安全

Data Infrastructure Insights

NetApp
February 03, 2026

目錄

安全

Data Infrastructure Insights安全

產品和客戶資料安全對於NetApp至關重要。Data Infrastructure Insights在整個發布生命週期中遵循安全最佳實踐，以確保以最佳方式保護客戶資訊和資料的安全。

安全概述

實體安全

Data Infrastructure Insights生產基礎設施託管在 Amazon Web Services (AWS) 中。Data Infrastructure Insights生產伺服器的實體和環境安全相關控制（包括建築物以及門上使用的鎖或鑰匙）由 AWS 管理。根據 AWS 的說法：「專業安全人員利用視訊監控、入侵偵測系統和其他電子手段在周邊和建築物入口處控制實體存取。授權人員利用多因素身份驗證機制存取資料中心樓層。 」

Data Infrastructure Insights遵循"共擔責任模型"由 AWS 描述。

產品安全

Data Infrastructure Insights遵循符合敏捷原則的開發生命週期，因此與較長的發布週期開發方法相比，我們可以更快地解決任何面向安全的軟體缺陷。使用持續整合方法，我們能夠快速回應功能和安全變更。變更管理程序和政策定義了變更發生的時間和方式，並有助於維持生產環境的穩定性。任何有影響的變更在發佈到生產環境之前都會得到正式溝通、協調、適當審查和批准。

網路安全

Data Infrastructure Insights環境中的資源網路存取由基於主機的防火牆控制。每個資源（例如負載平衡器或虛擬機器執行個體）都有一個基於主機的防火牆，將入站流量限製到該資源執行其功能所需的連接埠。

Data Infrastructure Insights使用包括入侵偵測服務在內的各種機制來監控生產環境中的安全異常。

風險評估

Data Infrastructure Insights團隊遵循正式的風險評估流程，提供系統化、可重複的方法來識別和評估風險，以便透過風險處理計劃對其進行適當的管理。

資料保護

Data Infrastructure Insights生產環境建立在高度冗餘的基礎設施中，利用所有服務和組件的多個可用區域。除了利用高可用性和冗餘的運算基礎設施外，還會定期備份關鍵資料並定期測試復原。正式的備份政策和程序可最大限度地減少業務活動中斷的影響，並保護業務流程免受資訊系統故障或災難的影響，並確保及時、充分地恢復。

身份驗證和存取管理

所有客戶對Data Infrastructure Insights的存取都是透過 https 上的瀏覽器 UI 互動完成的。身份驗證透過第三方服務 Auth0 完成。 NetApp已將其集中作為所有雲端資料服務的身份驗證層。

Data Infrastructure Insights遵循行業最佳實踐，包括圍繞Data Infrastructure Insights生產環境的邏輯存取的「最小特權」和「基於角色的存取控制」。存取權限嚴格按照需求進行控制，並且僅使用多因素身份驗證機制授予選

定的授權人員。

客戶資料的收集和保護

所有客戶資料在透過公共網路傳輸時和靜止時均經過加密。Data Infrastructure Insights利用系統各點的加密技術來保護客戶數據，使用的技術包括傳輸層安全性 (TLS) 和行業標準 AES-256 演算法。

客戶取消配置

電子郵件通知會以不同的時間間隔發送，告知客戶他們的訂閱即將到期。訂閱到期後，UI 將受到限制，並且資料收集的寬限期將開始。然後透過電子郵件通知客戶。試用訂閱有 14 天的寬限期，付費訂閱帳號有 28 天的寬限期。寬限期過後，將透過電子郵件通知客戶該帳戶將在 2 天內被刪除。付費客戶也可以直接要求停止服務。

在寬限期結束時或確認客戶終止其帳戶的請求後，Data Infrastructure Insights營運 (SRE) 團隊將刪除過期的租戶和所有相關的客戶資料。無論哪種情況，SRE 團隊都會執行 API 呼叫來刪除該帳戶。 API 呼叫刪除租用戶實例和所有客戶資料。透過呼叫相同的 API 並驗證客戶租用戶狀態是否為「已刪除」來驗證客戶刪除。

