色。本文說明FlexPod 了在發生攻擊時、使用混合雲基礎架構的功能如何協助快速恢復資料、也有助於完全預防攻擊。

概述FlexPod

NetApp是一種預先設計、整合及驗證的架構、將Cisco Unified Computing System (Cisco UCS) 伺服器、Cisco Nexus系列交換器、Cisco MDS架構交換器及NetApp儲存陣列、整合為單一靈活架構。FlexPod支援各種工作負載的支援、可在不發生單點故障的情況下、維持成本效益和設計靈活度、實現高可用度。FlexPod支援不同Hypervisor和裸機伺服器的支援功能、也可根據客戶工作負載需求調整規模及最佳化。FlexPod

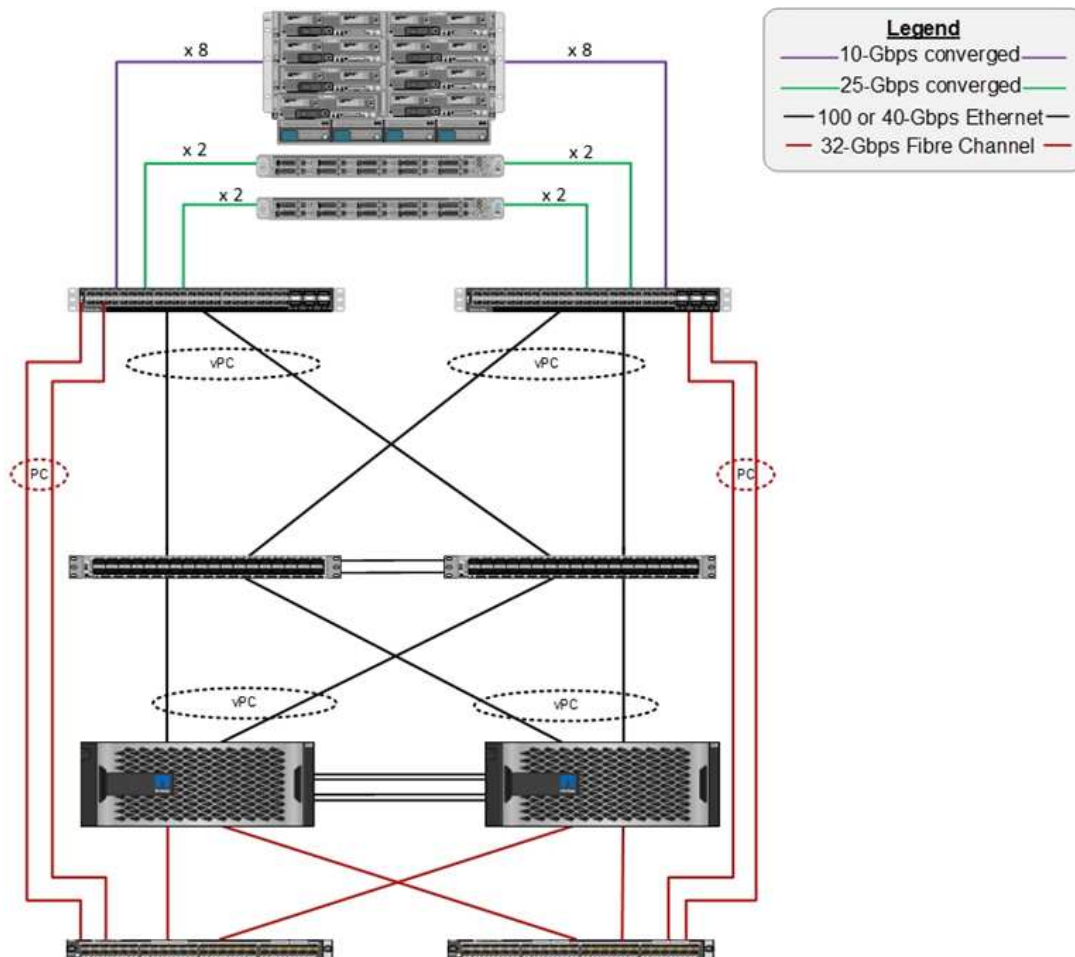
下圖說明FlexPod 了這個架構、並清楚強調堆疊所有層級的高可用度。儲存設備、網路和運算的基礎架構元件的設定方式、可在其中一個元件故障時、立即將作業容錯移轉至正常合作夥伴。

Cisco Unified Computing System
Cisco UCS 6454 Fabric Interconnects, UCS B-Series Blade Servers with UCS VIC 1440, and UCS C-Series Rack Servers with UCS VIC 1457

Cisco Nexus 9336C-FX2

NetApp storage controllers AFF-A800

Cisco MDS 9148T or 9132T switch



這個系統的主要優勢FlexPod 在於它是針對數個工作負載預先設計、整合及驗證的系統。每項解決方案驗證都會發佈詳細的設計與部署指南。這些文件包括您必須採用的最佳實務做法、讓工作負載能夠順暢地在FlexPod 運轉於整個過程中。這些解決方案是以同級最佳的運算、網路和儲存產品打造而成、並提供多項功能、著重於整個基礎架構的安全性和強化。

"IBM的X-Force威脅情報索引" 「造成三分之二的資料外洩事件的人為錯誤、包括錯誤設定的雲端基礎架構中歷史記錄的增加率達420%。」

有了NetApp驗證系統、您就能透過Ansible教戰手冊、根據Cisco驗證設計（CVD）和NetApp驗證架構（NVA）中所述的最佳實務做法、執行基礎架構的端點對端點設定、避免誤用基礎架構。FlexPod

勒索軟體保護措施

本節將討論NetApp ONTAP VMware資料管理軟體的主要功能、以及Cisco UCS和Cisco Nexus工具、您可以使用這些工具來有效保護和恢復勒索軟體攻擊。

儲存設備：ONTAP NetApp

支援資料保護的功能眾多、大部分免費提供給使用此系統的客戶。ONTAP ONTAP您可以隨時使用下列功能來保護資料免受攻擊：

- * NetApp Snapshot技術。* Snapshot複本是磁碟區的唯一映像、可在某個時間點擷取檔案系統的狀態。這些複本有助於保護資料、不會影響系統效能、同時也不會佔用大量的儲存空間。NetApp建議您建立建

立Snapshot複本的建立排程。您也應該維持較長的保留時間、因為某些惡意軟體可能會處於休眠狀態、然後在感染後的數週或數月內重新啟動。發生攻擊時、可以使用感染前所取得的Snapshot複本來復原磁碟區。

- * NetApp SnapRestore 支援技術。* SnapRestore 支援資料還原軟體對於從資料毀損中恢復或僅回復檔案內容非常實用。不還原磁碟區的屬性；它比系統管理員將檔案從Snapshot複本複製到作用中檔案系統所能達到的速度快得多。SnapRestore當許多檔案必須儘快恢復時、資料的恢復速度很有幫助。一旦發生攻擊、這項高效率的恢復程序有助於企業迅速恢復上線。
- * NetApp SnapCenter 功能* SnapCenter 。* Ses庫 軟體使用NetApp儲存型備份與複寫功能、提供應用程式一致的資料保護。此軟體可與企業應用程式整合、並提供應用程式專屬及資料庫專屬的工作流程、以滿足應用程式、資料庫及虛擬基礎架構管理員的需求。支援易於使用的企業平台、可安全地協調及管理應用程式、資料庫和檔案系統之間的資料保護。SnapCenter在資料恢復期間、提供應用程式一致的資料保護功能至關重要、因為它能讓您更快將應用程式還原至一致的狀態。
- * NetApp SnapLock 支援技術* SnapLock 。*支援特殊用途磁碟區、可將檔案儲存並承諾為不可刪除、不可重複寫入的狀態。使用者的資料駐留FlexVol 在一個支援的地方、可透過SnapLock NetApp SnapMirror或SnapVault 支援技術分別鏡射或保存到一個支援的地方。在保留期間結束之前、無法刪除位於現象磁碟區中的檔案SnapLock 、磁碟區本身及其託管Aggregate 。
- * NetApp FPolicy技術。*使用FPolicy軟體、禁止對具有特定副檔名的檔案執行作業、以防止攻擊。可針對特定檔案作業觸發FPolicy事件。此事件與原則有關、該原則會呼叫IT需要使用的引擎。您可以使用一組可能含有勒索軟體的副檔名來設定原則。當副檔名不允許的檔案嘗試執行未獲授權的作業時、FPolicy會防止該作業執行。

網路：Cisco Nexus

Cisco NX OS軟體支援NetFlow功能、可增強偵測網路異常狀況與安全性。NetFlow會擷取網路上每個對話的中繼資料、通訊相關各方、使用的傳輸協定、以及交易持續時間。在彙總和分析資訊之後、即可深入瞭解正常行為。

收集到的資料也能辨識可疑的活動模式、例如惡意軟體散佈於整個網路、否則可能無法察覺。

NetFlow使用流程來提供網路監控的統計資料。流程是一種單向封包串流、傳入來源介面（或VLAN）、金鑰的值相同。金鑰是封包內欄位的識別值。您可以使用流程記錄來建立流程、以定義流程的獨特按鍵。您可以使用流程匯出器、將NetFlow為流程收集的資料匯出至遠端NetFlow收集器、例如Cisco Stealthwatch。Stealthwatch會使用此資訊持續監控網路、並在發生勒索軟體疫情時提供即時威脅偵測和事件回應證明。

運算：Cisco UCS

Cisco UCS是FlexPod 架構中的運算端點。您可以使用多種Cisco產品、在作業系統層級保護堆疊的這一層。

您可以在運算或應用程式層中實作下列主要產品：

- *適用於端點的Cisco進階惡意軟體保護（AMP）。*此解決方案支援Microsoft Windows與Linux作業系統、整合了預防、偵測與回應功能。此安全軟體可防止資料外洩、在進入點封鎖惡意軟體、並持續監控及分析檔案與處理活動、以快速偵測、控制及補救可能規避第一線防禦的威脅。

AMP的惡意活動保護（MAP）元件會持續監控所有端點活動、並提供執行時間偵測、並封鎖端點上執行中程式的異常行為。例如、當端點行為顯示勒索軟體時、會終止違規的程序、以防止端點加密並停止攻擊。

- * Cisco進階的電子郵件安全惡意軟體保護。*電子郵件已成為散佈惡意軟體及進行網路攻擊的主要工具。平均而言、每天大約會交換1000億封電子郵件、讓攻擊者能夠在使用者的系統中擁有絕佳的滲透率。因此、防禦這類攻擊是絕對必要的。

擴大分析電子郵件中的威脅、例如零時差攻擊、以及隱藏在惡意附件中的惡意軟體。它也使用領先業界

的URL情報來對抗惡意連結。它能為使用者提供進階保護、防止針對性網頁仿冒、勒索軟體及其他複雜的攻擊。

- 新一代入侵防禦系統（**NGIPS**）。Cisco火力NGIPS可部署為資料中心的實體應用裝置、或部署為VMware上的虛擬應用裝置（NGIPSv for VMware）。這套高效率的入侵防禦系統可提供可靠的效能、並降低總體擁有成本。您可以選擇訂閱授權來擴充威脅保護、以提供擴大的應用程式可見度與控制能力、以及URL篩選功能。虛擬化的NGIPS會檢查虛擬機器（VM）之間的流量、並使在資源有限的站台上部署及管理NGIPS解決方案變得更容易、同時增加實體與虛擬資產的保護。

保護FlexPod 及恢復資料

本節說明當攻擊發生時、如何恢復終端使用者的資料、以及如何使用FlexPod 一套系統來防止攻擊。

測試床總覽

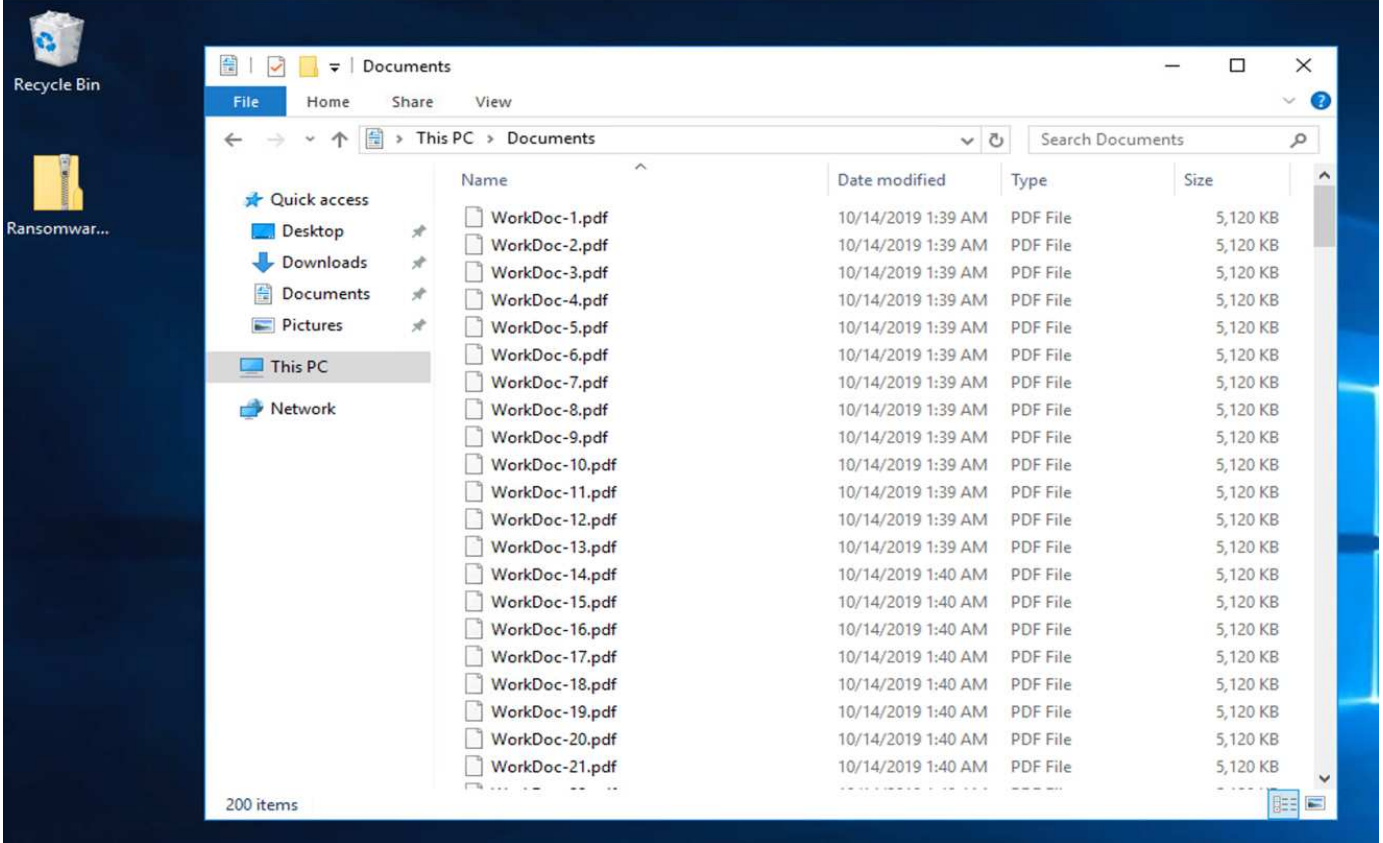
為了展示FlexPod 不偵測、補救和預防、測試平台是根據本文件撰寫時最新平台CVD所指定的準則而打造：["採用VMware vSphere 6.7 U1、Cisco UCS第4代及NetApp解決方案A系列CVD的資料中心FlexPod AFF"](#)。

在ONTAP VMware vSphere基礎架構中部署了Windows 2016 VM、該VM提供來自NetApp VMware vCenter軟體的CIFS共用區。然後在CIFS共用區上設定NetApp FPolicy、以防止執行具有特定副檔名類型的檔案。NetApp SnapCenter 支援軟體也能管理基礎架構中VM的Snapshot複本、以提供應用程式一致的Snapshot複本。

