安全性

Data Infrastructure Insights

NetApp
October 08, 2025

目錄

安全性

資料基礎架構洞見安全性

產品與客戶資料安全在NetApp是最重要的。Data Infrastructure Insights 在整個版本生命週期中遵循安全性最佳實務做法、確保以最佳方式保護客戶資訊和資料。

安全性總覽

實體安全性

Data Infrastructure Insights 正式作業基礎架構是以 Amazon Web Services （ AWS ）代管。資料基礎架構 Insights 正式作業伺服器的實體和環境安全相關控管措施、包括建築物、門上使用的鎖或鑰匙、均由 AWS 管理。根據AWS：「實體存取是由專業安全人員在邊界和建築物入口點控制、利用視訊監控、入侵偵測系統及其他電子方式。授權人員利用多因素驗證機制來存取資料中心樓層。」

Data Infrastructure Insights 遵循 "共同責任模式"AWS 所述的最佳實務做法。

產品安全性

Data Infrastructure Insights 遵循敏捷式開發原則的開發生命週期、因此相較於較長的發行週期開發方法、我們可以更快速地解決任何以安全為導向的軟體瑕疵。使用持續整合方法、我們能夠快速回應功能與安全性的變更。變更管理程序和原則定義變更的發生時間和方式、並有助於維持正式作業環境的穩定性。任何有影響力的變更都會在正式發佈至正式環境之前、正式傳達、協調、適當審查及核准。

網路安全

資料基礎架構 Insights 環境中的資源網路存取是由主機型防火牆所控制。每個資源（例如負載平衡器或虛擬機器執行個體）都有主機型防火牆、可將傳入流量限制在該資源執行其功能所需的連接埠。

Data Infrastructure Insights 使用各種機制、包括入侵偵測服務、來監控正式作業環境的安全異常狀況。

風險評估

Data Infrastructure Insights 團隊遵循正式化的風險評估程序、提供系統化、可重複的方法來識別及評估風險、以便透過風險處理計畫妥善管理風險。

資料保護

Data Infrastructure Insights 正式作業環境是在高度備援的基礎架構中設定、並針對所有服務和元件使用多個可用性區域。除了運用高可用度和備援的運算基礎架構、還會定期備份關鍵資料、並定期測試還原作業。正式備份原則與程序可將業務活動中斷的影響降至最低、並保護業務流程免受資訊系統或災難的故障影響、確保其能及時且充分地恢復運作。

驗證與存取管理

所有客戶存取 Data Infrastructure Insights 都是透過 https 的瀏覽器 UI 互動來完成。驗證是透過第三方服務（驗證0）來完成。NetApp已將此點集中做為所有雲端資料服務的驗證層。

Data Infrastructure Insights 遵循產業最佳實務做法、包括「最低權限」和「角色型存取控制」、以邏輯方式存

取 Data Infrastructure Insights 正式作業環境。存取權是嚴格控制需求、只有使用多因素驗證機制的特定授權人員才有權存取。

客戶資料的收集與保護

所有客戶資料都會在公共網路傳輸時加密、並在靜止狀態下加密。Data Infrastructure Insights 在系統的各個點使用加密技術、以包括傳輸層安全（ TLS ）和業界標準 AES-256 演算法的技術來保護客戶資料。

客戶取消資源配置

電子郵件通知會以不同的時間間隔寄出、通知客戶訂閱即將到期。訂閱一旦過期、UI就會受到限制、而且會開始收集資料的寬限期。然後透過電子郵件通知客戶。試用版訂閱有14天的寬限期、付費訂閱帳戶有28天的寬限期。寬限期到期後、系統會透過電子郵件通知客戶、該帳戶將在2天內刪除。付費客戶也可以直接申請離開服務。

資料基礎架構洞見營運（ SRE ）團隊會在寬限期結束時、或在確認客戶要求終止其帳戶時、刪除過期的租戶和所有相關的客戶資料。無論是哪一種情況、SRE團隊都會執行API呼叫來刪除帳戶。API呼叫會刪除租戶執行個體和所有客戶資料。透過呼叫相同的API並確認客戶租戶狀態為「已刪除」來驗證客戶刪除。

安全性事件管理

資料基礎架構洞見與 NetApp 的產品安全事件回應團隊（ PSIRT ）程序整合、可尋找、評估及解決已知的弱點。SIRT從多個管道接收弱點資訊、包括客戶報告、內部工程、以及廣為人知的來源（例如、CVE資料庫）。

