



設定及設定Keystone Keystone

NetApp
February 19, 2026

目錄

設定及設定Keystone	1
需求	1
Keystone Collector 的虛擬基礎架構需求	1
Keystone Collector 的 Linux 系統需求	2
Keystone對ONTAP和StorageGRID 的要求	5
安裝 Keystone Collector	8
在VMware vSphere系統上部署Keystone Collector	8
在 Linux 系統上安裝 Keystone Collector	10
Keystone 軟體的自動驗證	11
設定Keystone Collector	12
在Keystone Collector上設定HTTP Proxy	13
限制私有資料的收集	14
信任自訂根 CA	15
建立效能服務層級	16
安裝 ITOM Collector	19
Keystone ITOM Collector 的安裝要求	20
在 Linux 系統上安裝Keystone ITOM Collector	21
在 Windows 系統上安裝Keystone ITOM Collector	22
設定 Keystone 的 AutoSupport	22
監控與升級	24
監控 Keystone Collector 的健全狀況	24
手動升級 Keystone Collector	29
Keystone Collector 安全性	31
強化安全性	31
Keystone收集的使用者資料類型	32
資料收集ONTAP	32
資料收集StorageGRID	40
遙測數據收集	40
私密模式中的 Keystone	42
瞭解 Keystone (私有模式)	42
準備以私有模式安裝Keystone Collector	43
以私人模式安裝 Keystone Collector	44
在私人模式中設定 Keystone Collector	45
在私有模式中監控 Keystone Collector 健全狀況	50

設定及設定Keystone

需求

Keystone Collector 的虛擬基礎架構需求

您的 VMware vSphere 系統必須符合數項需求、才能安裝 Keystone Collector 。

Keystone Collector 伺服器 VM 的必要條件：

- 作業系統：VMware vCenter 伺服器和 ESXi 8.0 或更高版本
- 核心：1 個 CPU
- RAM：2 GB RAM
- 磁碟空間：20 GB vDisk

其他需求

確保符合下列一般要求：

網路需求

下表列出 Keystone Collector 的網路需求。



Keystone Collector 需要網際網路連線。您可以透過預設閘道（透過 NAT）或透過 HTTP Proxy 直接路由傳送來提供網際網路連線。這兩種變體都在這裡說明。

來源	目的地	服務	傳輸協定與連接埠	類別	目的
Keystone 收集器 (用於 Keystone ONTAP)	部門 (Unified Manager Active IQ Unified Manager)	HTTPS	TCP 443	必填 (若使 用 Keystone ONTAP)	Keystone Collector 使用量 數據收集 ONTAP 以供參考
Keystone 收集器 (用於 Keystone StorageGRID)	系統管理節 點 StorageGRID	HTTPS	TCP 443	必填 (若使 用 Keystone StorageGRID)	Keystone Collector 使用量 數據收 集 StorageGRID 以供參考
Keystone 收集器 (一般)	網際網路 (根據 稍後提供的 URL 需求)	HTTPS	TCP 443	必要 (網際網路 連線)	Keystone Collector 軟體、 作業系統更新和 計量資料上傳

Keystone收集器 (一般)	客戶HTTP Proxy	HTTP Proxy	客戶Proxy連接埠	必要 (網際網路連線)	Keystone Collector軟體、作業系統更新和計量資料上傳
Keystone收集器 (一般)	客戶DNS伺服器	DNS	TCP / udp 53	必填	DNS解析
Keystone收集器 (一般)	客戶NTP伺服器	NTP	udp 123	必填	時間同步
Keystone收集器 (用於Keystone ONTAP)	Unified Manager	MySQL	TCP 3306	選用功能	Keystone Collector的效能指標集合
Keystone收集器 (一般)	客戶監控系統	HTTPS	TCP 7777	選用功能	Keystone Collector健全狀況報告
客戶的營運工作站	Keystone收集器	SSH	TCP 22	管理	存取Keystone Collector Management
NetApp ONTAP的叢集與節點管理位址	Keystone收集器	HTTP 8000、ping	TCP 8000、ICMP回應要求/回覆	選用功能	Webserver、提供ONTAP 韌體更新功能



在全新安裝 Unified Manager 期間、MySQL 的預設連接埠 3306 僅限於 localhost、這會阻止 Keystone Collector 收集效能指標。如需更多資訊、請參閱 "需求 ONTAP"。

URL存取

Keystone Collector需要存取下列網際網路主機：

地址	理由
https://keystone.netapp.com	Keystone Collector軟體更新與使用量報告
https://support.netapp.com	NetApp HQ提供帳單資訊和AutoSupport 供應功能

Keystone Collector 的 Linux 系統需求

使用所需軟體準備 Linux 系統、可確保 Keystone Collector 能提供精確的安裝和資料收集。

請確定您的 Linux 和 Keystone Collector 伺服器 VM 具有這些組態。

Linux 伺服器：

- 作業系統：下列任何一項：
 - Debian 12.
 - Red Hat Enterprise Linux 8.6 或更新版本 8.x
 - Red Hat Enterprise Linux 9.0 或更高版本
 - CentOS 7（僅適用於現有環境）
- Chroyd時間同步
- 存取標準 Linux 軟體儲存庫

同一部伺服器也應該具有下列協力廠商套件：

- Pod管理程式
- SOS
- 時間
- Python 3（3.9.14 至 3.11.8）

Keystone Collector 伺服器 VM：

- 核心：2個CPU
- RAM：4 GB RAM
- 磁碟空間：50 GB vDisk

其他需求

確保符合下列一般要求：

網路需求

下表列出 Keystone Collector 的網路需求。



Keystone Collector需要網際網路連線。您可以透過預設閘道（透過NAT）或透過HTTP Proxy直接路由傳送來提供網際網路連線。這兩種變體都在這裡說明。

來源	目的地	服務	傳輸協定與連接埠	類別	目的
Keystone收集器 (用於Keystone ONTAP)	部門 (Unified Manager Active IQ Unified Manager)	HTTPS	TCP 443	必填 (若使用Keystone ONTAP)	Keystone Collector使用量數據收集ONTAP以供參考
Keystone收集器 (用於Keystone StorageGRID)	系統管理節點StorageGRID	HTTPS	TCP 443	必填 (若使用Keystone StorageGRID)	Keystone Collector使用量數據收集StorageGRID以供參考

Keystone收集器 (一般)	網際網路 (根據稍後提供的URL需求)	HTTPS	TCP 443	必要 (網際網路連線)	Keystone Collector軟體、作業系統更新和計量資料上傳
Keystone收集器 (一般)	客戶HTTP Proxy	HTTP Proxy	客戶Proxy連接埠	必要 (網際網路連線)	Keystone Collector軟體、作業系統更新和計量資料上傳
Keystone收集器 (一般)	客戶DNS伺服器	DNS	TCP / udp 53	必填	DNS解析
Keystone收集器 (一般)	客戶NTP伺服器	NTP	udp 123	必填	時間同步
Keystone收集器 (用於Keystone ONTAP)	Unified Manager	MySQL	TCP 3306	選用功能	Keystone Collector的效能指標集合
Keystone收集器 (一般)	客戶監控系統	HTTPS	TCP 7777	選用功能	Keystone Collector健全狀況報告
客戶的營運工作站	Keystone收集器	SSH	TCP 22	管理	存取Keystone Collector Management
NetApp ONTAP的叢集與節點管理位址	Keystone收集器	HTTP 8000、ping	TCP 8000、ICMP回應要求/回覆	選用功能	Webserver、提供ONTAP 韌體更新功能



在全新安裝 Unified Manager 期間、MySQL 的預設連接埠 3306 僅限於 localhost、這會阻止 Keystone Collector 收集效能指標。如需更多資訊、請參閱 "需求 ONTAP"。

URL存取

Keystone Collector需要存取下列網際網路主機：

地址	理由
https://keystone.netapp.com	Keystone Collector軟體更新與使用量報告
https://support.netapp.com	NetApp HQ提供帳單資訊和AutoSupport 供應功能

Keystone對ONTAP和StorageGRID 的要求

開始使用 Keystone 之前、您必須確保 ONTAP 叢集和 StorageGRID 系統符合數項需求。

ONTAP

軟體版本

1. 部分9.8或更新版本ONTAP
2. Active IQ Unified Manager (Unified Manager) 9.10 或更新版本

開始之前

如果您只想透過 ONTAP 收集使用資料，請符合下列要求：

1. 確定已設定 ONTAP 9.8 或更新版本。如需設定新叢集的相關資訊，請參閱下列連結：
 - ["使用系統管理員在新叢集上設定 ONTAP"](#)
 - ["使用CLI設定叢集"](#)
2. 建立具有特定角色的 ONTAP 登入帳戶。若要深入瞭解 ["瞭解如何建立 ONTAP 登入帳戶"](#)、請參閱。
 - 網路Ui
 - i. 使用您的預設認證登入 ONTAP 系統管理員。若要深入瞭解 ["使用System Manager進行叢集管理"](#)、請參閱。
 - ii. 建立具有「唯讀」角色和「http」應用程式類型的 ONTAP 使用者，並瀏覽至 * 叢集 > 設定 > 安全性 > 使用者 * 來啟用密碼驗證。
 - CL1
 - i. 使用預設認證登入 ONTAP CLI。若要深入瞭解 ["使用 CLI 進行叢集管理"](#)、請參閱。
 - ii. 建立具有「readonly」角色和「http」應用程式類型的 ONTAP 使用者，並啟用密碼驗證。若要深入瞭解驗證，請 ["啟用 ONTAP 帳戶密碼存取"](#)參閱。

如果您打算透過 Active IQ Unified Manager 收集使用資料，請符合下列要求：

1. 請確定 Unified Manager 9.10 或更新版本已設定完成。如需安裝Unified Manager的相關資訊、請參閱下列連結：
 - ["在VMware vSphere系統上安裝Unified Manager"](#)
 - ["在Linux系統上安裝Unified Manager"](#)
2. 確保ONTAP 已將該叢集新增至Unified Manager。如需新增叢集的相關資訊、請參閱 ["新增叢集"](#)。
3. 建立具有特定角色的Unified Manager使用者、以便收集使用量和效能資料。執行這些步驟。如需使用者角色的相關資訊、請參閱 ["使用者角色定義"](#)。
 - a. 使用安裝期間產生的預設應用程式管理員使用者認證、登入Unified Manager Web UI。請參閱 ["存取Unified Manager Web UI"](#)。
 - b. 建立Keystone Collector的服務帳戶 Operator 使用者角色：Keystone Collector服務API使用此服務帳戶與Unified Manager通訊、並收集使用資料。請參閱 ["新增使用者"](#)。
 - c. 建立 Database 使用者帳戶 Report Schema 角色：此使用者是收集效能資料的必要使用者。請參閱 ["建立資料庫使用者"](#)。



在全新安裝 Unified Manager 期間、MySQL 的預設連接埠 3306 僅限於 localhost、這會阻止 Keystone ONTAP 收集效能資料。您可以修改此組態、並使用 Unified Manager 維護主控台的選項、讓其他主機可以使用此連線 Control access to MySQL port 3306。如需相關資訊，請參閱 ["其他功能表選項"](#)。

4. 在 Unified Manager 中啟用 API 閘道。Keystone Collector 利用 API 閘道功能與 ONTAP 各種叢集進行通訊。您可以從 Web UI 或透過 Unified Manager CLI 執行幾個命令來啟用 API 閘道。

Web UI

若要從 Unified Manager Web UI 啟用 API 閘道、請登入 Unified Manager Web UI 並啟用 API 閘道。如需相關資訊、請參閱 ["啟用 API 閘道"](#)。