安全事件管理

Data Infrastructure Insights與 NetApp 的產品安全事件回應團隊 (PSIRT) 流程集成，以尋找、評估和解決已知漏洞。 PSIRT 從多個管道獲取漏洞訊息，包括客戶報告、內部工程以及 CVE 資料庫等廣泛認可的來源。

如果Data Infrastructure Insights工程團隊偵測到問題，該團隊將啟動 PSIRT 流程，評估並可能修復該問題。

Data Infrastructure Insights客戶或研究人員也可能會發現Data Infrastructure Insights產品的安全問題，並將該問題報告給技術支援或直接報告給 NetApp 的事件回應團隊。在這些情況下，Data Infrastructure Insights團隊將啟動 PSIRT 流程，評估並可能修復問題。

漏洞和滲透測試

Data Infrastructure Insights遵循行業最佳實踐，並使用內部和外部安全專業人員和公司定期執行漏洞和滲透測試。

安全意識培訓

所有Data Infrastructure Insights人員都接受針對各自角色開發的安全培訓，以確保每位員工都能夠應對其角色特定的安全挑戰。

遵守

Data Infrastructure Insights對其安全性、流程和服務進行獨立的第三方稽核和外部持牌 CPA 事務所的驗證，包括完成 SOC 2 稽核。

NetApp安全公告

您可以查看 NetApp 的可用安全公告"這裡"。

資訊和區域

NetApp非常重視客戶資訊的安全。以下是Data Infrastructure Insights儲存您的資訊的方式和位置。

Data Infrastructure Insights儲存哪些資訊？

Data Infrastructure Insights儲存以下資訊：

- 效能數據

  性能數據是提供有關受監控設備/源性能的信息的時間序列數據。例如，這包括儲存系統傳送的 IO 數量、光纖通道連接埠的吞吐量、Web 伺服器傳送的頁面數量、資料庫的回應時間等等。

- 庫存數據

  庫存資料由描述受監控設備/來源及其配置方式的元資料組成。例如，這包括安裝的硬體和軟體版本、儲存系統中的磁碟和 LUN、虛擬機器的 CPU 核心、RAM 和磁碟、資料庫的表空間、SAN 交換器上的連接埠數量和類型、目錄/檔案名稱（如果啟用了儲存工作負載安全性）等。

- 配置數據

  這總結了用於管理客戶庫存和操作的客戶提供的配置數據，例如受監控設備的主機名稱或 IP 位址、輪詢間隔、逾時值等。

- 秘密

  機密包括Data Infrastructure Insights獲取單元用於存取客戶設備和服務的憑證。這些憑證使用強非對稱加密進行加密，並且私鑰僅儲存在採集單元上，永遠不會離開客戶環境。由於這種設計，即使是特權Data Infrastructure InsightsSRE 也無法以純文字形式存取客戶機密。

- 功能數據

  這是NetApp提供雲端資料服務時產生的數據，用於為NetApp提供雲端資料服務的開發、部署、營運、維護和保護資訊。功能數據不包含客戶資訊或個人資訊。

- 使用者存取數據

  允許NetApp Console與區域Data Infrastructure Insights站點通訊的身份驗證和存取訊息，包括與使用者授權相關的資料。

- 儲存工作負載安全用戶目錄數據

  如果啟用了工作負載安全功能且客戶選擇啟用使用者目錄收集器，系統將儲存從 Active Directory 收集的使用者顯示名稱、公司電子郵件地址和其他資訊。

> ⓘ 使用者目錄資料是指工作負載安全使用者目錄資料收集器收集的使用者目錄信息，而不是Data Infrastructure Insights/工作負載安全使用者本身的資料。

沒有從基礎設施和服務資源收集明確的個人資料。收集的資訊僅包括效能指標、配置資訊和基礎設施元數據，與許多供應商電話主頁非常相似，包括NetApp自動支援和 ActiveIQ。但是，根據客戶的命名約定，共用、磁碟區、虛擬機器、配額樹、應用程式等的資料可能包含個人識別資訊。