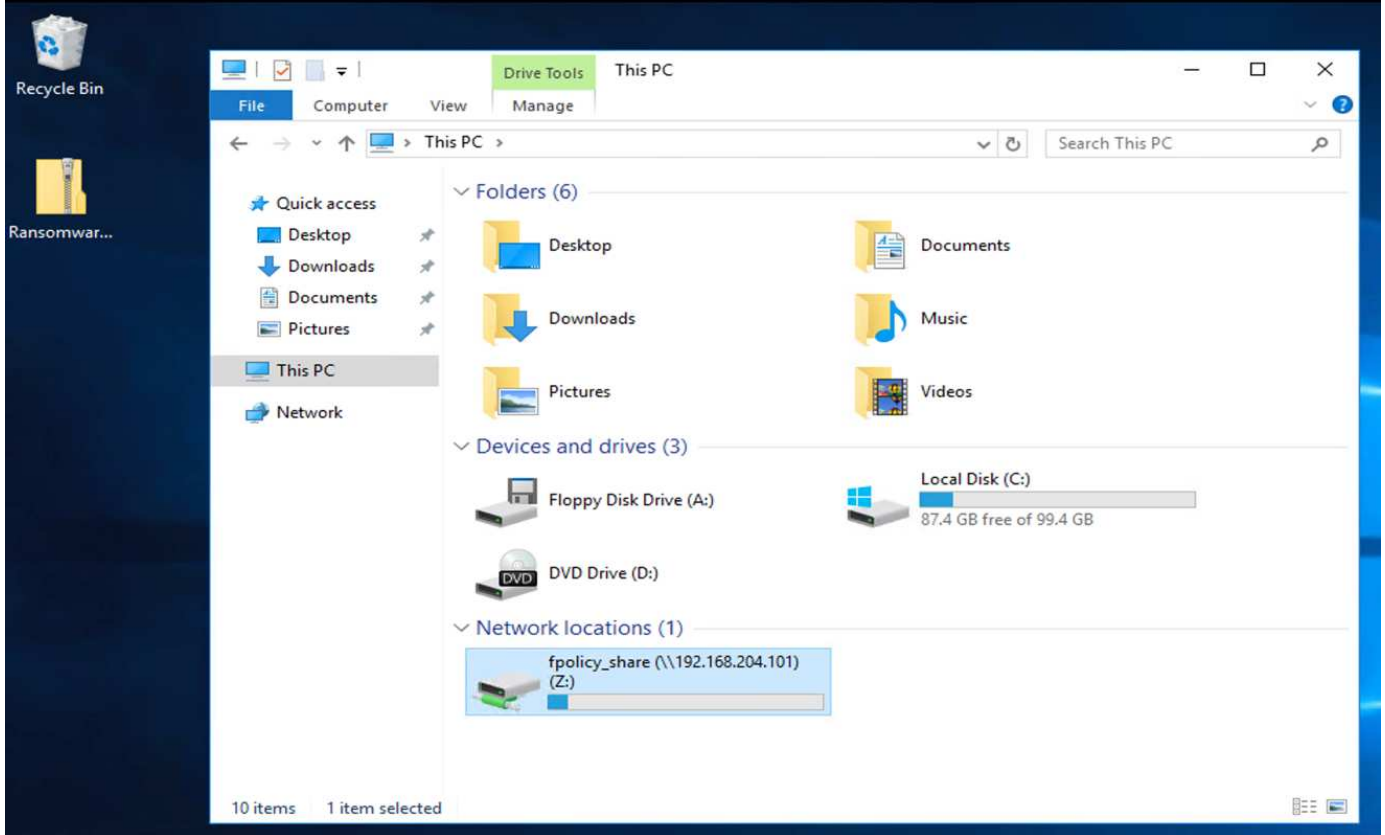
VM狀態及其檔案在攻擊之前

本節說明在攻擊VM之前的檔案狀態、以及對應到VM的CIFS共用區。

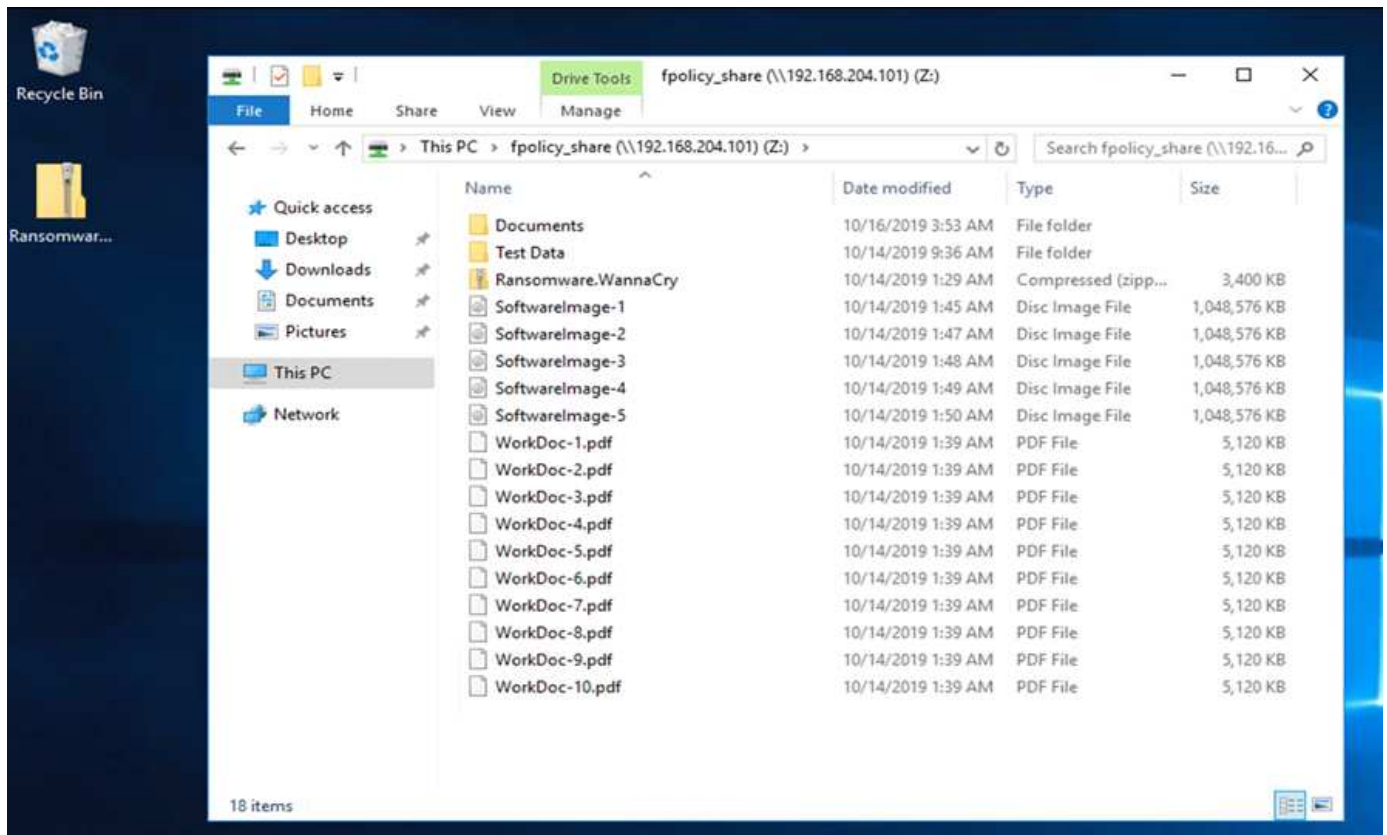
VM的「文件」資料夾中有一組尚未被WannaCry惡意軟體加密的PDF檔案。



下列螢幕快照顯示已對應至VM的CIFS共用區。



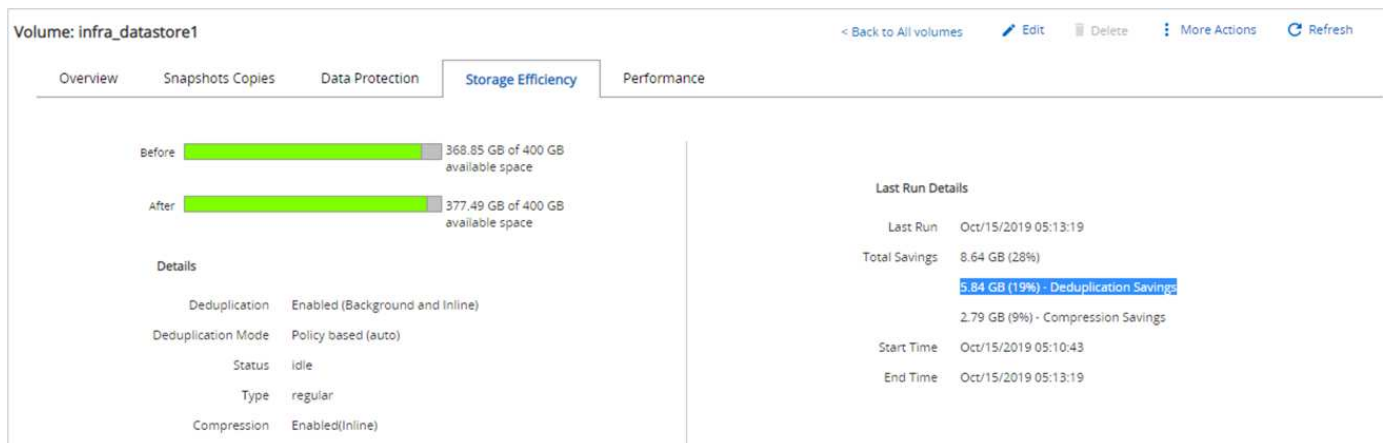
下列螢幕快照顯示CIFS共用區「fpolicy_share」上尚未被WannaCry惡意軟體加密的檔案。



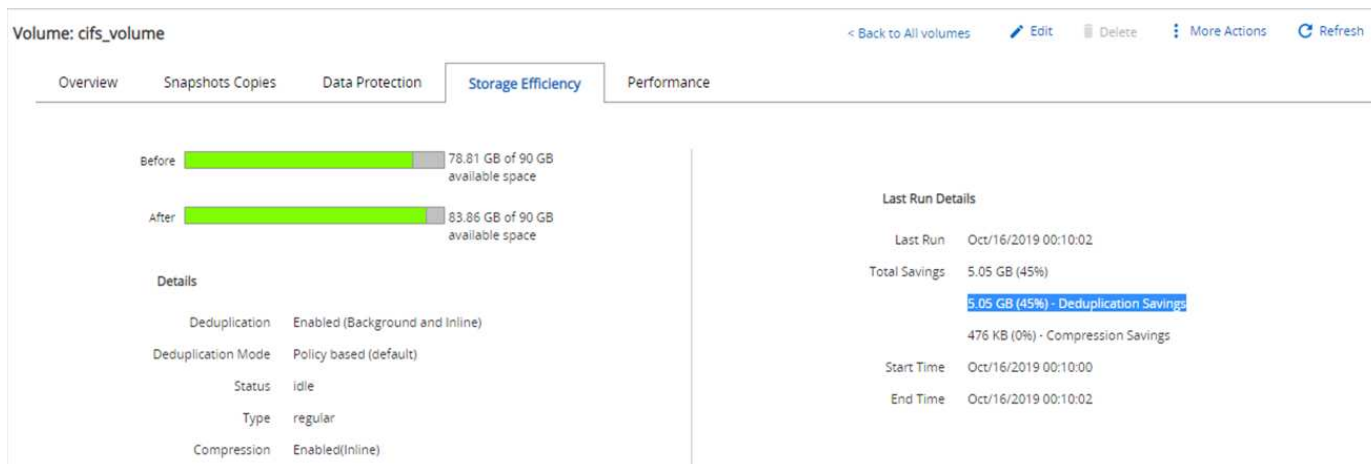
在攻擊之前提供重複資料刪除和Snapshot資訊

在攻擊之前、會指出Snapshot複本的儲存效率詳細資料和大小、並在偵測階段做為參考。

在託管VM的磁碟區上執行重複資料刪除技術、可節省19%的儲存空間。



CIFS共用區「fpolicy_share」上的重複資料刪除技術可節省45%的儲存空間。



針對裝載VM的磁碟區、觀察到Snapshot複本大小為456KB。

Volume: infra_datastore1

< Back to All volumes Edit Delete More Actions Refresh

Overview **Snapshots Copies** Data Protection Storage Efficiency Performance

+ Create Configuration Settings More Actions Delete Refresh

Status	State	Snapshot Name	Date Time	Total Size	Application Dependency
Normal	-NA-	before_attack	Oct/18/2019 01:44:26	456 KB	None

CIFS共用區的Snapshot複本大小為160KB。

Volume: cifs_volume

< Back to All volumes Edit Delete More Actions Refresh

Overview **Snapshots Copies** Data Protection Storage Efficiency Performance

+ Create Configuration Settings More Actions Delete Refresh

Status	State	Snapshot Name	Date Time	Total Size	Application Dependency
Normal	-NA-	before_attack_cifs	Oct/18/2019 01:45:26	160 KB	None

WannaCry感染VM和CIFS共用區

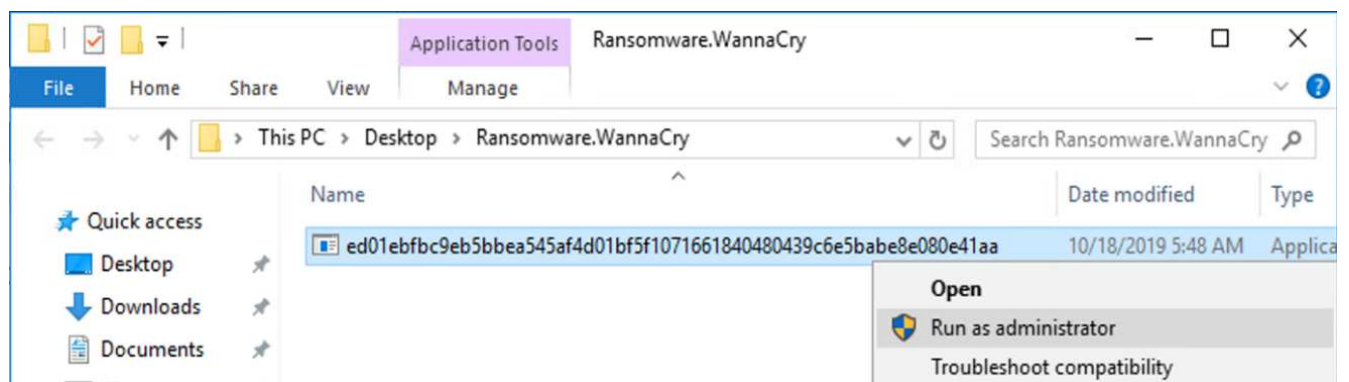
在本節中、我們將說明WannaCry惡意軟體是如何引進FlexPod 到這個環境、以及後續觀察到的系統變更。