CLI

若要透過 Unified Manager CLI 啟用 API 閘道、請遵循下列步驟：

- a. 在 Unified Manager 伺服器上、開始 SSH 工作階段並登入 Unified Manager CLI。
`\`um cli login -u <umadmin>` 如需 CLI 命令的相關資訊、請參閱 ["支援的 Unified Manager CLI 命令"](#)。
- b. 確認 API 閘道是否已啟用。
`um option list api.gateway.enabled` 答 `\`true` 值表示已啟用 API 閘道。
- c. 如果傳回的值為 `false`、請執行下列命令：
`\`um option set api.gateway.enabled=true`
- d. 重新啟動 Unified Manager 伺服器：
 - Linux：["重新啟動 Unified Manager"](#)。
 - VMware vSphere：["重新啟動 Unified Manager 虛擬機器"](#)。

StorageGRID

若要在 StorageGRID 更新版本上安裝 Keystone Collector、需要下列組態。

- StorageGRID 11.6.0 應安裝或更新版本。如需升級 StorageGRID 功能的相關資訊、請參閱 ["升級 StorageGRID 版軟體：總覽"](#)。
- 應建立一個支援使用資料收集功能的本地管理員使用者帳戶 StorageGRID。Keystone Collector 服務會使用此服務帳戶、StorageGRID 透過管理員節點 API 與效益進行通訊。

步驟

- a. 登入 Grid Manager。請參閱 ["登入 Grid Manager"](#)。
- b. 使用建立本機管理群組 Access mode: Read-only。請參閱 ["建立管理群組"](#)。
- c. 新增下列權限：
 - 租戶帳戶
 - 維護
 - 度量查詢
- d. 建立 Keystone 服務帳戶使用者、並將其與管理群組建立關聯。請參閱 ["管理使用者"](#)。

安裝 Keystone Collector

在VMware vSphere系統上部署Keystone Collector

在VMware vSphere系統上部署Keystone Collector包括下載OVA範本、使用*部署OVF範本*精靈來部署範本、驗證憑證的完整性、以及驗證VM的整備度。

部署OVA範本

請遵循下列步驟：

步驟

1. 請從下載OVA檔案 "[此連結](#)" 並將其儲存在VMware vSphere系統上。
2. 在VMware vSphere系統上、瀏覽至* VM and Templates" (虛擬機器與範本) 檢視。
3. 在虛擬機器 (VM) (或資料中心、如果未使用VM資料夾) 所需的資料夾上按一下滑鼠右鍵、然後選取*部署OVF範本*。
4. 在「部署**OVF**範本」精靈的「步驟1」上、按一下「選取」和「**OVF**範本」以選取下載的項目 KeystoneCollector-latest.ova 檔案：
5. 在步驟2_上、指定VM名稱並選取VM資料夾。
6. 在_Step 3_上、指定執行VM所需的運算資源。
7. 在步驟 4：檢查細節中，驗證 OVA 檔案的正確性和真實性。

vCenter 根信任庫僅包含 VMware 憑證。NetApp使用 Entrust 作為認證機構，這些憑證需要加入到 vCenter 信任庫中。

- a. 從 Sectigo 下載代碼簽署 CA 證書 "[請按這裡](#)"。
- b. 請遵循中的步驟 Resolution 本知識庫 (KB) 文章的一節：<https://kb.vmware.com/s/article/84240>。



對於 vCenter 7.x 及更早版本，您必須將 vCenter 和 ESXi 更新至 8.0 或更高版本。早期版本已不再支援。

當Keystone Collector OVA 的完整性和真實性得到驗證後，您就可以看到文字了。(Trusted certificate) 與出版商合作。

Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 Select storage
- 6 Select networks
- 7 Customize template
- 8 Ready to complete

Review details ✕

Verify the template details.

Publisher	Sectigo Public Code Signing CA R36 (Trusted certificate)
Product	Keystone-Collector
Version	3.12.31910
Vendor	NetApp
Download size	1.7 GB
Size on disk	3.9 GB (thin provisioned) 19.5 GB (thick provisioned)

CANCEL
BACK
NEXT

8. 在「部署**OVF**範本」精靈的步驟5_上、指定儲存VM的位置。
9. 在 *Step 6* 上、選取要用於虛擬機器的目的地網路。
10. 在步驟7自訂範本_上、指定管理使用者帳戶的初始網路位址和密碼。



管理密碼以可還原的格式儲存在 vCenter 中、並應作為引導式認證、以取得對 VMware vSphere 系統的初始存取權。在初始軟體組態期間、應變更此管理員密碼。應以CIDR表示法提供IPV4位址的子網路遮罩。例如、子網路遮罩的值為24、子網路遮罩為255 · 255 · 255 · 0。

11. 在「部署**OVF**範本」精靈的步驟8「準備好完成」上、檢閱組態並確認您已正確設定OVA部署的參數。

從範本部署VM並開啟電源後、請開啟VM的SSH工作階段、並以暫用的管理認證登入、以驗證VM是否已準備好進行組態。

初始系統組態

針對透過 OVA 部署的 Keystone Collector 伺服器、在 VMware vSphere 系統上執行下列步驟：



完成部署時、您可以使用Keystone Collector Management終端使用者介面 (TUI) 公用程式來執行組態和監控活動。您可以使用各種鍵盤控制項 (例如Enter和方向鍵) 來選取選項、並瀏覽此TUI。

1. 開啟至Keystone Collector伺服器的SSH工作階段。連線時、系統會提示您更新管理員密碼。視需要完成管理密碼更新。
2. 使用新密碼登入以存取 TUI 。登入時、便會顯示TUI。

或者、您也可以執行手動啟動 `keystone-collector-tui` CLI命令。

3. 如有需要、請在 TUI 的 * 組態 > 網路區段 * 中設定 Proxy 詳細資料。
4. 在「組態>系統」區段中設定系統主機名稱、位置和NTP伺服器。
5. 使用 * 維護 > 更新收集器 * 選項更新 Keystone 收集器。更新之後、請重新啟動 Keystone Collector 管理 TUI 公用程式以套用變更。

在 Linux 系統上安裝 **Keystone Collector**

您可以使用 RPM 或 Debian 套件，在 Linux 伺服器上安裝 Keystone Collector 軟體。根據您的 Linux 套裝作業系統，請遵循安裝步驟。

使用 RPM

1. SSH至Keystone Collector伺服器並升級至 root 權限：
2. 導入Keystone公共簽章：

```
# rpm --import https://keystone.netapp.com/repo1/RPM-GPG-NetApp-Keystone-20251020
```
3. 請透過檢查 RPM 資料庫中Keystone Billing Platform 的指紋，確保已匯入正確的公共憑證：

```
# rpm -qa gpg-pubkey --qf '%{Description}'|gpg --show-keys --fingerprint
```

 正確的指紋如下圖所示：
9297 0DB6 0867 22E7 7646 E400 4493 5CBB C9E9 FEDC
4. 下載 keystone.repo.rpm 文件：

```
curl -O https://keystone.netapp.com/repo1/keystone.repo.rpm
```
5. 驗證文件的真實性：

```
rpm --checksig -v keystone.repo.rpm
```

 正版文件的簽名如下所示：
Header V4 RSA/SHA512 Signature, key ID c9e9fedc: OK
6. 安裝YUM軟體儲存庫檔案：

```
# yum install keystone.repo.rpm
```
7. 安裝Keystone repo時、請透過YUM套件管理程式安裝Keystone收集器套件：

```
# yum install keystone-collector
```

對於 Red Hat Enterprise Linux 9，執行下列命令安裝 keystone-collector 套件：

```
# yum install keystone-collector-rhel9
```

使用 Debian

1. SSH 至 Keystone Collector 伺服器並提高 root 權限。

```
`sudo su
```
2. 下載 keystone-sw-repo.deb 檔案：

```
`curl -O https://keystone.netapp.com/downloads/keystone-sw-repo.deb
```
3. 安裝 Keystone 軟體儲存庫檔案：

```
# dpkg -i keystone-sw-repo.deb
```
4. 更新套件清單：

```
# apt-get update
```
5. 安裝 Keystone repo 後，請安裝 Keystone 收集器套件：

```
# apt-get install keystone-collector
```



完成安裝時、您可以使用Keystone Collector Management終端使用者介面（TUI）公用程式來執行組態和監控活動。您可以使用各種鍵盤控制項（例如Enter和方向鍵）來選取選項、並瀏覽此TUI。請參閱 "[設定Keystone Collector](#)" 和 "[監控系統健全狀況](#)" 以取得資訊。

Keystone 軟體的自動驗證

Keystone 儲存庫已設定為自動驗證 Keystone 軟體的完整性、因此您的站台只會安裝有效

且可靠的軟體。

中所提供的 Keystone YUM 儲存庫用戶端組態 `keystonerepo.rpm` 會使用強制 GPG 檢查 (`gpgcheck=1` (透過此儲存庫下載的所有軟體))。透過Keystone儲存庫下載的任何未通過簽章驗證的RPM都無法安裝。Keystone Collector 的排程自動更新功能會使用此功能、以確保您的站台僅安裝有效且可靠的軟體。

設定Keystone Collector

您需要完成幾項組態工作、才能讓Keystone Collector在儲存環境中收集使用資料。這是一次性活動、可啟動所需元件、並將其與儲存環境建立關聯。



- Keystone Collector 提供 Keystone Collector Management 終端機使用者介面 (TUI) 公用程式、可執行組態和監控活動。您可以使用各種鍵盤控制項 (例如Enter和方向鍵) 來選取選項、並瀏覽此TUI。
- Keystone Collector 可針對沒有網際網路存取權的組織進行設定、也稱為 `_Dark 站台_` 或 `_Private 模式_`。若要深入瞭解、請["私密模式中的 Keystone"](#)參閱。

步驟

1. 啟動 Keystone Collector 管理 TUI 公用程式：

```
$ keystone-collector-tui
```
2. 請移至「組態> **KS-Collector**」以開啟Keystone Collector組態畫面、以檢視可用的更新選項。
3. 更新必要選項。

不整合

- 收集**ONTAP** 資料使用：此選項可收集使用資料ONTAP 以供參考。新增Active IQ Unified Manager 有關伺服器 and 服務帳戶的詳細資料 (Unified Manager)。
- 收集**ONTAP** 效能資料：此選項可收集效能資料ONTAP 以供參考。此功能預設為停用。如果您的環境需要進行效能監控才能達到SLA目的、請啟用此選項。提供Unified Manager資料庫使用者帳戶詳細資料。如需建立資料庫使用者的相關資訊、請參閱 ["建立Unified Manager使用者"](#)。
- 移除私有資料：此選項會移除客戶的特定私有資料、預設為啟用。如需在啟用此選項時、從度量中排除哪些資料的相關資訊、請參閱 ["限制私有資料的收集"](#)。

物件：StorageGR物件

- 收集**StorageGRID** 資料使用：此選項可收集節點使用詳細資料。新增StorageGRID 不完整的節點位址和使用者詳細資料。
- 移除私有資料：此選項會移除客戶的特定私有資料、預設為啟用。如需在啟用此選項時、從度量中排除哪些資料的相關資訊、請參閱 ["限制私有資料的收集"](#)。

4. 切換「使用System*啟動KS-Collector」欄位。
5. 按一下「**儲存」。

```
NetApp Keystone Collector - Configure - KS Collector

[X] Start KS-Collector with System
[X] Collect ONTAP usage
AIQUM Address: 123.123.123.123
AIQUM Username: collector-user
AIQUM Password: -----
[X] Collect StorageGRID usage
StorageGRID Address: sgadminnode.address
StorageGRID Username: collector-user
StorageGRID Password: -----
[X] Collect ONTAP Performance Data
AIQUM Database Username: sla-reporter
AIQUM Database Password: -----
[X] Remove Private Data
Mode Standard
Logging Level info
                Tunables
                Save
                Clear Config
                Back
```

6. 返回TUI主畫面並確認「**服務狀態」資訊、以確保Keystone Collector處於正常狀態。系統應顯示服務處

```
Service Status
Overall: Healthy
UM: Running
chronyd: Running
ks-collector: Running
```