如果啟用了工作負載安全，系統也會查看 SMB 或其他共用上的檔案和目錄名稱，其中可能包含個人識別資訊。當客戶啟用工作負載安全性使用者目錄收集器（其本質上是透過 Active Directory 將 Windows SID 對應到使用者名稱）時，Data Infrastructure Insights將收集和儲存顯示名稱、公司電子郵件地址和任何選定的附加屬性。

此外，還會維護Data Infrastructure Insights的存取日誌，其中包含用於登入服務的使用者 IP 和電子郵件地址。

我的資訊儲存在哪裡？

Data Infrastructure Insights根據您創建環境的區域儲存資訊。

主機區域中儲存以下資訊：

- 遙測和資產/物件訊息，包括計數器和性能指標
- 採集單元資訊
- 功能數據
- 審計Data Infrastructure Insights內部使用者活動的訊息
- 工作負載安全性 Active Directory 訊息
- 工作負載安全審計信息

無論您的Data Infrastructure Insights環境託管在哪個區域，以下資訊都位於美國：

- 環境站點（有時稱為“租戶”）訊息，例如站點/帳戶所有者。
- 允許NetApp Console與區域Data Infrastructure Insights通訊的信息，包括與使用者授權有關的任何資訊。
- 與Data Infrastructure Insights用戶和租戶之間的關係相關的資訊。

主辦地區

主辦地區包括：

- 美國：us-east-1
- 歐洲、中東和非洲地區：eu-central-1
- 亞太地區：ap-southeast-2

更多資訊

您可以透過以下連結了解更多有關 NetApp 隱私和安全性的資訊：

- "信任中心"
- "跨境資料傳輸"
- "具有約束力的公司規則"
- "回應第三方資料請求"
- "NetApp隱私原則"

安全管理工具

Data Infrastructure Insights包括安全功能，可讓您的環境以增強的安全性運作。這些功能包括加密、密碼雜湊的改進，以及更改內部使用者密碼以及加密和解密密碼的金鑰對的能力。

為了保護敏感數據， NetApp建議您在安裝或升級後變更預設金鑰和_Acquisition_使用者密碼。

資料來源加密密碼儲存在Data Infrastructure Insights中，當使用者在資料收集器設定頁面輸入密碼時，它會使用公鑰對密碼進行加密。Data Infrastructure Insights沒有解密資料收集器密碼所需的私鑰；只有採集單元 (AU) 才具有解密資料收集器密碼所需的資料收集器私鑰。

升級和安裝注意事項

當您的 Insight 系統包含非預設安全性配置（即您已重新輸入密碼）時，您必須備份您的安全性設定。安裝新軟體，或在某些情況下升級軟體，會將您的系統還原為預設安全性配置。當您的系統恢復到預設配置時，您必須恢復非預設配置才能使系統正常運作。

管理採集單元的安全

SecurityAdmin 工具可讓您管理Data Infrastructure Insights的安全選項，並在擷取單元系統上執行。安全管理包括管理金鑰和密碼、儲存和還原您建立的安全性配置或將設定還原為預設值。

開始之前

- 您必須擁有 AU 系統的管理員權限才能安裝 Acquisition Unit 軟體（其中包括 SecurityAdmin 工具）。
- 如果您有非管理員使用者隨後需要存取 SecurityAdmin 工具，則必須將他們新增至 *cisys* 群組。 *cisys* 群組是在 AU 安裝期間建立的。

安裝 AU 後，可以在擷取單元系統的下列任一位置找到 SecurityAdmin 工具：

```
Windows - <install_path>\Cloud Insights\Acquisition
Unit\acq\securityadmin\bin\securityadmin.bat
Linux - /bin/oci-securityadmin.sh
```

使用 **SecurityAdmin** 工具

以互動模式（-i）啟動 SecurityAdmin 工具。

建議以互動模式使用 SecurityAdmin 工具，以避免在命令列上傳遞可以在日誌中擷取的機密。

將顯示以下選項：

[SecurityAdmin 工具的選項（Linux）]

1. 備份

   建立包含所有密碼和金鑰的保險庫備份 zip 文件，並將文件放置在使用者指定的位置或以下預設位置：

   ```
   Windows - <install_path>\Cloud Insights\Acquisition
   Unit\acq\securityadmin\backup\vault
   Linux - /var/log/netapp/oci/backup/vault
   ```

