安全性

Data Infrastructure Insights

NetApp
February 11, 2026

目录

安全性

Data Infrastructure Insights安全

产品和客户数据安全对于NetApp来说至关重要。Data Infrastructure Insights在整个发布生命周期中遵循安全最佳实践，以确保以最佳方式保护客户信息和数据的安全。

安全概述

物理安全

Data Infrastructure Insights生产基础设施托管在 Amazon Web Services (AWS) 中。Data Infrastructure Insights生产服务器的物理和环境安全相关控制（包括建筑物以及门上使用的锁或钥匙）由 AWS 管理。根据 AWS 的说法：“专业安全人员利用视频监控、入侵检测系统和其他电子手段在周边和建筑物入口处控制物理访问。授权人员利用多因素身份验证机制访问数据中心楼层。”

Data Infrastructure Insights遵循"共担责任模型"由 AWS 描述。

产品安全

Data Infrastructure Insights遵循符合敏捷原则的开发生命周期，因此与较长的发布周期开发方法相比，我们可以更快地解决任何面向安全的软件缺陷。使用持续集成方法，我们能够快速响应功能和安全变化。变更管理程序和政策定义了变更发生的时间和方式，并有助于维护生产环境的稳定性。任何有影响的变化在发布到生产环境之前都会得到正式沟通、协调、适当审查和批准。

网络安全

Data Infrastructure Insights环境中的资源网络访问由基于主机的防火墙控制。每个资源（例如负载均衡器或虚拟机实例）都有一个基于主机的防火墙，将入站流量限制到该资源执行其功能所需的端口。

Data Infrastructure Insights使用包括入侵检测服务在内的各种机制来监控生产环境中的安全异常。

风险评估

Data Infrastructure Insights团队遵循正式的风险评估流程，提供系统、可重复的方法来识别和评估风险，以便通过风险处理计划对其进行适当的管理。

数据保护

Data Infrastructure Insights生产环境建立在高度冗余的基础设施中，利用所有服务和组件的多个可用区域。除了利用高可用性和冗余的计算基础设施外，还会定期备份关键数据并定期测试恢复。正式的备份政策和程序可最大限度地减少业务活动中断的影响，并保护业务流程免受信息系统故障或灾难的影响，并确保及时、充分地恢复。

身份验证和访问管理

所有客户对Data Infrastructure Insights的访问都是通过 https 上的浏览器 UI 交互完成的。身份验证通过第三方服务 Auth0 完成。 NetApp已将此集中作为所有云数据服务的身份验证层。

Data Infrastructure Insights遵循行业最佳实践，包括围绕Data Infrastructure Insights生产环境的逻辑访问的“最小特权”和“基于角色的访问控制”。访问权限严格按照需求进行控制，并且仅使用多因素身份验证机制授予选定的

授权人员。

客户数据的收集和保护

所有客户数据在通过公共网络传输时均经过加密，并且在静止时也经过加密。Data Infrastructure Insights利用系统各个点的加密技术来保护客户数据，使用的技术包括传输层安全性 (TLS) 和行业标准 AES-256 算法。

客户取消配置

电子邮件通知会以不同的时间间隔发送，告知客户他们的订阅即将到期。订阅到期后，UI 将受到限制，并且数据收集的宽限期将开始。然后通过电子邮件通知客户。试用订阅有 14 天的宽限期，付费订阅帐户有 28 天的宽限期。宽限期过后，将通过电子邮件通知客户该帐户将在 2 天内被删除。付费客户也可以直接请求停止服务。

宽限期结束时或确认客户终止其帐户的请求后，Data Infrastructure Insights运营 (SRE) 团队将删除过期的租户和所有相关的客户数据。无论哪种情况，SRE 团队都会运行 API 调用来删除该帐户。 API 调用删除租户实例和所有客户数据。通过调用相同的 API 并验证客户租户状态是否为“已删除”来验证客户删除。

安全事件管理

Data Infrastructure Insights与 NetApp 的产品安全事件响应团队 (PSIRT) 流程集成，以查找、评估和解决已知漏洞。 PSIRT 从多个渠道获取漏洞信息，包括客户报告、内部工程以及 CVE 数据库等广泛认可的来源。