於「整體：健全」狀態。

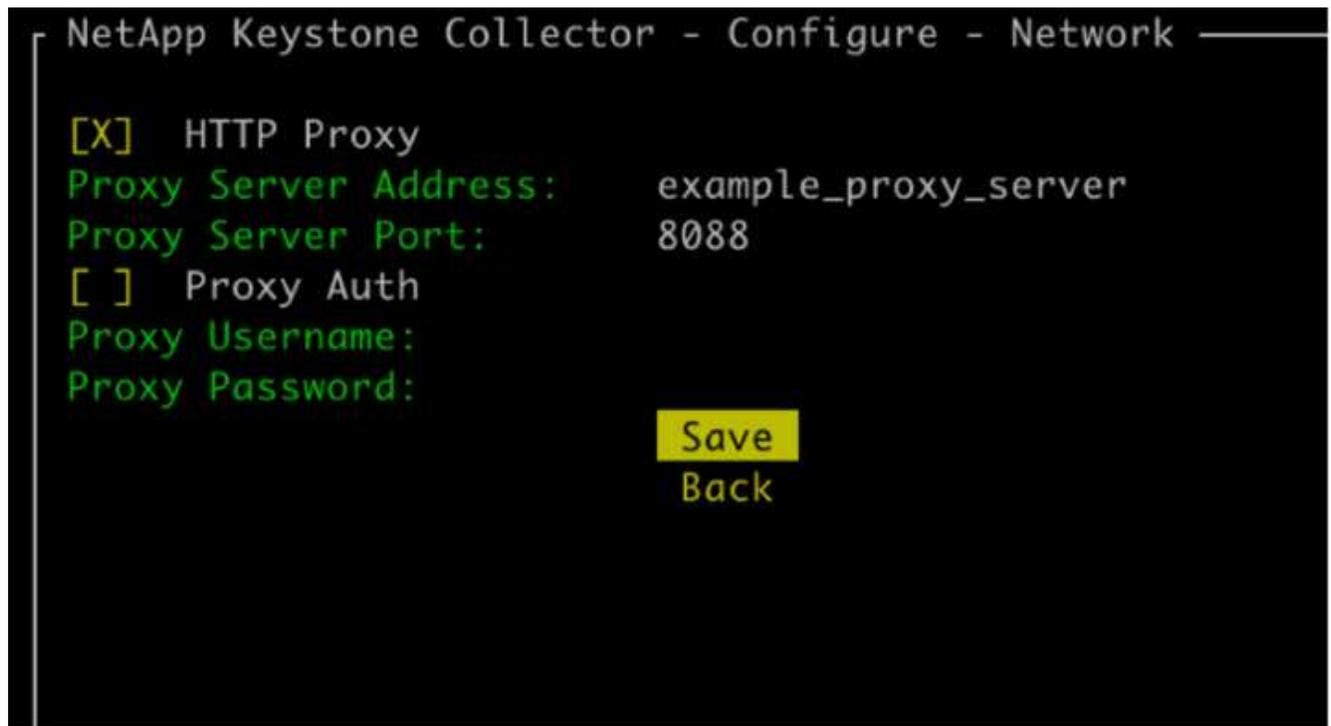
7. 在主畫面上選取「退出至Shell*」選項、結束Keystone Collector管理TUI。

在Keystone Collector上設定HTTP Proxy

Collector軟體支援使用HTTP Proxy與網際網路通訊。這可在TUI中設定。

步驟

1. 如果已關閉、請重新啟動 Keystone Collector 管理 TUI 公用程式：
\$ keystone-collector-tui
2. 切換「**HTTP Proxy**」欄位、並在需要驗證時新增HTTP Proxy伺服器、連接埠和認證的詳細資料。
3. 按一下「**儲存」。



限制私有資料的收集

Keystone Collector 會收集執行訂閱計量所需的有限組態、狀態和效能資訊。您可以選擇進一步限制所收集的資訊、方法是從上傳的內容中遮罩敏感資訊。這不會影響計費計算。不過、限制資訊可能會影響報告資訊的使用性、因為使用者可以輕易識別的部分元素（例如Volume名稱）會被UID取代。

在Keystone Collector TUI畫面上、限制特定客戶資料的收集是可設定的選項。此選項*移除私有資料*預設為啟用。

```
NetApp Keystone Collector - Configure - KS Collector

[X] Start KS-Collector with System
[X] Collect ONTAP usage
AIQUM Address:      123.123.123.123
AIQUM Username:    collector
AIQUM Password:    -----
[ ] Collect StorageGRID usage

[ ] Collect ONTAP Performance Data

[X] Remove Private Data
Mode              Standard
Logging Level     info
                  Tunables
                  Save
                  Clear Config
                  Back
```

如需ONTAP 瞭解有關在支援內部及StorageGRID 內部資料存取限制時所移除項目的資訊、請參閱 ["限制私有資料存取時移除的項目清單"](#)。

信任自訂根 CA

針對公共根憑證授權單位（CA）驗證憑證是 Keystone Collector 安全性功能的一部分。不過、如果需要、您可以將 Keystone Collector 設定為信任自訂根 CA。

如果您在系統防火牆中使用 SSL/TLS 檢查、則會導致網際網路流量使用自訂 CA 憑證重新加密。在接受根憑證並允許連線之前、必須設定設定以驗證來源為信任 CA。請遵循下列步驟：

步驟

- 1. 準備 CA 憑證。它應該是_base64 編碼的 X.509 檔案格式。

 支援的副檔名為 .pem、.crt、.cert。請確定憑證採用下列其中一種格式。

- 2. 將憑證複製到 Keystone Collector 伺服器。記下檔案複製的位置。
- 3. 在伺服器上開啟終端機、然後執行管理 TUI 公用程式。
\$ keystone-collector-tui
- 4. 移至 * 組態 > 進階 *。
- 5. 啟用選項 * 啟用自訂根憑證 *。
- 6. 針對 * 選取自訂根憑證路徑：*、選取 - Unset -
- 7. 按Enter。此時會顯示一個對話方塊、用於選取憑證路徑。

8. 從檔案系統瀏覽器選取根憑證、或輸入正確的路徑。
9. 按Enter。您將返回 * 進階 * 畫面。
10. 選擇*保存*。已套用組態。



CA憑證被複製到 /opt/netapp/ks-collector/ca.pem 在Keystone Collector 伺服器上。

```
NetApp Keystone Collector - Configure - Advanced
[ ] Darksite Mode
[X] TLS Verify on Connections to Internet
[X] Enable custom root certificate
Select custom root certificate path:
    - Unset -
[X] Finished Initial OVA Install
[X] Collector Auto-Update
Override Collector Images
Save
Back
```

建立效能服務層級

您可以使用Keystone Collector 管理 TUI 公用程式建立效能服務等級 (PSL)。透過 TUI 建立 PSL 會自動選擇為每個效能服務等級設定的預設值，從而減少透過Active IQ Unified Manager建立 PSL 時手動設定這些值時可能發生的錯誤的可能性。

若要深入瞭解 ISL、請["效能服務層級"](#)參閱。

若要深入瞭解服務層級，請["Keystone 中的服務層級"](#)參閱。

步驟

1. 啟動 Keystone Collector 管理 TUI 公用程式：
\$ keystone-collector-tui
2. 請移至 * 組態 > AIQUM* 以開啟 AIQUM 畫面。
3. 啟用選項 * 建立 AIQUM 效能設定檔 *。
4. 輸入 Active IQ Unified Manager 伺服器和使用者的詳細資料。這些詳細資料是建立 ISL 所必需的、不會儲存。

```
NetApp Keystone Collector - Configure - AIQUM
[ ] Enable Embedded UM
[X] Create AIQUM Performance Profiles
AIQUM Address:
AIQUM Username:
AIQUM Password:
Select Keystone version          -unset-
Select Keystone Service Levels

Save
Back

Provide the details of the AIQUM server and user account.
These details are required to create the Performance Service Levels
in the specified AIQUM server and will not be stored.
```

- 5. 對於 * 選擇 Keystone 版本 * ，請選擇 -unset- 。
- 6. 按Enter。隨即顯示用於選取 Keystone 版本的對話方塊。
- 7. 反白 STaaS 以指定 Keystone STaaS* 的 Keystone 版本、然後按 Enter 鍵。

```
NetApp Keystone Collector - Configure - AIQUM
Select Keystone version
AIQUM Ad  KFS
AIQUM Us  STaaS
AIQUM Pa
Select K
Select K

Save
Back

Provide the details of the AIQUM server and user account.
These details are required to create the Performance Service Levels
in the specified AIQUM server and will not be stored.
```



您可以反白Keystone訂閱服務版本 1 的 **KFS** 選項。Keystone訂閱服務與Keystone STaaS 在組成效能服務等級、服務產品和計費原則方面有所不同。要了解更多信息，請參閱"[Keystone 訂閱服務 | 版本 1](#)"。

8. 所有支援的Keystone效能服務等級將顯示在指定Keystone版本的 選擇**Keystone**服務等級 選項中。從清單中啟用所需的效能服務等級。

```
NetApp Keystone Collector - Configure - AIQUM
[ ] Enable Embedded UM
[X] Create AIQUM Performance Profiles
AIQUM Address:
AIQUM Username:
AIQUM Password:
Select Keystone version          STaaS
Select Keystone Service Levels  [X] Extreme
                                [X] Premium
                                [ ] Performance
                                [ ] Standard
                                [ ] Value
                                Save
                                Back
Provide the details of the AIQUM server and user account.
These details are required to create the Performance Service Levels
in the specified AIQUM server and will not be stored.
```



您可以同時選擇多個效能服務等級來建立 PSL。

9. 選取 * 儲存 *、然後按 Enter 鍵。將會建立效能服務層級。

您可以在 Active IQ Unified Manager 的 * 效能服務層級 * 頁面上檢視建立的 PSL、例如適用於 STaaS 的 Premium-KS-STaaS 或適用於 KFS 的 Extreme KFS。如果建立的 ISL 不符合您的需求、您可以修改 ISL 來滿足您的需求。若要深入瞭解、請 "[建立及編輯效能服務層級](#)" 參閱。

Performance Service Levels

View and manage the Performance Service Levels that you can assign to workloads.