下列步驟示範如何將WannaCry惡意軟體二進位檔引進VM：

1. 已擷取安全的惡意軟體。



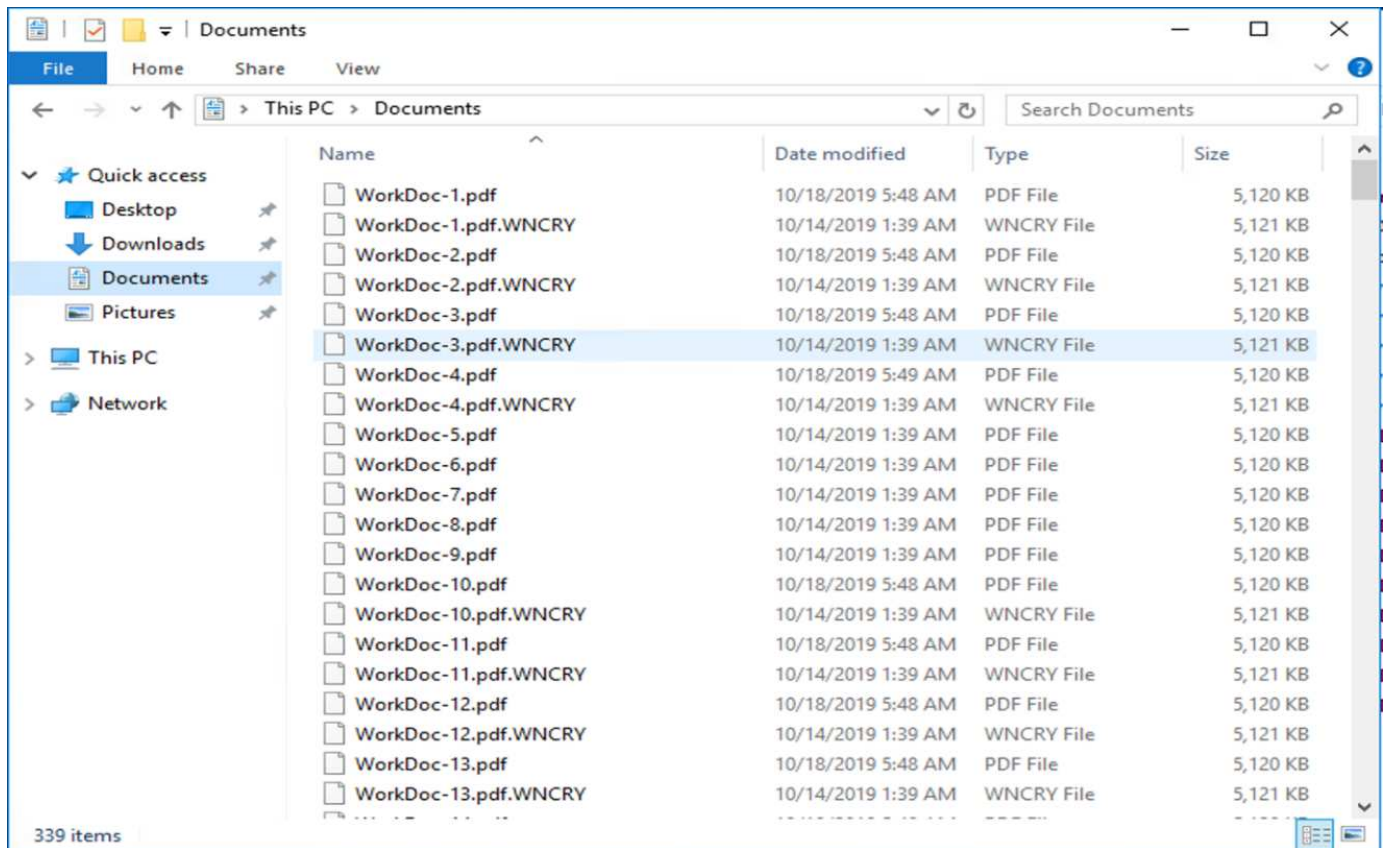
2. 執行二進位檔。



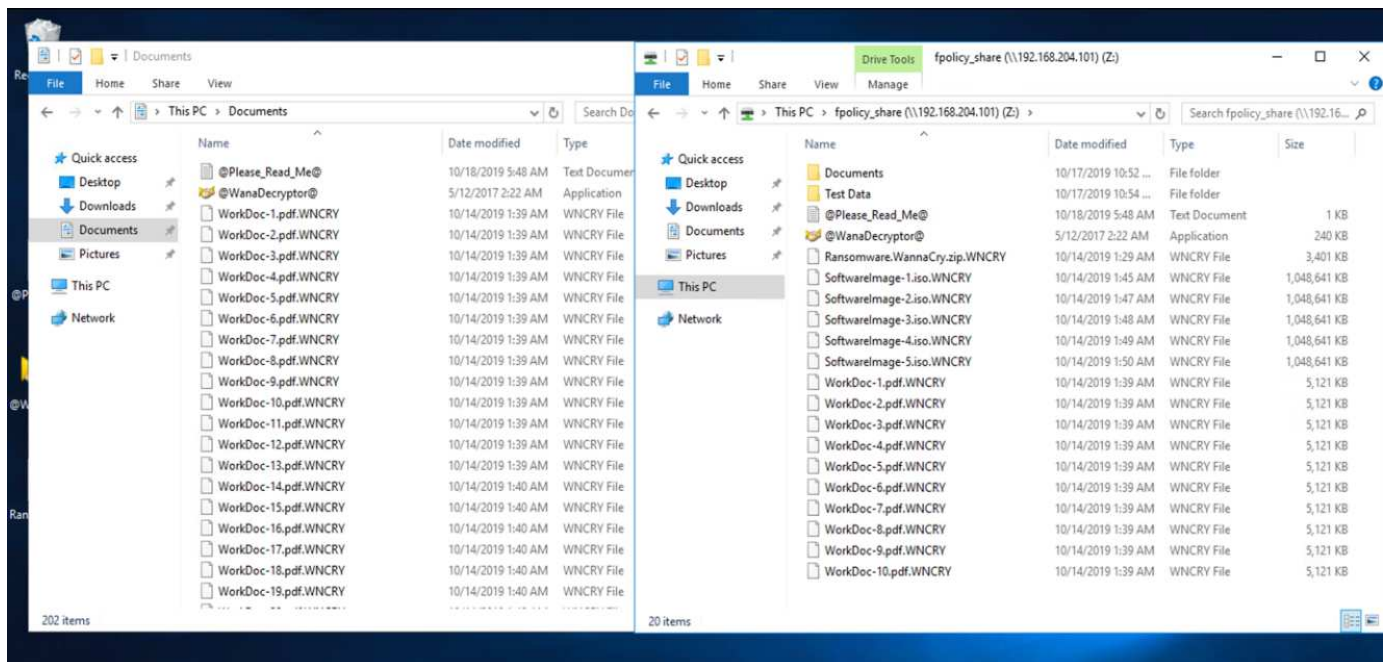
案例1：WannaCry會加密VM內的檔案系統及對應的CIFS共用區

WannaCry惡意軟體已加密本機檔案系統和對應的CIFS共用區。

惡意軟體開始使用WNCRY副檔名加密檔案。



惡意軟體會加密本機VM和對應共用區中的所有檔案。



偵測

從惡意軟體開始加密檔案的那一刻起、它就引發Snapshot複本的大小呈指數式增加、儲存效率百分比呈指數式降低。

我們偵測到、在攻擊期間、託管CIFS共用區的磁碟區的Snapshot大小大幅增加至820.98MB。

Volume: cifs_volume

< Back to All volumes Edit Delete More Actions Refresh

Overview Snapshots Copies Data Protection Storage Efficiency Performance

+ Create Configuration Settings More Actions Delete Refresh

Status	State	Snapshot Name	Date Time	Total Size	Application Dependency
Normal	-NA-	before_attack_cifs	Oct/18/2019 01:45:26	820.98 MB	None

我們偵測到裝載VM的磁碟區的Snapshot複本大小增加到404.3MB。

Volume: infra_datastore1

< Back to All volumes Edit Delete More Actions Refresh

Overview Snapshots Copies Data Protection Storage Efficiency Performance

+ Create Configuration Settings More Actions Delete Refresh

Status	State	Snapshot Name	Date Time	Total Size	Application Dependency
Normal	-NA-	before_attack	Oct/18/2019 01:44:26	404.3 MB	None

託管CIFS共享區的Volume儲存效率降低至34%。

Volume: cifs_volume

< Back to All volumes Edit Delete More Actions Refresh

Overview Snapshots Copies Data Protection Storage Efficiency Performance

Before 75.21 GB of 90 GB available space

After 80.21 GB of 90 GB available space

Details

Deduplication	Enabled (Background and inline)
Deduplication Mode	Policy based (default)
Status	idle
Type	regular
Compression	Enabled(inline)

Last Run Details

Last Run	Oct/16/2019 00:10:02
Total Savings	5 GB (34%)
	5 GB (34%) - Deduplication Savings
	180 KB (0%) - Compression Savings
Start Time	Oct/16/2019 00:10:00
End Time	Oct/16/2019 00:10:02

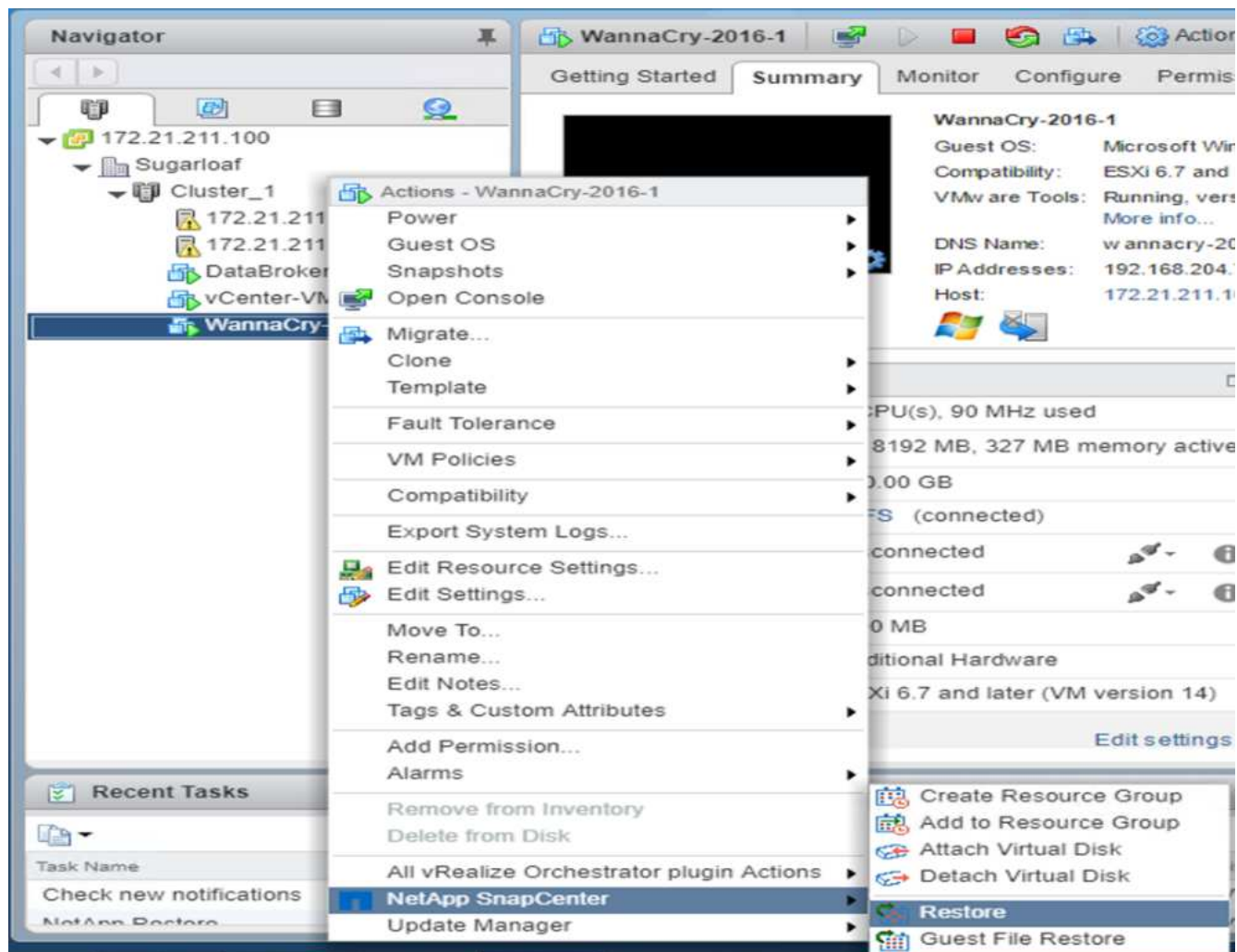
補救

使用攻擊前建立的全新Snapshot複本、還原VM和對應的CIFS共用區。

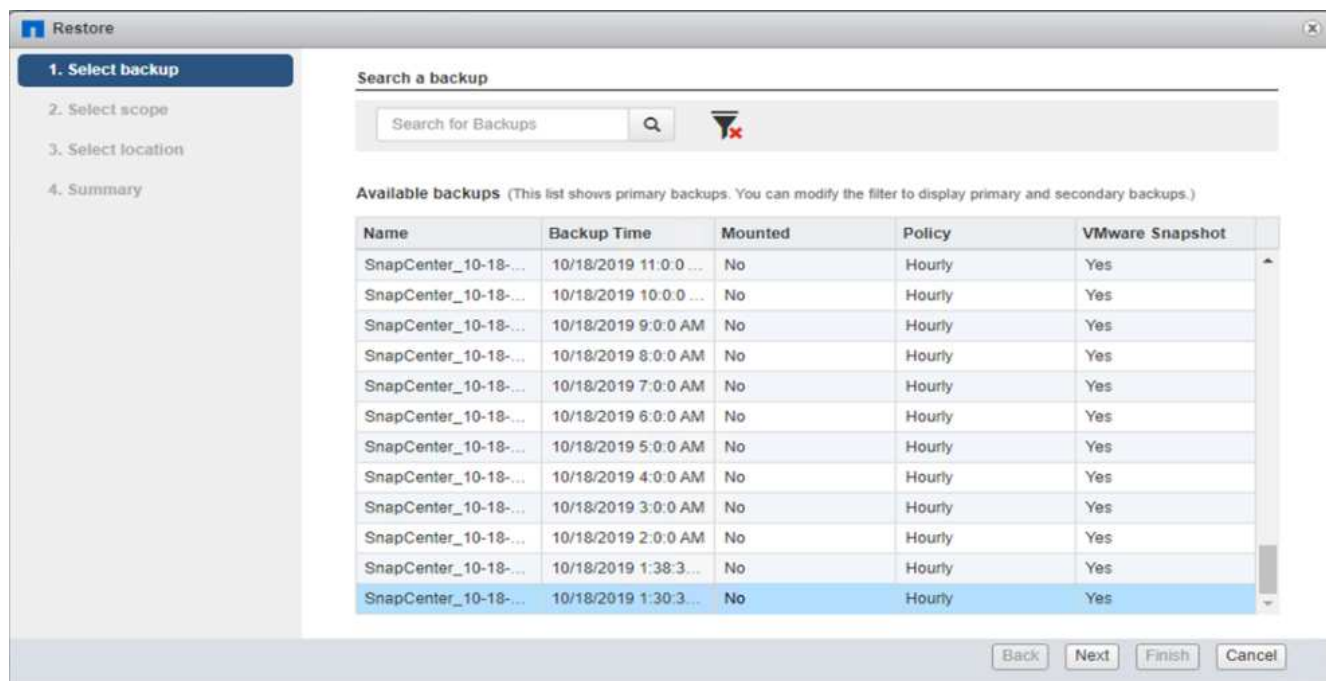
還原VM

若要還原VM、請完成下列步驟：

1. 使用SnapCenter 您使用NetApp建立的Snapshot複本來還原VM。



2. 選取所需的VMware一致Snapshot複本進行還原。



3. 整個VM都會還原並重新啟動。

The screenshot shows the 'Restore' wizard window. On the left, a sidebar lists four steps: 1. Select backup, 2. Select scope (highlighted with a green checkmark), 3. Select location, and 4. Summary. The main area contains the following configuration options:

Restore scope	Entire virtual machine
Restored VM name	WannaCry-2016-1
ESXi host name	172.21.211.10
Restart VM	☒

At the bottom right, there are four buttons: Back, Next, Finish, and Cancel.

4. 按一下「Finish（完成）」以開始還原程序。

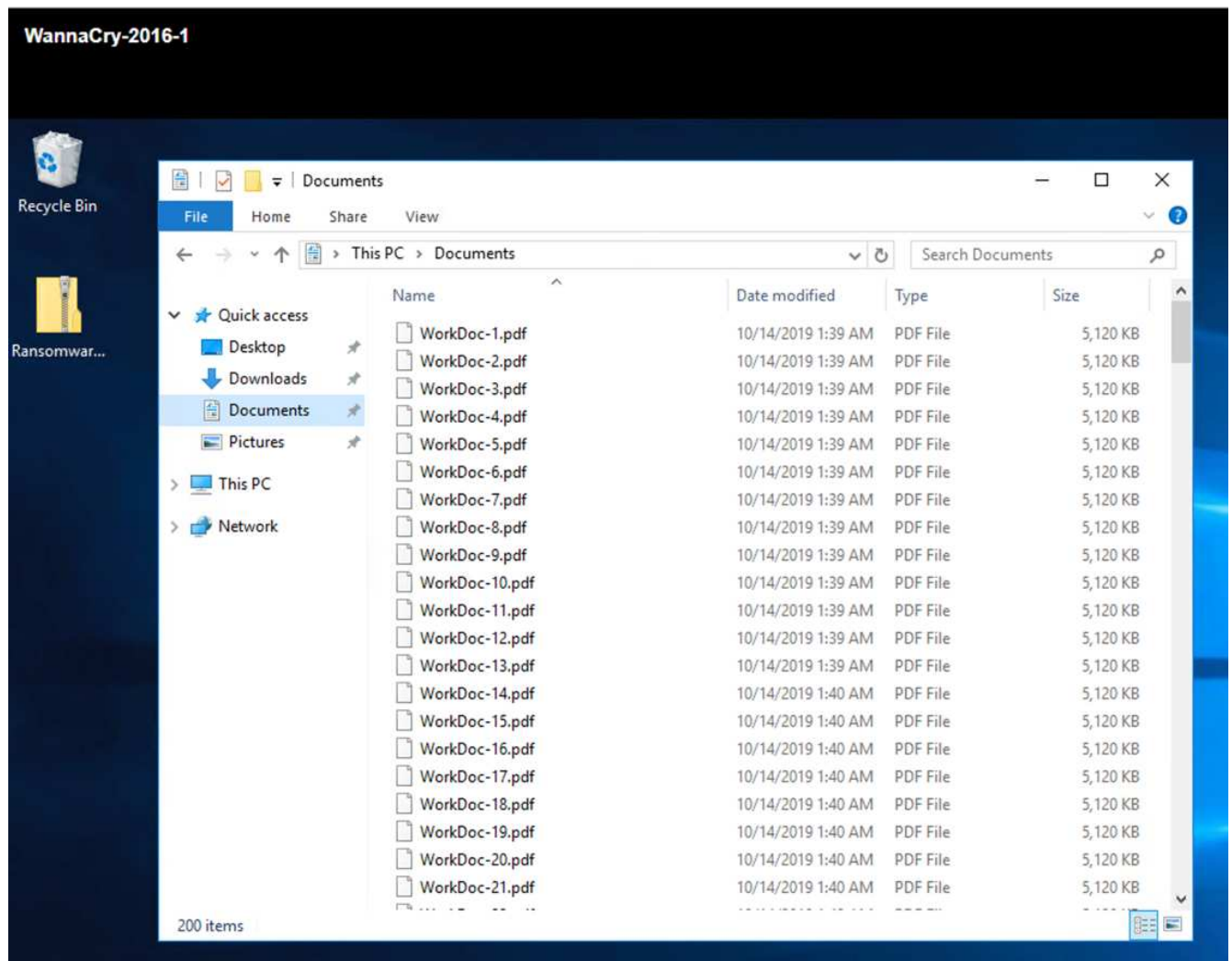
The screenshot shows the 'Restore' wizard window at the 'Summary' step. The sidebar on the left shows steps 1 through 4, all with green checkmarks, and '4. Summary' is highlighted. The main area displays a summary of the restore operation:

Virtual machine to be restored	WannaCry-2016-1
Backup name	SnapCenter_10-18-2019_01.30.35.0093
Restart virtual machine	Yes
ESXi host to be used to mount the backup	172.21.211.10

Below the summary table, there is a yellow warning icon and the text: "This virtual machine will be powered down during the process."