如果Data Infrastructure Insights工程团队检测到问题，该团队将启动 PSIRT 流程，评估并可能修复该问题。

Data Infrastructure Insights客户或研究人员也可能会发现Data Infrastructure Insights产品的安全问题，并将该问题报告给技术支持或直接报告给 NetApp 的事件响应团队。在这些情况下，Data Infrastructure Insights团队将启动 PSIRT 流程，评估并可能修复问题。

漏洞和渗透测试

Data Infrastructure Insights遵循行业最佳实践，并使用内部和外部安全专业人员和公司定期执行漏洞和渗透测试。

安全意识培训

所有Data Infrastructure Insights人员都接受针对各自角色开发的安全培训，以确保每位员工都能够应对其角色特定的安全挑战。

Compliance

Data Infrastructure Insights对其安全性、流程和服务进行独立的第三方审计和外部持牌 CPA 事务所的验证，包括完成 SOC 2 审计。

NetApp安全公告

您可以查看 NetApp 的可用安全公告"此处"。

信息和区域

NetApp非常重视客户信息的安全。以下是Data Infrastructure Insights存储您的信息的方式和位置。

Data Infrastructure Insights存储哪些信息？

Data Infrastructure Insights存储以下信息：

- 性能数据

  性能数据是提供有关受监控设备/源性能的信息的时间序列数据。例如，这包括存储系统传送的 IO 数量、光纤通道端口的吞吐量、Web 服务器传送的页面数量、数据库的响应时间等等。

- 库存数据

  库存数据由描述受监控设备/源及其配置方式的元数据组成。例如，这包括安装的硬件和软件版本、存储系统中的磁盘和 LUN、虚拟机的 CPU 核心、RAM 和磁盘、数据库的表空间、SAN 交换机上的端口数量和类型、目录/文件名（如果启用了存储工作负载安全性）等。

- 配置数据

  这总结了用于管理客户库存和操作的客户提供的配置数据，例如受监控设备的主机名或 IP 地址、轮询间隔、超时值等。

- 秘密

  机密包括Data Infrastructure Insights获取单元用于访问客户设备和服务的凭证。这些凭证使用强非对称加密进行加密，并且私钥仅存储在采集单元上，永远不会离开客户环境。由于这种设计，即使是特权Data Infrastructure InsightsSRE 也无法以纯文本形式访问客户机密。

- 功能数据

  这是NetApp提供云数据服务时生成的数据，用于为NetApp提供云数据服务的开发、部署、运营、维护和保护信息。功能数据不包含客户信息或个人信息。

- 用户访问数据

  允许NetApp Console与区域Data Infrastructure Insights站点通信的身份验证和访问信息，包括与用户授权相关的数据。

- 存储工作负载安全用户目录数据

  如果启用了工作负载安全功能并且客户选择启用用户目录收集器，系统将存储从 Active Directory 收集的用户显示名称、公司电子邮件地址和其他信息。

> ⓘ 用户目录数据是指工作负载安全用户目录数据收集器收集的用户目录信息，而不是Data Infrastructure Insights/工作负载安全用户本身的数据。

没有从基础设施和服务资源收集明确的个人数据。收集的信息仅包括性能指标、配置信息和基础设施元数据，与许多供应商电话主页非常相似，包括NetApp自动支持和 ActiveIQ。但是，根据客户的命名约定，共享、卷、虚拟机、配额树、应用程序等的数据可能包含个人身份信息。

如果启用了工作负载安全，系统还会查看 SMB 或其他共享上的文件和目录名称，其中可能包含个人身份信息。当客户启用工作负载安全用户目录收集器（其本质上是通过 Active Directory 将 Windows SID 映射到用户名）时，Data Infrastructure Insights将收集和存储显示名称、公司电子邮件地址和任何选定的附加属性。

此外，还会维护Data Infrastructure Insights的访问日志，其中包含用于登录服务的用户 IP 和电子邮件地址。

我的信息存储在哪里?