Search Performance Service Levels  Filter

[+ Add](#) [Modify](#) [Remove](#) 

<input type="checkbox"/>	Name ^	Type	Expected IOPS/TB	Peak IOPS/TB	Absolute Minim...	Expected Latency	Capacity	Workloads
<input checked="" type="checkbox"/>	Extreme - KFS	User-defined	6144	12288	1000	1	<div style="width: 100%;"><div style="width: 0%; background-color: #ccc;">Used: 0 bytes</div><div style="width: 100%; background-color: #ccc;">Available: 283.85 TiB</div></div>	0
<input checked="" type="checkbox"/>	Extreme - KS-STaaS	User-defined	6144	12288	1000	1	<div style="width: 100%;"><div style="width: 0%; background-color: #ccc;">Used: 0 bytes</div><div style="width: 100%; background-color: #ccc;">Available: 283.85 TiB</div></div>	0
Overview								
		Description	Extreme - KS-STaaS					
		Added Date	1 Aug 2024, 18:08					
		Last Modified Date	1 Aug 2024, 18:08					
<input checked="" type="checkbox"/>	Premium ...S-STaaS	User-defined	2048	4096	500	2	<div style="width: 100%;"><div style="width: 0%; background-color: #ccc;">Used: 0 bytes</div><div style="width: 100%; background-color: #ccc;">Available: 283.85 TiB</div></div>	0
Overview								
		Description	Premium - KS-STaaS					
		Added Date	1 Aug 2024, 18:08					
		Last Modified Date	1 Aug 2024, 18:08					

如果所選效能服務等級的 PSL 已存在於指定的 Active IQ Unified Manager 伺服器上，則無法再次建立它。如果您嘗試這樣做，您將收到一條錯誤訊息。



```
NetApp Keystone Collector - Configure - AIQUM

Warning
-----
AIQUM Ad Failed to create Performance Service Level for:
AIQUM Us Extreme. Error: <Response [400]>
AIQUM Pa
Select K
Select K

OK

> Save <
  Back

Provide the details of the AIQUM server and user account.
These details are required to create the Performance Service Levels
in the specified AIQUM server and will not be stored.
```

安裝 ITOM Collector

Keystone ITOM Collector 的安裝要求

安裝 ITOM Collector 之前，請先確定您的系統已準備好必要的軟體，並且符合所有必要的先決條件。

ITOM Collector 伺服器 VM 的必要條件：

- 支援的作業系統：
 - Debian 12 或更高版本
 - Windows Server 2016 或更高版本
 - Ubuntu 20.04 LTS 或更高版本
 - 紅帽企業 Linux (RHEL) 8.x
 - Red Hat Enterprise Linux 9.0 或更高版本
 - Amazon Linux 2023 或更高版本



建議使用的作業系統為 Debian 12 ， Windows Server 2016 或更新版本。

- 資源需求：根據所監控的 NetApp 節點數量，虛擬機器資源需求如下：
 - 2-10 個節點：4 個 CPU ， 8 GB RAM ， 40 GB 磁碟
 - 12-20 個節點：8 個 CPU ， 16 GB RAM ， 40 GB 磁碟
- 組態需求：確保在受監控的裝置上設定唯讀帳戶和 SNMP 。ITOM Collector 伺服器 VM 也需要設定為 NetApp 叢集和叢集交換器上的 SNMP 設陷主機和 Syslog 伺服器（如果適用）。

網路需求

下表列出了 ITOM Collector 的網路需求。

來源	目的地	傳輸協定	連接埠	說明
ITOM 收集器	NetApp ONTAP 叢集管理 IP	HTTPS ， SNMP	TCP 443 ， UDP 161	監控 ONTAP 控制器
NetApp ONTAP 叢集和節點管理 IP	ITOM 收集器	SNMP ， Syslog	UDP 162 ， UDP 514	控制器的 SNMP 設陷和 Syslog
ITOM 收集器	叢集交換器	SNMP	UDP 161	監控交換器
叢集交換器	ITOM 收集器	SNMP ， Syslog	UDP 162 ， UDP 514	來自交換器的 SNMP 設陷和 Syslog
ITOM 收集器	StorageGRID 節點 IP	HTTPS ， SNMP	TCP 443 ， UDP 161	StorageGRID 的 SNMP 監控
StorageGRID 節點 IP	ITOM 收集器	SNMP ， Syslog	UDP 162 ， UDP 514	StorageGRID 的 SNMP 設陷
ITOM 收集器	Keystone收集器	SSH ， HTTPS ， SNMP	TCP 22 ， TCP 443 ， UDP 161	Keystone Collector 監控與遠端管理

ITOM 收集器	本機 DNS	DNS	UDP 53	公有或私有 DNS 服務
ITOM 收集器	自選 NTP 伺服器	NTP	udp 123	保留時間

在 Linux 系統上安裝Keystone ITOM Collector

完成幾個步驟來安裝 ITOM Collector，它會收集您的儲存環境中的指標資料。您可以根據需求，在 Windows 或 Linux 系統上安裝。



Keystone 支援團隊提供動態連結，可下載 ITOM Collector 安裝檔案，該檔案將在兩小時內過期。

若要在 Windows 系統上安裝 ITOM Collector，請["在 Windows 系統上安裝 ITOM Collector"](#)參閱。

請依照下列步驟在 Linux 伺服器上安裝軟體：

開始之前

- 確認 Bourne Shell 適用於 Linux 安裝指令碼。
- 安裝 `vim-common` 套件以取得 ITOM Collector 安裝檔案所需的 *xxd* 二進位檔。
- 如果計畫以非 root 使用者身分執行 ITOM Collector，請確定 `sudo package` 已安裝。

步驟

1. 將 ITOM 收集器設定檔下載至 Linux 伺服器。
2. 在伺服器上開啟終端機，然後執行下列命令來變更權限，並使二進位檔可執行：


```
# chmod +x <installer_file_name>.bin
```
3. 執行命令以啟動 ITOM 收集器設定檔：


```
#./<installer_file_name>.bin
```
4. 執行安裝檔案會提示您：
 - a. 接受終端使用者授權合約（EULA）。
 - b. 輸入安裝的使用者詳細資料。
 - c. 指定安裝父目錄。
 - d. 選取收集器大小。
 - e. 如適用，請提供代理伺服器詳細資料。

每個提示都會顯示預設選項。除非您有特定需求，否則建議您選取預設選項。按 **Enter** 鍵選擇默認選項。安裝完成時，會出現訊息確認已成功安裝 ITOM Collector。



- ITOM Collector 安裝檔案會新增 `/etc/sudoers` 以處理服務重新啟動和記憶體傾印。
- 在 Linux 伺服器上安裝 ITOM Collector 會建立一個名為 **ITOM** 的預設使用者，在沒有根 Privileges 的情況下執行 ITOM Collector。您可以選擇不同的使用者或以 root 身分執行，但建議您使用 Linux 安裝指令碼所建立的 ITOM 使用者。

接下來呢？

成功安裝時，請聯絡 Keystone 支援團隊，透過 ITOM 支援入口網站驗證是否成功安裝 ITOM Collector。驗證之後，Keystone 支援團隊將從遠端設定 ITOM Collector，包括進一步的裝置探索和監控設定，並在組態完成後傳送確認訊息。如有任何疑問或其他資訊，請聯絡 keystone.services@NetApp。

在 Windows 系統上安裝 Keystone ITOM Collector

下載 ITOM Collector 安裝檔案，執行 Installshield 精靈，然後輸入必要的監控認證，即可在 Windows 系統上安裝 ITOM Collector。



Keystone 支援團隊提供動態連結，可下載 ITOM Collector 安裝檔案，該檔案將在兩小時內過期。

您可以根據自己的需求，在 Linux 系統上安裝。若要在 Linux 系統上安裝 ITOM Collector，請["在 Linux 系統上安裝 ITOM Collector"](#)參閱。

請依照下列步驟，在 Windows 伺服器上安裝 ITOM 收集器軟體：

開始之前

確保已在 Windows 伺服器本機安全性原則設定的本機原則 / 使用者權限指派下，授予 ITOM 收集器服務 * 以服務身分登入 *。

步驟

1. 將 ITOM 收集器設定檔下載至 Windows 伺服器。
2. 開啟安裝檔案以啟動「Installshield 精靈」。
3. 接受終端使用者授權合約（EULA）。InstallShield 精靈會擷取必要的二進位檔，並提示您輸入認證。
4. 輸入 ITOM Collector 將在下列情況下執行的帳戶認證：
 - 如果 ITOM Collector 未監控其他 Windows 伺服器，請使用本機系統。
 - 如果 ITOM Collector 正在監控同一個網域中的其他 Windows 伺服器，請使用具有本機系統管理員權限的網域帳戶。
 - 如果 ITOM Collector 正在監控其他不屬於同一個網域的 Windows 伺服器，請使用本機系統管理員帳戶，並使用本機系統管理員認證連線至每個資源。您可以選擇設定密碼，使其不會過期，以減少 ITOM 收集器與其受監控資源之間的驗證問題。
5. 選取收集器大小。根據設定檔，預設值為建議的大小。除非您有特定需求，否則請繼續使用建議的尺寸。
6. 選取 **下一步** 開始安裝。您可以使用填入的資料夾，或選擇不同的資料夾。狀態方塊會顯示安裝進度，接著顯示「完成安裝精靈」對話方塊。

接下來呢？

成功安裝時，請聯絡 Keystone 支援團隊，透過 ITOM 支援入口網站驗證是否成功安裝 ITOM Collector。驗證之後，Keystone 支援團隊將從遠端設定 ITOM Collector，包括進一步的裝置探索和監控設定，並在組態完成後傳送確認訊息。如有任何疑問或其他資訊，請聯絡 keystone.services@NetApp。

設定 Keystone 的 AutoSupport

當使用 AutoSupport 遙測機制時、Keystone 會根據 AutoSupport 遙測資料來計算使用量。若要達到必要的精細度、您應該將 AutoSupport 設定為將 Keystone 資料納入 ONTAP

叢集所傳送的每日支援套件組合中。

關於這項工作

在將 AutoSupport 設定為包含 Keystone 資料之前、請注意下列事項。

- 您可以使用 ONTAP CLI 編輯 AutoSupport 遙測選項。如需管理 AutoSupport 服務和系統（叢集）管理員角色的相關資訊、請參閱 ["管理AutoSupport 功能概述"](#) 和 ["叢集與SVM管理員"](#)。
- 您可以將子系統納入每日和每週 AutoSupport 套件、以確保 Keystone 的資料收集準確。如需 AutoSupport 子系統的相關資訊、請參閱 ["什麼是子系統AutoSupport"](#)。

步驟

1. 以系統管理員使用者身分、使用 SSH 登入 Keystone ONTAP 叢集。如需相關資訊、請參閱 ["使用 SSH 存取叢集"](#)。
2. 修改記錄內容。
 - 對於ONTAP 9.16.1 及更高版本，執行以下命令修改每日日誌內容：

```
autosupport trigger modify -node * -autosupport-message  
management.log -basic-additional  
wafl,performance,snapshot,object_store_server,san,raid,snapmirror  
-troubleshooting-additional wafl
```

如果叢集採用MetroCluster配置，請執行以下命令：

```
autosupport trigger modify -node * -autosupport-message  
management.log -basic-additional  
wafl,performance,snapshot,object_store_server,san,raid,snapmirror,met  
rocluster -troubleshooting-additional wafl
```

- 對於早期版本的ONTAP，執行以下命令來修改每日日誌內容：

```
autosupport trigger modify -node * -autosupport-message  
management.log -basic-additional  
wafl,performance,snapshot,platform,object_store_server,san,raid,snapm  
irror -troubleshooting-additional wafl
```

如果叢集採用MetroCluster配置，請執行以下命令：

```
autosupport trigger modify -node * -autosupport-message management.log  
-basic-additional  
wafl,performance,snapshot,platform,object_store_server,san,raid,snapmirr  
or,metrocluster -troubleshooting-additional wafl
```

- 執行此命令以修改每週記錄內容：

```
autosupport trigger modify -autosupport-message weekly
-troubleshooting-additional wafl -node *
```

如需此命令的詳細資訊、請參閱 ["系統節點AutoSupport 的不正常情況下修改觸發程序"](#)。

監控與升級

監控 **Keystone Collector** 的健全狀況

您可以使用任何支援 HTTP 要求的監控系統來監控 **Keystone Collector** 的健全狀況。監控健全狀況有助於確保 **Keystone** 儀表板上有資料可用。

根據預設、**Keystone** 健全狀況服務不接受來自 localhost 以外任何 IP 的連線。**Keystone**健全狀況端點為 /uber/health、並在連接埠上偵聽**Keystone Collector**伺服器的所有介面 7777。查詢時、端點會傳回具有Json輸出的HTTP要求狀態代碼作為回應、說明**Keystone Collector**系統的狀態。

Json實體提供的整體健全狀況狀態 is_healthy 屬性、為布林值、以及每個元件的詳細狀態清單 component_details 屬性。
範例如下：

```
$ curl http://127.0.0.1:7777/uber/health
{"is_healthy": true, "component_details": {"vicmet": "Running", "ks-
collector": "Running", "ks-billing": "Running", "chronyd": "Running"}}
```

這些狀態代碼會傳回：

- * 200*：表示所有受監控的元件都正常運作
- * 503 *：表示一或多個元件不正常
- * 409*：表示查詢健全狀況狀態的HTTP用戶端不在「允許」清單中、這是允許的網路CIDR清單。對於此狀態、不會傳回任何健全狀況資訊。「允許」清單使用網路CIDR方法來控制哪些網路裝置可以查詢**Keystone**健全狀況系統。如果您收到此錯誤、請從* **Keystone Collector management TUI > Configure > Health Monitoring** *將監控系統新增至_allow_清單。