At the bottom right, there are four buttons: Back, Next, Finish, and Cancel.

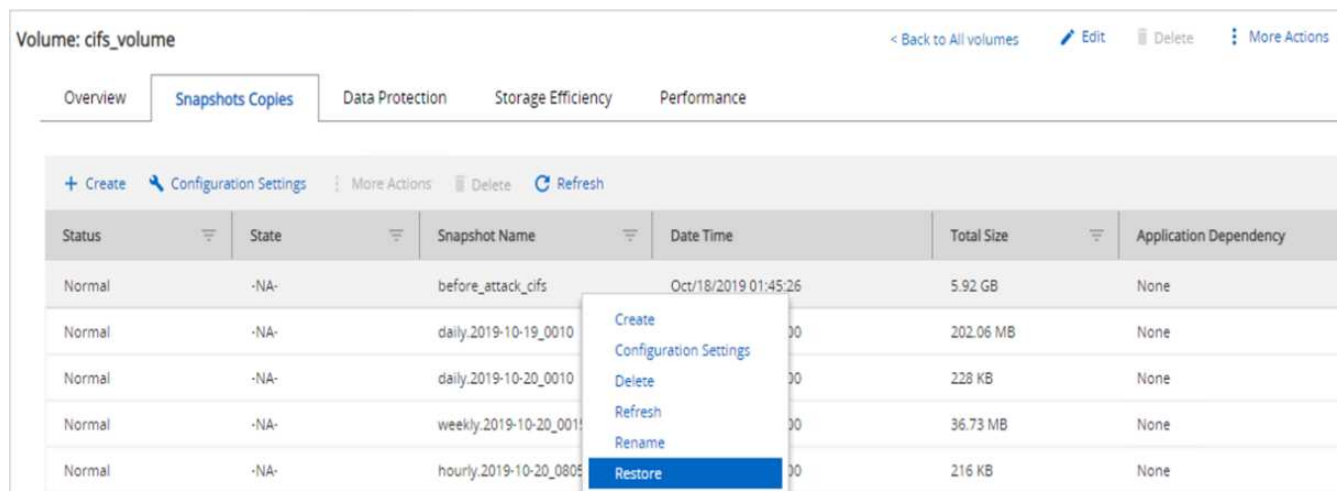
5. VM及其檔案將會還原。



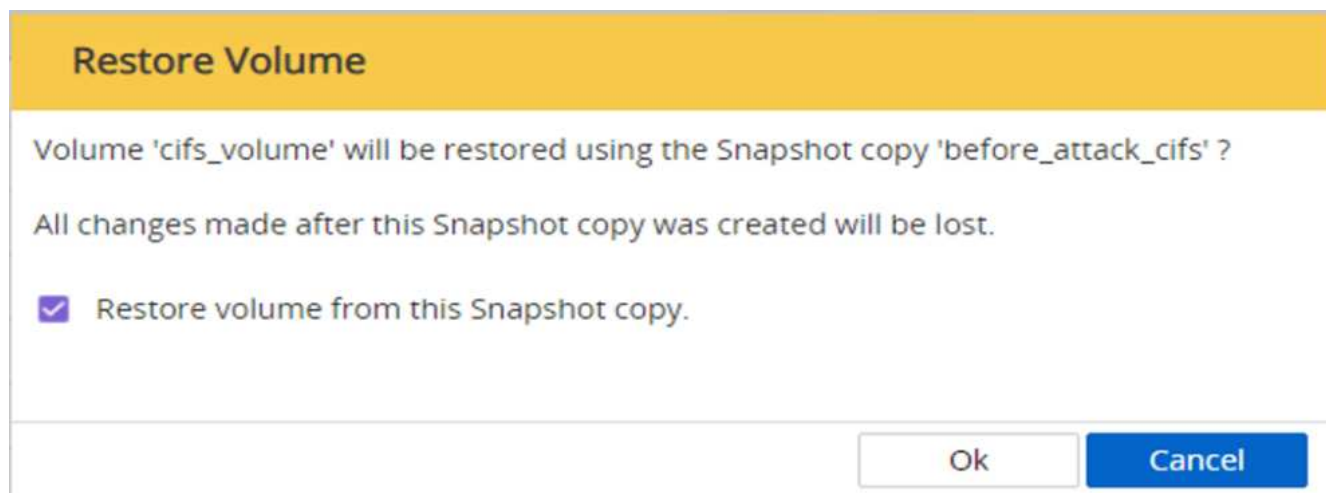
還原CIFS共用

若要還原CIFS共用區、請完成下列步驟：

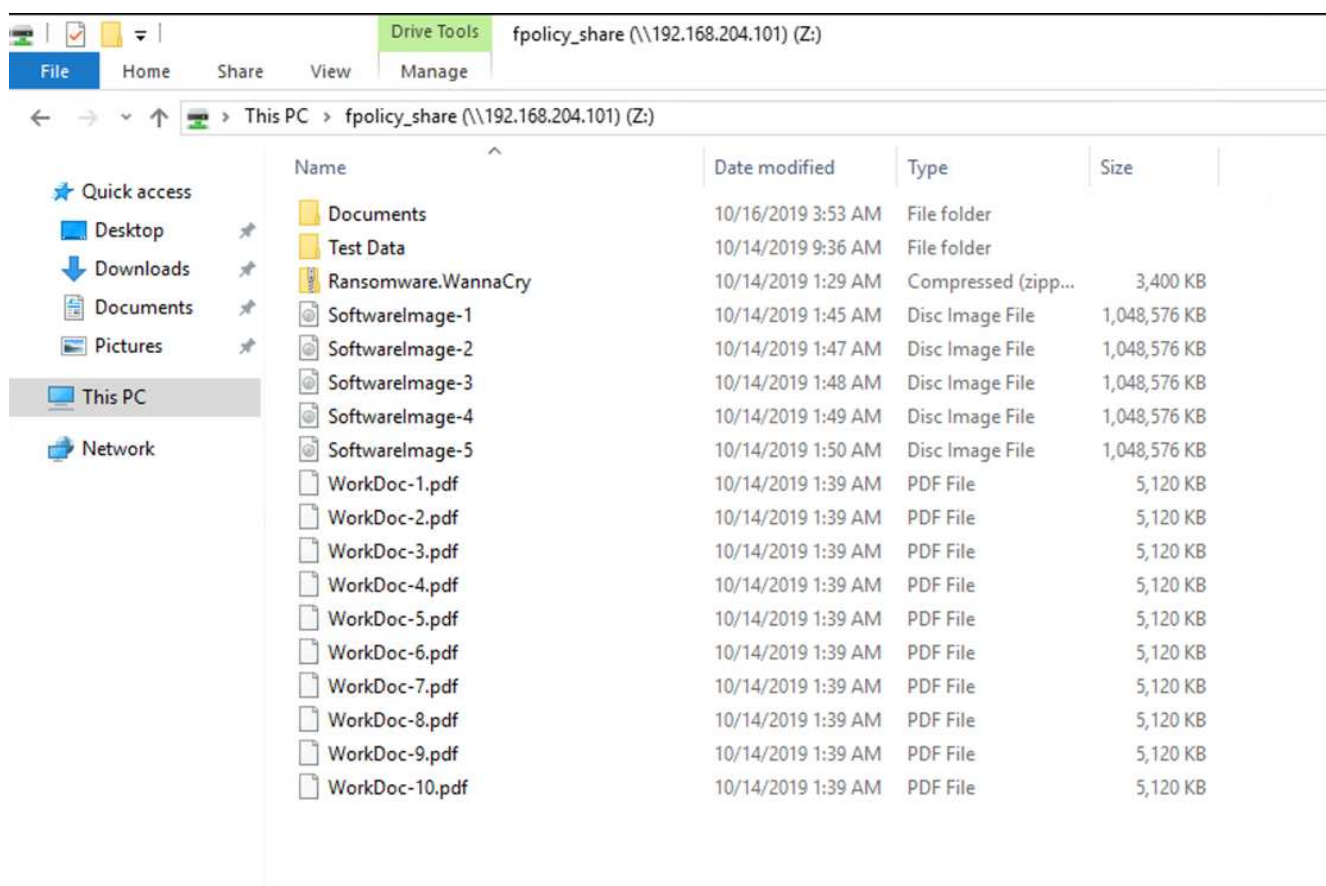
1. 使用攻擊前所取得磁碟區的Snapshot複本來還原共用區。



2. 按一下「確定」以啟動還原作業。



3. 還原後檢視CIFS共用區。



案例2：WannaCry會加密VM內的檔案系統、並嘗試加密透過FPolicy保護的對應CIFS共用

預防

設定FPolicy

若要在CIFS共用區上設定FPolicy、請在ONTAP Windows叢集上執行下列命令：

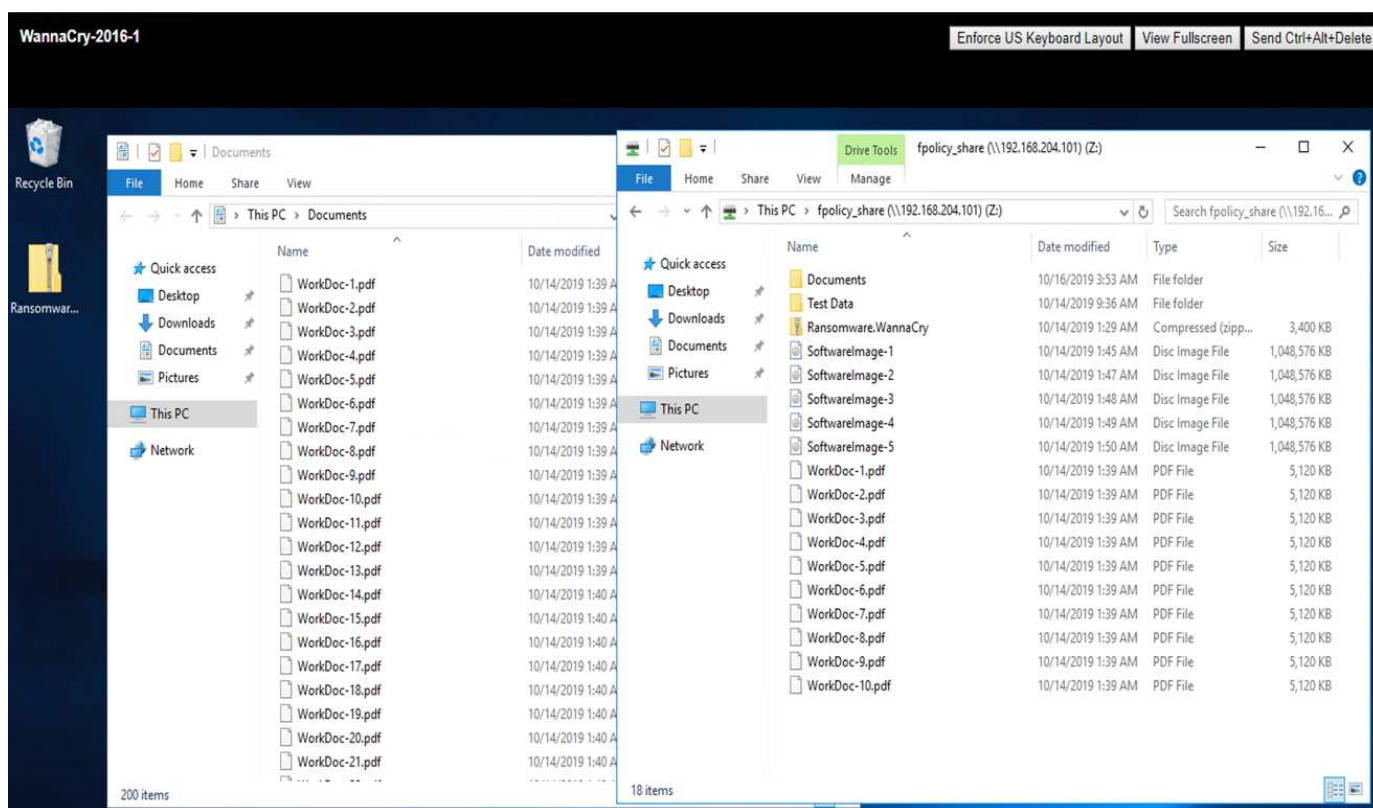
```

vserver fpolicy policy event create -vserver infra_svm -event-name
Ransomware_event -protocol cifs -file-operations create,rename,write,open
vserver fpolicy policy create -vserver infra_svm -policy-name
Ransomware_policy -events Ransomware_event -engine native
vserver fpolicy policy scope create -vserver infra_svm -policy-name
Ransomware_policy -shares-to-include fpolicy_share -file-extensions-to
-include WNCRY,Locky,ad4c
vserver fpolicy enable -vserver infra_svm -policy-name Ransomware_policy
-sequence-number 1

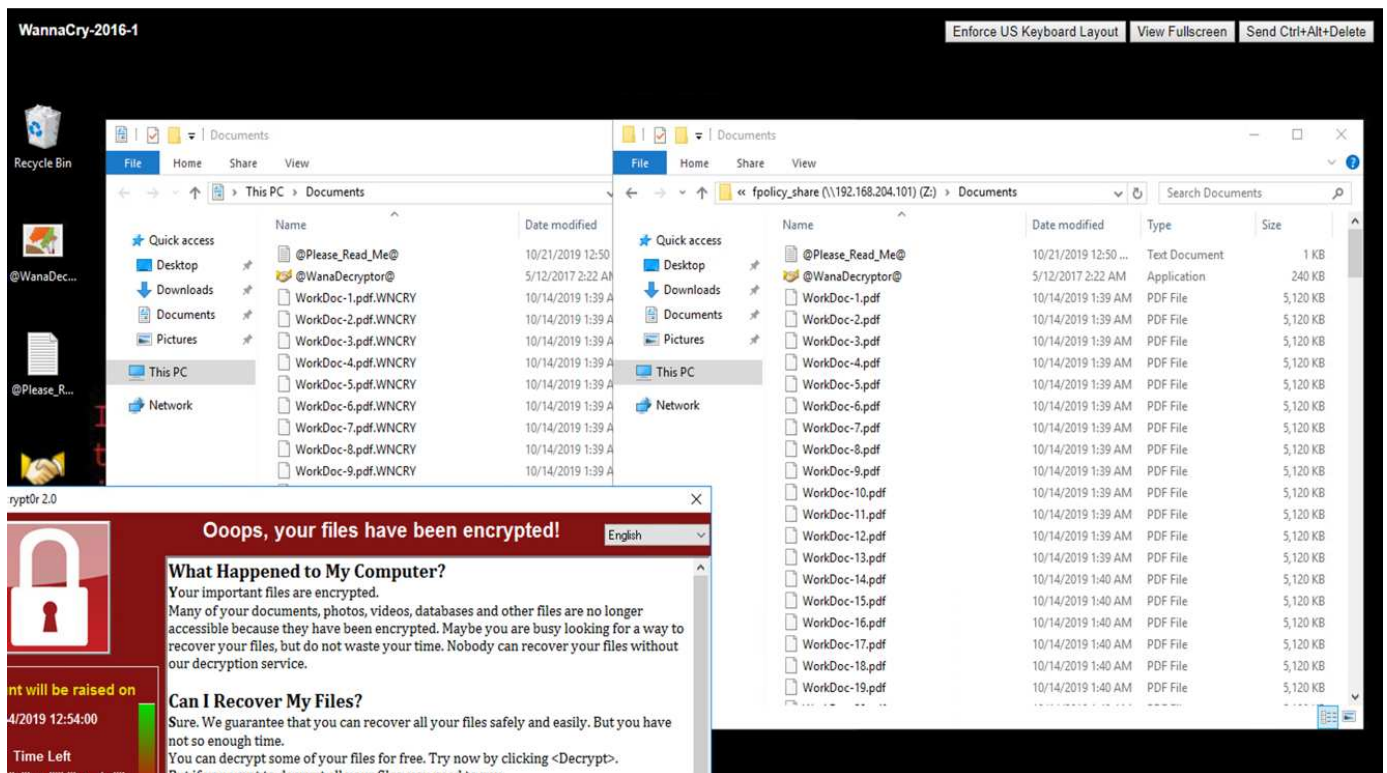
```