如果 Data Infrastructure Insights 工程團隊偵測到問題、團隊將會啟動 PSIRT 程序、評估問題、並可能修正問題。

此外、資料基礎架構洞見客戶或研究人員也可能發現資料基礎架構洞見產品的安全問題、並將問題回報給技術支援部門或直接回報給 NetApp 的事件回應團隊。在這些案例中、 Data Infrastructure Insights 團隊將啟動 PSIRT 程序、評估問題、並可能修正問題。

弱點與滲透測試

Data Infrastructure Insights 遵循業界最佳實務做法、並使用內部和外部安全專業人員和公司定期執行弱點和滲透測試。

安全性認知訓練

所有 Data Infrastructure Insights 人員都接受專為個別角色所開發的安全訓練、以確保每位員工都能因應其職務的特定安全性挑戰。

法規遵循

Data Infrastructure Insights 會從外部授權 CPA 公司執行獨立的第三方稽核和驗證、以確保其安全性、程序和服務、包括完成 SOC 2 稽核。

NetApp 安全性摘要報告

您可以查看 NetApp 的可用安全通報"請按這裡"。

資訊與地區

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

Data Infrastructure Insights 儲存哪些資訊？

Data Infrastructure Insights 儲存下列資訊：

- 效能資料

  效能資料是時間序列資料、提供有關受監控裝置/來源效能的資訊。例如、這包括儲存系統所交付的IOS數量、Fibre Channel連接埠的處理量、Web伺服器所傳送的頁數、資料庫的回應時間等等。

- 庫存資料

  庫存資料包含中繼資料、說明受監控的裝置/來源及其設定方式。例如、其中包括安裝的硬體和軟體版本、儲存系統中的磁碟和LUN、CPU核心、虛擬機器的RAM和磁碟、資料庫的表格空間、SAN交換器上的連接埠數目和類型、目錄/檔案名稱（如果已啟用儲存工作負載安全功能）等

- 組態資料

  此摘要說明客戶提供的組態資料、用於管理客戶的庫存和作業、例如受監控裝置的主機名稱或IP位址、輪詢時間間隔、逾時值等

- 機密

  機密包含 Data Infrastructure Insights Acquisition Unit 用來存取客戶裝置和服務的認證資料。這些認證會使用強式非對稱式加密來加密、私密金鑰只會儲存在擷取單元上、絕不會離開客戶環境。即使是特權資料基礎架構 Insights SRE 也無法以純文字存取客戶機密資料、因為這項設計。

- 功能資料

  這是NetApp提供雲端資料服務所產生的資料、可讓NetApp在雲端資料服務的開發、部署、營運、維護及安全方面、掌握最新資訊。功能資料不包含客戶資訊或個人資訊。

- 使用者存取資料

  允許NetApp控制台與區域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。

- 儲存工作負載安全性使用者目錄資料

  如果啟用工作負載安全功能、且客戶選擇啟用使用者目錄收集器、系統會儲存使用者顯示名稱、公司電子郵件地址、以及從Active Directory收集的其他資訊。

> ⓘ 使用者目錄資料是指由工作負載安全性使用者目錄資料收集器所收集的使用者目錄資訊、而非資料基礎架構 Insights / 工作負載安全性本身的使用者相關資料。

不會從基礎架構和服務資源收集明確的個人資料。收集的資訊僅包含效能指標、組態資訊和基礎架構中繼資料、與許多廠商的電話公司（包括NetApp自動支援和ActiveIQ）非常相似。不過、視客戶的命名慣例而定、共享

區、磁碟區、VM、qtree、 應用程式等可能包含個人識別資訊。

如果啟用「工作負載安全性」、系統會額外查看SMB或其他共用區上的檔案和目錄名稱、這些檔案和目錄名稱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（主要透過 Active Directory 將 Windows SID 對應至使用者名稱）時、「 Data Infrastructure Insights 」會收集並儲存顯示名稱、公司電子郵件地址和任何其他選取的屬性。

此外、也會維護 Data Infrastructure Insights 的存取記錄、其中包含使用者用來登入服務的 IP 和電子郵件地址。

我的資訊儲存在何處？

Data Infrastructure Insights 會根據建立環境的區域來儲存資訊。

下列資訊儲存在主機區域中：

- 遙測與資產/物件資訊、包括計數器和效能指標
- 擷取單位資訊
- 功能資料
- 資料基礎架構洞見內的使用者活動稽核資訊
- 工作負載安全性Active Directory資訊
- 工作負載安全稽核資訊

無論資料基礎架構 Insights 環境所在的地區為何、下列資訊都位於美國境內：

- 環境網站（有時稱為「租戶」）資訊、例如網站/帳戶擁有者。
- 允許NetApp控制台與區域Data Infrastructure Insights通訊的訊息，包括與使用者授權有關的任何資訊。
- 與 Data Infrastructure Insights 使用者與租戶之間關係相關的資訊。