Linux使用者請注意以下已知問題：



問題說明：**Keystone Collector**會在使用量測系統中執行多個容器。當Red Hat Enterprise Linux 8.x伺服器使用美國國防資訊系統署 (DISA) 安全技術實作指南 (STIG) 原則強化時、會間歇性看到有關fapolicyd (檔案存取原則精靈) 的已知問題。此問題識別為 ["錯誤1907870"](#)。因應措施：在Red Hat Enterprise解決之前、NetApp建議您採用以下方法來解決此問題 fapolicyd 進入許可模式。在中 /etc/fapolicyd/fapolicyd.conf、設定的值 permissive = 1。

檢視系統記錄

您可以檢視**Keystone Collector**系統記錄、以檢閱系統資訊、並使用這些記錄執行疑難排解。**Keystone Collector**使用主機的_journald記錄系統、系統記錄可透過標準_journalctl_系統公用程式檢閱。您可以使用下列關鍵服務

來檢查記錄：

- KS-collector
- KS-Health
- KS-aupdate

主要的資料收集服務_ks-collection_會以Json格式產生含有的記錄 run-id 與每個排程資料收集工作相關的屬性。以下是成功收集標準使用資料的範例：

```
{ "level": "info", "time": "2022-10-31T05:20:01.831Z", "caller": "light-collector/main.go:31", "msg": "initialising light collector with run-id cdf1m0f74cgphgfon8cg", "run-id": "cdf1m0f74cgphgfon8cg" }
{ "level": "info", "time": "2022-10-31T05:20:04.624Z", "caller": "ontap/service.go:215", "msg": "223 volumes collected for cluster a2049dd4-bfcf-11ec-8500-00505695ce60", "run-id": "cdf1m0f74cgphgfon8cg" }

{ "level": "info", "time": "2022-10-31T05:20:18.821Z", "caller": "ontap/service.go:215", "msg": "697 volumes collected for cluster 909cbacc-bfcf-11ec-8500-00505695ce60", "run-id": "cdf1m0f74cgphgfon8cg" }

{ "level": "info", "time": "2022-10-31T05:20:41.598Z", "caller": "ontap/service.go:215", "msg": "7 volumes collected for cluster f7b9a30c-55dc-11ed-9c88-005056b3d66f", "run-id": "cdf1m0f74cgphgfon8cg" }

{ "level": "info", "time": "2022-10-31T05:20:48.247Z", "caller": "ontap/service.go:215", "msg": "24 volumes collected for cluster a9e2dcff-ab21-11ec-8428-00a098ad3ba2", "run-id": "cdf1m0f74cgphgfon8cg" }

{ "level": "info", "time": "2022-10-31T05:20:48.786Z", "caller": "worker/collector.go:75", "msg": "4 clusters collected", "run-id": "cdf1m0f74cgphgfon8cg" }

{ "level": "info", "time": "2022-10-31T05:20:48.839Z", "caller": "reception/reception.go:75", "msg": "Sending file 65a71542-cb4d-bdb2-e9a7-a826be4fdb7_1667193648.tar.gz type=ontap to reception", "run-id": "cdf1m0f74cgphgfon8cg" }

{ "level": "info", "time": "2022-10-31T05:20:48.840Z", "caller": "reception/reception.go:76", "msg": "File bytes 123425", "run-id": "cdf1m0f74cgphgfon8cg" }

{ "level": "info", "time": "2022-10-31T05:20:51.324Z", "caller": "reception/reception.go:99", "msg": "uploaded usage file to reception with status 201 Created", "run-id": "cdf1m0f74cgphgfon8cg" }
```

以下是可選效能資料收集作業成功的範例：

```
{"level":"info","time":"2022-10-31T05:20:51.324Z","caller":"sql/service.go:28","msg":"initialising MySQL service at 10.128.114.214"}

{"level":"info","time":"2022-10-31T05:20:51.324Z","caller":"sql/service.go:55","msg":"Opening MySQL db connection at server 10.128.114.214"}

{"level":"info","time":"2022-10-31T05:20:51.324Z","caller":"sql/service.go:39","msg":"Creating MySQL db config object"}

{"level":"info","time":"2022-10-31T05:20:51.324Z","caller":"sla_reporting/service.go:69","msg":"initialising SLA service"}

{"level":"info","time":"2022-10-31T05:20:51.324Z","caller":"sla_reporting/service.go:71","msg":"SLA service successfully initialised"}

{"level":"info","time":"2022-10-31T05:20:51.324Z","caller":"worker/collector.go:217","msg":"Performance data would be collected for timerange: 2022-10-31T10:24:52~2022-10-31T10:29:52"}

{"level":"info","time":"2022-10-31T05:21:31.385Z","caller":"worker/collector.go:244","msg":"New file generated: 65a71542-cb4d-bdb2-e9a7-a826be4fdb7_1667193651.tar.gz"}

{"level":"info","time":"2022-10-31T05:21:31.385Z","caller":"reception/reception.go:75","msg":"Sending file 65a71542-cb4d-bdb2-e9a7-a826be4fdb7_1667193651.tar.gz type=ontap-perf to reception","run-id":"cdf1m0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-31T05:21:31.386Z","caller":"reception/reception.go:76","msg":"File bytes 17767","run-id":"cdf1m0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-31T05:21:33.025Z","caller":"reception/reception.go:99","msg":"uploaded usage file to reception with status 201 Created","run-id":"cdf1m0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-31T05:21:33.025Z","caller":"light-collector/main.go:88","msg":"exiting","run-id":"cdf1m0f74cgphgfon8cg"}
```

產生並收集支援套裝組合

Keystone Collector TUI可讓您產生支援套裝組合、然後將其新增至服務要求、以解決支援問題。請遵循下列程序：

步驟

1. 啟動 Keystone Collector 管理 TUI 公用程式：

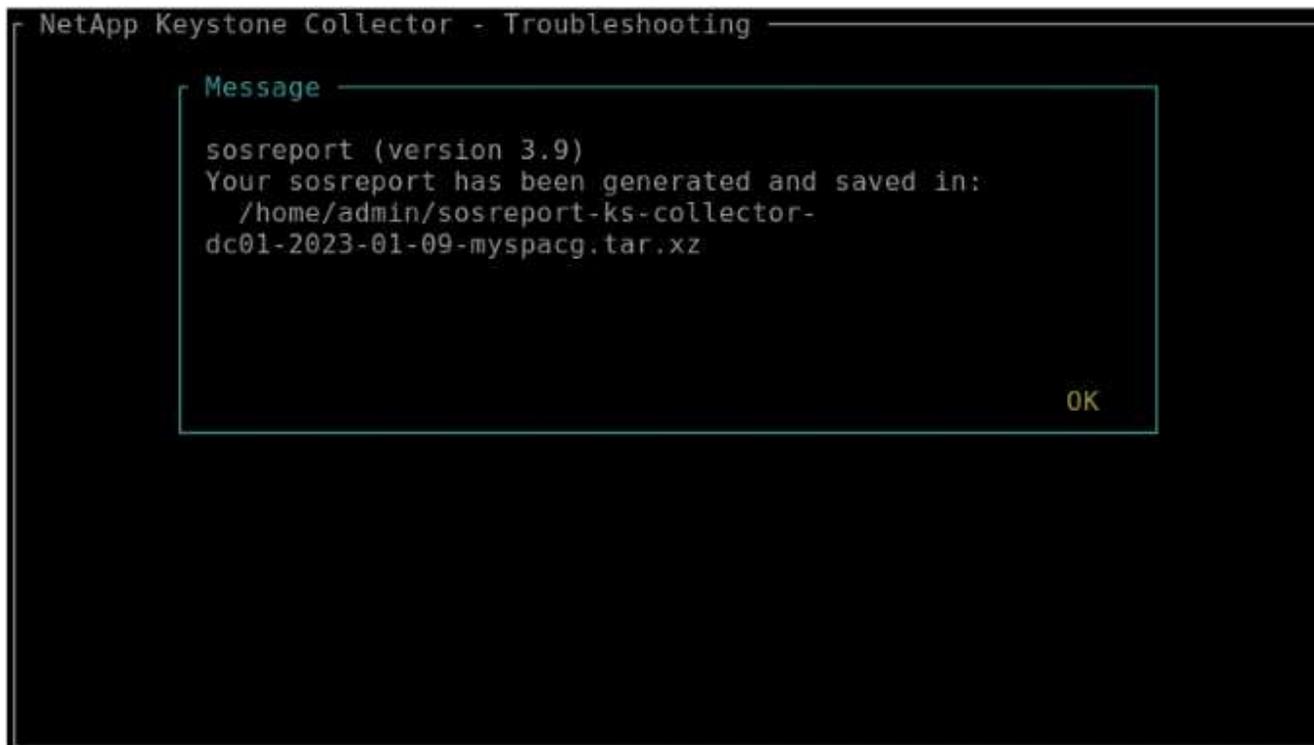
```
$ keystone-collector-tui
```

2. 請參閱*疑難排解>產生支援產品組合*。



```
NetApp Keystone Collector - Troubleshooting
Version
Generate Support Bundle
Back
```

3. 產生時、會顯示儲存套件組合的位置。使用FTP、SFTP或scp連線至該位置、並將記錄檔下載至本機系統。



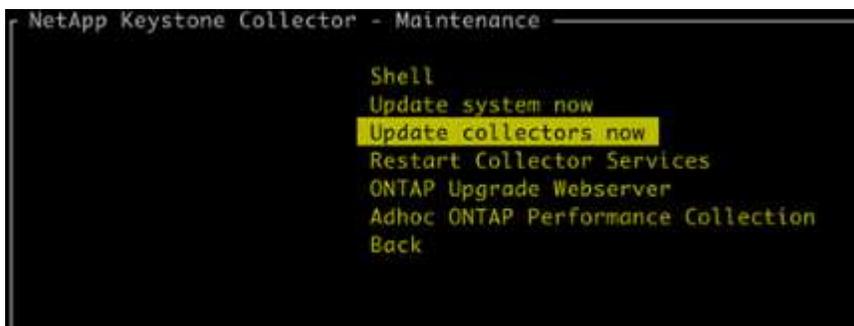
4. 下載檔案後，您可以將其附加到Keystone ServiceNow 支援票證。有關提高票數的信息，請參閱 "[正在產生服務要求](#)"。

手動升級 Keystone Collector

Keystone Collector 中的自動更新功能預設為啟用、會在每個新版本中自動升級 Keystone Collector 軟體。不過、您可以停用此功能並手動升級軟體。

步驟

1. 啟動 Keystone Collector 管理 TUI 公用程式：
\$ keystone-collector-tui
2. 在維護畫面上、選取 * 立即更新收集器 * 選項。



或者、請執行下列命令來升級版本：

對於 CentOS：


```
dpkg -l | grep keystone-collector
```

Keystone Collector 安全性

Keystone Collector 包含安全功能、可監控 Keystone 系統的效能和使用量指標、而不會危及客戶資料的安全性。

Keystone Collector 的功能是以下列安全原則為基礎：

- * 依設計的隱私權 * - Keystone 收集器會收集最小資料、以執行使用量測和效能監控。如需詳細資訊、請參閱 ["收集以供計費的資料"](#)。◦ ["移除私有資料"](#) 此選項預設為啟用、可遮罩及保護敏感資訊。
- * 最低權限存取 * - Keystone Collector 需要最低權限來監控儲存系統、如此可將安全風險降至最低、並防止對資料進行任何非預期的修改。這種方法符合最低權限原則、可強化受監控環境的整體安全狀態。
- * 安全軟體開發架構 * : Keystone 在整個開發週期中使用安全的軟體開發架構、可降低風險、減少弱點、並保護系統免於潛在威脅。