Data Infrastructure Insights根据您创建环境的区域存储信息。

主机区域中存储以下信息：

- 遥测和资产/对象信息，包括计数器和性能指标
- 采集单元信息
- 功能数据
- 审计Data Infrastructure Insights内部用户活动的信息
- 工作负载安全 Active Directory 信息
- 工作负载安全审计信息

无论您的Data Infrastructure Insights环境托管在哪个区域，以下信息都位于美国：

- 环境站点（有时称为“租户”）信息，例如站点/帐户所有者。
- 允许NetApp Console与区域Data Infrastructure Insights站点通信的信息，包括与用户授权有关的任何信息。
- 与Data Infrastructure Insights用户和租户之间的关系相关的信息。

主办地区

主办地区包括：

- 美国：us-east-1
- 欧洲、中东和非洲地区：eu-central-1
- 亚太地区：ap-southeast-2

更多信息

您可以通过以下链接了解有关 NetApp 隐私和安全的更多信息：

- "信任中心"
- "跨境数据传输"
- "具有约束力的公司规则"
- "响应第三方数据请求"
- "NetApp隐私原则"

安全管理工具

Data Infrastructure Insights包括安全功能，可让您的环境以增强的安全性运行。这些功能包括加密、密码散列的改进，以及更改内部用户密码以及加密和解密密码的密钥对的能力。

为了保护敏感数据， NetApp建议您在安装或升级后更改默认密钥和_Acquisition_用户密码。

数据源加密密码存储在Data Infrastructure Insights中，当用户在数据收集器配置页面输入密码时，它会使用公钥对密码进行加密。Data Infrastructure Insights没有解密数据收集器密码所需的私钥；只有采集单元 (AU) 才具有解密数据收集器密码所需的数据收集器私钥。

升级和安装注意事项

当您的 Insight 系统包含非默认安全配置（即您已重新输入密码）时，您必须备份您的安全配置。安装新软件，或者在某些情况下升级软件，会将您的系统恢复为默认安全配置。当您的系统恢复到默认配置时，您必须恢复非默认配置才能使系统正常运行。

管理采集单元的安全

SecurityAdmin 工具允许您管理Data Infrastructure Insights的安全选项，并在采集单元系统上运行。安全管理包括管理密钥和密码、保存和恢复您创建的安全配置或将配置恢复为默认设置。

开始之前

- 您必须拥有 AU 系统的管理员权限才能安装 Acquisition Unit 软件（其中包括 SecurityAdmin 工具）。
- 如果您有非管理员用户随后需要访问 SecurityAdmin 工具，则必须将他们添加到 *cisys* 组。 *cisys* 组是在 AU 安装期间创建的。

安装 AU 后，可以在采集单元系统的以下任一位置找到 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

以交互模式（-i）启动 SecurityAdmin 工具。

建议以交互模式使用 SecurityAdmin 工具，以避免在命令行上传递可以在日志中捕获的机密。

将显示以下选项：

[SecurityAdmin 工具选项（Linux）]

1. 备份

   创建包含所有密码和密钥的保险库备份 zip 文件，并将文件放置在用户指定的位置或以下默认位置：

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

建议妥善保管保险库备份，因为它们包含敏感信息。

2. 恢复

   恢复已创建的保管库的 zip 备份。一旦恢复，所有密码和密钥都将恢复为备份创建时存在的值。

   恢复可用于同步多台服务器上的密码和密钥，例如使用以下步骤：1）更改 AU 上的加密密钥。 2）创建保险库的备份。 3) 将保管库备份恢复到每个 AU。

3. 注册/更新外部密钥检索脚本

   使用外部脚本注册或更改用于加密或解密设备密码的 AU 加密密钥。

   当您更改加密密钥时，您应该备份新的安全配置，以便在升级或安装后恢复它。

   请注意，此选项仅在 Linux 上可用。

   当使用您自己的密钥检索脚本和 SecurityAdmin 工具时，请记住以下几点：

   - 当前支持的算法是最小 2048 位的 RSA。
   - 该脚本必须以纯文本形式返回私钥和公钥。该脚本不得返回加密的私钥和公钥。
   - 该脚本应返回原始的编码内容（仅限 PEM 格式）。
   - 外部脚本必须具有_执行_权限。