使用此原則時、不允許副檔名為WNCRY、Locky和ad4c的檔案執行建立、重新命名、寫入或開啟的檔案作業。

在遭受攻擊之前檢視檔案狀態、這些檔案未加密且位於乾淨的系統中。



VM上的檔案已加密。WannaCry惡意軟體嘗試加密CIFS共用區中的檔案、但FPolicy可防止其影響檔案。



無需支付贖金即可繼續營運

本文件所述的NetApp功能可協助您在攻擊發生後數分鐘內還原資料、並防止攻擊發生、讓您不受阻礙地繼續營運。

您可以設定Snapshot複本排程、以符合所需的恢復點目標（RPO）。Snapshot複製型還原作業非常快速、因此恢復時間目標（RTO）非常低。

最重要的是、您不需要支付任何攻擊所造成的贖金、也能迅速恢復正常營運。

結論

勒索軟體是有組織犯罪的產物、攻擊者的行為不符合道德規範。即使收到贖金、他們也可能不提供解密金鑰。受害者不僅遺失資料、也會損失大量金錢、並會面臨與生產資料遺失有關的後果。

根據A "Forbes文章"、只有19%的勒索軟體受害者在支付贖金後才取得資料。因此、作者建議在發生攻擊時不要支付贖金、因為這樣做可強化攻擊者對其商業模式的信心。

資料備份與還原作業是勒索軟體還原的重要部分。因此、必須將其納入業務規劃的一部分。這些作業的實作應列入預算、以便在發生攻擊時、恢復功能不會受到影響。

關鍵在於在這段旅程中選擇正確的技術合作夥伴、FlexPod 而在All Flash FAS 更新的系統中、無需額外成本、即可在原生環境中提供大部分所需的功能。

感謝

作者感謝下列人士對建立本文件的支持：

- NetApp公司的豪爾赫·高梅茲·納瓦雷特
- NetApp的Gannesh Kamath

其他資訊

若要深入瞭解本文所述資訊、請檢閱下列文件和 / 或網站：

- NetApp Snapshot軟體

["https://www.netapp.com/us/products/platform-os/snapshot.aspx"](https://www.netapp.com/us/products/platform-os/snapshot.aspx)

- 還原備份管理SnapCenter

["https://www.netapp.com/us/products/backup-recovery/snapcenter-backup-management.aspx"](https://www.netapp.com/us/products/backup-recovery/snapcenter-backup-management.aspx)

- 資料法規遵循SnapLock

["https://www.netapp.com/us/products/backup-recovery/snaplock-compliance.aspx"](https://www.netapp.com/us/products/backup-recovery/snaplock-compliance.aspx)

- NetApp 產品文件

["https://www.netapp.com/us/documentation/index.aspx"](https://www.netapp.com/us/documentation/index.aspx)

- Cisco進階惡意軟體保護（AMP）

["https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html"](https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html)

- Cisco Stealthwatch

["https://www.cisco.com/c/en_in/products/security/stealthwatch/index.html"](https://www.cisco.com/c/en_in/products/security/stealthwatch/index.html)

FIPS 140-2 FlexPod 安全性認證的醫療解決方案

TR-4892：FIPS 140-2安全性認證FlexPod 的醫療解決方案

Cisco NetApp John McAbel的JayaKishore Esanakula

《經濟與臨床健康資訊技術法案》（HITECH）要求聯邦資訊處理標準（FIPS）140至2驗證的電子保護健康資訊（ePHI）加密。健全狀況資訊技術（HIT）應用程式與軟體必須符合FIPS 140-2、才能取得促銷互通性方案（前身為「有意義的使用獎勵方案」）認證。符合資格的供應商和醫院必須使用符合FIPS 140-2（第1級）規定的醫療補助獎勵、以獲得醫療補助和醫療補助獎勵、並避免醫療補助和醫療補助中心（CMS）的補助罰金。FIPS 140-2認證的加密演算法符合技術保障要求 **"安全規則"** 《健康資訊可攜性與責任法案》（HIPAA）。

FIPS 140-2為美國政府標準、為保護敏感資訊的硬體、軟體和韌體中的密碼編譯模組設定安全需求。符合標準的規定必須由美國政府使用政府機構、也經常用於金融服務和醫療等受規範產業。本技術報告可協助讀者深入瞭解FIPS 140-2安全標準。這也有助於觀眾瞭解醫療組織所面臨的各種威脅。最後、技術報告可協助您瞭解FlexPod FIPS 140-2相容的支援功能、如何在FlexPod 部署於融合式基礎架構時、協助保護醫療資產。

範圍

本文件概述Cisco Unified Computing System (Cisco UCS)、Cisco Nexus、Cisco MDS及NetApp ONTAP FlexPod 架構的技術概況、可用於託管一或多個需要FIPS 140-2安全規範的醫療IT應用程式或解決方案。

目標對象

本文適用於醫療產業的技術領導者、以及Cisco與NetApp合作夥伴解決方案工程師與專業服務人員。NetApp假設讀者已充分瞭解運算與儲存規模的概念、以及對醫療威脅、醫療安全、醫療IT系統、Cisco UCS及NetApp儲存系統的技術熟悉度。

["下一步：醫療網路安全威脅。"](#)

醫療網路安全威脅

["上一篇：簡介。"](#)

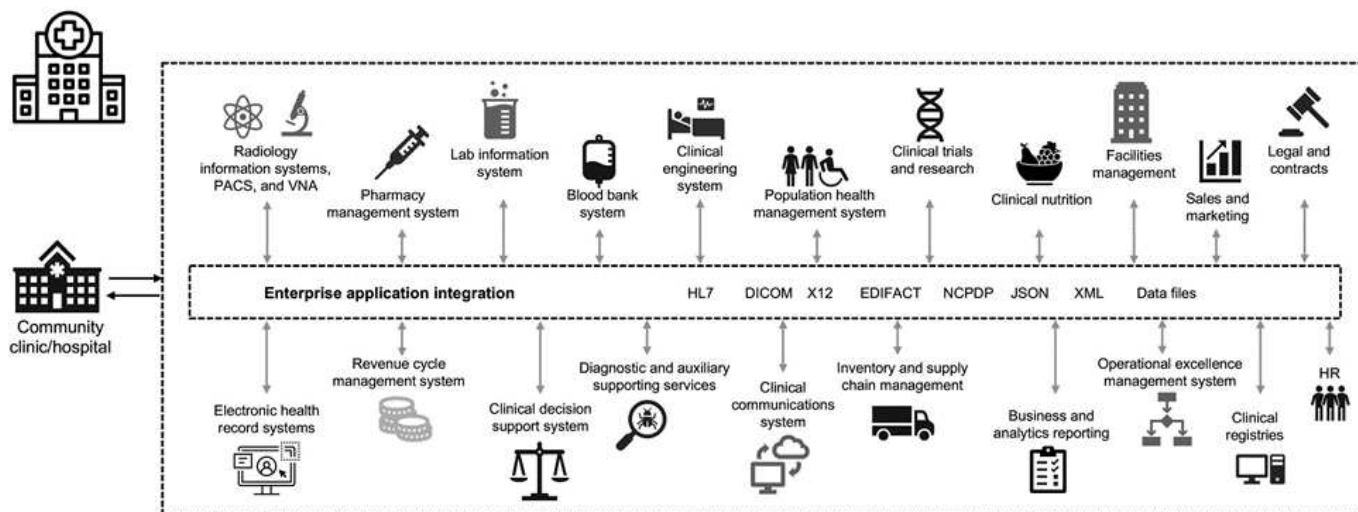
每個問題都帶來新的商機、COVID大流行病就是其中一個商機的例子。根據A ["報告"](#) 根據Health and HHS (HHS) 網路安全方案、COVID回應導致勒索軟體攻擊數量增加。在2020年3月的第三週、有6、000個新的網際網路網域已登錄。超過50%的網域託管惡意軟體。2020年、勒索軟體攻擊造成將近50%的醫療資料外洩、影響超過630家醫療機構、以及約2千9百萬筆醫療記錄。19個洩漏者/網站的勒索手法加倍。在2020年、醫療產業的資料外洩率最高、達到24.5%。

惡意代理程式試圖透過銷售資訊或威脅銷毀或揭露資訊、來破壞受保護健康資訊 (PHI) 的安全性和隱私。為了取得對ePHI的未獲授權存取、我們經常進行目標明確且大規模的廣播嘗試。2020年下半年曝露的病患記錄中、約有75%是因為業務夥伴遭到入侵。

下列醫療組織是惡意代理程式的目標對象：

- 醫院系統
- 生命科學實驗室
- 研究實驗室
- 恢復設施
- 社區醫院和診所

構成醫療組織的應用程式多樣性是無可否認的、而且複雜度也日益增加。資訊安全辦公室面臨挑戰、必須為各種IT系統和資產提供治理。下圖說明典型醫院系統的臨床功能。



病患資料是此影像的核心。病患資料遺失、以及與敏感醫療狀況相關的羞恥感、都是非常真實的。其他敏感問題包括社會排斥、勒索、檔案剖析、容易遭受目標式行銷、遭利用、以及可能對付款人造成的財務責任、使其瞭解付款人無法享有的醫療資訊。

醫療威脅的本質和影響都是多方面的。全球各國政府已頒佈多項規定、確保ePHI安全。醫療所面臨的不利影響和威脅的演變性質、讓醫療組織難以防禦所有威脅。

以下是醫療業常見威脅的清單：

- 勒索軟體攻擊
- 遺失或竊取含有敏感資訊的設備或資料
- 網路釣魚攻擊
- 攻擊可能影響病患安全的連線醫療裝置
- 電子郵件網路釣魚攻擊
- 設備或資料遺失或遭竊
- 遠端桌面傳輸協定遭到破壞
- 軟體弱點

醫療組織的營運環境與數位生態系統一樣複雜、而且是在法律和法規環境中運作。此環境包括但不限於下列項目：

- 國家協調員辦公室（醫療技術）ONC認證電子健康資訊技術互通性標準
- 醫療保險存取與兒童健康保險方案重新授權法案（MacRA）/有意義的使用
- 食品藥物管理局（FDA）規定的多重義務
- 聯合委員會的認證程序
- HIPAA要求
- HITECH需求
- 付款人可接受的最低風險標準
- 陳述隱私權與安全性規則

- 聯邦資訊安全現代化法規定、可透過國家醫療機構等機構納入聯邦合約和研究補助
- 支付卡產業資料安全標準（PCI-DSS）
- 藥物濫用與精神健康服務管理（SAMHSA）要求
- 金融處理的Gramm-Leach-Bliley法案
- 《標誌法》與向附屬組織提供服務有關
- 參與高等教育機構的《家庭教育權利與隱私權法案》（FERPA）
- 基因資訊不受歧視法（GINA）
- 歐盟新的一般資料保護規範（GDPR）

安全架構標準正快速演進、以防止惡意行為者影響醫療資訊系統。其中一項標準是FIPS 140-2、由國家標準與技術研究所（NIST）定義。FIPS出版物140-2詳述美國加密模組的政府要求。安全性需求涵蓋與加密模組安全設計及實作相關的領域、並可套用至受影響的領域。定義完善的密碼編譯邊界可讓安全管理更輕鬆、同時維持加密模組的最新狀態。這些界限有助於防止惡意行為者容易利用的薄弱加密模組。管理標準密碼編譯模組時、也有助於避免人為錯誤。

NIST與Communications Security之建立（CSE）已建立密碼編譯模組驗證方案（CMVP）、以驗證FIPS 140-2驗證層級的密碼編譯模組。聯邦組織必須使用FIPS 140-2認證模組、在閒置和移動時、都必須保護敏感或寶貴的資料。由於其成功保護敏感或寶貴資訊、許多醫療系統選擇使用FIPS 140-2密碼編譯模組來加密ePHI、使其超越法律規定的最低安全層級。

善用FlexPod 及實作FIPS 140-2功能只需數小時（而非數天）。無論規模大小、大多數醫療組織都能順利達成FIPS標準。透過清楚定義的密碼編譯界限、以及妥善記錄且簡單的實作步驟、符合FIPS 140-2的FlexPod 整套架構可為基礎架構奠定堅實的安全基礎、並可進行簡單的增強功能、進一步加強安全威脅的保護。

["下一步：FIPS 140-2概述。"](#)

FIPS 140-2總覽

["上一篇：醫療網路安全威脅。"](#)

"FIPS 140-2" 指定安全系統內用於保護電腦和電信系統中敏感資訊的密碼編譯模組安全需求。密碼編譯模組應為一組硬體、軟體、韌體或組合。FIPS適用於密碼編譯邊界內的密碼編譯演算法、金鑰產生和金鑰管理程式。請務必瞭解FIPS 140-2特別適用於密碼編譯模組、而非產品、架構、資料或生態系統。密碼編譯模組是本文稍後以關鍵詞彙定義的元件（無論是硬體、軟體及/或韌體）、可實作核准的安全功能。此外、FIPS 140-2指定四個層級。核准的密碼編譯演算法適用於所有層級。每個安全層級的關鍵要素與要求包括：

- 安全等級1
 - 指定密碼編譯模組的基本安全需求（至少需要一個核准的演算法或安全功能）。
 - 除了正式作業層級元件的基本需求之外、不需要針對層級1指定實體安全機制。
- 安全等級2
 - 透過使用防竄改解決方案（例如塗層或密封、可拆式機箱蓋或密碼模組門鎖）來增加防竄改證據的需求、進而強化實體安全機制。
 - 至少需要角色型存取控制（RBAC）、密碼編譯模組會驗證操作者或管理員的授權、以承擔特定角色並執行一組對應的功能。

- 安全等級3

- 建置於層級2的防竄改要求之上、並嘗試防止進一步存取密碼編譯模組內的關鍵安全參數（CSP）。
- 第3級所需的實體安全機制、是為了能夠偵測並回應實體存取嘗試、或是密碼編譯模組的任何使用或修改。例如強式機箱、竄改偵測和回應電路、可在密碼編譯模組上開啟卸除式機箱蓋時、將所有純文字CSP歸零。
- 需要身分識別型驗證機制、以強化第2層所指定之RBAC機制的安全性。密碼編譯模組會驗證操作員的身分、並驗證操作員是否有權使用角色並執行角色的功能。

- 安全等級4

- FIPS 140-2的最高安全等級。
- 最適合實體無保護環境中的作業層級。
- 在此層級、實體安全機制旨在提供密碼編譯模組的完整保護、以偵測及回應任何未獲授權的實體存取嘗試。
- 密碼編譯模組的滲透或曝險應具有很高的偵測機率、並導致所有不安全或純文字CSP立即歸零。

["下一步：控制面與資料面。"](#)

控制面與資料面

["上一篇：FIPS 140-2概述。"](#)

實作FIPS 140-2策略時、務必瞭解受到保護的內容。這很容易分成兩個領域：控制面板和資料平面。控制面板是指影響FlexPod 到元件在整個過程中的控制和操作的層面：例如、NetApp儲存控制器、Cisco Nexus交換器和Cisco UCS伺服器的管理存取。此層的保護是透過限制管理員可用來連線至裝置和進行變更的傳輸協定和密碼編譯密碼編譯器來提供。資料平面是指FlexPod 真實資訊、例如、在整個系統內的PHI。這是透過加密靜止的資料以確保使用中的密碼編譯模組符合標準來保護的。

["下一步：FlexPod Cisco UCS運算與FIPS 140-2。"](#)

Cisco UCS運算與FIPS 140-2 FlexPod

["上一個：控制面與資料平面。"](#)