建議妥善保管保險庫備份，因為它們包含敏感資訊。

2. 恢復

   還原已建立的保管庫的 zip 備份。一旦恢復，所有密碼和金鑰都將恢復為備份建立時存在的值。

   復原可用於同步多台伺服器上的密碼和金鑰，例如使用下列步驟：1）變更 AU 上的加密金鑰。 2）創建保險庫的備份。 3) 將保管庫備份還原到每個 AU。

3. 註冊/更新外部金鑰檢索腳本

   使用外部腳本註冊或變更用於加密或解密裝置密碼的 AU 加密金鑰。

   當您變更加密金鑰時，您應該備份新的安全配置，以便在升級或安裝後還原它。

   請注意，此選項僅在 Linux 上可用。

   當使用您自己的金鑰檢索腳本和 SecurityAdmin 工具時，請記住以下幾點：

   - 目前支援的演算法是最小 2048 位元的 RSA。
   - 該腳本必須以純文字形式傳回私鑰和公鑰。該腳本不得傳回加密的私鑰和公鑰。
   - 該腳本應傳回原始的編碼內容（僅限 PEM 格式）。
   - 外部腳本必須具有_執行_權限。

4. 輪換加密金鑰

   輪換您的加密金鑰（取消註冊當前金鑰並註冊新金鑰）。若要使用來自外部金鑰管理系統的金鑰，您必須指定公鑰 ID 和私鑰 ID。

5. 重設為預設鍵

   將取得使用者密碼和取得使用者加密金鑰重設為預設值，預設值是安裝期間提供的。

6. 更改信任庫密碼

   更改信任庫的密碼。

7. 更改金鑰庫密碼

   更改密鑰庫的密碼。

8. 加密收集器密碼

   加密資料收集器密碼。

9. 出口

   退出 SecurityAdmin 工具。

選擇您想要配置的選項並按照提示進行操作。

指定使用者來運行該工具

如果您處於受控的、注重安全的環境中，您可能沒有_cisys_群組，但仍可能希望特定使用者執行 SecurityAdmin 工具。

您可以透過手動安裝 AU 軟體並指定您想要存取的使用者/群組來實現這一點。

- 使用 API，將 CI 安裝程式下載到 AU 系統並解壓縮。
  - 您將需要一次性授權令牌。查看 API Swagger 文件（*Admin > API Access* 並選擇 *API Documentation* 連結）並找到 *GET /au/oneTimeToken* API 部分。
  - 取得令牌後，使用 *GET /au/installers/{platform}/{version}* API 下載安裝程式檔案。您需要提供平台（Linux 或 Windows）以及安裝程式版本。
- 將下載的安裝程式檔案複製到AU系統並解壓縮。
- 導覽至包含檔案的資料夾，並以 root 身分執行安裝程序，指定使用者和群組：

```
./cloudinsights-install.sh <User> <Group>
```

如果指定的使用者和/或群組不存在，則將建立它們。使用者將有權存取 SecurityAdmin 工具。

更新或刪除代理

可以使用 SecurityAdmin 工具設定或刪除採集單元的代理訊息，方法是運行帶有 *-pr* 參數的工具：

```
[root@ci-eng-linau bin]# ./securityadmin -pr
usage: securityadmin -pr -ap <arg> | -h | -rp | -upr <arg>

The purpose of this tool is to enable reconfiguration of security aspects
of the Acquisition Unit such as encryption keys, and proxy configuration,
etc. For more information about this tool, please check the Data
Infrastructure Insights
Documentation.

-ap,--add-proxy <arg>       add a proxy server.  Arguments: ip=ip
                             port=port user=user password=password
                             domain=domain
                             (Note: Always use double quote(") or single
                             quote(') around user and password to escape
                             any special characters, e.g., <, >, ~, `, ^,
                             !
                             For example: user="test" password="t'!<@1"
                             Note: domain is required if the proxy auth
                             scheme is NTLM.)
-h,--help
-rp,--remove-proxy          remove proxy server
-upr,--update-proxy <arg>   update a proxy.  Arguments: ip=ip port=port
                             user=user password=password domain=domain
                             (Note: Always use double quote(") or single
                             quote(') around user and password to escape
                             any special characters, e.g., <, >, ~, `, ^,
                             !
                             For example: user="test" password="t'!<@1"
                             Note: domain is required if the proxy auth
                             scheme is NTLM.)
```