強化安全性

依預設、Keystone Collector 會設定為使用安全強化的組態。以下是建議的安全組態：

- Keystone Collector 虛擬機器的作業系統：
 - 符合 CIS Debian Linux 12 基準測試標準。在 Keystone Collector 管理軟體之外對作業系統組態進行任何變更、可能會降低系統安全性。如需詳細資訊、請參閱 ["CIS 基準測試指南"](#)。
 - 自動接收及安裝 Keystone Collector 透過自動更新功能驗證的安全性修補程式。停用此功能可能會導致未修補的易受影響軟體。
 - 驗證從 Keystone Collector 收到的更新。停用 APT 儲存庫驗證可能會導致自動安裝未獲授權的修補程式、可能會造成弱點。
- Keystone Collector 會自動驗證 HTTPS 憑證、以確保連線安全。停用此功能可能會導致模擬外部端點和使用量資料外洩。
- Keystone Collector 支援 ["自訂信任的 CA"](#) 認證：依預設、它會信任由可辨識的公共根 CA 所簽署的憑證 ["Mozilla CA 憑證程式"](#)。Keystone Collector 可啟用其他信任的 CA、針對與呈現這些憑證的端點的連線、啟用 HTTPS 憑證驗證。
- Keystone 收集器預設會啟用 [* 移除私有資料 *](#) 選項、以遮罩及保護敏感資訊。如需詳細資訊、請參閱 ["限制私有資料的收集"](#)。停用此選項會導致其他資料傳輸至 Keystone 系統。例如、它可以包含使用者輸入的資訊、例如可能被視為敏感資訊的磁碟區名稱。

相關資訊

- ["Keystone Collector 總覽"](#)
- ["虛擬化基礎架構需求"](#)
- ["設定 Keystone Collector"](#)

Keystone收集的使用者資料類型

Keystone會從Keystone ONTAP和Keystone StorageGRID訂閱中收集配置、狀態和使用情況信息，以及從託管Keystone Collector 的虛擬機器 (VM) 中收集遙測資料。如果在Keystone Collector 中啟用了此選項，則它只能收集ONTAP的效能資料。

資料收集ONTAP

下表是針對ONTAP 下列項目收集的容量使用資料代表範例：

- 叢集
 - 叢集UUID
 - 叢集名稱
 - 序號
 - 位置（根據ONTAP 在叢集中輸入的值）
 - 聯絡人
 - 版本
- 節點
 - 序號
 - 節點名稱
- 磁碟區
 - Aggregate名稱
 - Volume名稱
 - Volume InstanceUUID
 - IsCloneVolume旗標
 - IsFlexGroup組成 旗標
 - IsspaceEnforcement邏輯 旗標
 - IsSpaceReporting邏輯 旗標
 - LogicalspaceUsedByAfs
 - PercentSnapshotSpace
 - Performance TierInactiveUserData
 - Performance TierInactiveUserDataPercent
 - QoSAdaptivePolicyGroup名稱
 - QoSPolicyGroup名稱
 - 尺寸
 - 已使用
 - 實體使用
 - SizeUsedBySnapshots
 - 類型
 - Volume樣式擴充
 - Vserver名稱
 - IsVsRoot旗標

- Vserver
 - VserverName
 - VserverUUID
 - 子類型
- 儲存Aggregate
 - 儲存類型
 - Aggregate名稱
 - Aggregate UUID
 - 物理使用
 - 可用尺寸
 - 尺寸
 - 使用尺寸
- Aggregate物件存放區
 - ObjectStoreName
 - ObjectStoreUUID
 - 提供者類型
 - Aggregate名稱
- 複製磁碟區
 - FlexClone
 - 尺寸
 - 已使用
 - Vserver
 - 類型
 - ParentVolume
 - ParentVserver
 - Is組成
 - SplitEstimate
 - 州/省
 - FlexCloneUedPercent
- 儲存LUN
 - LUN UUID
 - LUN名稱
 - 尺寸
 - 已使用
 - IsReserved旗標

- IsRequest旗標
- 邏輯單元名稱
- QoSPolicyUUID
- QoSPolicyName
- Volume UUID
- Volume名稱
- SVMUUID
- SVM名稱
- 儲存磁碟區
 - Volume InstanceUUID
 - Volume名稱
 - SVMName
 - SVMUUID
 - QoSPolicyUUID
 - QoSPolicyName
 - 電容TierFootprint
 - 效能TierFootprint
 - 總佔用空間
 - 分層政策
 - IsProtected旗標
 - Is目的地 旗標
 - 已使用
 - 實體使用
 - CloneParentUUID
 - LogicalspaceUsedByAfs
- QoS原則群組
 - PolicyGroup
 - QoSPolicyUUID
 - 最大處理量
 - 最小處理量
 - 最大輸入IOPS
 - 最大推入MBps
 - MinThroughputIOPS
 - MinThroughputMBps
 - IsShawred旗標

- 可調式QoS原則群組ONTAP
 - QoSPolicyName
 - QoSPolicyUUID
 - PeakIOPS
 - PeakIOPsAllocate
 - 絕對MinIOPS
 - 高效能IOPS
 - ExpedIOPSAllocate
 - 區塊大小
- 佔用空間
 - Vserver
 - Volume
 - 總佔用空間
 - Volume BlocksFootprintBin0
 - Volume BlocksFootprintBin1
- MetroCluster
 - 節點
 - Aggregate
 - LIF
 - 配置複製
 - 連接
 - 叢集
 - 磁碟區
- 叢集MetroCluster
 - 叢集UUID
 - 叢集名稱
 - RemoteClusterUUID
 - RemoteCluserName
 - 本地組態狀態
 - RemoteConfiguration狀態
- MetroCluster節點
 - DR鏡像狀態
 - 集群間 LIF
 - 節點可達性
 - 災難復原夥伴節點

- DR輔助合作夥伴節點
- DR、DR Aux 和 HA 節點對稱關係
- 自動排程外切換
- MetroCluster配置複製
 - 遠端心跳
 - 上次發送的心跳
 - 最後一次收到的心跳
 - 虛擬伺服器流
 - 集群流
 - 儲存設備
 - 正在使用的儲存量
- MetroCluster調解器
 - 調解員地址
 - 中介端口
 - 中介器已配置
 - 中介者可達
 - 模式
- 收集器伺服效能指標
 - 收集時間
 - 查詢的是應用程式介面API端點Active IQ Unified Manager
 - 回應時間
 - 記錄數
 - AIQUMInstance IP
 - CollectorInstance ID

下表為針對ONTAP VMware所收集之效能資料的代表性範例：

- 叢集名稱
- 叢集UUID
- ObjectID
- Volume名稱
- Volume執行個體UUID
- Vserver
- VserverUUID
- 節點序列
- ONTAPVersion
- AIQUM版本
- Aggregate
- AggregateUUID
- 資源金鑰
- 時間戳記
- IOPSPerTb
- 延遲
- 讀入延遲
- WriteMBps
- QoSMinThroughputLatency
- QoSNBladeLatency
- 已使用的「總部」
- CacheMissRatio
- 其他延遲
- QoSAggreggreggateLatency
- IOPS
- QoSNetworkLetency
- 可用作業
- 寫入延遲
- QoSClocks延遲
- QoSClusterInterconnectLatency
- 其他MBps
- QoSCopLatency
- QoSDBladeLatency

- 使用率
- ReadIOPS
- Mbps
- 其他IOPS
- QoSPolicyGroupLatency
- ReadMBps
- QoSSyncdSnapmirmirrorLatency
- 系統級數據
 - 寫入/讀取/其他/總 IOPS
 - 寫入/讀取/其他/總吞吐量
 - 寫入/讀取/其他/總延遲
- 寫入IOPS

限制私有資料存取時移除的項目 **** : **Learn **

在Keystone Collector上啟用「移除私有資料」選項時、ONTAP 下列使用資訊將不再用於支援。此選項預設為啟用。

- 叢集名稱
- 叢集位置
- 叢集聯絡人
- 節點名稱
- Aggregate名稱
- Volume名稱
- QoSAdaptivePolicyGroup名稱
- QoSPolicyGroup名稱
- Vserver名稱
- 儲存LUN名稱
- Aggregate名稱
- 邏輯單元名稱
- SVM名稱
- AIQUMInstance IP
- FlexClone
- RemoteClusterName

資料收集StorageGRID

為 **StorageGRID** 收集的 **** 相關資料： **Learn **

下列清單為代表性的範例 Logical Data 收集StorageGRID 對象：

- 身分證StorageGRID
- 帳戶ID
- 帳戶名稱
- 帳戶配額位元組
- 儲存區名稱
- 儲存區物件計數
- 儲存區資料位元組

下列清單為代表性的範例 Physical Data 收集StorageGRID 對象：

- 身分證StorageGRID
- 節點ID
- 站台ID
- 站台名稱
- 執行個體
- 顯示儲存使用率位元組StorageGRID
- 支援中繼資料位元組的儲存使用率StorageGRID

以下列表是 `Availability/Uptime Data` 為StorageGRID收集：

- SLA 正常運作時間百分比

限制私有資料存取時移除的項目 ****： **Learn **

在Keystone Collector上啟用「移除私有資料」選項時、StorageGRID 下列使用資訊將不再用於支援。此選項預設為啟用。

- 帳戶名稱
- BucketName
- 站台名稱
- 執行個體/節點名稱

遙測數據收集

從Keystone Collector VM 收集的遙測資料：了解詳情

以下列表是針對Keystone系統收集的遙測資料的代表性樣本：

- 系統資訊
 - 作業系統名稱
 - 作業系統版本
 - 作業系統 ID
 - 系統主機名
 - 系統預設IP位址
- 系統資源使用情況
 - 系統正常運作時間
 - CPU 核心數
 - 系統負載（1分鐘、5分鐘、15分鐘）
 - 總記憶體
 - 釋放記憶體
 - 可用記憶體
 - 共享記憶體
 - 緩衝記憶體
 - 快取記憶體
 - 總掉期
 - 免費掉期
 - 快取交換
 - 磁碟檔案系統名稱
 - 磁碟大小
 - 使用的磁碟
 - 磁碟可用
 - 磁碟使用率
 - 磁碟掛載點
- 已安裝的軟體包
- 收集器配置
- 服務日誌
 - 來自Keystone服務的服務日誌

私密模式中的 Keystone

瞭解 Keystone (私有模式)

Keystone 提供 `_Private` 部署模式、也稱為 `_Dark 站台_`、以滿足您的業務和安全需求。此模式適用於有連線限制的組織。

NetApp 針對網際網路連線能力有限或無網際網路連線能力的環境（也稱為黑暗網站）、提供專屬的 Keystone STaaS 部署。這些環境是安全或隔離的環境、因為安全性、法規遵循或營運需求而限制外部通訊。