可利用符合FIPS 140-2標準的Cisco UCS伺服器來設計一套架構。FlexPod美國美國NIST、Cisco UCS伺服器可在FIPS 140-2第1級法規遵循模式下運作。如需FIPS相容Cisco元件的完整清單、請參閱 ["Cisco FIPS 140頁面"](#)。Cisco UCS Manager已通過FIPS 140-2驗證。

Cisco UCS與Fabric互連

Cisco UCS Manager是從Cisco Fabric Interconnects（FIS）部署及執行。

如需Cisco UCS及如何啟用FIPS的詳細資訊、請參閱 ["Cisco UCS Manager文件"](#)。

若要在每個Fabric A和B的Cisco Fabric互連上啟用FIPS模式、請執行下列命令：

```
fp-health-fabric-A# connect local-mgmt
fp-health-fabric-A(local-mgmt)# enable fips-mode
FIPS mode is enabled
```



若要將Cisco UCS Manager 3.2版（3）叢集上的FI替換為Cisco UCS Manager 3.2版（3）之前的版本上的FI、請先在現有的FI上停用FIPS模式（停用「FIPS模式」）、再將替換的FI新增至叢集。建立叢集之後、Cisco UCS Manager開機時、FIPS模式會自動啟用。

Cisco提供下列關鍵產品、可在運算或應用程式層中實作：

- *適用於端點的Cisco進階惡意軟體保護（AMP）。*此解決方案支援Microsoft Windows與Linux作業系統、整合了預防、偵測與回應功能。此安全軟體可防止資料外洩、在進入點封鎖惡意軟體、並持續監控及分析檔案與處理活動、以快速偵測、控制及補救可能規避第一線防禦的威脅。AMP的惡意活動保護（MAP）元件會持續監控所有端點活動、並提供執行時間偵測、並封鎖端點上執行中程式的異常行為。例如、當端點行為顯示勒索軟體時、會終止違規的程序、以防止端點加密並停止攻擊。
- *電子郵件安全的AMP。*電子郵件已成為傳播惡意軟體及進行網路攻擊的主要工具。平均而言、每天大約會交換1000億封電子郵件、讓攻擊者能夠在使用者的系統中擁有絕佳的滲透率。因此、防禦這類攻擊是絕對必要的。擴大分析電子郵件中的威脅、例如零時差攻擊、以及隱藏在惡意附件中的惡意軟體。它也使用領先業界的URL情報來對抗惡意連結。它能夠為使用者提供進階保護、防止針對性網頁仿冒、勒索軟體及其他複雜的攻擊。
- 新一代入侵防禦系統（**NGIPS**）。Cisco火力NGIPS可部署為資料中心的實體應用裝置、或部署為VMware上的虛擬應用裝置（NGIPSv for VMware）。這套高效率的入侵防禦系統可提供可靠的效能、並降低總體擁有成本。您可以選擇訂閱授權來擴充威脅保護、以提供擴大的應用程式可見度與控制能力、以及URL篩選功能。虛擬化的NGIPS會檢查虛擬機器（VM）之間的流量、並使在資源有限的站台上部署和管理NGIPS解決方案變得更容易、同時增加實體與虛擬資產的保護。

"下一步：FlexPod Cisco網路功能與FIPS 140-2。"

Cisco網路與FIPS 140-2 FlexPod

"先前版本：FlexPod Cisco UCS運算與FIPS 140-2。"

Cisco MDS

Cisco MDS 9000系列平台搭配8.4.x軟體 "符合FIPS 140-2"。Cisco MDS可實作密碼編譯模組、以及下列適用於v3和SSH的服務。

- 支援每項服務的工作階段建立
- 所有基礎密碼編譯演算法均支援每項服務金鑰推導功能
- 每項服務的雜湊
- 每項服務的對稱加密

啟用FIPS模式之前、請先在MDS交換器上完成下列工作：

1. 請將密碼長度至少設定為八個字元。
2. 停用遠端登入。使用者應僅使用SSH登入。

3. 透過RADIUS / TACACS +停用遠端驗證。只有交換器本機的使用者才能通過驗證。
4. 停用SNMP v1和v2。交換器上任何已設定為使用v3的現有使用者帳戶、應僅設定為使用SHa進行驗證、使用AES-3DES進行隱私權設定。
5. 停用VRRP。
6. 刪除所有具有用於驗證的MD5或用於加密的Des的IKE原則。修改原則、使其使用SHa進行驗證、並使用3ES/AES進行加密。
7. 刪除所有SSH伺服器RSA1金鑰組。

若要啟用FIPS模式並在MDS交換器上顯示FIPS狀態、請完成下列步驟：

1. 顯示FIPS狀態。

```
MDSSwitch# show fips status
FIPS mode is disabled
MDSSwitch# conf
Enter configuration commands, one per line.  End with CNTL/Z.
```

2. 設定2048位元SSH金鑰。

```
MDSSwitch(config)# no feature ssh
XML interface to system may become unavailable since ssh is disabled
MDSSwitch(config)# no ssh key
MDSSwitch(config)# show ssh key
*****
could not retrieve rsa key information
bitcount: 0
*****
could not retrieve dsa key information
bitcount: 0
*****
no ssh keys present. you will have to generate them
*****
MDSSwitch(config)# ssh key
dsa    rsa
MDSSwitch(config)# ssh key rsa 2048 force
generating rsa key(2048 bits).....
...
generated rsa key
```

3. 啟用FIPS模式。

```
MDSSwitch(config)# fips mode enable
FIPS mode is enabled
System reboot is required after saving the configuration for the system
to be in FIPS mode
Warning: As per NIST requirements in 6.X, the minimum RSA Key Size has
to be 2048
```

4. 顯示FIPS狀態。

```
MDSSwitch(config)# show fips status
FIPS mode is enabled
MDSSwitch(config)# feature ssh
MDSSwitch(config)# show feature | grep ssh
sshServer          1          enabled
```

5. 將組態儲存至執行中的組態。

```
MDSSwitch(config)# copy ru st
[#####] 100%
exitCopy complete.
MDSSwitch(config)# exit
```

6. 重新啟動MDS交換器

```
MDSSwitch# reload
This command will reboot the system. (y/n)? [n] y
```

7. 顯示FIPS狀態。

```
Switch(config)# fips mode enable
Switch(config)# show fips status
```

如需詳細資訊、請參閱 ["啟用FIPS模式"](#)。

Cisco Nexus

Cisco Nexus 9000系列交換器（9.3版） ["符合FIPS 140-2"](#)。Cisco Nexus可為v3和SSH實作密碼編譯模組及下列服務。

- 支援每項服務的工作階段建立
- 所有基礎密碼編譯演算法均支援每項服務金鑰推導功能

- 每項服務的雜湊
- 每項服務的對稱加密

啟用FIPS模式之前、請先在Cisco Nexus交換器上完成下列工作：

1. 停用遠端登入。使用者應僅使用Secure Shell (SSH) 登入。
2. 停用SNMPv1和v2。裝置上任何已設定為使用v3的現有使用者帳戶、應僅設定為使用SHA進行驗證、使用AES-3DES進行隱私。
3. 刪除所有SSH伺服器RSA1金鑰配對。
4. 啟用HMA-SHA1訊息完整性檢查 (MIC)、以便在Cisco信任安全性關聯傳輸協定 (SAP) 協商期間使用。若要這麼做、請從「CTS-MANUAL」或「CTS-DOT1x」模式輸入SAP雜湊演算法「HMA-SHA-1」命令。

若要在Nexus交換器上啟用FIPS模式、請完成下列步驟：

1. 設定2048位元SSH金鑰。

```
NexusSwitch# show fips status
FIPS mode is disabled
NexusSwitch# conf
Enter configuration commands, one per line.  End with CNTL/Z.
```

2. 設定2048位元SSH金鑰。

```
NexusSwitch(config)# no feature ssh
XML interface to system may become unavailable since ssh is disabled
NexusSwitch(config)# no ssh key
NexusSwitch(config)# show ssh key
*****
could not retrieve rsa key information
bitcount: 0
*****
could not retrieve dsa key information
bitcount: 0
*****
no ssh keys present. you will have to generate them
*****
NexusSwitch(config)# ssh key
dsa    rsa
NexusSwitch(config)# ssh key rsa 2048 force
generating rsa key(2048 bits).....
...
generated rsa key
```

3. 啟用FIPS模式。

```

NexusSwitch(config)# fips mode enable
FIPS mode is enabled
System reboot is required after saving the configuration for the system
to be in FIPS mode
Warning: As per NIST requirements in 6.X, the minimum RSA Key Size has
to be 2048
Show fips status
NexusSwitch(config)# show fips status
FIPS mode is enabled
NexusSwitch(config)# feature ssh
NexusSwitch(config)# show feature | grep ssh
sshServer          1          enabled
Save configuration to the running configuration
NexusSwitch(config)# copy ru st
[#####] 100%
exitCopy complete.
NexusSwitch(config)# exit

```

4. 重新啟動Nexus交換器。

```

NexusSwitch# reload
This command will reboot the system. (y/n)? [n] y

```

5. 顯示FIPS狀態。

```

NexusSwitch(config)# fips mode enable
NexusSwitch(config)# show fips status

```

此外、Cisco NX OS軟體支援NetFlow功能、可增強偵測網路異常狀況與安全性。NetFlow會擷取網路上每個對話的中繼資料、通訊相關各方、使用的傳輸協定、以及交易持續時間。在彙總和分析資訊之後、即可深入瞭解正常行為。收集到的資料也能辨識可疑的活動模式、例如惡意軟體散佈於整個網路、否則可能無法察覺。NetFlow使用流程來提供網路監控的統計資料。流程是一種單向封包串流、傳入來源介面（或VLAN）、金鑰的值相同。金鑰是封包內欄位的識別值。您可以使用流程記錄來建立流程、以定義流程的獨特按鍵。您可以使用流程匯出器、將NetFlow為流程收集的資料匯出至遠端NetFlow收集器、例如Cisco Stealthwatch。Stealthwatch會使用此資訊持續監控網路、並在發生勒索軟體疫情時提供即時威脅偵測和事件回應證明。

"下一步：FlexPod NetApp ONTAP 不再是NetApp的不二儲存設備、以及FIPS 140-2。"

NetApp的不二儲存和FIPS 140-2 FlexPod ONTAP

"先前版本：FlexPod Cisco網路功能與FIPS 140-2。"

NetApp提供多種硬體、軟體和服務、包括根據標準驗證的密碼模組的各種元件。因此、NetApp針對控制面板和資料層面、採用多種FIPS 140-2法規遵循方法：

- NetApp提供的加密模組已達到傳輸中資料與閒置資料加密的層級1驗證。
- NetApp同時取得由這些元件供應商驗證的FIPS 140-2硬體和軟體模組。例如、NetApp儲存加密解決方案運用FIPS第2級驗證磁碟機。
- 即使產品或功能不在驗證範圍內、NetApp產品仍可使用符合標準的已驗證模組。例如、NetApp Volume Encryption (NVE) 符合FIPS 140-2標準。雖然未分別驗證、但它採用NetApp密碼編譯模組、已通過層級1驗證。如需瞭解ONTAP 您版本的更新法規遵循細節、請聯絡FlexPod 您的支援中心。
- NetApp密碼編譯模組已通過FIPS 140-2第1級驗證*
- NetApp密碼編譯安全模組 (NCSM) 已通過FIPS 140-2第1級驗證。
- NetApp自我加密磁碟機已通過FIPS 140-2第2級驗證*

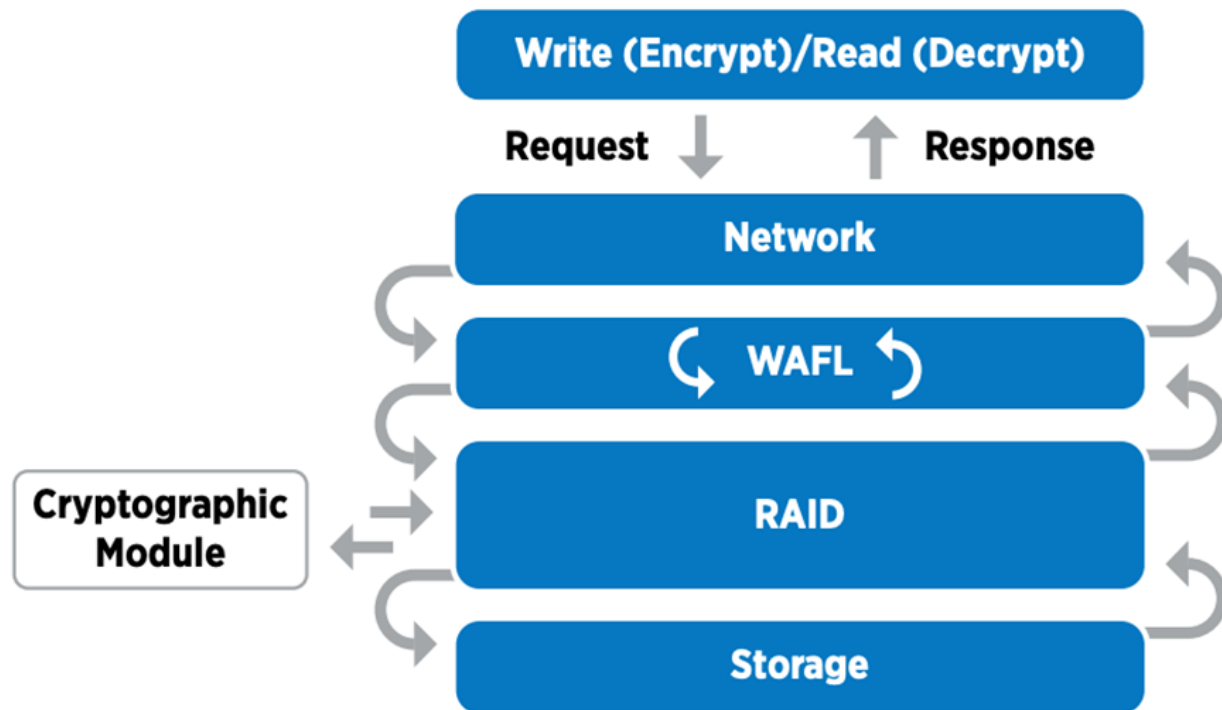
NetApp購買通過原始設備製造商 (OEM) 驗證的FIPS 140-2自加密磁碟機 (SED) ；尋求這些磁碟機的客戶必須在訂購時指定它們。磁碟機已在層級2驗證。下列NetApp產品可運用已驗證的SED：

- A系列與不完整的儲存系統AFF FAS
- E系列與EF系列儲存系統
- NetApp Aggregate Encryption與NetApp Volume Encryption*

NVE和NetApp Aggregate Encryption (NAE) 技術可分別在磁碟區和Aggregate層級加密資料、使解決方案不受實體磁碟機限制。

NVE是以軟體為基礎的靜止資料加密解決方案、從ONTAP 推出時起即為供應、ONTAP 且自推出版本號為2時起、已符合FIPS 140-2標準。NVE可ONTAP 加密每個磁碟區的資料、以達到精細度。Nae搭配ONTAP 使用NetApp 9.6、是NVE的一大優點；ONTAP 它可加密每個Volume的資料、而且磁碟區可在整個集合體之間共用金鑰。NVE 和 NAE 都使用 AES 256 位元加密。資料也可以儲存在磁碟上、而不需使用SED。NVE和NAE可讓您在啟用加密時使用儲存效率功能。只有應用程式層的加密技術、會讓儲存效率的所有效益都失去。有了NVE和NAE、儲存效率就能維持不變、因為資料是從網路經由NetApp WAFL ENetApp傳送到RAID層、而RAID層決定資料是否應加密。為了提高儲存效率、您可以搭配NAE使用Aggregate重複資料刪除技術。NVE磁碟區和NAE磁碟區可共存於同一個NAE Aggregate上。Nae Aggregate不支援未加密的磁碟區。

流程運作方式如下：資料加密後、會傳送至FIPS 140-2層級1驗證的密碼編譯模組。加密模組會加密資料、然後將其傳回RAID層。加密資料隨即傳送至磁碟。因此、結合NVE和NAE、資料在磁碟的傳輸過程中就已加密。讀取依循相反路徑。換句話說、資料會保留加密磁碟、傳送至RAID、由加密模組解密、然後傳送至堆疊的其餘部分、如下圖所示。



NVE使用經FIPS 140-2第1級驗證的軟體密碼編譯模組。

如需 NVE 的詳細資訊、請參閱 ["NVE資料表"](#)。

NVE可保護雲端中的資料。支援支援FIPS 140-2的資料加密功能。Cloud Volumes ONTAP Azure NetApp Files

從推出更新版本的支援方案開始、新建立的Aggregate和Volume會在您擁有NVE授權、以及內建或外部金鑰管理時、依預設進行加密。ONTAP從推出更新至更新、您可以使用Aggregate層級的加密功能、將金鑰指派給內含的Aggregate、以供加密的磁碟區使用。ONTAP您在Aggregate中建立的磁碟區預設會加密。加密磁碟區時、您可以覆寫預設值。