主機區域

主機區域包括：

- 美國：美國-東1
- EMEA：EU-Central 1
- 亞太地區：AP-東南亞-2

更多資訊

如需更多關於NetApp隱私權與安全性的資訊、請參閱下列連結：

- "信任中心"
- "跨境資料傳輸"
- "具約束力的企業規則"
- "回應第三方資料要求"
- "NetApp隱私權原則"

安全性管理工具

Data Infrastructure Insights 包含安全功能、可讓您的環境以增強的安全性運作。這些功能包括增強加密、密碼雜湊、變更內部使用者密碼的能力、以及加密和解密密碼的金鑰配對。

為保護敏感資料、 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組態頁面中輸入密碼時、會使用公開金鑰來加密密碼。Data Infrastructure Insights 沒有解密資料收集器密碼所需的私密金鑰；只有擷取單元（ Aus ）具有解密資料收集器密碼所需的資料收集器私密金鑰。

升級與安裝考量

如果Insight系統包含非預設的安全性組態（亦即您有重新輸入的密碼）、則必須備份安全性組態。安裝新軟體、或在某些情況下升級軟體、會將系統還原為預設的安全組態。當系統恢復為預設組態時、您必須還原非預設組態、系統才能正常運作。

管理採購單位的安全性

安全管理工具可讓您管理 Data Infrastructure Insights 的安全選項、並可在採購單元系統上執行。安全管理包括管理金鑰和密碼、儲存及還原您建立的安全組態、或將組態還原為預設設定。

開始之前

- 您必須在 AU 系統上擁有管理權限、才能安裝擷取單元軟體（包括安全管理工具）。
- 如果您的非管理員使用者之後需要存取安全性管理工具、則必須將其新增至 *cisys* 群組。*_cisys* 群組是在 AU 安裝期間建立。

AU 安裝之後、您可以在下列任一位置的採購單元系統上找到 securityadmin 工具：

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

使用 **securityadmin Tool**

以互動模式（ -I ）啟動安全管理工具。

建議您在互動模式中使用 securityadmin 工具、以避免在命令列上傳遞機密、而這些機密可以擷取在記錄中。

畫面會顯示下列選項：

[安全性管理工具選項（ Linux ）]

1. 備份

建立包含所有密碼和金鑰的資料保險箱備份壓縮檔、並將檔案放置在使用者指定的位置、或是下列預設位置：

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

建議您將資料保險箱備份保存在安全的位置、因為其中包含敏感資訊。

2. 還原

還原所建立之資料保存庫的壓縮備份。還原之後、所有密碼和金鑰都會還原為建立備份時的現有值。

還原可用於同步多部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) 建立資料保險箱的備份。3) 將資料保險箱備份還原至每個 Aus 。

3. * 註冊 / 更新外部金鑰擷取指令碼 *

使用外部指令碼來登錄或變更用於加密或解密裝置密碼的 AU 加密金鑰。

變更加密金鑰時、您應該備份新的安全性組態、以便在升級或安裝之後還原。

請注意、此選項僅適用於 Linux 。

將您自己的金鑰擷取指令碼搭配 securityadmin 工具使用時、請謹記下列事項：

- 目前支援的演算法是 RSA 、至少 2048 位元。
- 指令碼必須以純文字傳回私密金鑰和公開金鑰。指令碼不得傳回加密的私密金鑰和公開金鑰。
- 指令碼應傳回原始編碼內容（僅限 PEM 格式）。
- 外部指令碼必須具有 *executive* 權限。