對於 NetApp Keystone 而言、為 Dark 站台提供服務意味著提供 Keystone 彈性儲存訂閱服務的方式、必須遵守這些環境的限制。這包括：

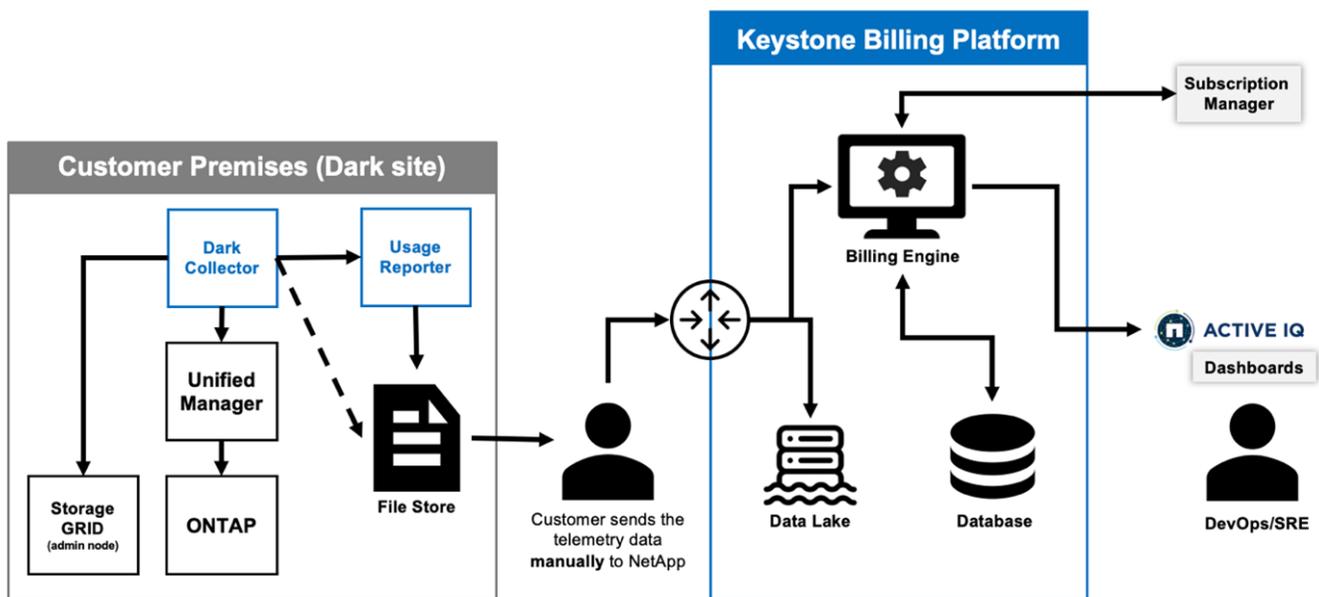
- * 本機部署 *：Keystone 可在獨立環境中獨立設定、確保不需要網際網路連線或外部人員進行設定存取。
- * 離線作業 *：所有具備健全狀況檢查與計費功能的儲存管理功能、皆可離線進行作業。
- * 安全性與法規遵循 *：Keystone 可確保部署符合黑暗網站的安全性與法規遵循要求、其中可能包括進階加密、安全存取控制及詳細的稽核功能。
- * 說明與支援 *：NetApp 提供全年無休的全球支援、並指派一位專屬 Keystone 成功經理給每個帳戶、以提供協助與疑難排解。



Keystone Collector 可在不受連線限制的情況下進行設定、也稱為 `_標準_` 模式。若要深入瞭解、請 ["瞭解 Keystone Collector"](#) 參閱。

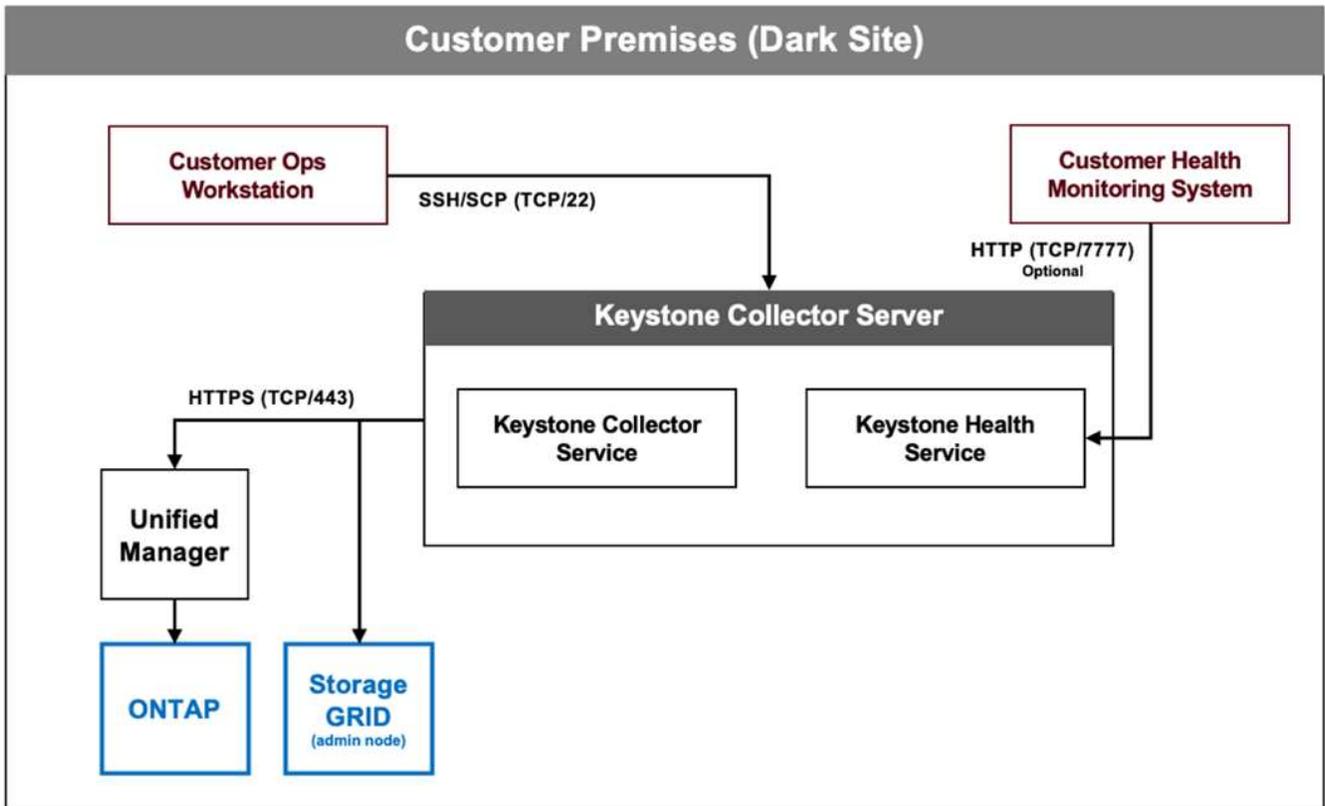
Keystone Collector 處於私有模式

Keystone Collector 負責定期從儲存系統收集使用量資料、並將度量匯出至離線使用量報告工具和本機檔案存放區。產生的檔案會以加密和純文字格式建立、然後在驗證檢查後由使用者手動轉送至 NetApp。NetApp 的 Keystone 計費平台收到後、會驗證及處理這些檔案、並將它們整合至計費與訂閱管理系統、以計算每月費用。



伺服器上的 Keystone Collector 服務的任務是定期收集使用資料、處理此資訊、以及在伺服器上本機產生使用檔

案。醫療服務會執行系統健全狀況檢查、並設計為與客戶使用的健全狀況監控系統相容。這些報告可供使用者離線存取、可進行驗證並協助疑難排解問題。



準備以私有模式安裝Keystone Collector

在沒有網際網路存取的環境中安裝 Keystone Collector 之前（也稱為 _Dark 站台_ 或 _Private 模式_）、請先確保系統已準備好必要的軟體、並符合所有必要的先決條件。

VMware vSphere 的需求

- 作業系統：VMware vCenter 伺服器 and ESXi 8.0 或更高版本
- 核心：1 個 CPU
- RAM：2 GB
- 磁碟空間：20 GB vDisk

Linux 的需求

- 作業系統（選擇一項）：
 - Red Hat Enterprise Linux (RHEL) 8.6 或任何更高版本的 8.x 系列
 - Red Hat Enterprise Linux 9.0 或更高版本
 - Debian 12.
- 核心：2 個 CPU

- RAM：4 GB
- 磁碟空間：50 GB vDisk
 - 至少 2 GB 可用空間 `/var/lib/`
 - 至少 48 GB 可用空間 `/opt/netapp`

同一部伺服器也應安裝下列協力廠商套件。如果透過儲存庫提供、這些套件將會自動安裝為先決條件：

- RHEL 8.6+ (8.x)
 - `python3 >=v3.6.8` 、 `python3 <=v3.9.13`
 - `podman`
 - `SOS`
 - `yum` 公用程式
 - `python3-DNF-plugin-versionlock`
- RHEL 9.0+
 - `python3 >= v3.9.0`, `python3 <= v3.9.13`
 - `podman`
 - `SOS`
 - `yum` 公用程式
 - `python3-DNF-plugin-versionlock`
- Debian v12
 - `python3 >= v3.9.0` 、 `python3 <= v3.12.0`
 - `podman`
 - 報告

網路需求

Keystone Collector 的網路需求包括：

- Active IQ Unified Manager (Unified Manager) 9.10 或更新版本、在啟用 API 閘道功能的伺服器上設定。
- Keystone Collector 伺服器應可在連接埠 443 (HTTPS) 上存取 Unified Manager 伺服器。
- Unified Manager 伺服器上的 Keystone Collector 應設定具有應用程式使用者權限的服務帳戶。
- 不需要外部網際網路連線。
- 每個月從Keystone Collector 匯出一個文件並透過電子郵件發送給NetApp支援團隊。如需了解如何聯絡支援團隊的更多信息，請參閱 "[取得 Keystone 的說明](#)"。

以私人模式安裝 **Keystone Collector**

請完成幾個步驟、以便在無法存取網際網路的環境中安裝 Keystone Collector 、也稱為「暗網站」或「私人模式」。這類安裝最適合安全的站台。

您可以在 VMware vSphere 系統上部署 Keystone Collector、或視需求在 Linux 系統上安裝。請遵循與您所選選項相對應的安裝步驟。

在 VMware vSphere 上部署

請遵循下列步驟：

1. 從下載 OVA 範本檔案 "[NetApp Keystone 入口網站](#)"。
2. 如需使用 OVA 檔案部署 Keystone 收集器的步驟"[部署OVA範本](#)"、請參閱一節。

在 Linux 上安裝

Keystone Collector 軟體是根據 Linux 套裝作業系統、使用提供的 .deb 或 .rpm 檔案安裝在 Linux 伺服器上。

請依照下列步驟在Linux伺服器上安裝軟體：

1. 將 Keystone Collector 安裝檔案下載或傳輸至 Linux 伺服器：

```
keystone-collector-<version>.noarch.rpm
```

2. 在伺服器上開啟終端機、然後執行下列命令以開始安裝。

- * 使用 Debian 套件 *

```
dpkg -i keystone-collector_<version>_all.deb
```

- * 使用 RPM 檔案 *

```
yum install keystone-collector-<version>.noarch.rpm
```

或

```
rpm -i keystone-collector-<version>.noarch.rpm
```

3. `y`當系統提示您安裝套件時、請輸入。

在私人模式中設定 Keystone Collector

完成一些組態工作、讓 Keystone Collector 能夠在無法存取網際網路的環境中收集使用資料、也稱為「暗站」或「私人模式」。這是一次性活動、可啟動所需元件、並將其與儲存環境建立關聯。設定完成後、Keystone 收集器會監控由 Active IQ Unified Manager 管理的所有 ONTAP 叢集。



Keystone Collector 提供 Keystone Collector Management 終端機使用者介面（TUI）公用程式、可執行組態和監控活動。您可以使用各種鍵盤控制項（例如Enter和方向鍵）來選取選項、並瀏覽此TUI。