例如，要刪除代理，請執行以下命令：

```
 [root@ci-eng-linau bin]# ./securityadmin -pr -rp
```

運行該指令後必須重新啟動採集單元。

要更新代理，命令是

```
./securityadmin -pr -upr <arg>
```

外部密鑰檢索

如果您提供 UNIX shell 腳本，則取得單元可以執行該腳本從您的金鑰管理系統中擷取 私鑰 和 公鑰。

為了檢索金鑰， Data Infrastructure Insights將執行腳本，並傳遞兩個參數：*key id* 和 *key type*。 *Key id* 可用來識別金鑰管理系統中的金鑰。 _密鑰類型_可以是「公共」或「私人」。當密鑰類型為“公共”時，腳本必須傳回公鑰。當金鑰類型為“private”時，必須傳回私鑰。

若要將密鑰傳回採集單元，腳本必須將密鑰列印到標準輸出。腳本必須僅將密鑰列印到標準輸出；不得將任何其他文字列印到標準輸出。一旦請求的鍵被列印到標準輸出，腳本必須以退出代碼 0 退出；任何其他返回代碼都被視為錯誤。

該腳本必須使用 SecurityAdmin 工具向採集單元註冊，該工具將與採集單元一起執行該腳本。該腳本必須具有 root 和「cisys」使用者的_read_和_execute_權限。如果註冊後shell腳本被修改，則必須將修改後的shell腳本重新向採集單位註冊。

輸入參數：密鑰ID	密鑰標識符用於在客戶密鑰管理系統中識別密鑰。
輸入參數：密鑰類型	公共或私人。
輸出	必須將請求的密鑰列印到標準輸出。目前支援 2048 位元 RSA 金鑰。密鑰必須按照以下格式進行編碼和列印 - 私鑰格式 - PEM、DER 編碼的 PKCS8 PrivateKeyInfo RFC 5958 公鑰格式 - PEM、DER 編碼的 X.509 SubjectPublicKeyInfo RFC 5280
退出代碼	退出代碼為零表示成功。所有其他退出值均視為失敗。
腳本權限	腳本必須具有 root 和「cisys」使用者的讀取和執行權限。
紀錄	腳本執行被記錄。日誌可以在以下位置找到 - /var/log/netapp/cloudinsights/securityadmin/securityadmin.log /var/log/netapp/cloudinsights/acq/acq.log

加密用於 **API** 的密碼

選項 8 允許您加密密碼，然後您可以透過 API 將其傳遞給資料收集器。

以互動模式啟動 SecurityAdmin 工具並選擇選項 8：加密密碼。

```
 securityadmin.sh -i
系統會提示您輸入要加密的密碼。請注意，您鍵入的字元不會顯示在螢幕上。出現提示時重新輸入密碼。
```

或者，如果您要在腳本中使用該命令，請在命令列上使用帶有「-enc」參數的_securityadmin.sh_，傳遞未加密的密碼：

```
 securityadmin -enc mypassword
image:SecurityAdmin_Encrypt_Key_API_CLI_Example.png["CLI 範例"]
```

加密的密碼顯示在螢幕上。複製整個字串，包括任何前導或尾隨符號。

[交互模式加密密碼，寬度=640]

若要將加密的密碼傳送給資料收集器，您可以使用資料收集 API。可以在 管理 **> API** 存取 中找到此 API 的 swagger，然後按一下「API 文件」連結。選擇「資料收集」API 類型。在 *data_collection.data_collector* 標題下，為本範例選擇 */collector/datasources* POST API。

[資料收集API]

如果將 *preEncrypted* 選項設為 *True*，則透過 API 指令傳遞的任何密碼都將被視為*已加密*；API 不會重新加密密碼。建置 API 時，只需將先前加密的密碼貼到適當的位置。

[API 範例，寬度=600]

版權資訊

商標資訊