4. * 旋轉加密金鑰 *

旋轉您的加密金鑰（取消登錄目前金鑰並登錄新金鑰）。若要使用外部金鑰管理系統的金鑰、您必須指定公開金鑰 ID 和私密金鑰 ID 。

5. * 重設為預設金鑰 *

將擷取使用者密碼和擷取使用者加密金鑰重設為預設值、預設值為安裝期間提供的值。

6. * 變更信任儲存密碼 *

變更信任存放區的密碼。

7. * 變更 Keystore 密碼 *

變更 Keystore 的密碼。

8. * 加密收集器密碼 *

加密資料收集器密碼。

9. 退出

   結束安全性管理工具。

選擇您要設定的選項、然後依照提示進行。

指定要執行工具的使用者

如果您處於受控且注重安全性的環境中、您可能沒有 _cisys 群組、但仍可能需要特定使用者執行安全性管理工具。

您可以手動安裝 AU 軟體、並指定您要存取的使用者 / 群組來達成此目標。

- 使用 API 、將 CI Installer 下載至 AU 系統、然後將其解壓縮。
  - 您需要一次性授權權杖。請參閱 API Swagger 文件（ *Admin > API Access* 、然後選取 *API Documentation* （ *_API* 說明文件）連結）、並找到 *_get /au/oneTimeToken* API 一節。
  - 擁有權杖後、請使用 _get /au/installer/｛ platform ｝ / ｛ version ｝ _ API 下載安裝程式檔案。您需要提供平台（ Linux 或 Windows ）和安裝程式版本。
- 將下載的安裝程式檔案複製到 AU 系統、然後將其解壓縮。
- 瀏覽至包含檔案的資料夾、並以 root 身分執行安裝程式、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、將會建立這些使用者和 / 或群組。使用者將可存取安全管理工具。

更新或移除 **Proxy**

securityadmin 工具可用來設定或移除擷取單元的 Proxy 資訊、方法是使用 _ pr_ 參數執行工具：

```
[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、若要移除 Proxy 、請執行下列命令：

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

執行命令後、您必須重新啟動擷取單元。

若要更新 Proxy 、命令是

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

外部金鑰擷取

如果您提供 UNIX Shell 指令碼、擷取單元可以執行該指令碼、從金鑰管理系統擷取 * 私密金鑰 * 和 * 公開金鑰 *

。

為了擷取關鍵資料、 Data Infrastructure Insights 將會執行指令碼、傳入兩個參數： *key id* 和 *key type* 。*Key ID* 可用於識別金鑰管理系統中的金鑰。_Key 類型 _ 為「公開」或「私人」。當金鑰類型為「公開」時、指令碼必須傳回公開金鑰。當金鑰類型為「私密」時、必須傳回私密金鑰。

若要將金鑰傳回擷取單元、指令碼必須將金鑰列印至標準輸出。指令碼必須列印 _ 僅 _ 標準輸出金鑰；不得將其他文字列印至標準輸出。一旦要求的金鑰列印至標準輸出、指令碼必須以 0 結束代碼結束、任何其他傳回代碼都會被視為錯誤。

指令碼必須使用 securityadmin 工具在擷取單元中登錄、該工具會執行指令碼和擷取單元。指令碼必須具有 root 和「 cisys 」使用者的 *read* 和 *executive* 權限。如果在登錄後修改 Shell 指令碼、則必須重新在擷取單元中登錄修改後的 Shell 指令碼。

輸入參數：金鑰 ID	用於識別客戶金鑰管理系統中金鑰的金鑰識別碼。
輸入參數：金鑰類型	公有或私有。
輸出	要求的金鑰必須列印至標準輸出。目前支援 2048 位元 RSA 金鑰。金鑰必須以下列格式進行編碼及列印：私密金鑰格式 - PEM ， DER 編碼的 PKCS8 Private KeyInfo RFC 5958 公開金鑰格式 - PEM ， DER 編碼的 X.509 SubjectPublicKeyInfo RFC 5280
結束代碼	結束碼為零、以取得成功。所有其他跳出值都視為失敗。
指令碼權限	指令碼必須具有 root 和「 cisys 」使用者的讀取和執行權限。
記錄	記錄指令碼執行。記錄可在 - NetApp /var/log/oracle/cloudinses/securityadmin/securityadmin.log NetApp /var/log/oracle/cloudses/acq/acq.log 中找到

加密用於 **API** 的密碼

選項 8 可讓您加密密碼、然後透過 API 將密碼傳遞給資料收集器。

以互動模式啟動安全性管理工具、然後選取選項 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、您輸入的字元不會顯示在畫面上。出現提示時、請重新輸入密碼。
```

或者、如果您要在指令碼中使用命令、請在命令列上使用 *securityadmin.sh* 搭配 "-enc" 參數、並傳入未加密的密碼：

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

加密的密碼會顯示在畫面上。複製整個字串、包括任何前置或結尾符號。

[互動模式加密密碼、寬度 =640]

若要將加密密碼傳送至資料收集器、您可以使用資料收集 API 。此 API 的瀏覽器可在 * 管理 > API 存取 * 中找到、然後按一下「 API 文件」連結。選取「資料收集」 API 類型。在 _data_collection.data_collector 標題下、為此範例選擇 __collector / datasources_POST API 。

[用於資料收集的 API]

如果您將 *preEncrypted* 選項設為 *Tru* 、則任何您透過 API 命令傳遞的密碼都會被視為 * 已加密 * ； API 將不會重新加密密碼。建置 API 時、只要將先前加密的密碼貼到適當的位置即可。

[API 範例、 width=600]

版權資訊

商標資訊