NAE CLI命令ONTAP

在執行下列CLI命令之前、請先確認叢集具有所需的NVE授權。

若要建立並加密Aggregate、請執行下列命令（在ONTAP 更新版本的叢集CLI上執行時）：

```
fp-health::> storage aggregate create -aggregate aggregatename -encrypt
-with-aggr-key true
```

若要將非NAE Aggregate轉換成NAE Aggregate、請執行下列命令（在ONTAP 更新版本的叢集CLI上執行時）：

```
fp-health::> storage aggregate modify -aggregate aggregatename -node
svmname -encrypt-with-aggr-key true
```

若要將NAE Aggregate轉換成非NAE Aggregate、請執行下列命令（在ONTAP 更新版本的叢集CLI上執行）：

```
fp-health::> storage aggregate modify -aggregate aggregatename -node  
svmname -encrypt-with-aggr-key false
```

支援NVE CLI命令ONTAP

從推出更新至更新、您可以使用Aggregate層級的加密功能、將金鑰指派給內含的Aggregate、以供加密的磁碟區使用。ONTAP您在Aggregate中建立的磁碟區預設會加密。

若要在已啟用NAE的集合體上建立磁碟區、請執行下列命令（在ONTAP 使用支援該功能的版本的叢集CLI上執行時）：

```
fp-health::> volume create -vserver svmname -volume volumename -aggregate  
aggregatename -encrypt true
```

若要在不移動磁碟區的情況下加密現有的磁碟區、請執行下列命令（在ONTAP 更新版本的叢集CLI上執行時）：

```
fp-health::> volume encryption conversion start -vserver svmname -volume  
volumename
```

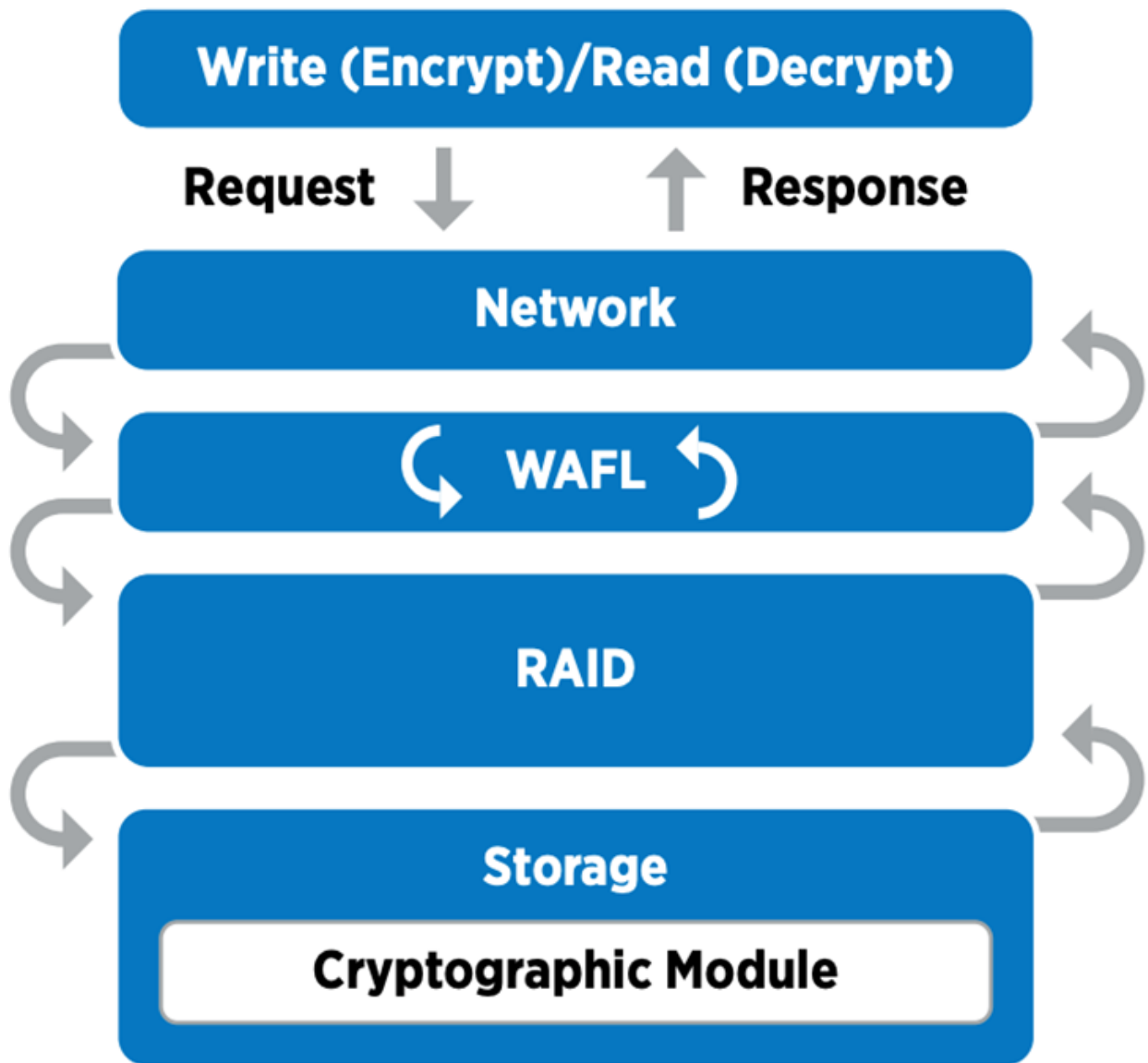
若要驗證磁碟區是否已啟用加密、請執行下列CLI命令：

```
fp-health::> volume show -is-encrypted true
```

NSE

NSE使用SED透過硬體加速機制執行資料加密。

NSE的設定是使用FIPS 140-2 Level 2自我加密磁碟機、透過AES 256位元透明磁碟加密來保護閒置的資料、以利法規遵循與備用磁碟的傳回。磁碟機會在內部執行所有的資料加密作業、如下圖所示、包括產生加密金鑰。為了防止未獲授權的資料存取、儲存系統必須使用磁碟機第一次使用時建立的驗證金鑰來驗證磁碟機本身。



NSE會在每個磁碟機上使用硬體加密、並通過FIPS 140-2第2級驗證。

如需 NSE 的詳細資訊，請參閱 "[NSE資料表](#)"。

金鑰管理

FIPS 140-2標準適用於邊界所定義的密碼編譯模組、如下圖所示。

2.1.1 Cryptographic Boundary

The logical cryptographic boundary of the CryptoMod module is the cryptomod_fips.ko component of ONTAP OS kernel. The logical boundary is depicted in the block diagram below. The Approved DRBG is used to supply the module's cryptographic keys. The physical boundary for the module is the enclosure of the NetApp controller.

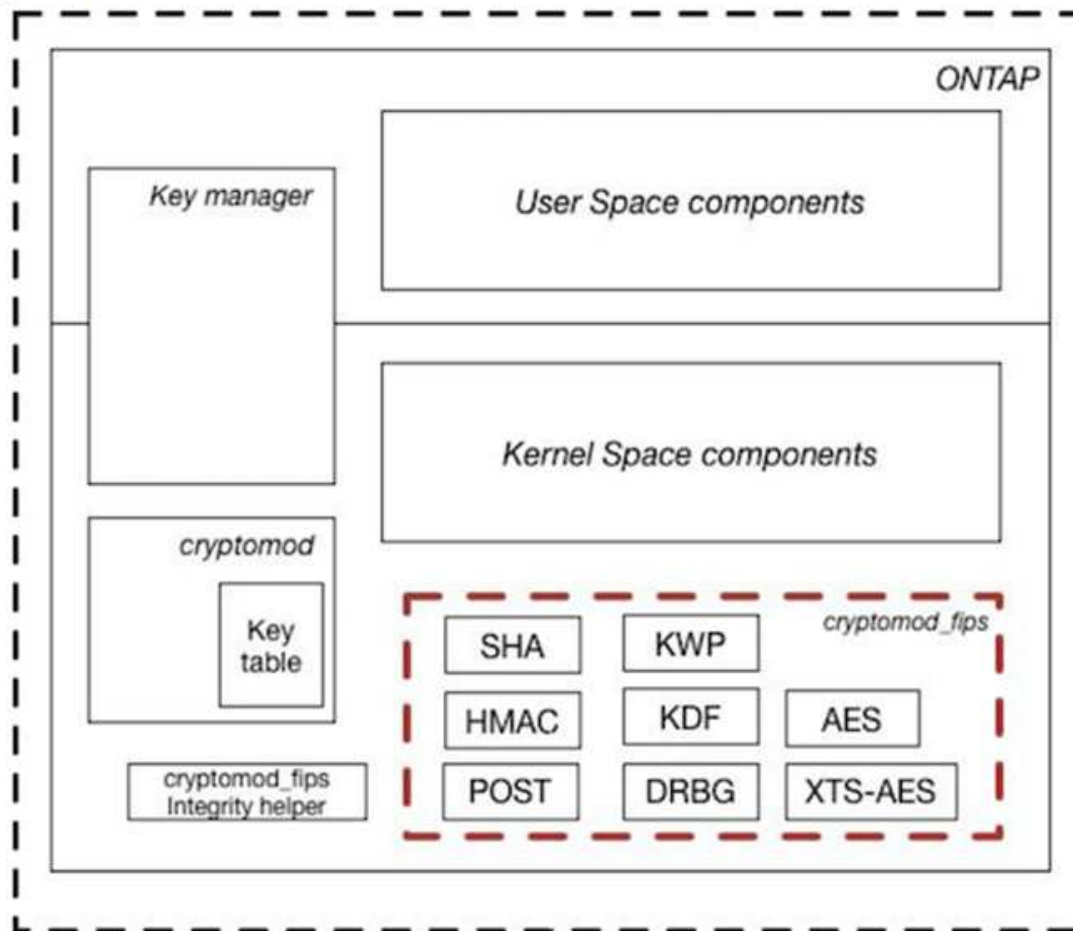


Figure 1 - Block Diagram

金鑰管理程式會追蹤ONTAP 所有由靜止所使用的加密金鑰。NSE SED使用金鑰管理程式來設定NSE SED的驗證金鑰。使用金鑰管理程式時、結合使用的NVE和NAE解決方案由軟體密碼編譯模組、加密金鑰和金鑰管理程式所組成。對於每個磁碟區、NVE都使用唯一的XTS-AES 256資料加密金鑰、金鑰管理程式會儲存此金鑰。用於資料磁碟區的金鑰對該叢集中的資料磁碟區而言是唯一的、而且會在建立加密磁碟區時產生。同樣地、NAE磁碟區每個Aggregate使用唯一的XTS-AES 256資料加密金鑰、金鑰管理程式也會儲存此金鑰。在建立加密的Aggregate時會產生Nae金鑰。不預先產生金鑰、重複使用金鑰或以純文字顯示、這些金鑰會由金鑰管理程式儲存及保護。ONTAP

支援外部金鑰管理程式

從推出支援外部關鍵管理程式的支援功能起、ONTAP NVE與NSE解決方案均支援外部關鍵管理程式。FIPS 140-2標準適用於特定廠商實作所使用的密碼編譯模組。最常見的情況FlexPod 是、客戶使用ONTAP 下列其中一項已驗證（根據 ["NetApp 互通性對照表"](#)）關鍵經理：

- Gemalto或SafeNet
- 公制（Thales）

- IBM SKLM
- Utimaco（前身為MicrofOCUS、HPE）

NSE和NVMe SED驗證金鑰會使用業界標準的OASIS金鑰管理互通性傳輸協定（KMIP）、備份至外部金鑰管理程式。只有儲存系統、磁碟機和金鑰管理程式可以存取金鑰、而且如果磁碟機移出安全性網域、就無法解除鎖定、因此可防止資料外洩。外部金鑰管理程式也會儲存NVE Volume加密金鑰和NAE Aggregate加密金鑰。如果控制器和磁碟已移動、且無法再存取外部金鑰管理程式、則無法存取NVE和NAE磁碟區、也無法解密。

下列命令範例將兩個金鑰管理伺服器新增至外部金鑰管理程式用於儲存虛擬機器（SVM）「vmname1」的伺服器清單。

```
fp-health::> security key-manager external add-servers -vserver svmname1
-key-servers 10.0.0.20:15690, 10.0.0.21:15691
```

在多租戶情境中使用某個不穩定資料中心時、由於SVM層級的安全考量、使用者可利用此功能來分隔租戶。FlexPod ONTAP

若要驗證外部金鑰管理程式清單、請執行下列CLI命令：

```
fp-health::> security key-manager external show
```

結合雙重加密（分層防禦）

如果您需要隔離資料存取、並確保資料隨時受到保護、NSE SED可與網路或網路層級的加密結合使用。如果系統管理員忘記設定或錯誤設定較高層級的加密、NSE SED就像是後置停止。對於兩個不同的加密層、您可以將NSE SED與NVE和NAE結合使用。

NetApp ONTAP 的整個叢集控制面板FIPS模式

NetApp ONTAP 支援的資料管理軟體採用FIPS模式組態、可為客戶提供更高層級的安全性。此FIPS模式僅適用於控制面板。啟用FIPS模式時、根據FIPS 140-2的關鍵元素、傳輸層安全性v1（TLSv1）和SSLv3會停用、而且只有TLS v1.1和TLS v1.2會維持啟用狀態。



FIPS模式下的整個叢集控制窗格符合FIPS 140-2第1級標準。ONTAP全叢集FIPS模式使用由NCSM提供的軟體型密碼編譯模組。

FIPS 140-2法規遵循模式、適用於叢集範圍的控制面板、可保護ONTAP 所有的資訊介面。預設會停用FIPS 140-2模式；不過、您可以針對「安全性組態修改」命令、將「啟用FIPS」參數設為「true」、以啟用此模式。

若要在ONTAP 支援FIPS的叢集上啟用FIPS模式、請執行下列命令：

```
fp-health::> security config modify -interface SSL -is-fips-enabled true
```

啟用SSL FIPS模式時、ONTAP 從支援到ONTAP 外部用戶端或不支援此功能的伺服器元件的SSL通訊、將使用FIPS Complaint密碼編譯來支援SSL。

若要顯示整個叢集的FIPS狀態、請執行下列命令：

```
fp-health::> set advanced
fp-health::*> security config modify -interface SSL -is-fips-enabled true
```

"下一步：FlexPod 解決方案優勢：融合式基礎架構。"

解決方案優勢FlexPod：融合式基礎架構

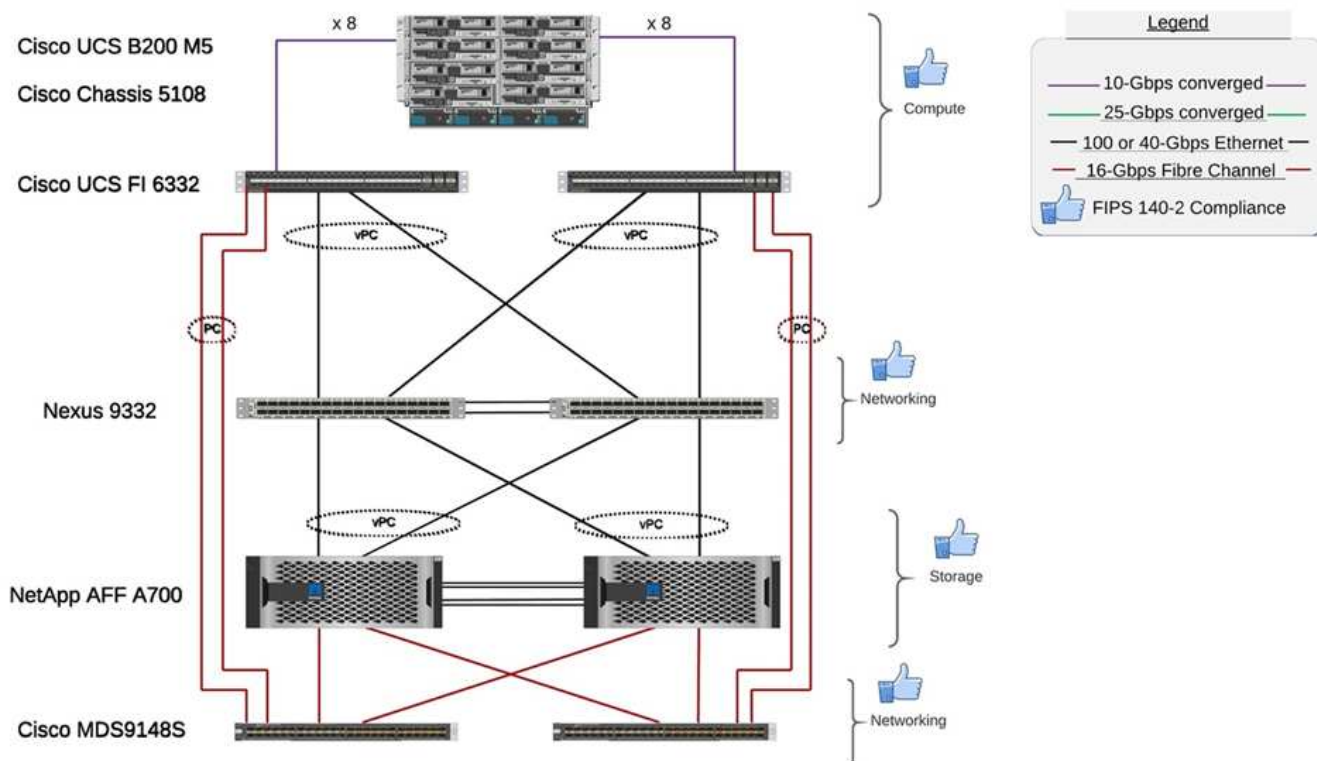
"上一篇：FlexPod NetApp ONTAP 的不整合儲存技術與FIPS 140-2。"