步驟

1. 啟動 Keystone Collector 管理 TUI 公用程式：

keystone-collector-tui

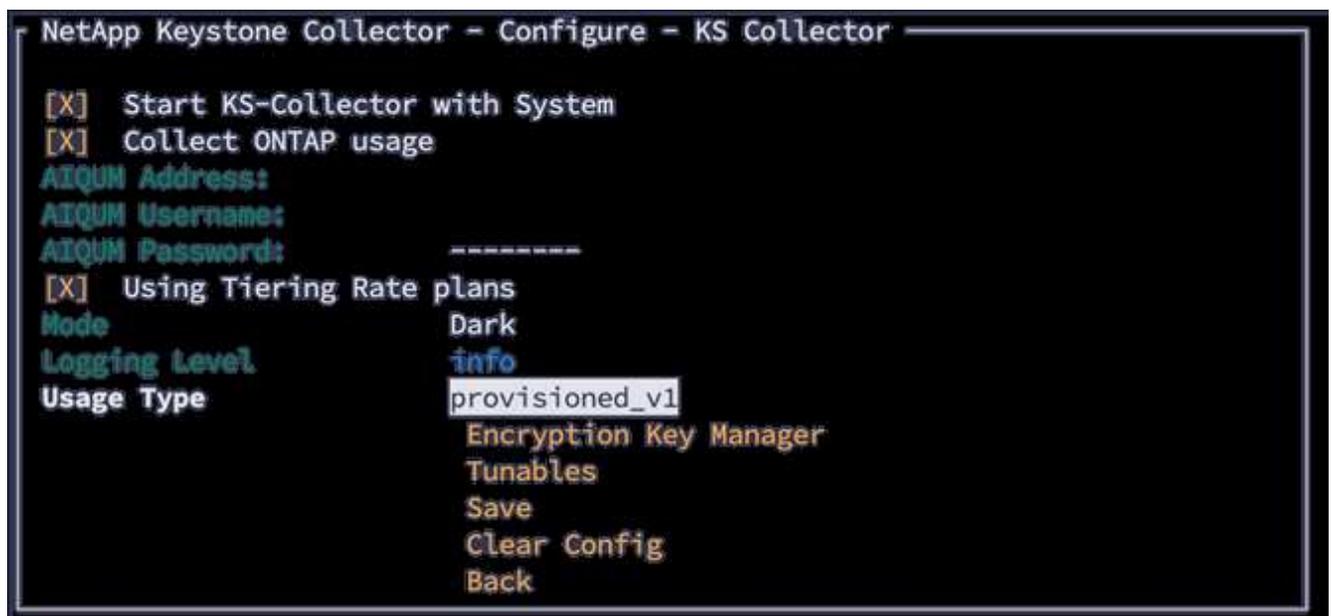
- 移至 * 組態 > 進階 * 。
- 切換 **Darksite Mode** 選項。



- 選擇*保存*。
- 前往 * 組態 > KS-Collector* 以設定 Keystone Collector 。
- 切換 * 使用 System* 啟動 KS Collector 欄位。
- 切換 * 收集 ONTAP 使用量 * 欄位。新增 Active IQ Unified Manager (Unified Manager) 伺服器和使用者帳戶的詳細資料。
- * 選用 * : 如果訂閱需要資料分層、請切換 * 使用分層率方案 * 欄位。
- 根據購買的訂閱類型、更新 * 使用類型 * 。



在設定之前、請確認與 NetApp 訂閱相關的使用類型。



10. 選擇*保存*。
11. 移至 * 組態 > KS-Collector* 以產生 Keystone Collector 金鑰組。
12. 移至 * 加密金鑰管理員 * 、然後按 Enter 鍵。

```
NetApp Keystone Collector - Configure - KS Collector

[X] Start KS-Collector with System
[X] Collect ONTAP usage
AIQUM Address:
AIQUM Username:
AIQUM Password: -----
[ ] Using Tiering Rate plans
Mode                Dark
Logging Level       info
Usage Type          provisioned_v1
                    Encryption Key Manager
                    Tunables
                    Save
                    Clear Config
                    Back
```

13. 選取 * 產生收集器鍵入式 * 、然後按 Enter 鍵。

```
NetApp Keystone Collector - Configure - KS Collector - Key Manager

                    Generate Collector Keypair
                    Back
```

14. 返回 TUI 的主畫面並驗證 **Service Status** 資訊、以確保 Keystone 收集器處於正常狀態。系統應顯示服務處於 * 整體：健全 * 狀態。如果在此期間之後整體狀態仍不正常、請等待 10 分鐘、檢閱先前的組態步驟、並聯絡 NetApp 支援團隊。

```
Service Status
Overall: Healthy
UM-Dark: Running
ks-billing: Running
ks-collector-dark: Running
Recent collector data: Healthy
ONTAP REST response time: Healthy
DB Disk space: Healthy
DB Disk space 30d: Healthy
DB API responses: Healthy
DB Concurrent flushes: Healthy
DB Slow insert rate: Healthy
```

15. 選取首頁畫面上的 * 結束至 Shell* 選項、結束 Keystone Collector 管理 TUI 。
16. 擷取產生的公開金鑰：

```
~/collector-public.pem
```

17. 將此文件透過電子郵件發送至 ng-keystone-secure-site-upload@netapp.com (用於安全的非 USPS 網站) 或 ng-keystone-secure-site-usps-upload@netapp.com (用於安全的 USPS 網站) 。

匯出使用報告

您應該在每個月底將每月使用摘要報告傳送給 NetApp 。您可以手動產生此報告。

請依照下列步驟產生使用報告：

1. 前往 Keystone Collector TUI 首頁畫面上的 * 匯出使用量 * 。
2. 收集文件並將其發送至 ng-keystone-secure-site-upload@netapp.com (用於安全的非 USPS 網站) 或發送至 ng-keystone-secure-site-usps-upload@netapp.com (用於安全的 USPS 網站) 。

Keystone 收集器會同時產生一個清除檔案和加密檔案、並手動傳送至 NetApp 。Clear 檔案報告包含下列可由客戶驗證的詳細資料。

```
node_serial,derived_service_level,usage_tib,start,duration_seconds
123456781,extreme,25.0,2024-05-27T00:00:00,86400
123456782,premium,10.0,2024-05-27T00:00:00,86400
123456783,standard,15.0,2024-05-27T00:00:00,86400

<Signature>
31b3d8eb338ee319ef1

-----BEGIN PUBLIC KEY-----
31b3d8eb338ee319ef1
-----END PUBLIC KEY-----
```

升級ONTAP

Keystone 收集器支援透過 TUI 進行 ONTAP 升級。

請依照下列步驟升級 ONTAP：

1. 前往 * 維護 > ONTAP 升級 Webserver* 。
2. 將 ONTAP 升級映像檔案複製到 * / opt NetApp / ONTAP 升級 /* 、然後選取 * 啟動 Webserver* 以啟動網路伺服器。



3. 請前往 `http://<collector-ip>:8000` 使用網頁瀏覽器以取得升級協助。

重新啟動 Keystone Collector

您可以透過 TUI 重新啟動 Keystone Collector 服務。移至 TUI 中的 * 維護 > 重新啟動 Collector* 服務。這會重新啟動所有收集器服務、並可從 TUI 主畫面監控其狀態。



在私有模式中監控 **Keystone Collector** 健全狀況

您可以使用任何支援 HTTP 要求的監控系統來監控 **Keystone Collector** 的健全狀況。

根據預設、**Keystone** 健全狀況服務不接受來自 localhost 以外任何 IP 的連線。**Keystone**健全狀況端點為 /uber/health、並在連接埠上偵聽**Keystone Collector** 伺服器的所有介面 7777。查詢時、端點會傳回具有Json輸出的HTTP要求狀態代碼作為回應、說明**Keystone Collector**系統的狀態。

Json實體提供的整體健全狀況狀態 is_healthy 屬性、為布林值、以及每個元件的詳細狀態清單 component_details 屬性。

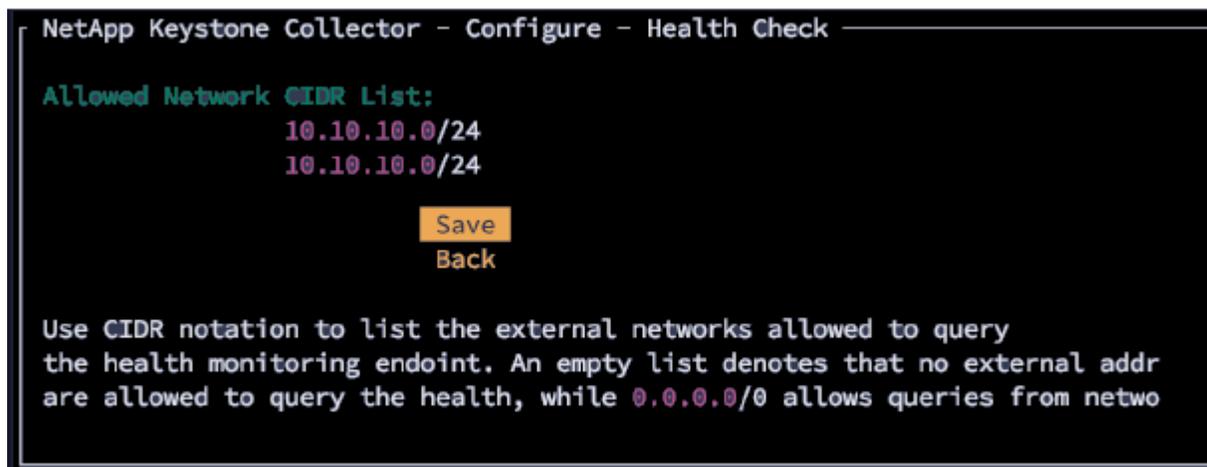
範例如下：

```
$ curl http://127.0.0.1:7777/uber/health
{"is_healthy": true, "component_details": {"vicmet": "Running", "ks-
collector": "Running", "ks-billing": "Running", "chronyd": "Running"}}
```

這些狀態代碼會傳回：

- * 200*：表示所有受監控的元件都正常運作
- * 503 *：表示一或多個元件不正常
- * 409*：表示查詢健全狀況狀態的HTTP用戶端不在「允許」清單中、這是允許的網路CIDR清單。對於此狀態、不會傳回任何健全狀況資訊。

「允許」清單使用網路CIDR方法來控制哪些網路裝置可以查詢**Keystone**健全狀況系統。如果您收到 403 錯誤、請將監控系統新增至 ***Keystone Collector Management TUI > Configure > Health Monitoring** * 的 allow 清單。

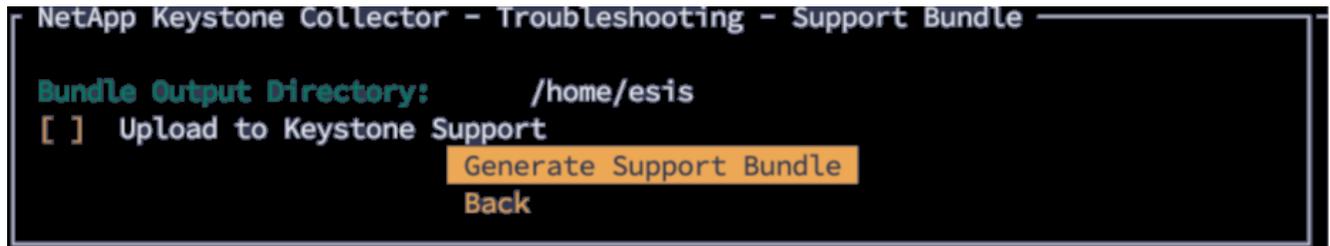


產生並收集支援套裝組合

若要疑難排解 Keystone 收集器的問題、您可以與 NetApp 支援部門合作、他們可能會要求提供 *.tar* 檔案。您可以透過 Keystone Collector 管理 TUI 公用程式產生此檔案。

請依照下列步驟產生一個 *.tar* 檔案：

1. 請參閱*疑難排解>產生支援產品組合*。
2. 選擇儲存套件的位置、然後按一下 * 產生支援套件 *。



```
NetApp Keystone Collector - Troubleshooting - Support Bundle
Bundle Output Directory: /home/esis
[ ] Upload to Keystone Support
    Generate Support Bundle
    Back
```

此程序會 `tar` 在所述位置建立套件、並可與 NetApp 分享以解決疑難排解問題。

3. 下載檔案後，您可以將其附加到 Keystone ServiceNow 支援票證。有關提高票數的信息，請參閱 "[正在產生服務要求](#)"。

版權資訊

Copyright © 2026 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 保留隨時變更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。