4. 轮换加密密钥

   轮换您的加密密钥（取消注册当前密钥并注册新密钥）。要使用来自外部密钥管理系统的密钥，您必须指定公钥 ID 和私钥 ID。

5. 重置为默认键

   将获取用户密码和获取用户加密密钥重置为默认值，默认值是安装期间提供的。

6. 更改信任库密码

   更改信任库的密码。

7. 更改密钥库密码

   更改密钥库的密码。

8. 加密收集器密码

   加密数据收集器密码。

9. 出口

   退出 SecurityAdmin 工具。

选择您想要配置的选项并按照提示进行操作。

指定用户来运行该工具

如果您处于受控的、注重安全的环境中，您可能没有_cisys_组，但仍可能希望特定用户运行 SecurityAdmin 工具。

您可以通过手动安装 AU 软件并指定您想要访问的用户/组来实现这一点。

- 使用 API，将 CI 安装程序下载到 AU 系统并解压缩。
  - 您将需要一次性授权令牌。查看 API Swagger 文档（*Admin > API Access* 并选择 *API Documentation* 链接）并找到 *GET /au/oneTimeToken* API 部分。
  - 获得令牌后，使用 *GET /au/installers/{platform}/{version}* API 下载安装程序文件。您需要提供平台（Linux 或 Windows）以及安装程序版本。
- 将下载的安装程序文件复制到AU系统并解压。
- 导航到包含文件的文件夹，并以 root 身份运行安装程序，指定用户和组：

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

如果指定的用户和/或组不存在，则将创建它们。用户将有权访问 SecurityAdmin 工具。

更新或删除代理

可以使用 SecurityAdmin 工具设置或删除采集单元的代理信息，方法是运行带有 *-pr* 参数的工具：

```
[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，要删除代理，请运行以下命令：

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

运行该命令后必须重新启动采集单元。

要更新代理，命令是

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

外部密钥检索

如果您提供 UNIX shell 脚本，则获取单元可以执行该脚本从您的密钥管理系统中检索 私钥 和 公钥。

为了检索密钥， Data Infrastructure Insights将执行脚本，并传递两个参数：*key id* 和 *key type*。 *Key id* 可用于识别密钥管理系统中的密钥。 _密钥类型_可以是“公共”或“私人”。当密钥类型为“公共”时，脚本必须返回公钥。当密钥类型为“private”时，必须返回私钥。

要将密钥发送回采集单元，脚本必须将密钥打印到标准输出。脚本必须仅将密钥打印到标准输出；不得将任何其他文本打印到标准输出。一旦请求的键被打印到标准输出，脚本必须以退出代码 0 退出；任何其他返回代码都被视为错误。

该脚本必须使用 SecurityAdmin 工具向采集单元注册，该工具将与采集单元一起执行该脚本。该脚本必须具有 root 和“cisys”用户的_read_和_execute_权限。如果注册后shell脚本被修改，则必须将修改后的shell脚本重新向采集单位注册。

输入参数：密钥ID	密钥标识符用于在客户密钥管理系统中识别密钥。
输入参数：密钥类型	公共或私人。
输出	必须将请求的密钥打印到标准输出。目前支持 2048 位 RSA 密钥。密钥必须按照以下格式进行编码和打印 - 私钥格式 - PEM、DER 编码的 PKCS8 PrivateKeyInfo RFC 5958 公钥格式 - PEM、DER 编码的 X.509 SubjectPublicKeyInfo RFC 5280
退出代码	退出代码为零表示成功。所有其他退出值均被视为失败。
脚本权限	脚本必须具有 root 和“cisys”用户的读取和执行权限。
logs	脚本执行被记录。日志可以在以下位置找到 - /var/log/netapp/cloudinsights/securityadmin/securityadmin.log /var/log/netapp/cloudinsights/acq/acq.log

加密用于 **API** 的密码

选项 8 允许您加密密码，然后您可以通过 API 将其传递给数据收集器。

以交互模式启动 SecurityAdmin 工具并选择选项 8：加密密码。

```
 securityadmin.sh -i
```

系统会提示您输入要加密的密码。请注意，您键入的字符不会显示在屏幕上。出现提示时重新输入密码。

或者，如果您要在脚本中使用该命令，请在命令行上使用带有“-enc”参数的_securityadmin.sh_，传递未加密的密码：

```
 securityadmin -enc mypassword
```

image:SecurityAdmin_Encrypt_Key_API_CLI_Example.png["CLI 示例"]

加密的密码显示在屏幕上。复制整个字符串，包括任何前导或尾随符号。

[交互模式加密密码，宽度=640]

要将加密的密码发送给数据收集器，您可以使用数据收集 API。可以在 管理 **> API** 访问 中找到此 API 的 swagger，然后单击“API 文档”链接。选择“数据收集”API 类型。在 *data_collection.data_collector* 标题下，为本示例选择 */collector/datasources* POST API。

[数据收集API]

如果将 *preEncrypted* 选项设置为 *True*，则通过 API 命令传递的任何密码都将被视为*已加密*；API 不会重新加密密码。构建 API 时，只需将先前加密的密码粘贴到适当的位置。

[API 示例，宽度=600]