醫療機構擁有數個關鍵任務系統。其中兩個最重要的系統是電子醫療記錄（EHR）系統和醫療影像系統。為了在FlexPod 一個不間斷系統上示範FIPS設定、我們使用開放原始碼EHR和開放原始碼圖片歸檔與通訊系統（PACS）系統、在FlexPod 這個不間斷系統上進行實驗室設定和工作負載驗證。如需EHR功能、EHR邏輯應用程式元件的完整清單、以及EHR系統在FlexPod 整個系統上實作時的效益、請參閱 ["TR-4881：FlexPod 《電子健康記錄系統的參考》"](#)。如需醫療影像系統功能、邏輯應用程式元件的完整清單、以及實作FlexPod 於效益評估（英文）時醫療影像系統的效益、請參閱 ["TR-4865：FlexPod 醫療成像的適用對象"](#)。

在FIPS設定和工作負載驗證期間、我們運用了代表典型醫療組織的工作負載特性。例如、我們採用開放原始碼的EHR系統來納入真實的病患資料存取和變更情境。此外、我們運用醫療影像工作負載、將數位影像和通訊資料納入「*」醫療（Dicom）物件。dcm檔案格式。含有中繼資料的DICOM物件會同時儲存在檔案和區塊儲存設備上。此外、我們也從虛擬化的RedHat Enterprise Linux（RHEL）伺服器中實作多重路徑功能。我們將DICOM物件儲存在NFS上、使用iSCSI掛載LUN、以及使用FC掛載LUN。在FIPS設定與驗證期間、我們發現FlexPod 這個融合式基礎架構超越了我們的期望、而且能順暢地執行。

下圖說明FlexPod FIPS設定與驗證所用的不實系統。我們運用了 ["採用VMware vSphere 7.0與NetApp的解決方案資料中心9.7 Cisco驗證設計（CVD）FlexPod ONTAP"](#) 在設定過程中。

FIPS 140-2 security compliant FlexPod for Healthcare



解決方案基礎架構硬體與軟體元件

以下兩個圖分別列出在FlexPod 執行支援的FIPS測試期間、分別使用的硬體和軟體元件。這些表格中的建議為範例、您應該與NetApp中小型企業合作、確保這些元件適合貴組織。此外、請確定支援中的元件和版本
["NetApp 互通性對照表工具"](#) (部分) IMT 和 ["Cisco硬體相容清單 \(HCL\)"](#)。

層級	產品系列	數量與模式	詳細資料
運算	Cisco UCS 5108機箱	1或2	
	Cisco UCS刀鋒伺服器	3 B200 M5	每個處理器具有2個20個以上核心、2.7GHz及128至384GB RAM
	Cisco UCS虛擬介面卡 (VIC)	Cisco UCS 1440	請參閱
	2個Cisco UCS Fabric互連	6332	-
網路	Cisco Nexus交換器	2倍Cisco Nexus 9332	-
儲存網路	透過SMB/CIFS、NFS或iSCSI傳輸協定進行儲存存取的IP網路	與上述相同的網路交換器	-
	透過FC存取儲存設備	2個Cisco MDS 9148S	-
儲存設備	NetApp AFF 產品豐富的NetApp解決方案：A700 All Flash儲存系統	1叢集	具有兩個節點的叢集

層級	產品系列	數量與模式	詳細資料
	磁碟櫃	一個DS224C或NS224磁碟櫃	已裝滿24個磁碟機
	SSD	大於24、1.2TB或更大容量	-

軟體	產品系列	版本或版本	詳細資料
多種	Linux	RHEL 7.X	-
	Windows	Windows Server 2012 R2 (64位元)	-
	NetApp ONTAP	更新版本ONTAP	-
	Cisco UCS光纖互連	Cisco UCS Manager 4.1或更新版本	-
	Cisco乙太網路3000或9000系列交換器	9000系列、7.0 (3) i7 (7) 或更新版本適用於3000系列、9.2 (4) 或更新版本	-
	Cisco FC：Cisco MDS 9132T	8.4(1a)或更新版本	-
	Hypervisor	VMware vSphere ESXi 6.7 U2或更新版本	-
儲存設備	Hypervisor管理系統	VMware vCenter Server 6.7 U3 (vCSA) 或更新版本	-
網路	NetApp虛擬儲存主控台 (VSC)	VSC 9.7或更新版本	-
	NetApp SnapCenter	不含更新版本SnapCenter	-
	Cisco UCS Manager	4.1 (1c) 或更新版本	
Hypervisor	ESXi		
管理	Hypervisor管理系統VMware vCenter Server 6.7 U3 (vCSA) 或更新版本		
	NetApp虛擬儲存主控台 (VSC)	VSC 9.7或更新版本	
	NetApp SnapCenter	不含更新版本SnapCenter	
	Cisco UCS Manager	4.1 (1c) 或更新版本	

"下一步：其他FlexPod 的安全考量。"

其他FlexPod 的安全考量

"先前版本：FlexPod 解決方案優勢：融合式基礎架構。"

此功能為模組化、融合式、可選擇性虛擬化、可擴充（橫向擴充和垂直擴充）、以及具成本效益的平台。FlexPod有了FlexPod 這個平台、您就能獨立橫向擴充運算、網路和儲存設備、加速應用程式部署。此外、模組化架構還能在系統橫向擴充和升級活動期間、維持不斷營運。

HIT系統的不同元件需要將資料儲存在SMB/CIFS、NFS、ext4和NTFS檔案系統中。這項需求表示基礎架構必須透過NFS、CIFS和SAN傳輸協定提供資料存取。單一NetApp儲存系統可支援所有這些傳輸協定、不需要傳統的傳輸協定專用儲存系統實務做法。此外、單一NetApp儲存系統可支援多種受影響的工作負載、例如EHRs、PACS或VNA、基因組學、VDI等、提供保證且可設定的效能等級。

當部署FlexPod 在一個不受限的系統中時、HIT可提供醫療產業特有的多項優點。下列清單是這些優點的詳細說明：

- 安全。FlexPod安全性是FlexPod 整個過程的基礎。過去幾年、勒索軟體已成為威脅。勒索軟體是一種以密碼學為基礎的惡意軟體、使用密碼編譯來建置惡意軟體。此惡意軟體可以同時使用對稱和非對稱金鑰加密來鎖定受害者的資料、並要求贖金提供金鑰來解密資料。若要瞭解 FlexPod 解決方案如何協助減輕勒索軟體等威脅、請參閱 ["TR-4802：勒索軟體解決方案"](#)。FlexPod 基礎架構元件也包括 ["符合FIPS 140-2標準"](#)在內。
- * Cisco Intersight * Cisco Intersight是一款創新的雲端型管理即服務平台、提供單一窗口來進行完整堆疊FlexPod 的功能、以利進行全面的視覺化管理與協調。Intersight平台使用FIPS 140-2安全性相容的密碼編譯模組。此平台的額外管理架構使其超出某些標準或稽核的範圍、例如HIPAA。網路上的任何個人識別健全狀況資訊都不會傳送至Intersight入口網站。
- * NetApp FPolicy技術。* NetApp FPolicy（名稱檔案原則的演進）是檔案存取通知架構、可用來監控及管理NFS或SMB/CIFS傳輸協定上的檔案存取。這項技術已成為ONTAP VMware資料管理軟體的一部分超過十年、對於協助偵測勒索軟體非常有用。這款Zero Trust引擎提供額外的安全措施、超越存取控制清單（ACL）的權限。FPolicy有兩種操作模式：原生和外部：
 - 原生模式同時提供檔案副檔名的黑名單和白名單。
 - 外部模式的功能與原生模式相同、但它也與FPolicy伺服器整合、該伺服器可在ONTAP 外部執行至整個作業系統、以及安全資訊與事件管理（SIEM）系統。如需如何對抗勒索軟體的詳細資訊、請參閱 ["對抗勒索軟體：第三部分ONTAP：另一項強大的原生（又稱為免費）工具《SfPolicy》"](#) 部落格：
- 靜止資料。更新版本包含三種符合FIPS 140-2標準的靜止資料加密解決方案：ONTAP
 - NSE是使用自我加密磁碟機的硬體解決方案。
 - NVE是一種軟體解決方案、可加密任何磁碟機類型的任何資料磁碟區、每個磁碟區都有一個唯一的金鑰。
 - Nae是一種軟體解決方案、可加密任何磁碟機類型上的任何資料磁碟區、並為每個Aggregate啟用唯一金鑰。



從NetApp NVE 9.7開始ONTAP、如果已有名為VE的NetApp NVE授權套件、則預設會啟用NAE和NVE。

- 飛行中的資料。從ONTAP S9.8開始、網際網路傳輸協定安全性（IPsec）可為用戶端與ONTAP SVM之間的所有IP流量提供端點對端點加密支援。所有IP流量的IPsec資料加密包括NFS、iSCSI及SMB/CIFS傳輸協定。IPsec為iSCSI流量提供唯一的傳輸加密選項。
- 跨混合式多雲端資料架構的端點對端點資料加密。使用靜止資料加密技術（例如NSE或NVE）和叢集對等加密（CPE）來進行資料複製流量的客戶、現在可以透過升級至ONTAP RES9.8或更新版本、並使用IPsec、在混合式多雲端資料架構的用戶端與儲存設備之間使用端對端加密。從ONTAP 功能支援範圍9開始、您可以針對整個叢集的控制面板介面啟用FIPS 140-2相容模式。預設會停用FIPS 140-2模式。從推出《支援SnapMirror 9.6的支援方案》開始ONTAP、持續提供TLS 1.2 AES-256 GCM加密支援ONTAP、以支援諸如NetApp SnapMirror、NetApp SnapVault SnapMirror和NetApp FlexCache 等各種資料複製技術。加密是

透過兩個叢集對等端點之間的預先共用金鑰（PSK）來設定。

- 安全的多租戶共享。支援虛擬化伺服器與儲存共享基礎架構的需求增加、可安全地多租戶共享特定設施的資訊、尤其是在託管多個資料庫和軟體執行個體時。

"下一步：結論。"

結論

"上一篇：FlexPod 其他的不安全考量。"

透過在支援FIPS 140-2的平台上執行醫療應用程式FlexPod、您的醫療機構將獲得更好的保護。在運算、網路和儲存等每個元件上、均提供多層保護。FlexPod資料保護功能可在閒置或飛行時保護資料、並在需要時確保備份安全且準備就緒。FlexPod

運用FlexPod 通過Cisco與NetApp策略合作夥伴、經過嚴格測試的融合式基礎架構、預先驗證的NetApp設計、避免人為錯誤。設計與設計旨在提供可預測、低延遲的系統效能與高可用度、即使在運算、網路和儲存層啟用FIPS 140-2、也能發揮極低的影響。FlexPod這種方法可為您的命中率系統使用者提供優異的使用者體驗、並為其提供最佳的回應時間。

"下一步：感謝、版本歷程記錄、以及何處可以找到其他資訊。"

感謝、版本歷程記錄、以及何處可以找到其他資訊

"上一篇：結論。"

若要深入瞭解本文所述資訊、請檢閱下列文件與網站：

- Cisco MDS 9000系列NX-OS安全組態指南

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/8_x/config/security/cisco_mds9000_security_config_guide_8x/configuring_fips.html#task_1188151

- Cisco Nexus 9000系列NX-OS安全組態指南、9.3（x）版

<https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/93x/security/configuration/guide/b-cisco-nexus-9000-nx-os-security-configuration-guide-93x/m-configuring-fips.html>

- NetApp與聯邦資訊處理標準（FIPS）出版品140-2

<https://www.netapp.com/company/trust-center/compliance/fips-140-2/>

- FIPS 140-2

<https://fieldportal.netapp.com/content/902303>

- 《NetApp ONTAP ®9強化指南》

<https://www.netapp.com/pdf.html?item=/media/10674-tr4569pdf.pdf>

- NetApp加密電源指南

<https://docs.netapp.com/ontap-9/index.jsp?topic=%2Fcom.netapp.doc.pow-nve%2Fhome.html>

- NVE與NAE資料表

<https://www.netapp.com/pdf.html?item=/media/17070-ds-3899.pdf>

- NSE資料表

<https://www.netapp.com/pdf.html?item=/media/7563-ds-3213-en.pdf>

- 供應說明文件中心 ONTAP

<http://docs.netapp.com>

- NetApp與聯邦資訊處理標準（FIPS）出版品140-2

<https://www.netapp.com/company/trust-center/compliance/fips-140-2/>

- Cisco與FIPS 140-2法規遵循

<https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/fips-140.html>

- NetApp密碼編譯安全模組

<https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp2648.pdf>

- 中型和大型醫療組織的網路安全實務做法

<https://www.phe.gov/Preparedness/planning/405d/Documents/tech-vol2-508.pdf>

- Cisco與密碼編譯模組驗證方案（CMVP）

<https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search?SearchMode=Basic&Vendor=cisco&CertificateStatus=Active&ValidationYear=0>

- NetApp儲存加密、NVMe自我加密磁碟機、NetApp Volume加密及NetApp Aggregate加密

<https://www.netapp.com/pdf.html?item=/media/17073-ds-3898.pdf>

- NetApp Volume Encryption與NetApp Aggregate Encryption

<https://www.netapp.com/pdf.html?item=/media/17070-ds-3899.pdf>

- NetApp儲存加密

<https://www.netapp.com/pdf.html?item=/media/7563-ds-3213-en.pdf>

- 適用於電子健康記錄系統FlexPod

<https://www.netapp.com/pdf.html?item=/media/22199-tr-4881.pdf>

- Data Now：利用雲端連線的Flash技術、提升Epic EHR環境的效能

<https://www.netapp.com/media/10809-cloud-connected-flash-wp.pdf>

- 適用於Epic EHR基礎架構的Datacenter FlexPod
<https://www.netapp.com/pdf.html?item=/media/17061-ds-3683.pdf>
- 《Datacenter for Epic EHR部署指南》FlexPod
<https://www.netapp.com/media/10658-tr-4693.pdf>
- 適用於MEDITECH軟體的資料中心基礎架構FlexPod
<https://www.netapp.com/media/8552-flexpod-for-meditech-software.pdf>
- 此功能延伸至MEDITECH軟體FlexPod
<https://blog.netapp.com/the-flexpod-standard-extends-to-meditech-software/>
- 適用於MEDITECH方向調整指南FlexPod
<https://www.netapp.com/pdf.html?item=/media/12429-tr4774.pdf>
- 醫療影像用的FlexPod
<https://www.netapp.com/media/19793-tr-4865.pdf>
- 醫療業的AI
<https://www.netapp.com/pdf.html?item=/media/7393-na-369pdf.pdf>
- 適用於醫療業的可讓您輕鬆轉型FlexPod
<https://flexpod.com/solutions/verticals/healthcare/>
- Cisco與NetApp提供的解決方案FlexPod
<https://flexpod.com/>

感謝

- NetApp技術行銷工程師Abhinav Singh
- Brian O'Meahony、NetApp解決方案架構設計師Healthcare（Epic）
- NetApp追求業務開發經理Brian Pruitt
- NetApp資深解決方案架構設計師Arvind Ramakrishnan
- Michael Hommer、FlexPod NetApp全球現場技術長

版本歷程記錄

版本	日期	文件版本歷程記錄
1.0版	2021年4月	初始版本

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。